Content

Chapter 1 MSTP Configuration

1.1 Introduction to MSTP

The MSTP (Multiple STP) is a new spanning-tree protocol which is based on the STP and the RSTP. It runs on all the bridges of a bridged-LAN. It calculates a common and internal spanning tree (CIST) for the bridge-LAN which consists of the bridges running the MSTP, the RSTP and the STP. It also calculates the independent multiple spanning-tree instances (MSTI) for each MST domain (MSTP domain). The MSTP, which adopts the RSTP for its rapid convergence of the spanning tree, enables multiple VLANs to be mapped to the same spanning-tree instance which is independent to other spanning-tree instances. The MSTP provides multiple forwarding paths for data traffic and enables load balancing. Moreover, because multiple VLANs share a same MSTI, the MSTP can reduce the number of spanning-tree instances, which consumes less CPU resources and reduces the bandwidth consumption.

1.1.1 MSTP Region

Because multiple VLANs can be mapped to a single spanning tree instance, IEEE 802.1s committee raises the MST concept. The MST is used to make the association of a certain VLAN to a certain spanning tree instance.

A MSTP region is composed of one or multiple bridges with the same MCID (MST Configuration Identification) and the bridged-LAN (a certain bridge in the MSTP region is the designated bridge of the LAN, and the bridges attaching to the LAN are not running STP). All the bridges in the same MSTP region have the same MSID.

MSID consists of 3 attributes:

- ☞ Configuration Name: Composed by digits and letters
- ☞ Revision Level
- ☞ Configuration Digest: VLANs mapping to spanning tree instances

The bridges with the same 3 above attributes are considered as in the same MST region.

When the MSTP calculates CIST in a bridged-LAN, a MSTP region is considered as a bridge. See the figure below:

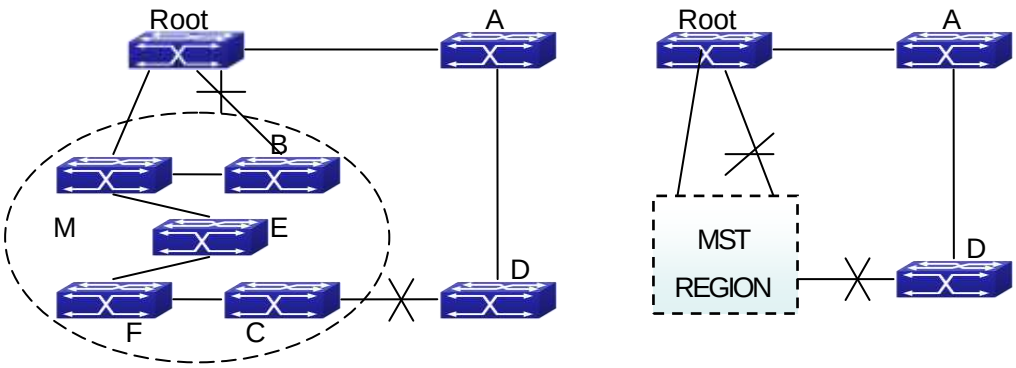


Fig 1-1 Example of CIST and MST Region

In the above network, if the bridges are running the STP or the RSTP, one port between Bridge M and Bridge B should be blocked. But if the bridges in the yellow range run the MSTP and are configured in the same MST region, MSTP will treat this region as a bridge. Therefore, one port between Bridge B and Root is blocked and one port on Bridge D is blocked.

1.1.1.1 Operations within an MSTP Region

The IST connects all the MSTP bridges in a region. When the IST converges, the root of the IST becomes the IST master, which is the switch within the region with the lowest bridge ID and path cost to the CST root. The IST master is also the CST root if there is only one region within the network. If the CST root is outside the region, one of the MSTP bridges at the boundary of the region is selected as the IST master.

When an MSTP bridge initializes, it sends BPDUs claiming itself as the root of the CST and the IST master, with both of the path costs to the CST root and to the IST master set to zero. The bridge also initializes all of its MST instances and claims to be the root for all of them. If the bridge receives superior MST root information (lower bridge ID, lower path cost, and so forth) than currently stored for the port, it relinquishes its claim as the IST master.

Within a MST region, the IST is the only spanning-tree instance that sends and receives BPDUs. Because the MST BPDU carries information for all instances, the number of BPDUs that need to be processed by a switch to support multiple spanning-tree instances is significantly reduced.

All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root switch ID, root path cost, and so forth.

1.1.1.2 Operations between MST Regions

If there are multiple regions or legacy 802.1D bridges within the network, MSTP establishes and maintains the CST, which includes all MST regions and all legacy STP bridges in the network. The MST instances combine with the IST at the boundary of the region to become the CST.

The MSTI is only valid within its MST region. An MSTI has nothing to do with MSTIs in other MST regions. The bridges in a MST region receive the MST BPDU of other regions through Boundary Ports. They only process CIST related information and abandon MSTI information.

1.1.2 Port Roles

The MSTP bridge assigns a port role to each port which runs MSTP.

- ☞ CIST port roles: Root Port, Designated Port, Alternate Port and Backup Port
- ☞ On top of those roles, each MSTI port has one new role: Master Port.

The port roles in the CIST (Root Port, Designated Port, Alternate Port and Backup Port) are defined in the same ways as those in the RSTP.

1.1.3 MSTP Load Balance

In a MSTP region, VLANs can by mapped to various instances. That can form various topologies. Each instance is independent from the others and each distance can have its own attributes such as bridge priority and port cost etc. Consequently, the VLANs in different instances have their own paths. The traffic of the VLANs are load-balanced.

1.2 MSTP Configuration Task List

MSTP configuration task list:

1. Enable the MSTP and set the running mode
2. Configure instance parameters
3. Configure MSTP region parameters
4. Configure MSTP time parameters
5. Configure the fast migrate feature for MSTP
6. Configure the format of port packet
7. Configure the spanning-tree attribute of port
8. Configure the snooping attribute of authentication key
9. Configure the FLUSH mode once topology changes

1. Enable MSTP and set the running mode

Command	Explanation
Global Mode and Port Mode	
spanning-tree **no spanning-tree**	Enable/Disable MSTP.
Global Mode	
spanning-tree mode {mstp|stp|rstp} **no spanning-tree mode**	Set MSTP running mode.
Port Mode	
spanning-tree mcheck	Force port migrate to run under MSTP.

2. Configure instance parameters

Command	Explanation
Global Mode	
spanning-tree mst <*instance-id*> priority <*bridge-priority*> **no spanning-tree mst <*instance-id*> priority**	Set bridge priority for specified instance.
spanning-tree priority <*bridge-priority*> **no spanning-tree priority**	Configure the spanning-tree priority of the switch.
Port Mode	
spanning-tree mst <*instance-id*> cost <*cost*> **no spanning-tree mst <*instance-id*> cost**	Set port path cost for specified instance.
spanning-tree mst <*instance-id*> port-priority <*port-priority*> **no spanning-tree mst <*instance-id*> port-priority**	Set port priority for specified instance.
spanning-tree mst <*instance-id*> rootguard **no spanning-tree mst <*instance-id*> rootguard**	Configure currently port whether running rootguard in specified instance, configure the rootguard port can't turn to root port.
spanning-tree rootguard **no spanning-tree rootguard**	Configure currently port whether running rootguard in instance 0, configure the rootguard port can't turn to root port.
spanning-tree [mst <instance-id>]	Enable loopguard function on specified

loopguard **no spanning-tree [mst <instance-id>] loopguard**	instance, the no command disables this function.

