Layer-2 Module Configuration

Table of Contents

Chapter 1 Physical Features of Ports

1.1 Setting the Rate

The Ethernet rate can be realized not only through auto-negotiation but also through interface configuration.

Command	Function
Speed {**10**|**100**|**auto**}	Sets the rate of fast Ethernet to 10M, 100M or auto-negotiation.
No speed	Resumes the default settings. The rate is auto-negotiation.

By default, the Ethernet interface can be auto, half duplex or full duplex.

Command	Function
duplex {**full**|**half**|**auto**}	Sets the duplex mode of an Ethernet interface.
No duplex	Resumes the default settings. The duplex mode is auto-negotiation.

1.2 Setting Flow Control on an Interface

When an interface is in full duplex mode, flow control is realized through the 802.3X-defined PAUSE frame; when an interface is in half duplex mode, flow control is realized through backpressure.

Command	Function
flow-control [**on|off**]	Enables or disables flow control on an interface.
no flow-control	Resumes the default settings, that is, there is no flow control on an interface.

Chapter 2 Port Protection and Security

2.1 Port Protection Configuration Task List

- Setting or Cancelling Port Isolation

2.2 Port Protection Configuration Task

2.2.1 Setting or Cancelling Port Isolation

Generally, the packets between different ports of a switch can be freely forwarded. In some cases, data flows between ports need be forbidden and that’s why port isolation is needed. There must not exist packet channel between isolated ports, however, packets between non-isolated ports or between isolated port and non-isolated port can be normally forwarded.

Command	Purpose
configure	Enters the global configuration mode.
[no] switchport protected	Sets or cancels port isolation in L2 port configuration mode.
exit	Goes back to the EXEC mode.
write	Saves the settings.

2.3 Interface Security Configuration Task List

- Binding MAC/IP to an Interface
- Filtering MAC/IP on an Interface
- Permitting or Denying Static MAC Address on an Interface
- Limiting Dynamic MAC Address on an Interface

2.4 Interface Security Configuration Tasks

2.4.1 Binding MAC/IP on an Interface

You can enter the layer-2 port configuration mode, bind MAC or IP to a port and make relevant settings to allow packets whose source addresses are the designated MAC or IP address to pass through this port.

Command	Purpose

[no] switchport port-security bind mac *mac-addr*	Binds a MAC address. **mac-addr** stands for the designated MAC address.
[no] switchport port-security bind ip *ip-addr*	Binds the IP address. **ip-addr** stands for the IP address.
[no] switchport port-security bind ip *ip-addr* **mac** *mac-addr*	Binds the MAC address and the IP address simultaneously. **ip-addr** stands for the IP address. **mac-addr** stands for the designated MAC address.

2.4.2 Filtering MAC/IP on an Interface

You can enter the layer-2 port configuration mode, filter MAC or IP on a port and make relevant settings to forbid packets whose source addresses are the designated MAC or IP address to pass through this port.

Command	Purpose
[no] switchport port-security block mac *mac-addr*	Filters the MAC address. **mac-addr** stands for the designated MAC address.
[no] switchport port-security block ip *ip-addr*	Filters the IP address. **ip-addr** stands for the IP address.
[no] switchport port-security block ip *ip-addr* **mac** *mac-addr*	Filters the MAC address and the IP address simultaneously. **ip-addr** stands for the IP address. **mac-addr** stands for the designated MAC address.

2.4.3 Permitting or Denying Static MAC Address on an Interface

You can enter the L2 port configuration mode, set the static MAC address table of the security port, permit or deny the packets whose source MAC address matches to pass through the port.

Command	Purpose
[no] switchport port-security static mac-address *mac-addr*	Set the static MAC address table on a security port. **mac-addr** stands for the designated MAC address.
[no] switchport port-security mode static *[accept | reject]*	Sets the **accept** or **reject** mode. **accept** means that only those packets whose source MAC addresses are in the static

	address table are allowed to pass through this port. **reject** means that only those packets whose source MAC addresses are in the static address table are rejected to pass through this port.

2.4.4 Limiting Dynamic MAC Address on an Interface

You can enter the L2 port configuration mode, set the mode of the security port to be the dynamic MAC address mode and configure the maximum number of the MAC addresses. After all these settings, packets with other MAC addresses cannot pass through this port. Only one allowable dynamic MAC address by default in dynamic port security mode

Command	Purpose
[no] switchport port-security dynamic maximum <*number*>	Sets the maximum number of dynamic MAC addresses on a security port. **number** stands for the maximum number of dynamic MAC addresses.
[no] switchport port-security mode dynamic	Means the configuration mode is a dynamic mode.

Chapter 3 Control of Port Block and Storm

3.1 Port Block Configuration Task List

- Limiting Broadcast Packets
- Limiting Multicast Packets
- Limiting Unknown Unicast Packets

3.2 Configuration Tasks of Port Block

3.2.1 Limiting Packets

To limit packets of a designated type to pass through a L2 port, enable port block on this L2 port.

Command	Purpose
[no] switchport block [broadcast | multicast | unicast]	Sets or cancels port block in L2 port configuration mode. **broadcast** means that the broadcast packets are limited to pass through this port. **multicast** means that the multicast packets are limited to pass through this port. **unicast** means that the unknown unicast packets are limited to pass through this port.

