Content

CHAPTER 1 VRRP CONFIGURATION 1-1

1.1 INTRODUCTION TO VRRP 1-1

1.2 VRRP CONFIGURATION TASK LIST 1-1

1.3 VRRP TYPICAL EXAMPLES 1-2

1.4 VRRP TROUBLESHOOTING 1-3

CHAPTER 2 IPV6 VRRPV3 CONFIGURATION 2-1

2.1 INTRODUCTION TO VRRPV3 2-1

2.1.1 The Format of VRRPv3 Message 2-1

2.1.2 VRRPv3 Working Mechanism 2-2

2.2 VRRPV3 CONFIGURATION 2-3

2.2.1 Configuration Task Sequence 2-3

2.3 VRRPV3 TYPICAL EXAMPLES 2-4

2.4 VRRPV3 TROUBLESHOOTING 2-5

CHAPTER 3 MRPP CONFIGURATION 3-1

3.1 INTRODUCTION TO MRPP 3-1

3.1.1 Conception Introduction 3-1

3.1.2 MRPP Protocol Packet Types 3-2

3.1.3 MRPP Protocol Operation System 3-2

3.2 MRPP CONFIGURATION TASK LIST 3-3

3.3 MRPP TYPICAL SCENARIO 3-4

3.4 MRPP TROUBLESHOOTING 3-5

CHAPTER 4 ULPP CONFIGURATION 4-1

4.1 INTRODUCTION TO ULPP 4-1

4.2 ULPP CONFIGURATION TASK LIST 4-2

4.3 ULPP TYPICAL EXAMPLES 4-4
4.3.1 ULPP Typical Example1.....4-4
4.3.2 ULPP Typical Example2.....4-5
4.4 ULPP TROUBLESHOOTING 4-6
CHAPTER 5 ULSM CONFIGURATION.....5-1
5.1 INTRODUCTION TO ULSM 5-1
5.2 ULSM CONFIGURATION TASK LIST.....5-1
5.3 ULSM TYPICAL EXAMPLE 5-2
5.4 ULSM TROUBLESHOOTING.....5-3

Chapter 1 VRRP Configuration

1.1 Introduction to VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault tolerant protocol designed to enhance connection reliability between routers (or L3 Ethernet switches) and external devices. It is developed by the IETF for local area networks (LAN) with multicast/broadcast capability (Ethernet is a Configuration Example) and has wide applications.

All hosts in one LAN generally have a default route configured to specified default gateway, any packet destined to an address outside the native segment will be sent to the default gateway via this default route. These hosts in the LAN can communicate with the external networks. However, if the communication link connecting the router serving as default game and external networks fails, all hosts using that gateway as the default next hop route will be unable to communicate with the external networks.

VRRP emerged to resolve such problem. VRRP runs on multiple routers in a LAN, simulating a "virtual" router (also referred to as a "Standby cluster") with the multiple routes. There is an active router (the "Master") and one or more backup routers (the "Backup") in the Standby cluster. The workload of the virtual router is actually undertaken by the active router, while the Backup routers serve as backups for the active router.

The virtual router has its own "virtual" IP address (can be identical with the IP address of some router in the Standby cluster), and routers in the Standby cluster also have their own IP address. Since VRRP runs on routes or Ethernet Switches only, the Standby cluster is transparent to the hosts with the segment. To them, there exists only the IP address of the Virtual Router instead of the actual IP addresses of the Master and Backup(s). And the default gateway setting of all the hosts uses the IP address of the Virtual Router. Therefore, hosts within the LAN communicate with the other networks via this Virtual Router. But basically, they are communicating with the other networks via the Master. In the case when the Master of the Standby cluster fails, a backup will take over its task and become the Master to serve all the hosts in the LAN, so that uninterrupted communication between LAN hosts and external networks can be achieved.

To sum it up, in a VRRP Standby cluster, there is always a router/Ethernet serving as the active router (Master), while the rest of the Standby cluster servers act as the backup router(s) (Backup, can be multiple) and monitor the activity of Master all the time. Should the Master fail, a new Master will be elected by all the Backups to take over the work and

continue serving the hosts within the segment. Since the election and take-over duration is brief and smooth, hosts within the segment can use the Virtual Router as normal and uninterrupted communication can be achieved.

1.2 VRRP Configuration Task List

Configuration Task List:

1. Create/Remove the Virtual Router (required)
2. Configure VRRP dummy IP and interface (required)
3. Activate/Deactivate Virtual Router (required)
4. Configure VRRP sub-parameters (optional)
   - (1) Configure the preemptive mode for VRRP
   - (2) Configure VRRP priority
   - (3) Configure VRRP Timer intervals
   - (4) Configure VRRP interface monitor

1. Create/Remove the Virtual Router

Command	Explanation
Global Mode	
router vrrp <*vrid*> **no router vrrp <*vrid*>**	Creates/Removes the Virtual Router.

2. Configure VRRP Dummy IP Address and Interface

Command	Explanation
VRRP protocol configuration mode	
virtual-ip <*ip*> **no virtual-ip**	Configures VRRP Dummy IP address; the **"no virtual-ip"** command removes the virtual IP address.
interface {IFNAME | Vlan <*ID*>} **no interface**	Configures VRRP interface, the "**no interface**" command removes the interface.

3. Activate/Deactivate Virtual Router

Command	Explanation
VRRP protocol configuration mode	
enable	Activates the Virtual Router.
disable	Deactivates the Virtual Router.

4. Configure VRRP Sub-parameters

(1) Configure the preemptive mode for VRRP

Command	Explanation
VRRP protocol configuration mode	
preempt-mode {true| false}	Configures the preemptive mode for VRRP.

(2) Configure VRRP priority

Command	Explanation
VRRP protocol configuration mode	
priority <*priority*>	Configures VRRP priority.

(3) Configure VRRP Timer intervals

Command	Explanation
VRRP protocol configuration mode	
advertisement-interval <*time*>	Configures VRRP timer value (in seconds).

(4) Configure VRRP interface monitor

Command	Explanation
VRRP protocol configuration mode	
circuit-failover {IFNAME | Vlan <*ID*> } <*value_reduced*> **no circuit-failover**	Configures VRRP interface monitor, the **"no circuit-failover"** removes monitor to the interface.

1.3 VRRP Typical Examples

As shown in the figure below, SwitchA and SwitchB are Layer three Ethernet Switches in the same group and provide redundancy for each other.

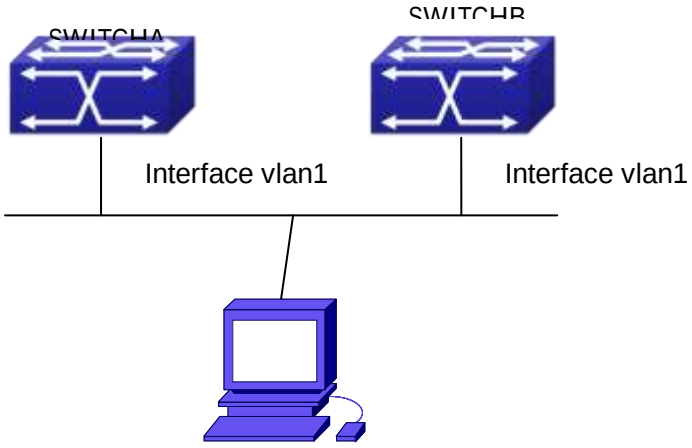

Fig 1-1 VRRP Network Topology

Configuration of SwitchA:

SwitchA(config)#interface vlan 1

SwitchA (Config-if-Vlan1)# ip address 10.1.1.1 255.255.255.0

SwitchA (config)#router vrrp 1

SwitchA(Config-Router-Vrrp)# virtual-ip 10.1.1.5

SwitchA(Config-Router-Vrrp)# interface vlan 1

SwitchA(Config-Router-Vrrp)# enable

Configuration of SwitchB:

SwitchB(config)#interface vlan 1

SwitchB (Config-if-Vlan1)# ip address 10.1.1.7 255.255.255.0

SwitchB(config)#router vrrp 1

SwitchB (Config-Router-Vrrp)# virtual-ip 10.1.1.5

SwitchB(Config-Router-Vrrp)# interface vlan 1

SwitchB(Config-Router-Vrrp)# enable

1.4 VRRP Troubleshooting

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

- Good condition of the physical connection.
- All interface and link protocols are in the UP state (use "**show interface**" command).
- Ensure VRRP is enabled on the interface. Verify the authentication mode of different routers (or L3 Ethernet switches) in the same standby cluster are the same.
- Verify the timer time of different routers (or L3 Ethernet switches) in the same standby cluster are the same.