3. Configure MSTP region parameters

Command	Explanation
Global Mode	
spanning-tree mst configuration **no spanning-tree mst configuration**	Enter MSTP region mode. The no command restores the default setting.
MSTP region mode	
show	Display the information of the current running system.
instance <*instance-id*> vlan <*vlan-list*> **no instance <*instance-id*> [vlan <*vlan-list*>]**	Create Instance and set mapping between VLAN and Instance.
name <*name*> **no name**	Set MSTP region name.
revision-level <*level*> **no revision-level**	Set MSTP region revision level.
abort	Quit MSTP region mode and return to Global mode without saving MSTP region configuration.
exit	Quit MSTP region mode and return to Global mode with saving MSTP region configuration.
no	Cancel one command or set initial value.

4. Configure MSTP time parameters

Command	Explanation
Global Mode	
spanning-tree forward-time <*time*> **no spanning-tree forward-time**	Set the value for switch forward delay time.
spanning-tree hello-time <*time*> **no spanning-tree hello-time**	Set the Hello time for sending BPDU messages.
spanning-tree maxage <*time*> **no spanning-tree maxage**	Set Aging time for BPDU messages.
spanning-tree max-hop <*hop-count*> **no spanning-tree max-hop**	Set Maximum number of hops of BPDU messages in the MSTP region.

5. Configure the fast migrate feature for MSTP

Command	Explanation
Port Mode	
spanning-tree link-type p2p {auto|force-true|force-false} **no spanning-tree link-type**	Set the port link type.
spanning-tree portfast [bpdufilter| bpduguard] [recovery <30-3600>] **no spanning-tree portfast**	Set and cancel the port to be an boundary port. bpdufilter receives the BPDU discarding; bpduguard receives the BPDU will disable port; no parameter receives the BPDU, the port becomes a non-boundary port.

6. Configure the format of MSTP

Command	Explanation
Port Mode	
spanning-tree format standard **spanning-tree format privacy** **spanning-tree format auto** **no spanning-tree format**	Configure the format of port spanning-tree packet, standard format is provided by IEEE, privacy is compatible with CISCO and auto means the format is determined by checking the received packet.

7. Configure the spanning-tree attribute of port

Command	Explanation
Port Mode	

spanning-tree cost **no spanning-tree cost**	Set the port path cost.
spanning-tree port-priority **no spanning-tree port-priority**	Set the port priority.
spanning-tree rootguard **no spanning-tree rootguard**	Set the port is root port.
Global Mode	
spanning-tree transmit-hold-count <tx-hold-count-value> **no spanning-tree transmit-hold-count**	Set the max transmit-hold-count of port.
spanning-tree cost-format {dot1d | dot1t}	Set port cost format with dot1d or dot1t.

8. Configure the snooping attribute of authentication key

Command	Explanation
Port Mode	
spanning-tree digest-snooping **no spanning-tree digest-snooping**	Set the port to use the authentication string of partner port. The no command restores to use the generated string.

9. Configure the FLUSH mode once topology changes

Command	Explanation
Global Mode	
spanning-tree tcflush {enable| disable| protect} **no spanning-tree tcflush**	Enable: the spanning-tree flush once the topology changes. Disable: the spanning tree don't flush when the topology changes. Protect: the spanning-tree flush not more than one time every ten seconds. The no command restores to default setting, enable flush once the topology changes.
Port Mode	
spanning-tree tcflush {enable| disable| protect} **no spanning-tree tcflush**	Configure the port flush mode. The no command restores to use the global configured flush mode.

1.3 MSTP Example

The following is a typical MSTP application example:

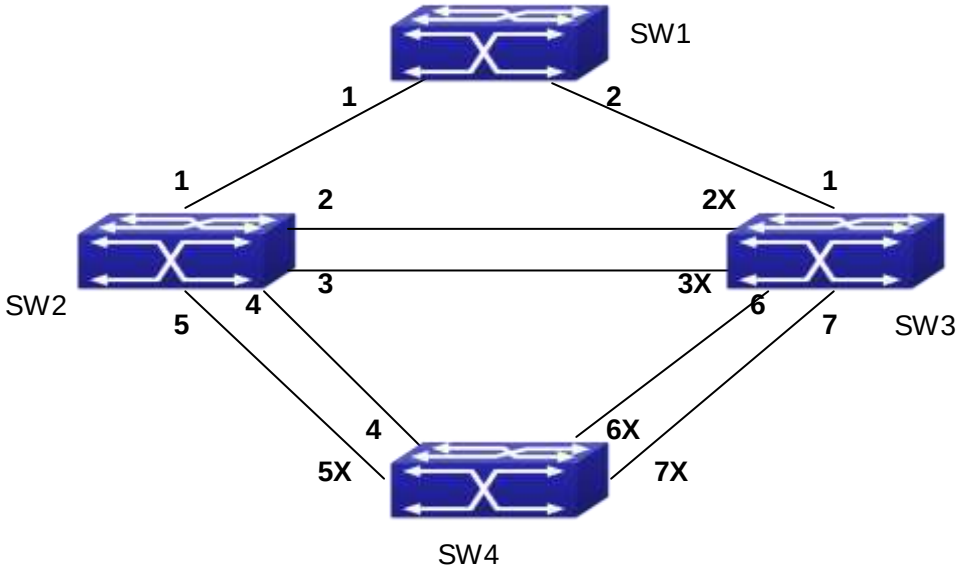


Fig 1-2 Typical MSTP Application Scenario

The connections among the switches are shown in the above figure. All the switches run in the MSTP mode by default, their bridge priority, port priority and port route cost are all in the default values (equal). The default configuration for switches is listed below:

Bridge Name		SW1	SW2	SW3	SW4
Bridge MAC Address		…00-00-01	…00-00-02	…00-00-03	…00-00-04
Bridge Priority		32768	32768	32768	32768
Port Priority	port 1	128	128	128	
	port 2	128	128	128	
	port 3		128	128	
	port 4		128		128
	port 5		128		128
	port 6			128	128
	port 7			128	128
Route Cost	port 1	200000	200000	200000	
	port 2	200000	200000	200000	
	port 3		200000	200000	
	port 4		200000		200000

	port 5		200000		200000
	port 6			200000	200000
	port 7			200000	200000

By default, the MSTP establishes a tree topology (in blue lines) rooted with SwitchA. The ports marked with "x" are in the discarding status, and the other ports are in the forwarding status.

Configurations Steps:

Step 1: Configure port to VLAN mapping:

- ☞ Create VLAN 20, 30, 40, 50 in Switch2, Switch3 and Switch4.
- ☞ Set ports 1-7 as trunk ports in Switch2 Switch3 and Switch4.

Step 2: Set Switch2, Switch3 and Switch4 in the same MSTP:

- ☞ Set Switch2, Switch3 and Switch4 to have the same region name as mstp.
- ☞ Map VLAN 20 and VLAN 30 in Switch2, Switch3 and Switch4 to Instance 3; Map VLAN 40 and VLAN 50 in Switch2, Switch3 and Switch4 to Instance 4.

Step 3: Set Switch3 as the root bridge of Instance 3; Set Switch4 as the root bridge of Instance 4

- ☞ Set the bridge priority of Instance 3 in Switch3 as 0.
- ☞ Set the bridge priority of Instance 4 in Switch4 as 0.