3.3 Storm Control Configuration Task List

- Limiting the Flux of Broadcast Packets
- Limiting the Flux of Multicast Packets
- Limiting the Flux of Unknown Unicast Packets

3.4 Storm Control Configuration Tasks

3.4.1 Setting the Flux Threshold of Packets

To set storm control on a L2 port, you have to set the flux threshold for a designated kind of packets to pass through the L2 port.

Command	Purpose
[no] storm-control [broadcast | multicast | unicast] **threshold** <number>	Sets or cancels the flux threshold of a designated kind of packets in L2 port configuration port. **broadcast** means that the flux threshold of broadcast packets will be set. **multicast** means that the flux threshold of multicast packets will be set. **unicast** means that the flux threshold of unknown unicast packets will be set. **number** means the value of the flux threshold.

Chapter 4 Port Mirror

4.1 Port Mirror Configuration Task List

- Setting Port Mirror
- Display the Information About Port Mirror

4.1.1 Port Mirror Configuration Tasks

1. Setting port mirror

In order to make switch management easy, you can set port mirror and use a port of the switch to observe the flux that runs through a group of ports.

Enter the privilege mode and set port mirror according to the following steps:

Command	Purpose
configure	Enters the global configuration mode.
mirror session *session_number* **{destination {interface** *interface-id***} | source {interface** *interface-id* **[, | -] [both | rx | tx] }**	Sets port mirror. **session-number** means the number of port mirror. **destination** means the destination port of mirror. **source** means the source port of mirror. **both | rx | tx** means the data flow that will be mirrored. **rx** means that only the input data is mirrored; **tx** means that only the output data is mirrored; **both** means both the input data and the output data are mirrored.
exit	Goes back to the EXEC mode.
write	Saves the settings.

2. Displaying the Information About Port Mirror

To display the configuration information about port mirror, run the following command:

Command	Purpose
show mirror [**session** *session_number]*	Displays the information about port mirror. **session-number** means the number of port mirror.

Chapter 5 MAC Configuration

5.1 MAC Configuration Task List

- Configuring the Static MAC Address
- Configuring the Aging Time of the MAC Address
- Displaying the MAC Address Table
- Removing Dynamic MAC Address

5.2 MAC Address Configuration Tasks

5.2.1 Configuring the Static MAC Address

The static MAC address entries mean those MAC address entries that cannot be aged by the switch but only be removed manually. According to actual requirements, you can decide whether to add or remove static MAC addresses. Enter the privilege mode and run the following commands to add or delete a static MAC address.

Command	Purpose
configure	Enters the global configuration mode.
[no] mac address-table static *mac-addr* **vlan** *vlan-id* **interface** *interface-id*	Adds or deletes a static MAC address. **mac-addr** means a MAC address. **vlan-id** means a VLAN number, which ranges between 1 and 4094. **interface-id** means an interface name.
exit	Goes back to the EXEC mode.
write	Saves the settings.

5.2.2 Configuring the Aging Time of the MAC Address

When a dynamic MAC address is not used during a designated aging time, the switch will remove the dynamic MAC from the MAC address table. The MAC aging time of a switch can be set according to actual needs and the default aging time is 300 seconds.

Enter the privilege mode and run the following commands to set the MAC aging time:

Command	Purpose
configure	Enters the global configuration mode.

mac address-table aging-time [**0 | 10-1000000**]	Sets the aging time of the MAC address table. **0** means that the MAC addresses will not age. **10-1000000** means the value range of the MAC aging time, whose unit is second.
exit	Goes back to the EXEC mode.
write	Saves the settings.

5.2.3 Displaying the MAC Address Table

Run the following command to display the content in the MAC address table of a switch:

Command	Purpose
show mac address-table {**dynamic** [**interface** interface-id **| vlan** vlan-id] **| static**}	Displays the content in the MAC address table.**dynamic** means the MAC address which is learned dynamically. **vlan-id** means a VLAN number, which ranges between 1 and 4094. **interface-id** means an interface name. **static** means the static MAC address table.

5.2.4 Removing the Dynamic MAC Address

In some cases, some learned MAC addresses need be removed.

Enter the privilege mode and run the following command to delete a dynamic MAC address:

Command	Purpose
clear mac address-table dynamic [address *mac-addr* | **interface** *interface-id* **| vlan** *vlan-id*]	Deletes a dynamic MAC address. **dynamic** means the MAC address which is learned dynamically. **mac-addr** means a MAC address. **interface-id** means an interface name. **vlan-id** means a VLAN number, which ranges between 1 and 4094.

Chapter 6 Layer-2 (L2) Tunnel Protocol Configuration

6.1 Overview

The tunnel of layer-2 protocol allows users who connect the two terminals of a switch to transmit the designated layer-2 protocol packets transparently in their own networks through the switch without the affection of the corresponding layer-2 protocol module of this switch. The switch here is just a transparent transmission medium for users.