- ☞ Verify the dummy IP address is in the same network segment of the interface's actual IP address.
- ☞ If the examination remains unsolved, please use **debug vrrp** and other debugging command and copy the DEBUG message within 3 minutes, send the recorded message to the technical server center of our company.

Chapter 2 IPv6 VRRPv3 Configuration

2.1 Introduction to VRRPv3

VRRPv3 is a virtual router redundancy protocol for IPv6. It is designed based on VRRP (VRRPv2) in IPv4 environment. The following is a brief introduction to it.

In a network based on TCP/IP protocol, in order to guarantee the communication between the devices which are not physically connected, routers should be specified. At present there are two most commonly used methods to specify routers: one is to study dynamically via routing protocols (such as internal routing protocols RIP and OSPF); the other is to configure statically. Running dynamical routing protocol on each terminal is unrealistic, since most operating systems for client end do not support dynamical routing protocol, even if they do, they are limited by the overheads of management, convergence, security and many other problems. So the common method is to adopt static routing configuration on terminal IP devices, which usually means specify one or more default gateway for terminal devices. Static routing simplifies the management of network and reduces the communication overheads of terminal devices, but it still has a disadvantage: if the router acting as the default gateway breaks, the communication of all the hosts which use this gateway as their next hop host. Even if there are more than one default gateways, before rebooting the terminal devices, they can not switch to the new gateway. Adopting virtual router redundancy protocol (VRPR) can effectively avoid the flaws of statically specifying gateways.

In VRRP protocol, there are two groups of import concepts: VRRP routers and virtual routers, master routers and backup routers. VRRP routers are routers running VRRP, which are physical entities; virtual routers are the ones created by VRRP, which are logical concepts. A group of VRRP routers cooperate to comprise a virtual router, which acts outwardly as a logical router with a unique fixed IP address and MAC address. The routers belonging to the same VRRP group play two mutually exclusive roles at the same time: master routers and backup routers. One VRRP group can only have one master router other but one or more backup routers. VRRPv3 protocol uses selection policy to select a master router from the router group to take charge of responding ND(Neighbor Discovery) neighbor request messages(ARP in IPv4) and forwarding IP data packets, while the other routers in the group will be in a state of waiting as backups. When the master router has a problem for some season, the backup router will be updated to the master router after a delay of a few seconds. Since this switch is very fast and does not need to change IP address or MAC address, it will be transparent to terminal user

systems.

In IPv6 environment, the hosts in a LAN usually learn the default gateway via neighbor discovery protocol (NDP), which is implemented based on regularly receiving advertisement messages from routers. The NDP of IPv6 has a mechanism called Neighbor Unreachability Detection, which checks whether a neighbor node is failed by sending unicast neighbor request messages to it. In order to reduce the overheads of sending neighbor request messages, these messages are only sent to those neighbor nodes which are sending flows, and are only sent if there is no instruction of UP state of the router in a period of time. In Neighbor Unreachability Detection, if adopting default parameters, it will take about 38 seconds to detect an unreachable router, which is a delay not ignorable for users and might cause a time-out in some transport protocols. Compared with NDP, VRRP provides a fast default gateway switch. In VRRP, backup routers can take up the unavailable master router in about 3 seconds (default parameter), and this process needs no interaction with hosts, which means being transparent to hosts.

2.1.1 The Format of VRRPv3 Message

VRRPv3 has its own message format, VRRP messages are used to communicate the priority of routers and the state of Master in the backup group, they are encapsulated in IPv6 messages to send, and are sent to the specified IPv6 multicast address. The format of VRRPv3 message is shown in Graph 1. The source address of the IPv6 message encapsulating the VRRPv3 message is the local address of the outbound interface of the message, and the destination address of it is the IPv6 multicast address(the multicast allocated to VRRPv3 is FF02:0:0:0:0:0:0:12). The number of hops should be limited to 255, and the next message head is 112(representing a VRRP message).

The meaning of each field in a VRRPv3 message is shown as follows:

Version: The version of VRRPv3, whose value is 3;

Type: The type of VRRP messages. There is only one type: ADVERTISEMENT, and its value is 1;

Virtual Rtr ID：The ID of the virtual router;

Priority：Priority, ranging from 0 to 255;

Count IPv6 Addr：The number of IPv6 addresses in a VRRPv3 message, the minimum of which is 1;

Rsvd：Reserved field, whose value is 0;

Adver Int：The advertisement interval of VRRPv3 messages, in seconds;

Checksum: The checksum, taking account of the whole VRRPv3 message and an IPv6 pseudo head (please refer to RFC2460 for details);

IPv6 Address(es): one or more IPv6 addresses related to the virtual router, the number of which is the same with "Count IPv6 Addr", and the first one of which should be the virtual IPv6 address of the virtual router.

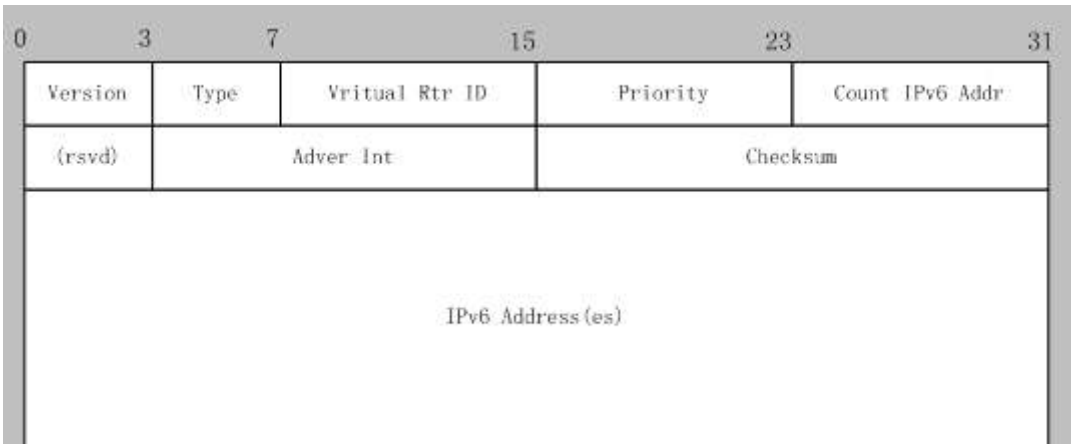

Fig 2-1 VRRPv3 message

2.1.2 VRRPv3 Working Mechanism

The working mechanism of VRRPv3 is the same with that of VRRPv2, which is mainly implemented via the interaction of VRRP advertisement messages. It will be briefly described as follows:

Each VRRP router has a unique ID: VRIP, ranging from 1 to 255. This router has a unique virtual MAC address outwardly, and the format of which is 00-00-5E-00-02-{VRID} (the format of virtual MAC address in VRRPv2 is 00-00-5E-00-01-{VRID}). Master router is in charge of using this MAC address to respond to ND neighbor request (it is ARP request in VRRPv2). Thus, no matter what switch is made, the terminal devices will get the same IP and MAC address all the time, reducing the affection that the switch causes on terminal devices.