The detailed configuration is listed below:

Switch2:

```
Switch2(config)#vlan 20
Switch2(Config-Vlan20)#exit
Switch2(config)#vlan 30
Switch2(Config-Vlan30)#exit
Switch2(config)#vlan 40
Switch2(Config-Vlan40)#exit
Switch2(config)#vlan 50
Switch2(Config-Vlan50)#exit
Switch2(config)#spanning-tree mst configuration
Switch2(Config-Mstp-Region)#name mstp
Switch2(Config-Mstp-Region)#instance 3 vlan 20;30
Switch2(Config-Mstp-Region)#instance 4 vlan 40;50
Switch2(Config-Mstp-Region)#exit
Switch2(config)#interface e1/0/1-7
```

Switch2(Config-Port-Range)#switchport mode trunk
Switch2(Config-Port-Range)#exit
Switch2(config)#spanning-tree

Switch3:

Switch3(config)#vlan 20
Switch3(Config-Vlan20)#exit
Switch3(config)#vlan 30
Switch3(Config-Vlan30)#exit
Switch3(config)#vlan 40
Switch3(Config-Vlan40)#exit
Switch3(config)#vlan 50
Switch3(Config-Vlan50)#exit
Switch3(config)#spanning-tree mst configuration
Switch3(Config-Mstp-Region)#name mstp
Switch3(Config-Mstp-Region)#instance 3 vlan 20;30
Switch3(Config-Mstp-Region)#instance 4 vlan 40;50
Switch3(Config-Mstp-Region)#exit
Switch3(config)#interface e1/0/1-7
Switch3(Config-Port-Range)#switchport mode trunk
Switch3(Config-Port-Range)#exit
Switch3(config)#spanning-tree
Switch3(config)#spanning-tree mst 3 priority 0

Switch4:

Switch4(config)#vlan 20
Switch4(Config-Vlan20)#exit
Switch4(config)#vlan 30
Switch4(Config-Vlan30)#exit
Switch4(config)#vlan 40
Switch4(Config-Vlan40)#exit
Switch4(config)#vlan 50
Switch4(Config-Vlan50)#exit
Switch4(config)#spanning-tree mst configuration
Switch4(Config-Mstp-Region)#name mstp
Switch4(Config-Mstp-Region)#instance 3 vlan 20;30
Switch4(Config-Mstp-Region)#instance 4 vlan 40;50
Switch4(Config-Mstp-Region)#exit

```
Switch4(config)#interface e1/0/1-7
Switch4(Config-Port-Range)#switchport mode trunk
Switch4(Config-Port-Range)#exit
Switch4(config)#spanning-tree
Switch4(config)#spanning-tree mst 4 priority 0
```

After the above configuration, Switch1 is the root bridge of the instance 0 of the entire network. In the MSTP region which Switch2, Switch3 and Switch4 belong to, Switch2 is the region root of the instance 0, Switch3 is the region root of the instance 3 and Switch4 is the region root of the instance 4. The traffic of VLAN 20 and VLAN 30 is sent through the topology of the instance 3. The traffic of VLAN 40 and VLAN 50 is sent through the topology of the instance 4. And the traffic of other VLANs is sent through the topology of the instance 0. The port 1 in Switch2 is the master port of the instance 3 and the instance 4.

The MSTP calculation generates 3 topologies: the instance 0, the instance 3 and the instance 4 (marked with blue lines). The ports with the mark “x” are in the status of discarding. The other ports are the status of forwarding. Because the instance 3 and the instance 4 are only valid in the MSTP region, the following figure only shows the topology of the MSTP region.