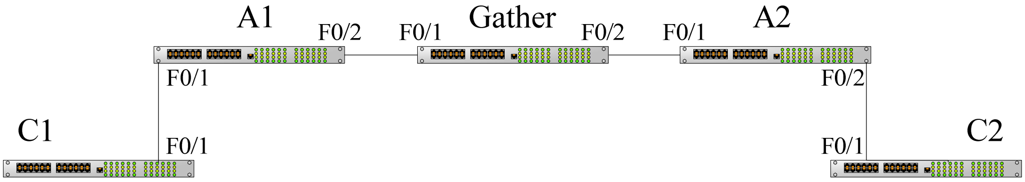
6.2 Layer-2 (L2) Tunnel Protocol Configuration

Run the following commands to set the L2 tunnel function on a L2 protocol:

Command	**Remarks**
configure	Enters the global configuration mode.
interface ***<intf_name>***	Enters the interface configuration mode of a switch port. Only the switch ports support the L2 tunnel (including physical ports and aggregation ports)
[**no**] **l2protocol-tunnel** *[stp]*	Sets the L2 protocol, which is used to enable the tunnel function, on this switch port. Currently only the tunnel function of the STP protocol is supported.
[CTRL] + Z	Goes back to the EXEC mode.
write	Saves the settings.

6.3 L2 Protocol Tunnel Configuration Example

The network topology is shown in the following figure:



A1/A2/Gather belongs to a core network. C1/C2 stands for two switches locating in two branches of a customer. The customer wants the two networks to be managed as an independent network, that is, the core network is just like a transparent transmission channel for this customer. To realize STP transparent transmission, the customer needs to make the following settings on each switch:

1. Set port f0/2 of switch A1, port f0/1 of switch Gather and port f0/1 of switch A2 to the trunk mode respectively.

2. Set port f0/1 of switch A1 and port f0/2 of switch A2 to **access**, and then enable the tunnel function of the STP protocol on the two ports.

Chapter 7 VLAN Configuration

7.1 VLAN Introduction

The virtual local area network (VLAN) is an exchange network which logically groups the devices in LAN. IEEE issued the IEEE 802.1Q standard in 1999 for realizing the VLAN standard. The VLAN technology can divide a physical LAN logic address into different broadcast domains. Each VLAN has a group of devices which have the same demands but the same attributes with those on the physical LAN. Because it is a logical group, the devices in a same VLAN can be in different physical spaces. The broadcast/unicast flow within a VLAN can not be forwarded to other VLANs. Such advantages as flow control, low device investment, easy network management and high network security, hence, are obtained.

- Supporting port-based VLAN
- Supporting 802.1Q relay mode
- Supporting the access port

  The port-based VLAN is to classify the port into a subset of VLAN supported by the switch. If the VLAN subnet includes only one VLAN, the port is the access port; if the VLAN subnet has multiple VLANs, the port is a trunk port; there is a default VLAN among these VLANs, which is the native VLAN of the port and whose ID is **PVID**.

- Supporting VLAN range control

  The **vlan-allowed** parameter is used to control the VLAN range; the **vlan-untagged** parameter is used to control the transmission of the untagged VLAN packet from the port to the corresponding VLAN.

7.2 VLAN Configuration Task List

- Adding/Deleting VLAN
- Configuring the Port of the Switch
- Monitoring the VLAN Configuration and VLAN State

7.3 VLAN Configuration Task

7.3.1 Adding/Deleting VLAN

VLAN is grouped according to different functions, project groups or different applications, not based on the physical locations of these users. VLAN has the similar attributes as the physical LAN, but can group terminals in different physical LANs into a same VLAN. One VLAN can have multiple ports, while all unicast/broadcast/multicast packets can be forwarded or diffused to the terminals through a same VLAN. Each VLAN is a logical network; to forward one packet to another VLAN, the routes or bridge must be used to forward it.

Run the following commands to configure VLAN:

Command	Purpose
vlan *vlan-id*	Enters the VLAN configuration mode.
name *str*	Name in the VLAN configuration mode
Exit	Exits the VLAN configuration mode and creates the VLAN.
vlan *vlan-range*	Creates multiple VLANs simultaneously.
no vlan *vlan-id* | *vlan-range*	Deletes one or multiple VLANs.

You can use the GVRP protocol to dynamically add or delete the VLAN.

7.3.2 Configuring the Port of the Switch

The switch's port supports the following modes: the access mode, the relay mode, the VLAN tunnel mode, the VLAN translating tunnel mode and the VLAN tunnel uplink mode.

- The access mode indicates that the port belongs to just one VLAN; only the untagged Ethernet frame can be transmitted and received.

- The relay mode indicates that the port connects other switches and the tagged Ethernet frame can be transmitted and received.

- The VLAN tunnel mode is a sub mode based on the access mode. The packets received by the port are thought to those without tag no matter whether they have VLAN tags, and the switching chip automatically add the PVID of the port to them as their new tag. Some switch models can modify the TPID value of new tag on the downlink port. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.

- The VLAN translating tunnel mode is a sub mode based on the relay mode. The port looks up the VLAN translation table according to the VLAN tag of received packets to obtain corresponding SPVLAN, and then the switching chip replaces the original tag with SPVLAN or adds the SPVLAN tag to the outside layer of the original tag. When the packets is forwarded out of the port, the SPVLAN will be replaced by the original tag or the SPVLAN tag will be removed mandatorily. Hence, the switch omits different VLAN partitions that access the network, and then passes them without change to the other subnet that connects the other port of the same client, realizing transparent transmission.

- The VLAN tunnel uplink mode is a sub mode based on the relay mode. The SPVLAN should be set when packets are forwarded out of the port. If the packets are in the untagged range, all these packets are forwarded out without any change. When the packets are received by the port, their TPIDs will be checked. If difference occurs or they are untagged packets, the SPVLAN tag which contains their own TPID will be added to them as their outer-layer tag.