There is only one kind of VRRP control message: VRRP advertisement. It uses IP multicast data packets to encapsulate, and the format of multicast addresses is FF02:0:0:0:0:0:XXXX:XXXX. In order to keep a consistence with the multicast address in VRRPv2 (224.0.0.18), the multicast addresses used by VRRPv3 advertisement messages can be FF02:0:0:0:0:0:0:12, and the advertisement is limited within the same LAN. Thus, different VRID are guaranteed to be used repeatedly in different networks. In order to reduce the overheads of network bandwidth, only master routers can send VRRP advertisement messages regularly. Backup routers will start a new round of VRRP

selection if it hasn't received a VRRP advertisement in 3 advertisement intervals in a row or if it receives an advertisement with a priority of 0.

In a VRRP router group, the master router is selected according to priority. The range of priority in VRRP protocol is 0-255. If the IP address of a VRRP router is the same to that of the virtual router interface, then the virtual router will be called the IP address owner in the VRRP group; the IP address owner automatically has the highest priority: 255. The priority of 0 is usually used when the IP address owner gives up the role of master. The range of priority can be configured is 1-254. The configuration rule of priority can be set according to the speed and cost of the link, the performance and reliability of the router and other management policies. In the selection of the master router, the virtual router with high priority will win. So, if there is an IP owner in the VRRP group, it will always be the master router. For the candidate routers having the same priority, selection will be done according to the magnitude of IP addresses (the bigger IP address takes precedence). VRRP also provides a preemptive priority policy. If such policy is configured, the backup router with higher priority will preempt the role of new master router over the current master router with lower priority.

In order to avoid the fault of returning a physical MAC address when Pinging virtual IP, it is regulated that virtual IP can not be the real IP of the interface. Thus, all the interfaces participating of the backup group selection will be backup by default.

2.2 VRRPv3 Configuration

2.2.1 Configuration Task Sequence

1. Create/delete the virtual router (necessary)
2. Configure the virtual IPv6 address and interface of VRRPv3 (necessary)
3. Enable/disable the virtual router (necessary)
4. Configure VRRPv3 assistant parameters (optional)
   (1) Configure VRRPv3 preempt mode
   (2) Configure VRRPv3 priority
   (3) Configure the VRRPv3 advertisement interval
   (4) Configure the monitor interface of VRRPv3

1. Create/delete the virtual router

Command	Explanation
Global Configuration Mode	
router ipv6 vrrp <*vrid*> **no router ipv6 vrrp <*vrid*>**	Create/delete the virtual router.

2. Configure the virtual IPv6 address and interface of VRRPv3

Command	Explanation
VRRPv3 Protocol Mode	
virtual-ipv6 <*ipv6-address*> Interface {Vlan <*ID*> | *IFNAME* } **no virtual-ipv6 interface**	Configure the virtual IPv6 address and interface of VRRPv3, the no operation of this command will delete the virtual IPv6 address and interface.

3. Enable/disable the virtual router

Command	Explanation
VRRPv3 Protocol Mode	
enable	Enable the virtual router.
disable	Disable the virtual router.

4. Configure VRRPv3 assistant parameters

(1) Configure VRRPv3 preempt mode

Command	Explanation
VRRPv3 Protocol Mode	
preempt-mode {true| false}	Configure VRRPv3 preempt mode.

(2) Configure VRRPv3 priority

Command	Explanation
VRRPv3 Protocol Mode	
priority < *priority* >	Configure VRRPv3 priority.

(3) Configure the VRRPv3 advertisement interval

Command	Explanation
VRRPv3 Protocol Mode	
advertisement-interval <time>	Configure the VRRPv3 advertisement interval (in cent seconds).

(4) Configure the monitor interface of VRRPv3

Command	Explanation
VRRPv3 Protocol Mode	
circuit-failover {vlan <*ID*>| *IFNAME*} <*value_reduced*> **no circuit-failover**	Configure the monitor interface of VRRPv3, the no operation of this command will delete the monitor interface.

2.3 VRRPv3 Typical Examples

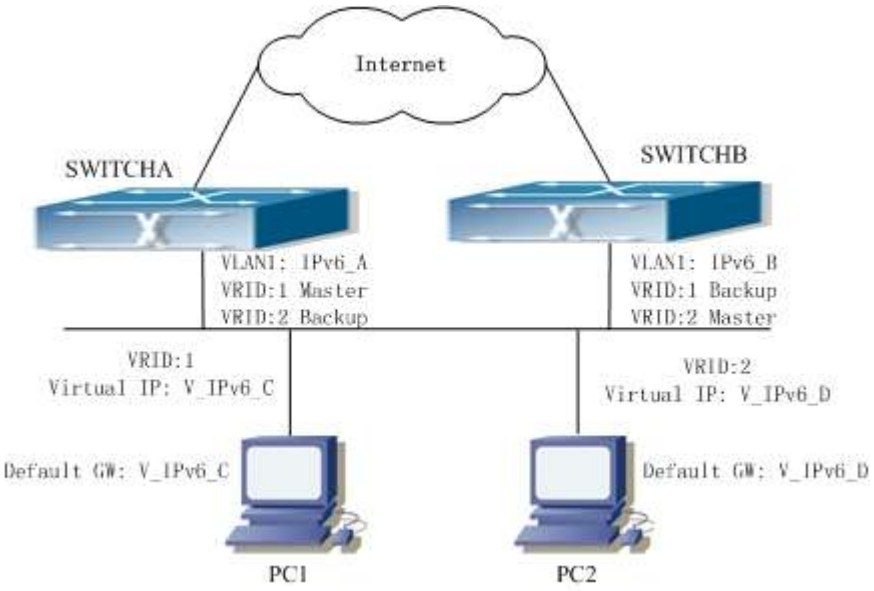

Fig 2-2 VRRPv3 Typical Network Topology

As shown in graph, switch A and switch B are backups to each other, switch A is the master of backup group 1 and a backup of backup group 2. Switch B is the master of backup group 2 and a Backup of backup group 1. The IPv6 addresses of switch A and switch B are “IPv6_A” and “IPv6_ B” respectively (it is recommended that IPv6_A and IPv6_B are in the same segment), the virtual IPv6 address of backup group 1 and backup group are “V_IPv6_C” and “V_IPV6_D” respectively, and the default IPv6 gateway address are configured as “V_IPv6_C” and “V_IPv6_D” respectively (in reality, the IPv6 gateway address of hosts are usually learnt automatically via router advertisements, thus, the IPv6 next hop of the hosts will have some randomness). Doing this will not only implement router backup but also the flow sharing function in the LAN.