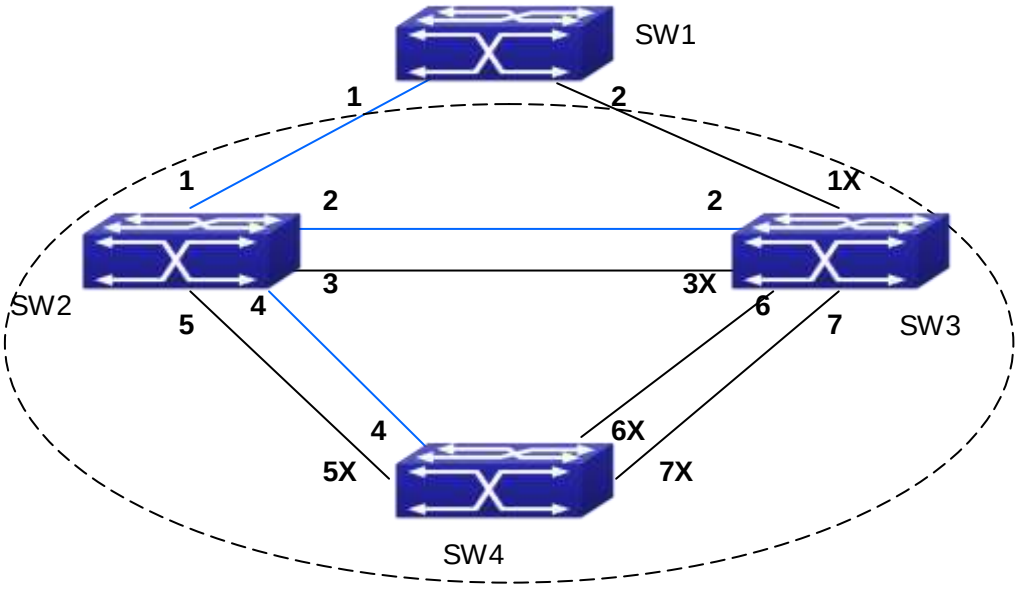


Fig 1-3 The Topology Of the Instance 0 after the MSTP Calculation

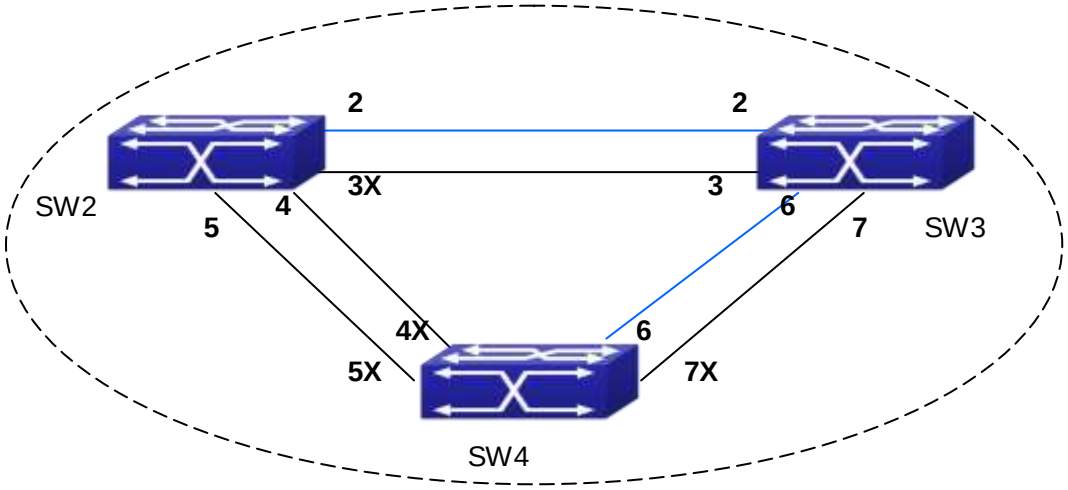


Fig 1-4 The Topology Of the Instance 3 after the MSTP Calculation

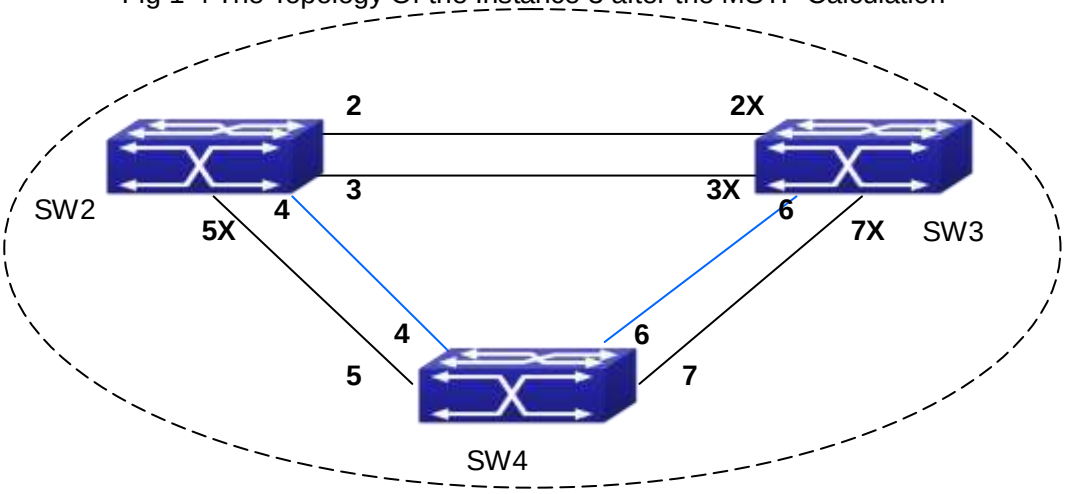


Fig 1-5 The Topology Of the Instance 4 after the MSTP Calculation

1.4 MSTP Troubleshooting

- In order to run the MSTP on the switch port, the MSTP has to be enabled globally. If the MSTP is not enabled globally, it can't be enabled on the port.
- The MSTP parameters co work with each other, so the parameters should meet the following conditions. Otherwise, the MSTP may work incorrectly.

  2×(Bridge_Forward_Delay -1.0 seconds) >= Bridge_Max_Age

  Bridge_Max_Age >= 2 ×(Bridge_Hello_Time + 1.0 seconds)
- When users modify the MSTP parameters, they have to be sure about the changes of the topologies. The global configuration is based on the bridge. Other configurations are based on the individual instances.

Chapter 2 ERPS Configuration

2.1 Introduction to ERPS

ERPS (Ethernet Ring Protection Switching) is a kind of layer2 anti-ring protocol which is defined by ITU-T; the standard number is ITU-T G.8032/Y1344, also known as G.8032. G.8032 Ethernet standard absorbs the advantages of the ring network protection technology of EAPS, RPR, SDH, STP.etc. It optimizes the detection mechanism and it can detect the two-way/single-way fault, support the structure with multi-ring and multi-domain. At the same time of achieving rotating of 50ms, it supports the master and slave and load sharing. It becomes the newest standard of the Ethernet ring technology.

ERPS is the anti-ring protocol used in ring network protection. It includes: link switching in loop fault, notification and loop rotating after loop restored, but it does not include the discovery of link fault. The CCM function defined by 802.1ag protocol can be used in fault discovery and the physical link fault detection can also be used. The principle is that it must be flexible no matter which detection mechanism was used, the link fault can be found in a short time and it will be noticed to the erps module. The link fault rotating time that erps asks is: flow discontinuity time is 50ms at most with that the link length is in 1200km and in 16 nodes. It is demanding for the link fault discovery and loop protection protocol rotating time.

2.1.1 ERPS Terminology

Ethernet ring: It is the closed physical ring network which is made up by many ring nodes, every node on the ring has only two ports connecting to this ring network.

Ring protection link: RPL is a link on the ring network. When the ring network is healthy, the link blocked by the node cannot transmit the data flow.

RPL owner node: When the ring network is healthy, the nodes connected to RPL will block the RPL. At the same time, it will launch the link rotating when the ring network restored and it is configured as reversion.

RPL neighbor node: RPL neighbor node, it is the other node connected to RPL. When the ring network is healthy, it will block the RPL.

Interconnection node: Cross node, when there are many rings are crossed, it is the node

in the cross position. On the cross nodes, there is one or more rings can be connected through two ports. The ring connected through one port is the sub-ring, the ring connected through two ports is the main ring.

R-APS virtual channel: It is the link which makes the sub-ring connect between two interconnection nodes out of the sub-ring path. Its transmission characteristic is related to the out ring network.

major-ring: It is the ring which connects the two ports on the interconnection node.

sub-ring: It is the ring which connects to other network through two interconnection nodes. it is not a ring network, it will make up a ring network only when connect it through the interconnection node.

ERP instance: It is a set protected by many vlan. The packet transmission of the vlan in this instance pass the same ring network link, every vlan only belongs to one instance.

Revertive switch: After learning of the ring network fault restored, the RPL owner node will restore the blockade status of RPL and make the network flow transmission path restore to the link before the fault.

Non-revertive switch: After learning of the ring network fault restored, the RPL owner node will not block the RPL, the network flow transmission path is same as before.

2.1.2 ERPS Function

2.1.2.1 Fault Switchover

The following is the single-ring and single link fault.

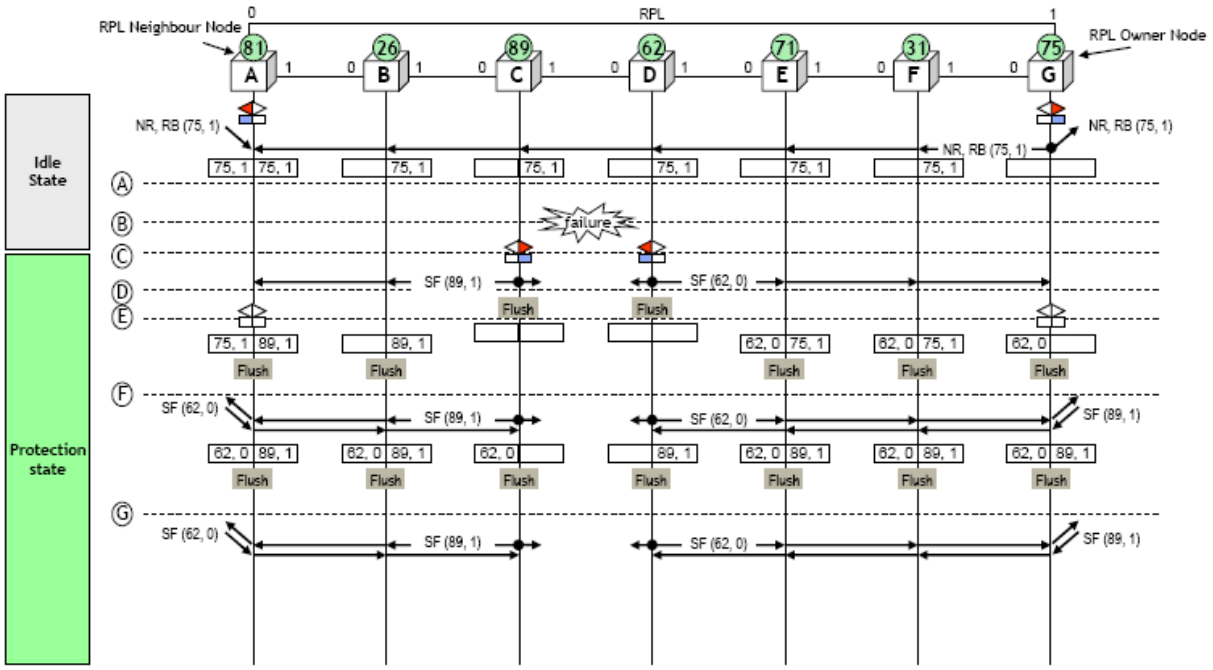


Fig 2-1 single-link fault

The steps of fault switchover:

a) The ring network status is normal; RPL owner node of G sends the R-APS (NR, RB) packet periodically. This packet explains that RPL link is in blockade status and the ring network is healthy.

b) There is fault on the link between node C and D.

c) The node C and D detected the fault, they block the port which connected to the fault link respectively and run the flush FDB.

d) At the same time, the node C and D send the fault notification packet of R-APS (SF) respectively through the port connected to the ring network.

e) All the nodes which received R-APS (SF) packet will run the flush FDB. At the same time, RPL owner node of G and RPL neighbor node of A will configure the RPL connection port as forward. The node G will stop sending R-APS (NR,RB) packet.

f) Because RPL link has removed the blockade, all nodes can receive two R-APS (SF) packets (sent by node C and D). after receiving the new R-APS (SF) packet, it will run the flush FDB.

g) Link fault message of R-APS (SF) will transmitting always in the ring network.