Each port has a default VLAN and PVID; all VLAN-untagged data received on the port belongs to the packets of the VLAN.

The relay mode can group the port to multiple VLANs; at the same time, you can configure the type of to-be-forwarded packets and the quantity of the corresponding VLANs.

Run the following commands to configure the switch's port:

Command	Purpose
switchport pvid *vlan-id*	Configures PVID of the switch's interface.
switchport mode {access | trunk}	Configures the interface mode of the switch.
switchport trunk vlan-allowed …	Configures the VLAN range of the switch's interface.
switchport trunk vlan-untagged …	Configures the untagged VLAN ranges of the switch's port.

7.3.3 Monitoring the VLAN Configuration and VLAN State

To monitor the VLAN state, run the following command in EXEC mode:

Command	Purpose
show vlan [id *x* **| interface** *intf* **]**	Displays the VLAN state.

Chapter 8 STP Configuration

8.1 STP Introduction

STP, defined in IEEE 802.1D, simplifies a LAN topology of several bridges into an independent spanning tree to avoid network loops and secure stable network operation.

The spanning-tree algorithm and the spanning-tree protocol can set any bridge LAN to be a simply connected mobile topology. In the mobile topology, some bridge ports can forward frames, while other ports are blocked and cannot forward data. A port in blocked state can also be contained in the mobile topology. When some network device is out of effect, added or removed, the port in blocked state will enter the forwarding state.

In the spanning-tree topology, a bridge is regarded as a root or a root bridge. Each LAN segment has a bridge port to take in charge of data forwarding from this network segment to the root. This bridge port is regarded as the designated port of this LAN segment, while the bridge where the bridge port locates is regarded as the designated bridge of LAN The root is the designated bridge of each LAN segment that connects this root. In each bridge port, the port that is nearest to the root bridge is the root port of this bridge and only the root port and the designated port are in forwarding state; another kind of ports are open, but they are not root ports or designated ports but standby ports.

The following parameters decide the structure of the stabile mobile topology:

(1) Each unique bridge identifier

(2) path cost of each port

(3) ID of each bridge port

The bridge with the highest priority (the identifier value is the smallest) will be chosen as the root bridge. The ports of each bridge in the network all have root path cost, that is, the root path cost is the smallest value of the path cost sum of all ports between the root bridge and the bridge. The designated port of each LAN segment means the port that connect this LAN segment and has the smallest root path cost; if several ports have the same root path cost, their bridge identifiers will first be compared and then their port identifiers. According to this method, each LAN segment has only one designated port and each bridge has only one root port.

The spanning tree topology makes the loop inexistent in a network, guaranteeing the stability and fault recovery of the network.

Rapid Spanning-Tree Protocol (RSTP) is an important update of 802.1D STP. When faults occur in the bridge, bridge port or LAN segment in a network, RSTP will realize the rapid convergence of the network topology. In this case, the new root port on the bridge will enter the forwarding state promptly, and at the same time the direct acceptance between bridges can make a designated port to forward data immediately. For RSTP settings, see the part “Setting RSTP”.

Note:
802.1D STP and 802.1w RSTP mentioned in this text are simplified as SSTP and RSTP respectively. SSTP here is the shortened form of Single Spanning-Tree Protocol.

8.2 SSTP Configuration Task List

- Choosing the STP Mode
- Disabling/Enabling STP
- Disabling/Enabling STP on a Port
- Setting the Bridge Priority
- Setting the Hello Time
- Setting the Max Age
- Setting the Forward Delay
- Setting the Port Priority
- Setting the Port Path Cost
- Setting Automatic Port Designation
- Monitoring the STP State
- Setting the SNMP Trap

8.3 SSTP Configuration Tasks

8.3.1 Choosing the STP Mode

Run the following command to set the STP mode:

Command	Purpose
spanning-tree mode {sstp | rstp | mstp | pvst}	Selects the STP mode.

8.3.2 Disabling/Enabling STP

By default, when STP is started, the running mode is RSTP; if STP is not required, you can stop it from running.

Run the following command to disable STP:

Command	Purpose
no spanning-tree	Disables STP.

Run the following commands to enable STP:

Command	Purpose
spanning-tree	Enables STP that runs in default mode—RSTP.
spanning-tree mode {sstp | rstp | mstp | pvst}	Selects a mode for the enabled STP.

8.3.3 Disabling/Enabling STP on a Port

By default, STP is running on all switch ports; if you want to disable STP, you can run the following command in port configuration mode to stop STP running.

Command	Purpose
no spanning-tree	Disables STP to run on the ports.

After STP is forbidden to run on a port, this port maintains a designated port and its forwarding state and stops to transmit BPDU again. However, each STP mode still has such operations as type checkup, numbering, edge information update and topology information update towards BPDU that a port receives.

Note:
When **no spanning-tree** is set and a port has served as a root port, alternate port, master port or backup port, the protocol information that this port receives in SSTP/MSTP mode will age immediately and transfer to be a designated port, while the protocol information that this port receives in SSTP/PVST mode will remain the original role for a certain period and then age after the timer times out.

Note:
Every STP mode supports the BPDU Guard function on the port on which **no spanning-tree** is set.