The configuration of SwitchA:

SwitchA (config)#interface vlan 1
SwitchA (config)#router ipv6 vrrp 1
SwitchA (config-router)#virtual-ipv6 fe80::2 interface vlan 1
SwitchA (config-router)#priority 150
SwitchA (config-router)#enable
SwitchA (config)#router ipv6 vrrp 2
SwitchA (config-router)#virtual-ipv6 fe80::3 interface vlan 1
SwitchA (config-router)#enable

The configuration of SwitchB:

```
SwitchB (config)# interface vlan 1
SwitchB (config)# router ipv6 vrrp 2
SwitchB (config-router)# virtual-ipv6 fe80::3 interface vlan 1
SwitchB (config-router)# priority 150
SwitchB (config-router)# enable
SwitchB (config)# router ipv6 vrrp 1
SwitchB (config-router)# virtual-ipv6 fe80::2 interface vlan 1
SwitchB (config-router)# enable
```

2.4 VRRPv3 Troubleshooting

When configuring and using VRRPv3 protocol, it might operate abnormally because of incorrect physical connections and configuration. So, users should pay attention to the following points:

- First, the physical connections should be correct;
- Next, the interface and link protocol are UP (use **show ipv6 interface** command);
- And then, make sure that IPv6 forwarding function is enabled (use **ipv6 enable** command);
- Besides, make sure that VRRPv3 protocol is enable on the interface;
- Check whether the time of timer in different routers (or layer-three Ethernet switch) within the same backup group is the same;
- Check whether the virtual IPv6 addresses in the same backup group is the same.

Chapter 3 MRPP Configuration

3.1 Introduction to MRPP

MRPP (Multi-layer Ring Protection Protocol), is a link layer protocol applied on Ethernet loop protection. It can avoid broadcast storm caused by data loop on Ethernet ring, and restore communication among every node on ring network when the Ethernet ring has a break link. MRPP is the expansion of EAPS (Ethernet link automatic protection protocol).

MRPP protocol is similar to STP protocol on function, MRPP has below characters, compare to STP protocol:

<1> MRPP specifically uses to Ethernet ring topology

<2> fast convergence, less than 1 s. ideally it can reach 100-50 ms.

3.1.1 Conception Introduction

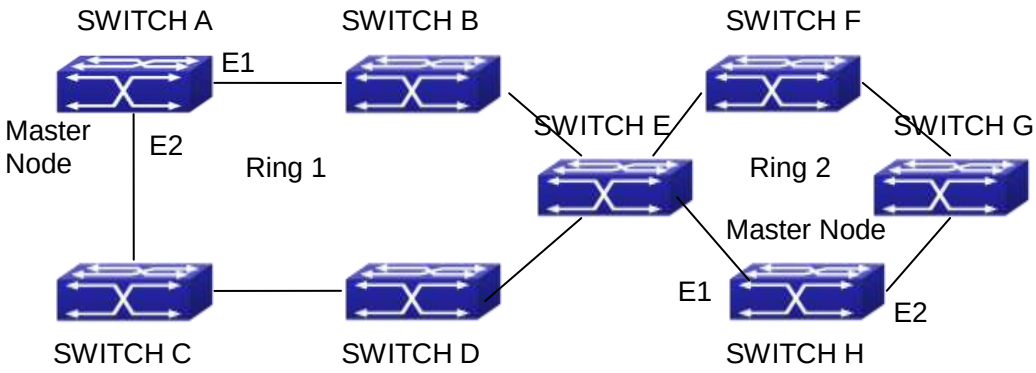

Fig 3-1 MRPP Sketch Map

1. Control VLAN

Control VLAN is a virtual VLAN, only used to identify MRPP protocol packet transferred in the link. To avoid confusion with other configured VLAN, avoids configuring control VLAN ID to be the same with other configured VLAN ID. The different MRPP ring should configure the different control VLAN ID.

2. Ethernet Ring (MRPP Ring)

Ring linked Ethernet network topology.

Each MRPP ring has two states.

Health state: The whole ring net work physical link is connected.

Break state: one or a few physical link break in ring network

3. nodes

Each switch is named after a node on Ethernet. The node has some types:

Primary node: each ring has a primary node, it is main node to detect and defend.

Transfer node: except for primary node, other nodes are transfer nodes on each ring. The node role is determined by user configuration. As shown Fig 3-1, Switch A is primary node of Ring 1, Switch B. Switch C; Switch D and Switch E are transfer nodes of Ring 1.

4. Primary port and secondary port

The primary node and transfer node have two ports connecting to Ethernet separately, one is primary port, and another is secondary port. The role of port is determined by user configuration.

Primary port and secondary port of primary node.

The primary port of primary node is used to send ring health examine packet (hello), the secondary port is used to receive Hello packet sending from primary node. When the Ethernet is in health state, the secondary port of primary node blocks other data in logical and only MRPP packet can pass. When the Ethernet is in break state, the secondary port of primary node releases block state, and forwards data packets.

There are no difference on function between Primary port and secondary port of transfer node.

The role of port is determined by user configuration. As shown Fig 3-1, Switch A E1 is primary port, E2 is secondary port.

5. Timer

The two timers are used when the primary node sends and receives MRPP protocol packet: Hello timer and Fail Timer.

Hello timer: define timer of time interval of health examine packet sending by primary node primary port.

Fail timer: define timer of overtime interval of health examine packet receiving by primary node primary port. The value of Fail timer must be more than or equal to the 3 times of value of Hello timer.

3.1.2 MRPP Protocol Packet Types

Packet Type	Explanation

Hello packet (Health examine packet) Hello	The primary port of primary node evokes to detect ring, if the secondary port of primary node can receive Hello packet in configured overtime, so the ring is normal.
LINK-DOWN (link Down event packet)	After transfer node detects Down event on port, immediately sends LINK-DOWN packet to primary node, and inform primary node ring to fail.
LINK-DOWN-FLUSH_FDB packet	After primary node detects ring failure or receives LINK-DOWN packet, open blocked secondary port, and then uses two ports to send the packet, to inform each transfer node to refresh own MAC address.
LINK-UP-FLUSH_FDB packet	After primary detects ring failure to restore normal, and uses packet from primary port, and informs each transfer node to refresh own MAC address.

3.1.3 MRPP Protocol Operation System

1. Link Down Alarm System

When transfer node finds themselves belonging to MRPP ring port Down, it sends link Down packet to primary node immediately. The primary node receives link down packet and immediately releases block state of secondary port, and sends LINK-DOWN-FLUSH-FDB packet to inform all of transfer nodes, refreshing own MAC address forward list.

2. Poll System

The primary port of primary node sends Hello packet to its neighbors timely according to configured Hello-timer.

If the ring is health, the secondary port of primary node receives health detect packet, and the primary node keeps secondary port.

If the ring is break, the secondary port of primary node can't receive health detect packet when timer is over time. The primary releases the secondary port block state, and sends LINK-DOWN-FLUSH_FDB packet to inform all of transfer nodes, to refresh own MAC address forward list.

3. Ring Restore

After the primary node occur ring fail, if the secondary port receives Hello packet sending from primary node, the ring has been restored, at the same time the primary node

block its secondary port, and sends its neighbor LINK-UP-Flush-FDB packet.

After MRPP ring port refresh UP on transfer node, the primary node maybe find ring restore after a while. For the normal data VLAN, the network maybe forms a temporary ring and creates broadcast storm. To avoid temporary ring, transfer node finds it to connect to ring network port to refresh UP, immediately block temporarily (only permit control VLAN packet pass), after only receiving LINK-UP-FLUSH-FDB packet from primary node, and releases the port block state.

3.2 MRPP Configuration Task List

1) Globally enable MRPP
2) Configure MRPP ring
3) Configure the query time of MRPP
4) Configure the compatible mode
5) Display and debug MRPP relevant information

1) Globally enable MRPP

Command	Explanation
Global Mode	
mrpp enable **no mrpp enable**	Globally enable and disable MRPP.