2.1.2.2 Failure Recovery

When the ring link restored, there are two methods on the ring nodes: one is Revertive switch. After the ring link restored to be normal, the ring network will block the RPL, and restore the forwarding status of the fault link. At this time, the forwarding path of the data packet is same as the last once when it is normal. Another one is Non-revertive switch. After the ring link restored to be normal, the link will keep the block

status. The data packet will continue to be forwarded with the current path.

The environments of the two methods are different. When the block RPL can make the data flow transmission path be the best, use the Revertive switch; when the path costs are similar, there is no difference no matter which path will be blocked, for preventing the secondary interruption of data flow, use the Non-revertive switch.

1. Revertive switch

The following is the single-ring and single link fault.

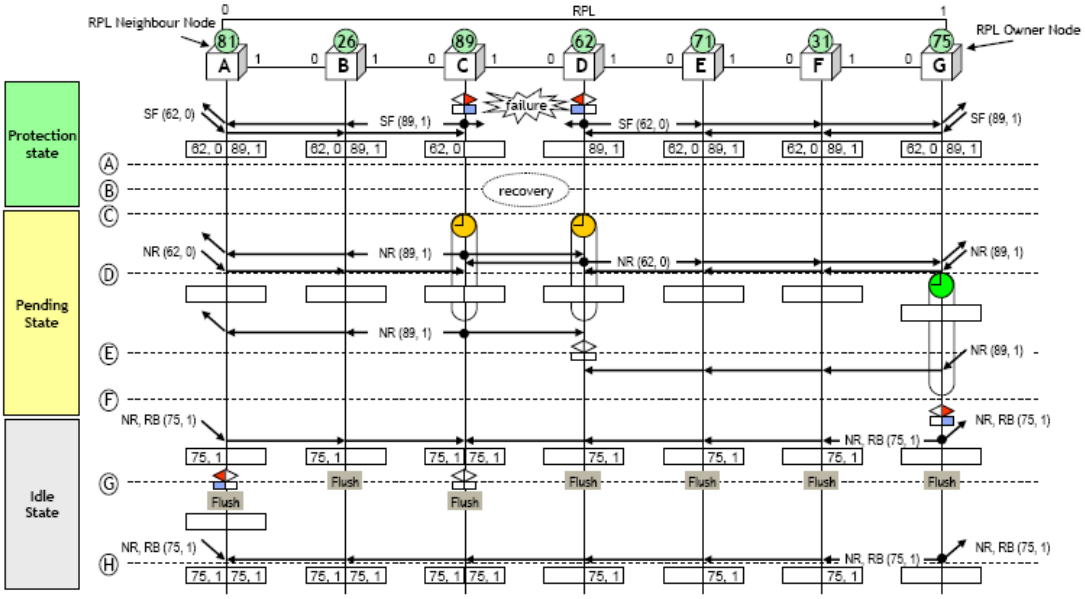


Fig 2-2 Revertive switch fault restoration of single link

The steps:

a) The fault still existed, the node which has detected the fault will send the R-APS (SF) packets with the fault message periodically;

b) Fault restoration on the link;

c) The nodes of C and D detects the fault restoration, they will start the guard timer and send the fault restoration packets of R-APS (NR) on the ports of the ring network at the same time;

d) When the RPL owner node detected R-APS (NR) packets, it will start the WTR timer and clear the local node fault message at the same time;

e) After the nodes C and D are time out, they receives the R-APS (NR) packets from the peer. The node D thinks the priority of node C is higher, so it will stop sending the R-APS (NR) packets with the local message and relieve the block of the port;

f) When the WTR timer of RPL owner node G is time out, it will block the port connected to RPL and send the R-APS (NR, RB) packets through the ring network port to notify other nodes that RPL link has been blocked. At the same time, the node G run the flush FDB;

g) When the node C received the R-APS (NR, RB) packets sent by RPL owner node, it will relieve the block of the local port and stop sending NR packets at the

same time. After RPL neighbor node A received this packet, it will block the port connected to RPL. Other, all nodes will run the flush FDB after received R-APS (NR, RB) packets.

2. Non-revertive switch

The following example is about the single-ring and single link fault as shown in Fig 2-3.

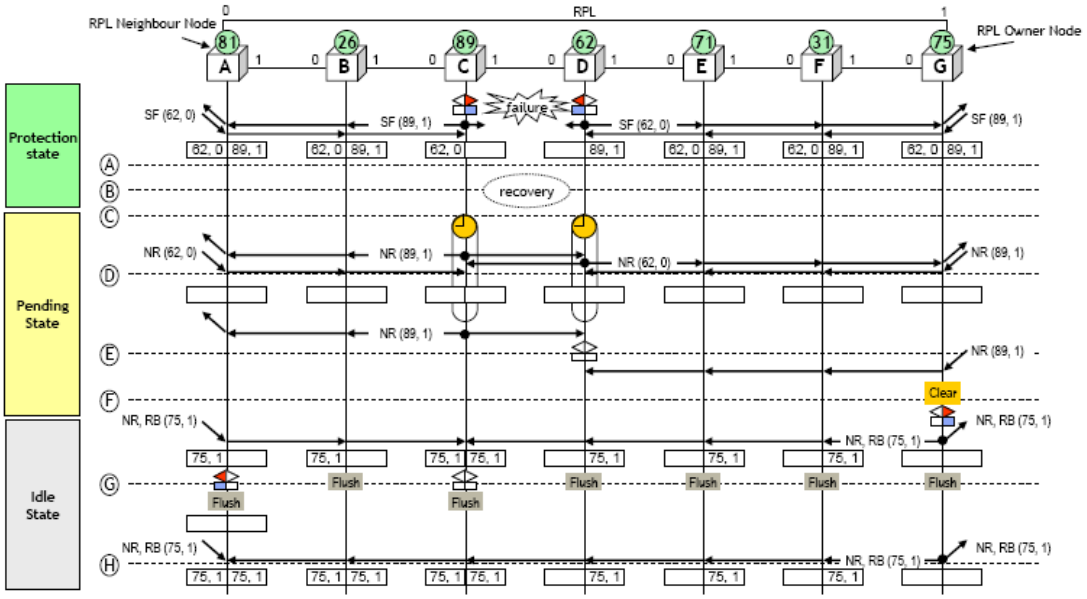


Fig 2-3 Non-revertive switch fault restoration of single link

The steps:

a) The fault still existed, the node which has detected the fault will send the R-APS (SF) packets with the fault message periodically;

b) Fault restoration on the link;

c) The nodes of C and D detects the fault restoration, they will start the guard timer and send the fault restoration packets of R-APS (NR) on the ports of the ring network at the same time;

d) When the RPL owner node G detected the R-APS (NR) packets, it will clear the local node fault message because of the configured non-revertive method, but it will not start the WTR timer;

e) After the nodes C and D are time out, they receives the R-APS (NR) packets from the peer. The node D thinks the priority of node C is higher, so it will stop sending the R-APS (NR) packets and relieve the block of the local port;

f) If RPL owner node G runs clear command, it will be recovered to be revertive method and it will block the port connected to RPL and send R-APS (NR, RB) packets through the ring network port to notify other nodes that the RPL link has been blocked. At the same time, it will run flush FDB;

g) When the node C received the packets sent by RPL owner node, it will relieve the block of the local port and stop sending R-APS (NR) packets at the same time. After RPL neighbor node A received this packet, it will block the port

connected to RPL. Other, all nodes will run the flush FDB after received the packets.