8.3.4 Setting Bridge Priority

You can choose the spanning-tree root of the network topology by changing the bridge priority of a switch.

Run the following commands to set the bridge priority of SSTP:

Command	Purpose
spanning-tree sstp priority *value*	Modifies the bridge priority of the SSTP mode.
no spanning-tree sstp priority	Resumes the SSTP bridge priority to the default value, 32768.

8.3.5 Setting the Hello Time

You can configure the SSTP hello time to decide the packet transmission interval when the switch works as the root.

Run the following commands to set the SSTP hello time.

Command	Purpose
spanning-tree sstp hello-time *value*	Modifies the hello time in SSTP mode.
no spanning-tree sstp hello-time	Resumes the SSTP hello time to the default value, 4 seconds.

8.3.6 Setting the Max Age

You can configure the SSTP max age to decide the maximum lifespan of the packet when the switch works as the root.

Run the following commands to configure the SSTP max age.

Command	Purpose
spanning-tree sstp max-age *value*	Modifies the Max Age of the SSTP mode.
no spanning-tree sstp max-age	Resumes the max age to the default value, 20 seconds.

8.3.7 Setting the Forward Delay

You can decide the state transfer interval of a network node when a switch is used as the root bridge by configuring the SSTP forward delay.

Run the following commands to configure the SSTP forward delay.

Command	Purpose
spanning-tree sstp *forward-time*	Modifies the forward time of the SSTP mode.
no spanning-tree sstp forward-time	Resumes the default forward time, 15 seconds.

8.3.8 Setting the Port Priority

When a loop generates, STP will change the states of some ports to the blocking state to cut off the loop. You can control whether to block a port by setting the port priority and the port path cost.

Run the following commands to set the port priority of SSTP:

Command	Purpose
spanning-tree port-priority *value*	Sets the port priority in all modes.
spanning-tree sstp port-priority *value*	Modifies the port priority of the SSTP mode.
no spanning-tree sstp port-priority	Resumes the port priority to the default value, 128.

8.3.9 Setting the Port Path Cost

Run the following commands to set the port path cost of SSTP.

Command	Purpose
spanning-tree cost *value*	Sets the port priority in all modes.
spanning-tree sstp cost *value*	Modifies the port path cost in SSTP mode.
no spanning-tree sstp cost	Resumes the port path cost to the default value.

8.3.10 Monitoring the STP state

To monitor STP configuration and STP's state, run the following commands in EXEC mode:

Command	Purpose
show spanning-tree	Displays the state of STP in current mode.
show spanning-tree detail	Displays the detailed information about STP in current mode.
show spanning-tree interface	Displays the information about a port in STP in current mode.

8.3.11 Setting the SNMP Trap

You can monitor the change of STP in a switch remotely from the network management software of the host by configuring the trap function of STP. STP protocols support two types of traps: newRoot and topologyChange. When a switch changes from a non-root to a root, the **newRoot Trap** message will be transmitted; when the topology change is detected, such as a non-edge port is changed from the non-forwarding state to the forwarding state, the **topologyChange Trap** message will be transmitted.

Note:
The STP trap can be received only when the network management software supports trap reception. The network management need be imported into the bridge MIB and OID is 1.3.6.1.2.1.17.

Run the following commands in global configuration mode to enable the STP trap:

Command	Purpose
spanning-tree management trap **[newroot | topologychange]**	Enables the STP trap. If the trap type is not designated, two kinds of traps will be enabled at the same time.
no spanning-tree management trap	Shuts down the STP trap.

8.4 Setting the Spanning Tree of VLAN

8.4.1 Overview

In SSTP mode, the whole network only has one spanning-tree instance, and the state of a port in the spanning tree decides its state in all VLANs. When multiple VLANs exist in a network, the isolation between SSTP and VLAN topology may lead to the communication block of some network parts.

PVST supports that independent SSTP runs on a certain number of VLANs and guarantees that a port has different states in different VLANs. At the same time the flow balance can be realized between VLANs.

It is especially noted that the maximum number of VLANs on which independent STP can run is 64, while other VLAN topologies are not controlled by STP.

8.4.2 VLAN STP Configuration Tasks

Run the following commands to set the features of SSTP in VLAN:

Command	Purpose
spanning-tree mode pvst	Enables STP distribution according to VLAN.
spanning-tree vlan *vlan-list*	Distributes the STP instance for a designated VLAN. **vlan-list** means the VLAN list.
no spanning-tree vlan *vlan-list*	Deletes the spanning-tree instance in a designated VLAN
spanning-tree vlan *vlan-list* priority *value*	Sets the spanning-tree priority in a designated VLAN.
no spanning-tree *vlan-list* priority	Resumes the spanning-tree priority in a VLAN to the default value.
spanning-tree vlan *vlan-list* forward-time *value*	Sets the Forward Delay of a designated VLAN.
no spanning-tree vlan *vlan-list* forward-time	Resumes the Forward Delay of a designated VLAN.
spanning-tree vlan *vlan-list* max-age *value*	Sets the max age of a designated VLAN.
no spanning-tree vlan *vlan-list* max-age	Resumes the Max-Age of a designated VLAN to the default value.
spanning-tree vlan *vlan-list* hello-time *value*	Sets the Hello-time of a designated VLAN.
no spanning-tree vlan *vlan-list* hello-time	Resumes the hello-time of a designated VLAN to the default value.