2) Configure MRPP ring

Command	Explanation
Global Mode	
mrpp ring <*ring-id*> **no mrpp ring <*ring-id*>**	Create MRPP ring. The “no” command deletes MRPP ring and its configuration.
MRPP ring mode	
control-vlan <*vid*> **no control-vlan**	Configure control VLAN ID, format “no” deletes configured control VLAN ID.
node-mode {master | transit}	Configure node type of MRPP ring (primary node or secondary node).
hello-timer < *timer*> **no hello-timer**	Configure Hello packet timer sending from primary node of MRPP ring, format “no” restores default timer value.

fail-timer <*timer*> **no fail-timer**	Configure Hello packet overtime timer sending from primary node of MRPP ring, format "no" restores default timer value.
enable **no enable**	Enable MRPP ring, format "no" disables enabled MRPP ring.
Port mode	
mrpp ring <*ring-id*> primary-port **no mrpp ring <*ring-id*> primary-port**	Specify primary port of MRPP ring.
mrpp ring <*ring-id*> secondary-port **no mrpp ring <*ring-id*> secondary-port**	Specify secondary port of MRPP ring.

3) Configure the query time of MRPP

Command	Explanation
Global Mode	
mrpp poll-time <20-2000>	Configure the query interval of MRPP.

4) Configure the compatible mode

Command	Explanation
Global Mode	
mrpp errp compatible **no mrpp errp compatible**	Enable the compatible mode for ERRP, the no command disables the compatible mode.
mrpp eaps compatible **no mrpp eaps compatible**	Enable the compatible mode for EAPS, the no command disables the compatible mode.
errp domain <*domain-id*> **no errp domain <*domain-id*>**	Create ERRP domain, the no command deletes the configured ERRP domain.

5) Display and debug MRPP relevant information

Command	Explanation
Admin Mode	
debug mrpp **no debug mrpp**	Disable MRPP module debug information, format "no" disable MRPP debug information output.
show mrpp {<*ring-id*>}	Display MRPP ring configuration information.
show mrpp statistics {<*ring-id*>}	Display receiving data packet statistic information of MRPP ring.

clear mrpp statistics {<*ring-id*>}	Clear receiving data packet statistic information of MRPP ring.

3.3 MRPP Typical Scenario

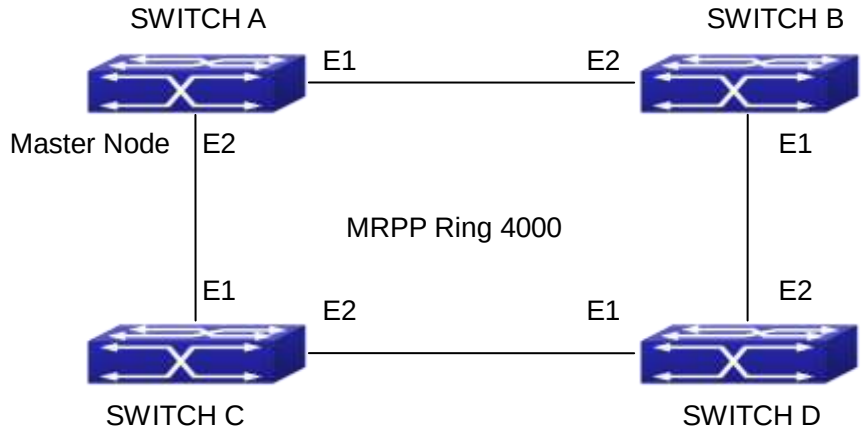

Fig 3-2 MRPP typical configuration scenario

The above topology often occurs on using MRPP protocol. The multi switch constitutes a single MRPP ring, all of the switches only are configured an MRPP ring 4000, thereby constitutes a single MRPP ring.

In above configuration, SWITCH A configuration is primary node of MRPP ring 4000, and configures E1/0/1 to primary port, E1/0/2 to secondary port. Other switches are secondary nodes of MRPP ring, configures primary port and secondary port separately.

To avoid ring, it should temporarily disable one of the ports of primary node, when it enables each MRPP ring in the whole MRPP ring; and after all of the nodes are configured, open the port.

When disable MRPP ring, it needs to insure the MRPP ring doesn't have ring.

SWITCH A configuration Task Sequence:

Switch(Config)#mrpp enable

Switch(Config)#mrpp ring 4000

Switch(mrpp-ring-4000)#control-vlan 4000

Switch(mrpp-ring-4000)#fail-timer 18

Switch(mrpp-ring-4000)#hello-timer 5

Switch(mrpp-ring-4000)#node-mode master

Switch(mrpp-ring-4000)#enable

Switch(mrpp-ring-4000)#exit

Switch(Config)#interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port

Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#

SWITCH B configuration Task Sequence:
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#

SWITCH C configuration Task Sequence:
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#

SWITCH D configuration Task Sequence:
Switch(Config)#mrpp enable
Switch(Config)#mrpp ring 4000
Switch(mrpp-ring-4000)#control-vlan 4000
Switch(mrpp-ring-4000)#enable
Switch(mrpp-ring-4000)#exit
Switch(Config)#interface ethernet 1/0/1

```
Switch(config-If-Ethernet1/0/1)#mrpp ring 4000 primary-port
Switch(config-If-Ethernet1/0/1)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#mrpp ring 4000 secondary-port
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#
```

3.4 MRPP Troubleshooting

The normal operation of MRPP protocol depends on normal configuration of each switch on MRPP ring, otherwise it is very possible to form ring and broadcast storm:

- Configuring MRPP ring, you'd better disconnected the ring, and wait for each switch configuration, then open the ring.
- When the MRPP ring of enabled switch is disabled on MRPP ring, it ensures the ring of the MRPP ring has been disconnected.
- When there is broadcast storm on MRPP ring, it disconnects the ring firstly, and ensures if each switch MRPP ring configuration on the ring is correct or not; if correct, restores the ring, and then observes the ring is normal or not.
- The convergence time of MRPP ring net is relative to the response mode of up/down. If use poll mode, the convergence time as hundreds of milliseconds in simple ring net, if use interrupt mode, the convergence time within 50 milliseconds.
- Generally, the port is configured as poll mode, interrupt mode is only applied to better performance environment, but the security of poll mode is better than interrupt mode, port-scan-mode {interrupt | poll} command can be consulted.
- In normal configuration, it still forms ring broadcast storm or ring block, please open debug function of primary node MRPP, and used show MRPP statistics command to observe states of primary node and transfer node and statistics information is normal or not, and then sends results to our Technology Service Center.

Chapter 4 ULPP Configuration

4.1 Introduction to ULPP

Each ULPP group has two uplink ports, they are master port and slave port. The port may be a physical port or a port channel. The member ports of ULPP group have three states: Forwarding, Standby, Down. Normally, only one port at the forwarding state, the other port is blocked at the Standby state. When the master port has the link problem, the master port becomes down state, and the slave port is siwthed to forwarding state.