2.1.2.3 Interconnection Ring Model

ERPS protocol can support the protection and switching of the interconnection ring. The interconnection ring includes two types: the interconnection ring model with virtual channel and the interconnection ring model without virtual channel.

1. The interconnection ring model with virtual channel

As shown in Fig 2-4, three ring networks are interconnection. Ring 1 is the major ring and it is made up with the ring nodes A, B, G, H and the links of them. When ring 1 is health, it will block the link between nodes A and B. ring 2 is another major ring, it is made up with the ring nodes C, D, E, F and the links of them. When ring 2 is health, it will block the link between node C and D. ring 3 is a sub ring, it is made up with the nodes B, C, F, G and the links of B-C and G-F. When ring 3 is health, it will block the link of B-C. B-G links are the interconnection links of ring 1 and ring 3 and it belongs to ring 1. C-F links are the interconnection links of ring 2 and ring 3 and it belongs to ring 2. Ring 1 and ring 2 are both the close ring network, ring 3 is not a ring network. If treat ring 1 as the link between the interconnection nodes B and G of ring 3 (virtual channel), and treat ring 2 as the link between the interconnection nodes C and F of ring 3 (virtual channel), ring 3 will be a ring network.

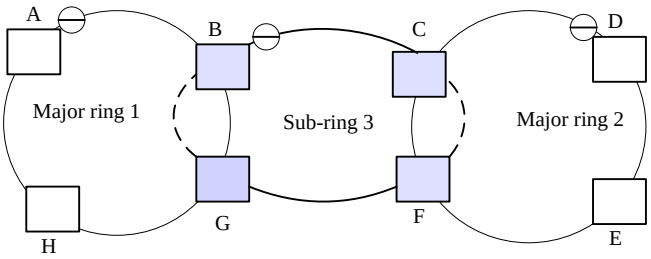


Fig 2-4 the interconnection ring topology with virtual channel

The R-APS virtual channel supported by ring 1 and ring 2 treats ring 3 protocol packets as the data packets. The transmission method of the packets is same as the method of data packets. The node B of ring 3 sends and receives the ring 3 erps protocol packets sent by node G, at the same time, the node G sends and receives the ring 3 erps protocol packets sent by node B. For distinguishing the erps packets of ring 3 and the erps packets of this major ring in ring 1 and ring 2, different control vlan can be used to the protocol packets transmission of every ring.

When the sub ring 3 is changing, it should notify ring 1 and ring 2. The node on the major ring will run flush FDB. The topology changing of the major ring 1 and ring 2 will not affect the sub ring 3. Other, the topology changing of the major ring 1 and ring 2 will not affect each other either.

2. The interconnection ring model without virtual channel

Change the way to understand the ring network as shown in Fig 2-5: ring 1 is the major ring and it is made up with the ring nodes A, B, G, H and the links of them. When ring 1 is health, it will block the link between nodes A and B. ring 2 is sub ring, it is made up with the ring nodes C, D, E, F and the links of C-D, D-E and E-F. When ring 2 is health, it will block the link between node C and D. ring 3 is another sub ring, it is made up with the nodes B, C, F, G and the links of B-C, C-F and F-G. When ring 3 is health, it will block the link of B-C. B-G links are the interconnection links of ring 1 and ring 3 and it belongs to ring 1. C-F links are the interconnection links of ring 2 and ring 3 and it belongs to ring 3. Ring 1 is the close ring network; ring 2 and ring 3 are not the ring network.

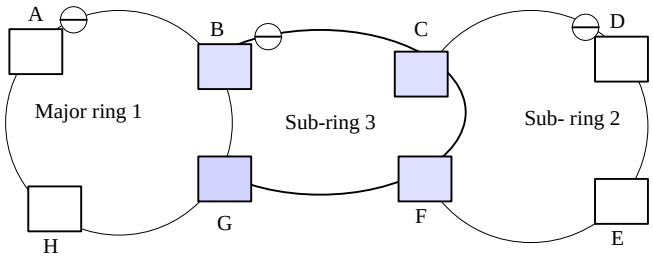


Fig 2-5 the interconnection ring topology without virtual channel

Although ring 2 and ring 3 are not ring network neither, the erps packets of these two sub ring need to be transmitted to all ring nodes. So, the block link should still transmit erps protocol packets if the links of B-C and C-D are blocked, and the nodes B, C and C, D of the block link should also receive and send the erps protocol packets.

When the sub ring 3 is changing, it should notify ring 1. The node on the major ring will run flush FDB. The topology changing will not affect the sub ring 2. When the sub ring 2 is changing, it will affect the sub ring 3 and the major ring 1. The node on the major ring should run flush FDB. But, the topology changing of the major ring 1 will not affect the sub ring 2 and ring 3.

2.1.3 ERPS Application

ERPS is used for ring network and it is located in convergence layer, the convergence loop can complete the layer2 convergence of business; insert the layer3 network to deal with the business at the same time. The convergence loop runs ERPS protocol and provides layer2 redundancy protection exchange function of convergence loop.

2.2 ERPS Configuration

ERPS Configuration task list as below:

1) Create the instance; the map is corresponding to the vlan which should be protected

2) Create ERPS loop, and configure the member port information. The default configuration: support version V2, the main loop closing type and monitor the physical status of port

3) Configure ERPS loop instance and configure the protection instance, port roles. Configure the ERPS loop instance name, R-APS level, timer information. Configure the controlling VLAN at last and select the port to configure it as RPL owner and RPL Neighbor

1. Create the MSTP instance

Command	Explanation
Global Mode	
spanning-tree mst configuration **no spanning-tree mst configuration**	Enter into the MST configuration mode, configure the parameters of MSTP domain; the no command recovers to be the default.
MST Mode	
instance <instance value > vlan <vlan-list> **no instance [instance-value]**	Configure vlan which needs to be protected by the instance and mapping; the no command deletes the appointed instance.

2. Create ERPS ring and configure the member ports information

Command	Explanation
Global Mode	
erps ring <ring-name> **no erps ring <ring-name>**	Create ERPS ring and enter into the ERPS ring configuration mode; the no command deletes the appointed erps ring.
Port Mode	
erps-ring <ring-name> port0 **erps-ring <ring-name> port1** **erps-ring <ring-name> port0** **erps-ring <ring-name> port1**	Configure the port0 or port1 which is the ring node of port; the no command deletes their property.