Run the following commands to set the port's features in switch port configuration mode:

Command	Purpose
spanning-tree vlan *vlan-list* cost	Sets the path cost of a port in a designated VLAN.
no spanning-tree vlan *vlan-list* cost	Resumes the path cost of a port in VLAN to the default value.
spanning-tree vlan *vlan-list* port-priority	Sets the port priority in VLAN.
no spanning-tree vlan *vlan-list* port-priority	Resumes the priority of a port in VLAN to the default value.

In monitor or configuration mode, run the following commands to browse the state of the spanning tree in a designated VLAN:

Command	Purpose
show spanning-tree vlan *vlan-list*	Browses the state of the spanning tree in a VLAN.

8.5 RSTP Configuration Task List

- Enabling or Disabling RSTP
- Setting the Bridge Priority
- Setting the Forward Time
- Setting the Hello Time
- Setting the Max Age
- Setting the Port Path Cost
- Setting the Port Priority
- Setting the Edge Port
- Setting the Port Connection Type
- Restarting Protocol Transfer Checkup

8.6 RSTP Configuration Tasks

8.6.1 Enabling or Disabling RSTP

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree mode rstp	Enables RSTP.

no spanning-tree mode	Disables STP.

8.6.2 Setting the Bridge Priority

The bridge priority decides whether this bridge can be chosen as the root bridge of the whole spanning tree. Setting a comparatively low priority can make a bridge to be the root bridge of the spanning tree.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp priority *value*	Sets the priority of a bridge.
no spanning-tree rstp priority	Resumes the bridge priority to be the default value.

It is especially noted that if the priorities of all bridges in an entire switch network have the same value the bridge with the smallest MAC address will be chosen as the root bridge. In case that RSTP is enabled, if the bridge priority is changed the spanning tree will be calculated again.

In the default settings, the bridge priority is set to 32768.

8.6.3 Setting the Forward Time

Link fault will trigger the recalculation of the spanning-tree structure, but the new configuration information, which is obtained through recalculation, cannot be sent to the whole network immediately; if the newly chosen root port and designated port starts data forwarding immediately, temporary loop may be caused. To solve this problem, RSTP adopts a state removal mechanism. Before the root port and the designated port begin to forward data, an intermediate state must be experienced. The intermediate state changes into the forwarding state after the forward delay that guarantees the new configuration information has spread all over the whole network. The Forward Delay of a bridge depends on the diameter of the switch network. Generally speaking, the longer the network diameter is, the longer the forward delay should be set to be.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp forward-time *value*	Sets the Forward Delay.
no spanning-tree rstp forward-time	Resumes the default forward delay, 15 seconds.

It is especially noted that if Forward Delay is set too small the temporary redundant path may occur in the network, but if Forward Delay is set too big the network may be disconnected for a long time. That's why users are recommended to take the default value.

In the default settings, the forward delay of a bridge is 15 seconds.

8.6.4 Setting the Hello Time

A suitable hello time not only guarantees that a bridge can detect a link fault in a network promptly but also occupies a few network resources.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp hello-time *value*	Sets the Hello Time.
no spanning-tree rstp hello-time	Resumes the hello time to the default value.

It takes attention that if a long hello time is set, packet loss in the links may cause a bridge not to receive the hello packets for a long time and the bridge then regards the occurrence of link faults and starts spanning-tree recalculation, but if a too short hello time is set the bridge will frequently send the configuration information and then the network bandwidth will be heavily occupied and the network/CPU load will be increased. That's why users are recommended to take the default value.

In the default settings, the hello time of a bridge is 4 seconds.

8.6.5 Setting the Max Age

The max age is used to judge whether the configuration information expires. Users can set the max age according actual conditions.

Run the following commands in global configuration mode.

Command	Purpose
spanning-tree rstp max-age *value*	Sets the Max Age.
no spanning-tree rstp max-age	Resumes the max age to the default value, 20 seconds.

It is recommended that users take the default value.

8.6.6 Value of the path cost of a port

The path cost is related with the link rate of the port. If the link rate is required to be high, the path cost should be set to a small value; when the path cost is set to its default value, RSTP can automatically check the link rate of the current Ethernet port and calculate the corresponding path cost.

Run the following commands in interface configuration mode.

Command	Purpose
spanning-tree rstp cost *value*	Sets the path cost of a port.
no spanning-tree rstp cost	Resumes the path cost of a port to the default value.

It is especially noted that the settings of the path cost will lead to the recalculation of the spanning tree, so users are recommended to take the default value and wait RSTP to calculate the path cost of the current Ethernet port automatically.

By default, the path costs of all Ethernet ports of a bridge are all set to 2000,000 at the 10Mbps port rate, or set to 200,000 at the 100Mbps port rate.

8.6.7 Setting the Port Priority

Port priority settings can be used to designate a specific Ethernet port to be contained in the spanning tree. In general, the smaller the value is, the higher the port priority is, and the Ethernet port has more possibility to be contained in the spanning tree. If all Ethernet ports of a bridge adopt the same priority value, the index number of an Ethernet port decides whether the Ethernet port has a high priority or not.

Run the following commands in interface configuration mode.