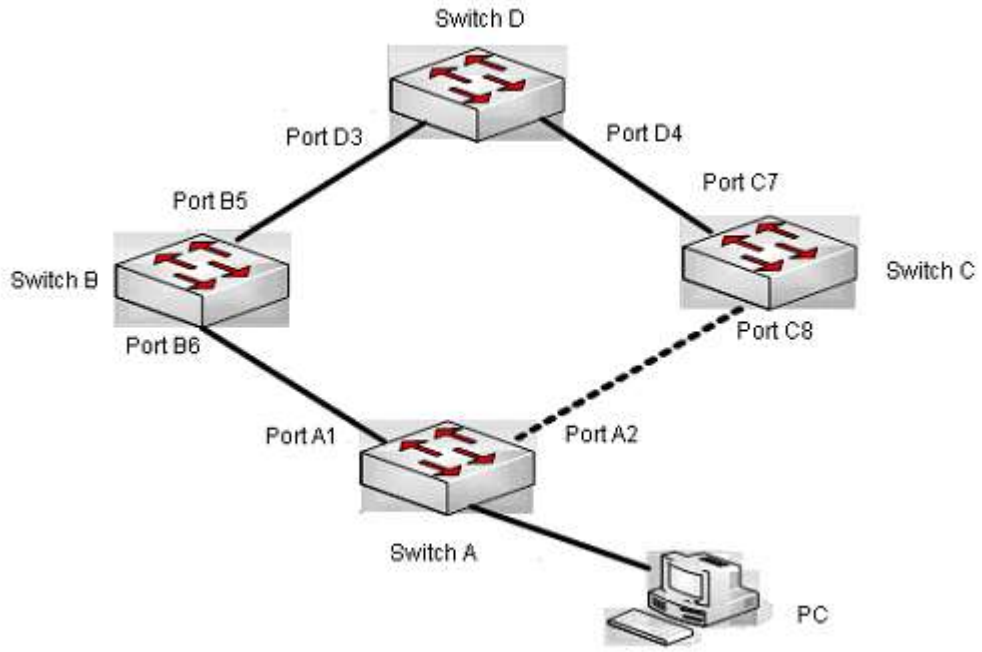

Fig 4-1 the using scene of ULPP

The above figure uses the double-uplink network, this is the typical application scene of ULPP. SwitchA goes up to SwitchD through SwitchB and SwitchC, port A1 and port A2 are the uplink ports. SwitchA configures ULPP, thereinto port A1 is set as the master port, port A2 is set as the slave port. When port A1 at forwarding state has the problem, switch the uplink at once, port A2 turns into forwarding state. After this, when recovering the master port, if the preemption mode is not configured, port A2 keeps the Forwarding state, port A1 turns into the Standby state.

After the preemption mode is enabled, so as to the master port preempts the slave port when it recovered from the problem. For avoiding the frequent uplink switch caused by the abnormity problem, the preemption delay mechanism is imported, and it needs to

wait for some times before the master port preempt the slave port. For keeping the continuance of the flows, the master port does not process to preempt by default, but turns into the Standby state.

When configuring ULPP, it needs to specify the VLAN which is protected by this ULPP group through the method of MSTP instances, and ULPP does not provide the protection to other VLANs.

When the uplink switch is happennig, the primary forwarding entries of the device will not be applied to new topology in the network. In the figure, SwitchA configures ULPP, the portA1 as the master port at forwarding state, here the MAC address of PC is learned by Switch D from portD3. After this, portA1 has the problem, the traffic is switched to portA2 to be forwarded. If there is the data sent to PC by SwitchD, still the data will be forwarded from portD3, and will be losed. Therefore, when switching the uplink, the device of configuring ULPP needs to send the flush packets through the port which is switched to Forwarding state, and update MAC address tables and ARP tables of other devices in the network. ULPP respectively uses two kinds of flush packets to update the entries: the updated packets of MAC address and the deleted packets of ARP.

For making use of the bandwidth resource enough, ULPP can implement VLAN load balance through the configuration. As the picture illustrated, SwitchA configures two ULPP groups: portA1 is the master port and portA2 is the slave port in group1, portA2 is the master port and portA1 is the slave port in group2, the VLANs are protected by group1 and group2, they are 1-100 and 101-200. Here both portA1 and portA2 at the forwarding state, the master port and the slave port mutually backup, and respectively forward the packets of the different VLAN ranges. When portA1 has the problem, the traffic of VLAN 1-200 are forwarded by portA2. After this, when portA1 is recovering the normal state, portA2 forwards the data of VLAN 101-200 sequentially, but the data of VLAN 1-100 is switched to portA1 to forward.

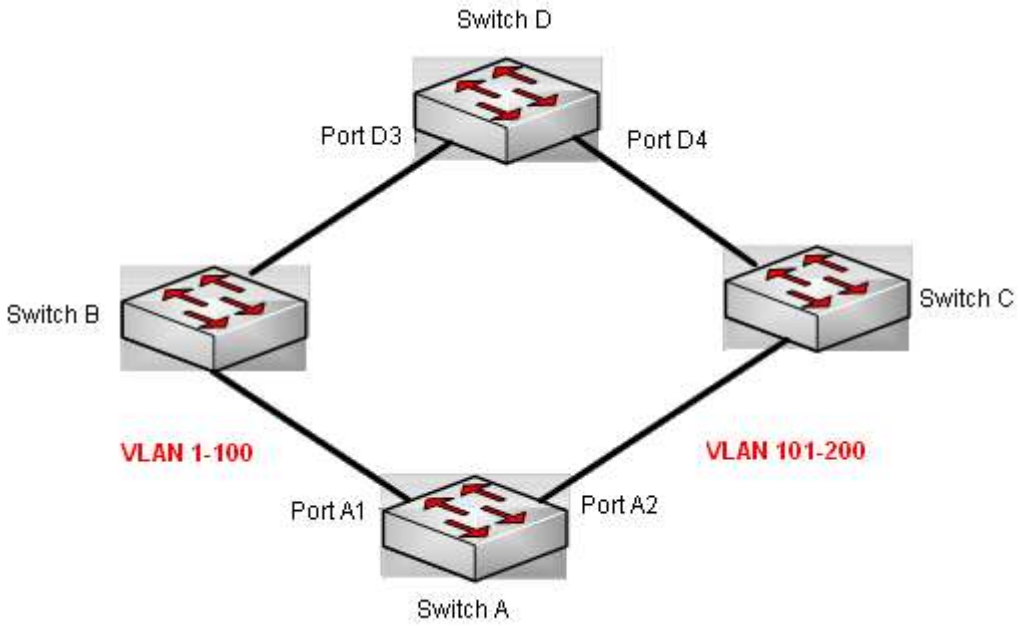

Fig 4-2 VLAN load balance

4.2 ULPP Configuration Task List

1. Create ULPP group globally
2. Configure ULPP group
3. Show and debug the relating information of ULPP

1. Create ULPP group globally

Command	Expalnation
Global mode	
ulpp group <*integer*> **no ulpp group <*integer*>**	Configure and delete ULPP group globally.

2. Configure ULPP group

Command	Explanation
ULPP group configuration mode	
preemption mode **no preemption mode**	Configure the preemption mode of ULPP group. The no operation deletes the preemption mode.

preemption delay <*integer*> **no preemption delay**	Configure the preemption delay, the no operation restores the default value 30s.
control vlan <*integer*> **no control vlan**	Configure the sending control VLAN, no operation restores the default value 1.
protect vlan-reference-instance <*instance-list*> **no protect vlan-reference-instance <*instance-list*>**	Configure the protection VLANs, the no operation deletes the protection VLANs.
flush enable mac **flush disable mac**	Enable or disable sending the flush packets which update MAC address.
flush enable arp **flush disable arp**	Enable or disable sending the flush packets which delete ARP.
flush enable mac-vlan **flush disable mac-vlan**	Enable or disable sending the flush packets of deleting the dynamic unicast mac according to vlan.
description <*string*> **no description**	Configure or delete ULPP group description.
Port mode	
ulpp control vlan <*vlan-list*> **no ulpp control vlan <*vlan-list*>**	Configure the receiving control VLANs, no operation restores the default value 1.
ulpp flush enable mac **ulpp flush disable mac**	Enable or disable receiving the flush packets which update the MAC address.
ulpp flush enable arp **ulpp flush disable arp**	Enable or disable receiving the flush packets which delete ARP.
ulpp flush enable mac-vlan **ulpp flush disable mac-vlan**	Enable or disable receiving the flush packets of mac-vlan type.
ulpp group <*integer*> master **no ulpp group <*integer*> master**	Configure or delete the master port of ULPP group.
ulpp group <*integer*> slave **no ulpp group <*integer*> slave**	Configure or delete the slave port of ULPP group.