3. Configure ERPS ring instance

Command	Explanation
Global Mode	
erps ring <ring-name>	Create ERPS ring and enter into the

no erps ring <ring-name>	ERPS ring configuration mode; the no command deletes the appointed erps ring.
ERPS Ring Configuration Mode	
eprs-instance <instance-id> **no eprs-instance <instance-id>**	Create ERPS ring instance and enter into the ERPS ring configuration mode; the no command deletes the appointed ring node instance.
description <*instance-name*> ***no* description**	Configure the description string of ERPS instance; the no command deletes the appointed string.
rpl {port0 | port1} {owner | neighbour} **no rpl {port0 | port1}**	Configure the member port of ERPS ring instance as RPL owner or RPL neighbor; the no command deletes the appointed owner or neighbor node.
raps-mel <level-value> **no raps-mel**	Configure the level of R-APS channel, the MEL field in the protocol packets is used to detect if the current packet can pass by; the no command deletes the level of R-APS channel.
protected-instance <*instance-list*> **no protected-instance**	Configure the protection instance of ERPS ring instance. The no command deletes the protection instance.
wtr-timer <*wtr-times*> **no wtr-timer**	Configure the WTR timer. The WTR timer is used to avoid the configuration of frequent switching of RPL owner node because of the periodic (discontinuity) fault. The no command deletes the wtr timer.
guard-timer <*guard-times*> **no guard-timer**	Configure the Guard timer. The Guard timer is used in Ethernet ring node to avoid the wrong configuration according to the outdated R-APS packets and avoid the close loop. The no command deletes the guard timer.
holdoff –timer <*holdoff-times*> **no holdoff –timer**	Configure the Holdoff timer. The Holdoff timer is used for Ethernet ring node blocking fault report time. The no

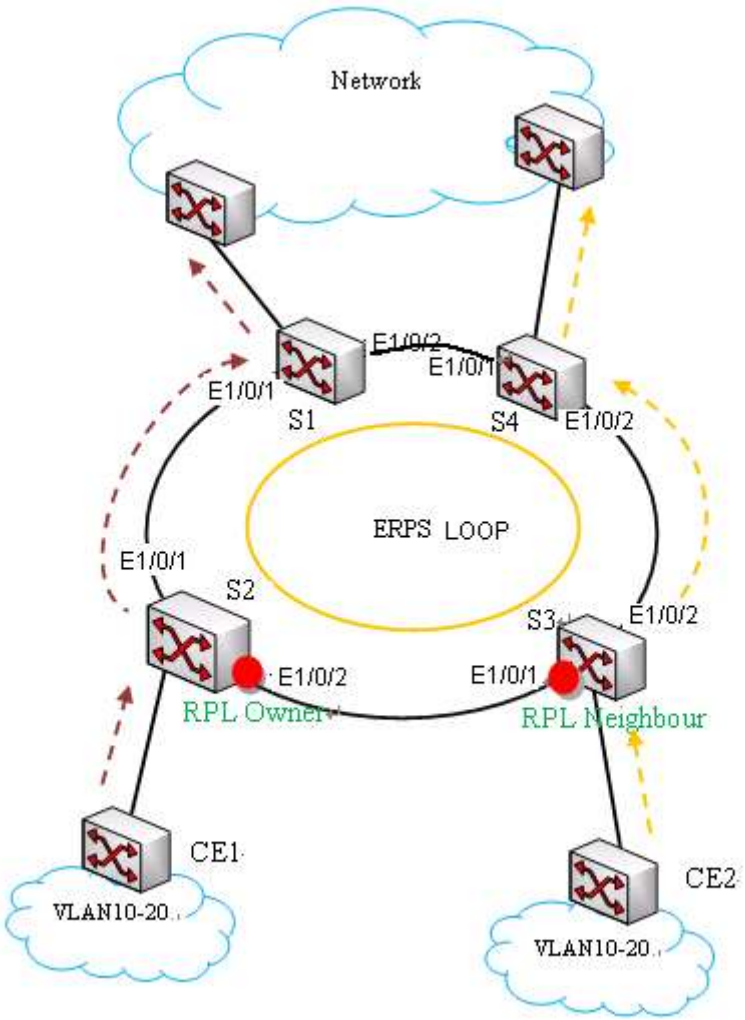
	command deletes the Holdoff timer.
control-vlan <*vlan-id*> **no control-vlan**	Configure the control vlan of R-APS channel transmission R-APS packets. In the ERPS ring instance, this vlan is used to deliver the ERPS protocol packets but not to forward the user business packets. It improves the security of ERPS protocol. The no command deletes the Control Vlan.

4. Show the configuration information of ERPS

Command	Explanation
Global Mode	
show erps ring {<ring-name> | brief}	Show ERPS ring information.
show erps instance [ring <ring-name> [instance <instance-id>]]	Show ERPS ring instance information.
show erps status [ring <ring-name> [instance <instance-id>]]	Show ERPS ring instance status information.
show erps statistics [ring <ring-name> [instance <instance-id>]]	Show ERPS ring instance statistic information.

2.3 ERPS Examples

Case 1:



As shown in the picture above, it is the explanation of ERPS configuration and application. S1~S4 make up the ring network and provide the layer2 redundancy protection transform function. For preventing the packets in VLAN10 ~ VLAN20 come to be loop, deploy the ERPS protocol on the devices which make up the ring network. The forwarding path of user data inserted through CE1 is S2-S1 and it is S3-S4 for the data which is deserted through CE2. For protecting the Ethernet loop switching, configure it as below:

1. Configuration thinking

Configure ERPS loop redundancy protection as below:

Create ERPS loop of maijor_ring1 and configure the loop member port;

Configure the instance 1 on ERPS loop of maijor_ring1 and configure the protection instance, member port role, timer and controlling VLAN.

2. Configuration steps

Step1: Create instance 2, VLAN2 and VLAN10-20 on S1 ~ S4, VLAN2 is used to transmit the protocol packets, VLAN10-20 are used to transmit the data packets.

Configuration of S1:

S1#config

S1(config)#spanning-tree mst configuration

S1(Config-Mstp-Region) instance 2 vlan 2;10-20

S1(Config-Mstp-Region)#exit

S1(config)#interface e1/0/1-2

S1(Config-If-Port-Range)#switchport mode trunk

The configuration of S2, S3 and S4 is same as S1.

Step2: Create ERPS loop and configure the member port information. The default configuration: support version V2, main loop closing type and monitor the physical status of port.

Configuration of S1:

S1(config)#erps-ring maijor_ring1

S1(config-erps-ring)#exit

S1(config)# interface e1/0/1

S1(config-if-ethernet1/0/1)erps-ring maijor_ring1 port 0

S1(config-if-ethernet1/0/1)interface e1/0/2

S1(config-if-ethernet1/0/2)erps-ring maijor_ring1 port 1

Step3: Configure ERPS loop instance and configure the protection instance, port role. Configure the ERPS loop instance name, R-APS level, timer information. Configure the controlling VLAN at last and configure the port e1/0/2 of S2 as RPL owner and RPL Neighbor is for e1/0/1 of S3.

Configuration of S1:

S1(config)# erps-ring maijor_ring1

S1(config-erps-ring)#erps-instance 1

S1(config-erps-ring-inst-1)#description instance1

S1(config-erps-ring-inst-1)#raps-mel 3

S1(config-erps-ring-inst-1)#protected-instance 2

S1(config-erps-ring-inst-1)#wtr-timer 8

S1(config-erps-ring-inst-1)#guard-timer 100

S1(config-erps-ring-inst-1)#holdoff-timer 5

S1(config-erps-ring-inst-1)# control-vlan 2

The configuration of S4 is same as S1.

Configuration of S2:

S2(config)# erps-ring maijor_ring1

S2(config-erps-ring)#erps-instance 1
S2(config-erps-ring-inst-1)#description instance1
S2(config-erps-ring-inst-1)#rpl port 1 owner
S2(config-erps-ring-inst-1)#non-revertive
S2(config-erps-ring-inst-1)#raps-mel 3
S2(config-erps-ring-inst-1)#protected-instance 2
S2(config-erps-ring-inst-1)#wtr-timer 8
S2(config-erps-ring-inst-1)#guard-timer 100
S2(config-erps-ring-inst-1)#holdoff-timer 5
S2(config-erps-ring-inst-1)# control-vlan 2

Configuration of S3:
S3(config)# erps-ring maijor_ring1
S3(config-erps-ring)#erps-instance 1
S3(config-erps-ring-inst-1)#description instance1
S3(config-erps-ring-inst-1)# rp0 port 1 neighbour
S3(config-erps-ring-inst-1)#raps-mel 3
S3(config-erps-ring-inst-1)#protected-instance 2
S3(config-erps-ring-inst-1)#wtr-timer 8
S3(config-erps-ring-inst-1)#guard-timer 100
S3(config-erps-ring-inst-1)#holdoff-timer 5
S3(config-erps-ring-inst-1)# control-vlan 2

Step 4: Check the configuration result. After the configuration above is successful, check the configuration result and below is for S2.