Command	Purpose
spanning-tree rstp port-priority *value*	Sets the port priority.
no spanning-tree rstp port-priority	Resumes the port priority to the default value.

It should be noted that the change of the priority of an Ethernet port can lead to the recalculation of the spanning tree.

The priority of all Ethernet ports of a bridge is 128 by default.

8.6.8 Setting the Edge Port

The edge port means this port connects terminal devices of a network. A mandatory edge port will enter the forwarding state after link-up. In port configuration mode, run the following command to set the edge port of RSTP:

Command	Purpose
spanning-tree rstp edge [**force-true** | **force-false** | **auto**]	Sets the edge port. force-true：Mandatorily makes the edge port valid. force-false：Mandatorily makes the edge port invalid. auto：Automatically checks the edge port.

In auto mode, if a port has not received BPDU in a certain time this port is viewed as the edge port.

8.6.9 Setting the Port Connection Type

If network nodes, on which RSTP is run, are in the point-to-point connection, these nodes can establish a topology rapidly through the handshake mechanism.

By default, RSTP will judge whether a port is in the point-to-point connection according to the duplex mode of this port. If this port works in full duplex mode, RSTP regards this port is in a point-to-point connection; if this port works in half duplex mode, RSTP regards this port’s connection is shared.

If it is confirmed that RSTP or MSTP is running on the network nodes connected by a port, you should set this port's connection type to point-to-point, which guarantees fast handshake.

In the port configuration mode, run the following command to set the connection type of a port.

Command	Purpose
spanning-tree rstp point-to-point [**force-true** | **force-false** | **auto**]	Sets the edge port. force-true：Mandatorily sets the connection to point-to-point. force-false：Mandatorily sets the connection to sharing. auto：Automatically checks the port type.

8.6.10 Restarting the protocol conversion check

RSTP makes a switch to work together with a traditional 802.1D STP switch through a protocol transfer mechanism. If one port of a switch receives the STP configuration information, this port will change to only forward the STP packets.

After a port enters the STP-compatible state, even if this port does not receive 802.1D STP BPDU again, this port will not resume the RSTP state. In this case, you can run **spanning-tree rstp migration-check** to enable the protocol transfer checkup process and resume this port to the RSTP mode.

In global mode run the following command to restart RSTP transfer checkup:

Command	Purpose
spanning-tree rstp migration-check	Restarts RSTP transfer checkup on all ports.

In switch port configuration mode, run the following command to conduct protocol transfer checkup on this port:

Command	Purpose
spanning-tree rstp migration-check	Restarts RSTP transfer checkup on the current port.

Chapter 9 802.1x Configuration

9.1 802.1x Configuration Task List

- Configuring 802.1x Authentication on the Port
- Configuring 802.1x on Multiple Ports of the Host
- Configuring the Maximum Times of 802.1x ID Authentication Request
- Configuring 802.1x Re-Authentication
- Configuring 802.1x transmission frequency
- Configuring 802.1x User Binding
- Configuring the Authentication Method on the 802.1x Port
- Selecting the Authentication Mode for the 802.1x Port
- Configuring guest-vlan
- Resuming the Default Settings of 802.1x
- Monitoring the 802.1x Authentication Configuration and State

9.2 802.1x Configuration Tasks

9.2.1 Configuring 802.1x Authentication on the Port

802.1x has three modes to control the port: force-authorized, force-unauthorized and enable.

Force-authorized means that the port has been authenticated and thus no authentication process is needed. In this mode, all users can conduct the data access control through the port. This mode is the default mode of the port. **Force-unauthorized** means that port authentication is not passed no matter what kind of authentication method you apply. In this mode, all users cannot conduct the data access control through the port.

Enable means that the 802.1x authentication protocol will be run on the port and the users who access the port will be authenticated by 802.1x. The successfully-authenticated users can conduct the data access control through the port. 启动端口的 802.1x 的认证后还要配置 AAA 的认证方法。

Before the 802.1x is configured, you have to enable the 802.1x function by running the following commands:

Command	Purpose

dot1x enable	Enables the 802.1x function.

Run the following commands to enable the 802.1x authentication:

Command	Purpose
dot1x port-control auto	Sets the port to the 802.1x control mode.
aaa authentication dot1x {default |list name} method	Configures 802.1x AAA authentication.

Run one of the following commands in interface configuration mode to select the 802.1x control mode:

Command	Purpose
dot1x port-control auto	Enables the 802.1x authentication method on the port
dot1x port-control force-authorized	The port authentication is authorized mandatorily.
dot1x port-control force-unauthorized	The port authentication is unauthorized mandatorily.

9.2.2 Configuring 802.1x on Multiple Ports of the Host

The 802.1x authentication is mainly for the single host user. At this time, the switch allows only one user to conduct the authentication and the access control. However, sometimes the port may connect multiple hosts through 802.1x-unsupported switching device, such as switch 1108. In order to make these hosts' users access successfully, you can enable the multi-host port access function.

Theoretically, 802.1x does not limit the number of the host's users. Howerver, because the switch controls the user's authentication by controlling the MAC address of the user, the number of the host's users will be limited by the size of the MAC address of the switch.

Run the following command in interface configuration mode to activate the 802.1x multi-host port authentication:

Command	Purpose
dot1x multiple-hosts	Configures the 802.1x multi-host port authentication.