3. Show and debug the relating information of ULPP

Command	Explanation

Admin mode	
show ulpp group [group-id]	Show the configuration information of the configured ULPP group.
show ulpp flush counter interface {ethernet <IFNAME> | <IFNAME>}	Show the statistic information of the flush packets.
show ulpp flush-receive-port	Show flush type and control VLAN received by the port.
clear ulpp flush counter interface <*name*>	Clear the statistic information of the flush packets.
debug ulpp flush {send | receive} interface <*name*> **no debug ulpp flush {send | receive} interface <*name*>**	Show the information of the receiving and sending flush packets, the no operation disables the shown information.
debug ulpp flush content interface <*name*> **no debug ulpp flush content interface <*name*>**	Show the contents of the received flush packets, the no operation disables the showing.
debug ulpp error **no debug ulpp error**	Show the error information of ULPP, the no operation disables the showing.
debug ulpp event **no debug ulpp event**	Show the event information of ULPP, the no operation disables the showing.

4.3 ULPP Typical Examples

4.3.1 ULPP Typical Example1

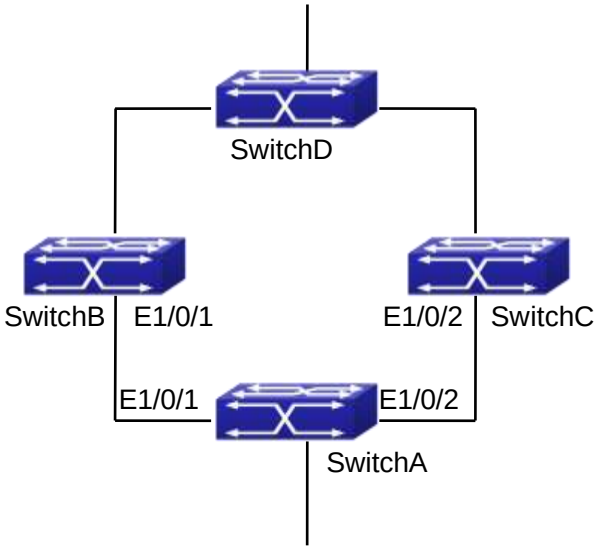

Fig 4-3 ULPP typical example1

The above topology is the typical application environment of ULPP protocol.

SwitchA has two uplinks, they are SwitchB and SwitchC. When any protocols are not enabled, this topology forms a ring. For avoiding the loopback, SwitchA can configure ULPP protocol, the master port and the slave port of ULPP group. When both master port and slave port are up, the slave port will be set as standby state and will not forward the data packets. When the master port is down, the slave port will be set as forwarding state and switch to the uplink. SwitchB and SwitchC can enable the command that receives the flush packets, it is used to associate with ULPP protocol running of SwitchA to switch the uplink immediately and reduce the switch delay.

When configuring ULPP protocol of SwitchA, first, create a ULPP group and configure the protection VLAN of this group as vlan10, then configure interface Ethernet 1/0/1 as the master port, interface Ethernet 1/0/2 as the slave port, the control VLAN as 10. SwitchB and SwitchC configure the flush packets that receive ULPP.

SwitchA configuration task list:

```
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1; 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 10
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#control vlan 10
```

Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit

SwitchB configuration task list:
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/1
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp
Switch(config-If-Ethernet1/0/1)# ulpp control vlan 10

SwitchC configuration task list:
Switch(Config)#vlan 10
Switch(Config-vlan10)#switchport interface ethernet 1/0/2
Switch(Config-vlan10)#exit
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)# ulpp flush enable arp
Switch(config-If-Ethernet1/0/2)# ulpp control vlan 10

4.3.2 ULPP Typical Example2

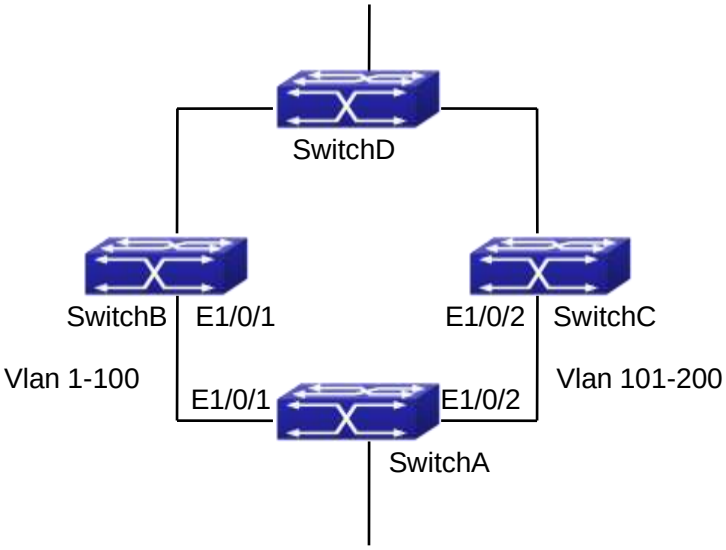

Fig 4-4 ULPP typical example2

ULPP can implement the VLAN-based load balance. As the picture illustrated, SwitchA configures two ULPP groups: port E1/0/1 is the master port and port 1/0/2 is the slave port in group1, port 1/0/2 is the master port and port 1/0/1 is the slave port in group2. The VLANs protected by group1 are 1-100 and by group2 are 101-200. Here both port E1/0/1 and port E1/0/2 at the forwarding state, the master port and the slave port mutually backup, respectively forward the packets of different VLAN ranges. When port E1/0/1 has the problem, the traffic of VLAN 1-200 are forwarded by port E1/0/2. When port E1/0/1 is recovering the normal state, still port E1/0/2 forwards the data of VLAN 101-200, the data of VLAN 1-100 are switched to port E1/0/1 to forward.

SwitchA configuration task list:

Switch(Config)#spanning-tree mst configuration
Switch(Config-Mstp-Region)#instance 1 vlan 1-100
Switch(Config-Mstp-Region)#instance 2 vlan 101-200
Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-1)#exit
Switch(Config)#ulpp group 2
Switch(ulpp-group-2)#protect vlan-reference-instance 2
Switch(ulpp-group-1)#preemption mode
Switch(ulpp-group-2)#exit
Switch(Config)#interface ethernet 1/0/1

Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)#ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#ulpp group 2 slave
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#switchport mode trunk
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)# ulpp group 2 master
Switch(config-If-Ethernet1/0/2)#exit

SwitchB configuration task list:
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#switchport mode trunk
Switch(config-If-Ethernet1/0/1)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/1)# ulpp flush enable arp

SwitchC configuration task list:
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# switchport mode trunk
Switch(config-If-Ethernet1/0/2)# ulpp flush enable mac
Switch(config-If-Ethernet1/0/2)# ulpp flush enable arp

4.4 ULPP Troubleshooting

- At present, configuration of more than 2 multi-uplinks is allowed, but it may cause loopback, so is not recommended.
- With the normal configuration, if the broadcast storm happen or the communication along the ring is broken, please enable the debug of ULPP, copy the debug information of 3 minutes and the configuration information, send them to our technical service center.