S2# show erps ring brief

Ring-ID	Description	Ring-topo	Port0	Port1	Version	Inst-Count
1	maijor_ring1	maijor-ring	1/0/1	1/0/2	V2	1

Switch#show erps instance
ERPS Ring maijor_ring1
Instance 1
Description: instance1
Protected Instance : 2 Revertive mode: revertive
RAPS MEL: 3 R-APS-Virtual-Channel:
Control Vlan : 2

Guard Timer (csec) : 100

Holdoff Timer (seconds) : 5

WTR Timer (min) : 8

Port	Role	Port-Status
port0	Common	Forwarding
port1	RPL Owner	Blocked

3. Configure the file

The configuration file of S1:

```
S1#config
S1(config)#erps-ring maijor_ring1
S1(config)#spanning-tree mst configuration
S1(Config-Mstp-Region) instance 2 vlan 2;10-20
S1(Config-Mstp-Region)#exit
S1(config)#interface e1/0/1-2
S1(Config-If-Port-Range)#switchport mode trunk
S1(Config-If-Port-Range)#exit
S1(config)# interface e1/0/1
S1(config-if-ethernet1/0/1)erps-ring maijor_ring1 port 0
S1(config-if-ethernet1/0/1)interface e1/0/2
S1(config-if-ethernet1/0/2)erps-ring maijor_ring1 port 1
S1(config-if-ethernet1/0/2)exit
S1(config)#erps-ring maijor_ring1
S1(config-erps-ring)#erps-instance 1
S1(config-erps-ring-inst-1)#description instance1
S1(config-erps-ring-inst-1)#raps-mel 3
S1(config-erps-ring-inst-1)#protected-instance 2
S1(config-erps-ring-inst-1)#wtr-timer 8
S1(config-erps-ring-inst-1)#guard-timer 100
S1(config-erps-ring-inst-1)#holdoff-timer 5
S1(config-erps-ring-inst-1)# control-vlan 2
```

The configuration file of S2:

```
S2#config
S2(config)#erps-ring maijor_ring1
S2(config)#spanning-tree mst configuration
S2(Config-Mstp-Region) instance 2 vlan 2;10-20
S2(Config-Mstp-Region)#exit
```

S2(config)#interface e1/0/1-2
S2(Config-If-Port-Range)#switchport mode trunk
S2(Config-If-Port-Range)#exit
S2(config)# interface e1/0/1
S2(config-if-ethernet1/0/1)erps-ring maijor_ring1 port 0
S2(config-if-ethernet1/0/1)interface e1/0/2
S2(config-if-ethernet1/0/2)erps-ring maijor_ring1 port 1
S2(config-if-ethernet1/0/2)exit
S2(config)#erps-ring maijor_ring1
S2(config-erps-ring)#erps-instance 1
S2(config-erps-ring-inst-1)#description instance1
S2(config-erps-ring-inst-1)#rpl port1 owner
S2(config-erps-ring-inst-1)#non-revertive
S2(config-erps-ring-inst-1)#raps-mel 3
S2(config-erps-ring-inst-1)#protected-instance 2
S2(config-erps-ring-inst-1)#wtr-timer 8
S2(config-erps-ring-inst-1)#guard-timer 100
S2(config-erps-ring-inst-1)#holdoff-timer 5
S2(config-erps-ring-inst-1)# control-vlan 2

The configuration file of S3:
S3#config
S3(config)#erps-ring maijor_ring1
S3(config)#spanning-tree mst configuration
S3(Config-Mstp-Region) instance 2 vlan 2;10-20
S3(Config-Mstp-Region)#exit
S3(config)#interface e1/0/1-2
S3(Config-If-Port-Range)#switchport mode trunk
S3(Config-If-Port-Range)#exit
S3(config)# interface e1/0/1
S3(config-if-ethernet1/0/1)erps-ring maijor_ring1 port 0
S3(config-if-ethernet1/0/1)interface e1/0/2
S3(config-if-ethernet1/0/2)erps-ring maijor_ring1 port 1
S3(config-if-ethernet1/0/2)exit
S3(config)#erps-ring maijor_ring1
S3(config-erps-ring)#erps-instance 1
S3(config-erps-ring-inst-1)#description instance1
S3(config-erps-ring-inst-1)#rpl port1 neighbour

S3(config-erps-ring-inst-1)#raps-mel 3
S3(config-erps-ring-inst-1)#protected-instance 2
S3(config-erps-ring-inst-1)#wtr-timer 8
S3(config-erps-ring-inst-1)#guard-timer 100
S3(config-erps-ring-inst-1)#holdoff-timer 5
S3(config-erps-ring-inst-1)# control-vlan 2

The configuration file of S4:
S4#config
S4(config)#erps-ring maijor_ring1
S4(config)#spanning-tree mst configuration
S4(Config-Mstp-Region) instance 2 vlan 2;10-20
S4(Config-Mstp-Region)#exit
S4(config)#interface e1/0/1-2
S4(Config-If-Port-Range)#switchport mode trunk
S4(Config-If-Port-Range)#exit
S4(config)# interface e1/0/1
S4(config-if-ethernet1/0/1)erps-ring maijor_ring1 port 0
S4(config-if-ethernet1/0/1)interface e1/0/2
S4(config-if-ethernet1/0/2)erps-ring maijor_ring1 port 1
S4(config-if-ethernet1/0/2)exit
S4(config)#erps-ring maijor_ring1
S4(config-erps-ring)#erps-instance 1
S4(config-erps-ring-inst-1)#description instance1
S4(config-erps-ring-inst-1)#raps-mel 3
S4(config-erps-ring-inst-1)#protected-instance 2
S4(config-erps-ring-inst-1)#wtr-timer 8
S4(config-erps-ring-inst-1)#guard-timer 100
S4(config-erps-ring-inst-1)#holdoff-timer 5
S4(config-erps-ring-inst-1)# control-vlan 2

2.4 ERPS Troubleshooting

If the configured ERPS loop cannot achieve the Ethernet loop switching protection, check if it was wrong with the following reasons:

- ☞ Check if the basic configuration is correct and check if the protection instance of every node, control-vlan, wtr-timer, guard-timer and raps-mel are consistent.
- ☞ Check if the vlan that user data flow is in is not the same one that control-vlan is in.

In the ERPS loop instance, control vlan is only used to transmit ERPS protocol packet but not the user business packet; it improves the security of ERPS protocol. User ensures the uniqueness of the configuration. This VLAN is as the vlan tag when sending R-APS packet. In the instance, the protection VLAN configuration of all nodes must be consistent.

☞ We suggest the port which user configured on ERPS node is trunk port and ensure that the vlan and control vlan that data packet is in are in the protection instance and ERPS only protect the data and protocol packet in the instance. For instance, the switch enables a protocol (CFM, EFM, Layer3 interface) and it makes the switch send the protocol packet out. Then, if the vlan ID which sends the packet is not in the protection instance, there will be the loop in the topology.

☞ If configure the port status test method as fastlink, the hardware must support fastlink function. Break off the notification of port status changing; disable the mac soft study function at the same time.

☞ If it is configured associating with CFM, the hardware must support CC function and it can achieve the ability of CCM sending packet in 3.3ms.