9.2.3 Configuring the Maximum Times of 802.1x ID Authentication Request

When the 802.1x authentication starts or during re-authentication, the ID authentication request will be sent to the client host and, however, lost or delayed because of the network problem. In this case, the request packet need be resent. After a certain times of request resending, the authentication request will be terminated because there is no client hosts carrying on the authentication. The authentication thus fails.

You can modify the maximum times of ID authentication request according to different network environments, ensuring that the authentication between the client and the authentication server passes.

To configure the maximum times of ID authentication requests, run the following command in interface configuration mode:

Command	Purpose
dot1x max-req *count*	Configures the maximum times of 802.1x ID authentication request.

9.2.4 Configuring 802.1x Re-Authentication

After the authentication is passed, the authentication to the client will still be conducted every interval to ensure the legality of the client's authentication.

In this case, you need to enable the re-authentication function. After the re-authentication is started, the authentication request will be periodically sent to the host.

Run the following commands to configure the re-authentication function.

Command	Purpose
dot1x re-authentication	Enables the re-authentication function.
dot1x timeout re-authperiod *time*	Configures the period of the re-authentication function.
dot1x reauth-max *time*	Configures the retry times after the re-authentication function fails.

9.2.5 Configuring 802.1x Transmission Frequency

During 802.1x authentication, the packets will be transmitted to the client's host. You can adjust the data transmission to ensure the response of the client's host by controlling the 802.1x transmission frequency.

Run the following command to configure the transmission frequency.

Command	Purpose
dot1x timeout tx-period *time*	Sets the transmission frequency of the 802.1x packet.

9.2.6 Configuring 802.1x User Binding

You can bind the user to a certain port during 802.1x authentication to ensure the security of the interface access. To enable the 802.1x user binding, run the following command in interface configuration mode:

Command	Purpose
dot1x user-permit *xxxz*	Configures the user which is bound to the interface.

9.2.7 Configuring the Authentication Method on the 802.1x Port

Different ports will be applied with different authentication methods during 802.1x authentication. By default, the 802.1x authentication adopts the default method.

To configure the 802.1x authentication method, run the following command in interface configuration mode:

Command	Purpose
dot1x authentication method *yyy*	Configures the 802.1x authentication method.

9.2.8 Selecting the Authentication Mode for the 802.1x Port

The authentication mode can be selected during the 802.1x authentication. The authentication class decides whether AAA uses the CHAP authentication or the EAP authentication. If the CHAP authentication is used, the challenge required by MD5 is locally generated; if the EAP authentication is used, the challenge is generated on the authentication server. Only one authentication mode can be applied to one interface. By default, the authentication mode is applied in global mode. When an authentication mode is configured for an interface, the authentication mode will be always used on the interface unless the negative form of the command is run to resume the default settings.

Run the following command in global configuration mode to configure an authentication mode:

Command	Purpose
dot1x authen-type {**chap**|**eap**}	Selects CHAP or EAP.

To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x authentication type {**chap**|**eap**}	Selects CHAP or EAP, or just uses the configuration class in global mode.

9.2.9 Resuming the Default Settings of 802.1x

This command is used to resume all global configurations to the default settings. To configure the authentication mode, you also can run the following command in interface configuration mode:

Command	Purpose
dot1x default	This command is used to resume all global configurations to the default settings.

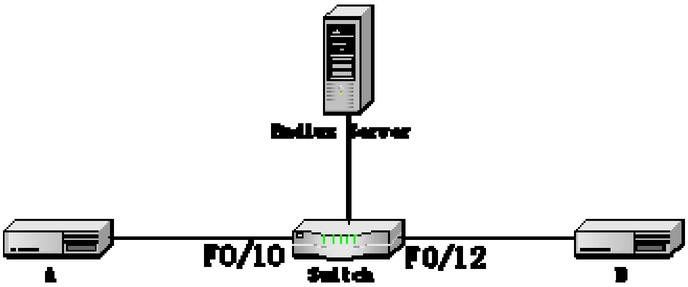
9.2.10 Monitoring the 802.1x Authentication Configuration and State

To monitor the 802.1x authentication configuration and state, run the following commands in EXEC mode:

Command	Purpose
show dot1x {*interface ….*}	Displays the 802.1x authentication configuration and state.

9.3 802.1x Configuration Example

See the following figure:



Host A connects interface f0/0 of the router; host B connects interface f0/12 of the switch. The IP address of the radius server is 192.168.20.2 and the radius key is TST. The authentication of interface f0/10 adopts the remote radius authentication and the user binding function. The authentication of interface f0/12 adopts the local authentication without user binding, however, the EAP authentication mode and multi-host authentication will be employed.

Global configuration

```
username switch password 0 TST
username TST password 0 TST
aaa authentication dot1x TST-F0/10 radius
aaa authentication dot1x TST-F0/12 local
interface VLAN1
 ip address 192.168.20.24 255.255.255.0
radius-server host 192.168.20.2 auth-port 1812 acct-port 1813
radius-server key TST
```

Configuration of interface f0/10

```
interface FastEthernet0/10
 dot1x port-control auto
 dot1x authentication method TST-F0/10
 dot1x user-permit radius-TST
```

Configuration of interface f0/12

```
interface FastEthernet0/12
 dot1x multiple-hosts
 dot1x port-control auto
dot1x authentication method TST-F0/12
 dot1x authentication type eap
```