Chapter 5 ULSM Configuration

5.1 Introduction to ULSM

ULSM (Uplink State Monitor) is used to process the port state synchronization. Each ULSM group is made up of the uplink port and the downlink port, both the uplink port and the downlink port may be multiple. The port may be a physical port or a port channel, but it can not be a member port of a port channel, and each port only belongs to one ULSM group.

The uplink port is the monitored port of ULSM group. When all uplink ports are down or there is no uplink port in ULSM group, ULSM group state is down. ULSM group state is up as long as one uplink port is up.

The downlink port is the controlled port, its state changes along with Up/Down of ULSM group and is always the same with ULSM group state.

ULSM associates with ULPP to enable the downstream device to apperceive the link problem of the upstream device and process correctly. As the picture illustrated, SwitchA configures ULPP, here the traffic is forwarded by port A1. If the link between SwitchB and Switch D has the problem, SwitchA can not apperceive the problem of the upstream link and sequentially forward the traffic from port A1, cause traffic losing.

Configuring ULSM on SwitchB can solve the above problems. The steps are: set port B5 as the uplink port of ULSM group, port B6 as the downlink port. When the link between SwitchB and SwitchD has the problem, both the downlink port B6 and the state of ULSM group are down. It causes Switch A on which ULPP is configured to process uplink switchover and avoid the data dropped.

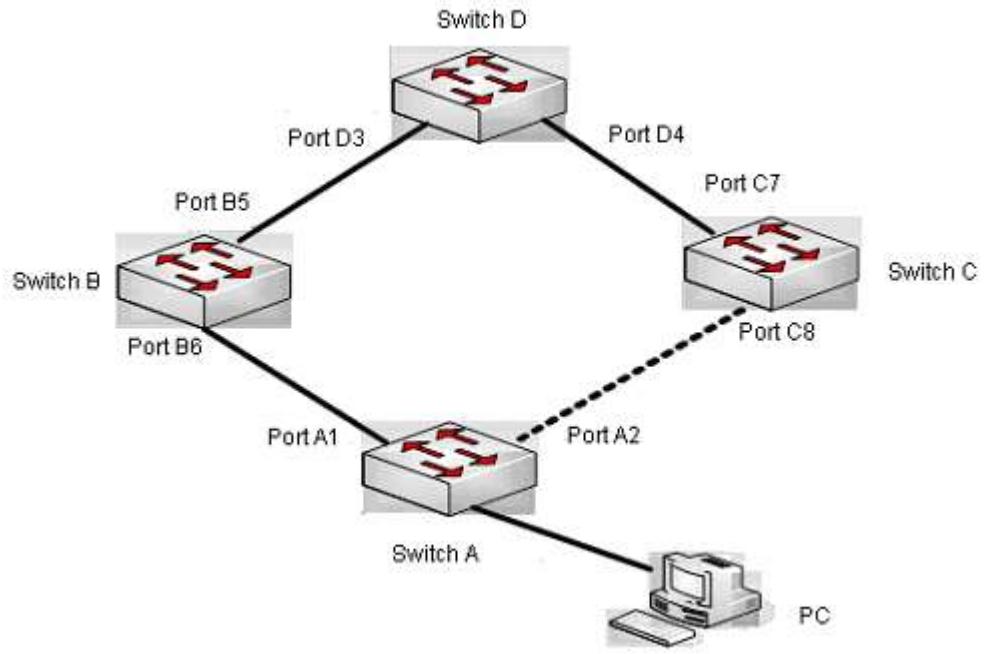

Fig 5-1 ULSM using scene

5.2 ULSM Configuration Task List

1. Create ULSM group globally
2. Configure ULSM group
3. Show and debug the relating information of ULSM

1. Create ULSM group globally

Command	explanation
Global mode	
ulsm group <*group-id*> **no ulsm group <*group-id*>**	Configure and delete ULSM group globally.

2. Configure ULSM group

Command	explanation
Port mode	
ulsm group <*group-id*> {uplink | downlink} **no ulsm group <*group-id*> {uplink | downlink}**	Configure the uplink/downlink port of ULSM group, the no command deletes the uplink/downlink port.

3. Show and debug the relating information of ULSM

Command	Explanation
Admin mode	
show ulsm group [group-id]	Show the configuration information of ULSM group.
debug ulsm event **no debug ulsm event**	Show the event information of ULSM, the no operation disables the shown information.

5.3 ULSM Typical Example

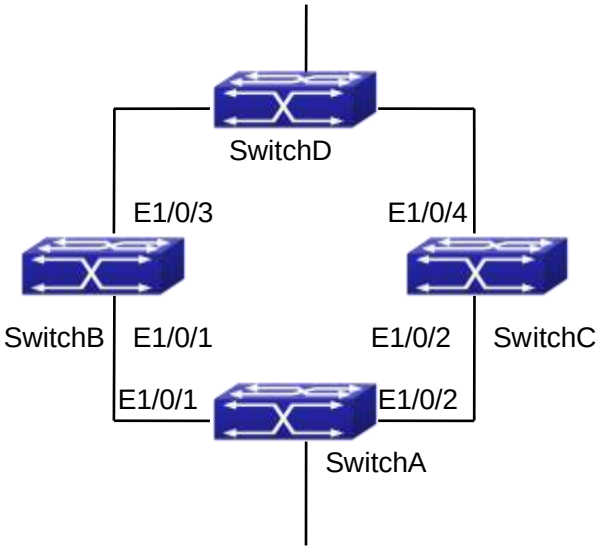

Fig 5-2 ULSM typical example

The above topology is the typical application environment which is used by ULSM and ULPP protocol.

ULSM is used to process the port state synchronization, its independent running is useless, so it usually associates with ULPP protocol to use. In the topology, SwitchA enables ULPP protocol, it is used to switch the uplink. SwitchB and SwitchC enable ULSM protocol to monitor whether the uplink is down. If it is down, then ULSM will execute the down operation for the downlink port to shutdown it, so ULPP protocol of Swtich A executes the relative operation of the uplink switchover.

SwitchA configuration task list:

Switch(Config)#spanning-tree mst configuration

Switch(Config-Mstp-Region)#instance 1 vlan 1

Switch(Config-Mstp-Region)#exit
Switch(Config)#ulpp group 1
Switch(ulpp-group-1)#protect vlan-reference-instance 1
Switch(ulpp-group-1)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)# ulpp group 1 master
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface Ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)# ulpp group 1 slave
Switch(config-If-Ethernet1/0/2)#exit

SwitchB configuration task list:
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/1
Switch(config-If-Ethernet1/0/1)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/1)#exit
Switch(Config)#interface ethernet 1/0/3
Switch(config-If-Ethernet1/0/3)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/3)#exit

SwitchC configuration task list:
Switch(Config)#ulsm group 1
Switch(Config)#interface ethernet 1/0/2
Switch(config-If-Ethernet1/0/2)#ulsm group 1 downlink
Switch(config-If-Ethernet1/0/2)#exit
Switch(Config)#interface ethernet 1/0/4
Switch(config-If-Ethernet1/0/4)#ulsm group 1 uplink
Switch(config-If-Ethernet1/0/4)#exit

5.4 ULSM Troubleshooting

☞ With the normal configuration, if the downlink port does not responds the down event of the uplink port, please enable the debug function of ULSM, copy the debug information of 3 minutes and the configuration information, and send them to our technical service center.