FiberstoreOS

Reliability Configuration Guide

Contents

List of Figures

1 Configuring BHM

1.1 Overview

BHM is a module which is used to monitor other PMs. When a monitored PM is uncontrolled, the BHM module will take measures, such as printing warning on screen, shutting all ports, or restarting the system, to help or remind users to recover the system.

The monitored PMs include RIP, RIPNG, OSPF, OSPF6, BGP, LDP, RSVP, PIM, PIM6, 802.1X, LACP MSTP, DHCP-RELAY, DHCP-RELAY6, RMON, OAM, ONM, SSH, SNMP, PTP, SSM. In addition, some system procedures are also monitored, including NSM, IMI, CHSM, HSRVD.

There are three activations of BHM, including “reload system”, “warning”, “shutdown port”.

1.2 Terminology

BHM: Beat heart monitor

1.3 Configuration

The follow example shows how to configure the bhm module.

Switch# configure terminal	Enter configuration mode
Switch(config)# sysmon enable	Enable sysmon
Switch(config)# heart-beat-monitor enable	Enable BHM
Switch(config)# heart-beat-monitor reactivate reload system	Config reactivation to “reload system”

1.4 Validation

The result of show heart-beat-monitor is

```
Switch1# show heart-beat-monitor
heart-beat-monitor enable.
heart-beat-monitor reactivation: restart system.
```

2 Configuring EFM OAM

This chapter contains a complete sample EFM OAM configuration. To see details on the commands used in this example, or to see the outputs of the validation commands, refer to the OAM Command Reference. To avoid repetition, some Common commands, like configure terminal, have not been listed under the commands used sections.

2.1 Overview

The main functions of Ethernet to the First Mile - Operation Administration and Maintenance (EFM-OAM) are link performance monitoring, fault detection, fault signaling and loopback signaling. OAM information is conveyed in Slow Protocol frames called OAM Protocol Data Units (OAMPDUs). OAMPDUs contain the appropriate control and status information used to monitor, test and troubleshoot OAM-enabled links.

2.2 References

IEEE 802.3ah (2004)

2.3 Configuring Enable EFM

2.3.1 Topology

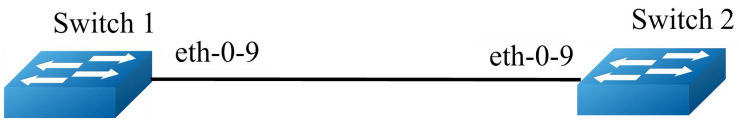


Figure 1-1 EFM Topology

2.3.2 Configuration

Bridge1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch1(config-if)# ethernet oam enable	Enable Ethernet OAM on eth-0-9
Switch1(config-if)# ethernet oam mode active	Configure Ethernet OAM mode as active (The default mode is passive)
Switch1(config-if)# ethernet oam link-monitor frame threshold high 10 window 50	Configure link event： link event will generate if the port get 10 error packet in 5 seconds
Switch1(config-if)# end	Exit the Interface mode

Bridge2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch2(config-if)# ethernet oam enable	Enable Ethernet OAM in eth-0-9
Switch2(config-if)# ethernet oam mode active	Configure Ethernet OAM mode as active. (The default mode is passive)
Switch2(config-if)# ethernet oam link-monitor frame threshold high 10 window 50	Configure link event： link event will generate if the port get 10 error packet in 5 seconds

Switch2(config-if)# end	Exit the Interface mode

The EFM Discovery Machine State should be “send any" in both machines. This is the expected normal operating state for OAM on fully-operational links.

The various states of OAM discovery state machine are defined below.

- **ACTIVE_SEND_LOCAL**: A DTE configured in Active mode sends Information OAMPDUs that only contain the Local Information TLV. This state is called ACTIVE_SEND_LOCAL. While in this state, the local DTE waits for Information OAMPDUs received from the remote DTE.
- **PASSIVE_WAIT:** DTE configured in Passive mode waits until receiving Information OAMPDUs with Local Information TLVs before sending any Information OAMPDUs with Local Information TLVs. This state is called PASSIVE_WAIT. By waiting until first receiving an Information OAMPDU with the Local Information TLV, a Passive DTE cannot complete the OAM Discovery process when connected to another Passive DTE.
- **SEND_LOCAL_REMOTE**: Once the local DTE has received an Information OAMPDU with the Local Information TLV from the remote DTE, the local DTE begins sending Information OAMPDUs that contain both the Local and Remote Information TLVs. This state is called SEND_LOCAL_REMOTE.
- **SEND_LOCAL_REMOTE_OK**: If the local OAM client deems the settings on both the local and remote DTEs are acceptable, it enters the SEND_LOCAL_REMOTE_OK state.
- **SEND_ANY**: Once an OAMPDU has been received indicating the remote device is satisfied with the respective settings, the local device enters the SEND_ANY state. This is the expected normal operating state for OAM on fully operational links.
- **FAULT**: If OAM is reset, disabled, or the link timer expires, the Discovery process returns to the FAULT state.

2.3.3 Validation

```
Switch1# show ethernet oam discovery interface eth-0-9
eth-0-9
Local client:
-------------
```

```
  Administrative configurations:
     Mode:                             active
     Unidirection:                     not supported
     Link monitor:                     supported(on)
     Remote Loopback:                  not supported
     MIB retrieval:                    not supported
     MTU Size    :                     1518
  Operational status:
     Port status:                      send any
     Loopback status:                  no loopback
     PDU revision:                     1

Remote client:
--------------
  MAC address: e6c2.47f6.7809
  PDU revision: 1
  Vendor(oui): e6 c2 47

  Administrative configurations:
     Mode:                             active
     Unidirection:                     not supported
     Link monitor:                     supported
     Remote Loopback:                  not supported
     MIB retrieval:                    not supported
     MTU Size    :                     1518
```

```
Switch2# show ethernet oam discovery interface eth-0-9
eth-0-9

Local client:
-------------
  Administrative configurations:
     Mode:                             active
     Unidirection:                     not supported
     Link monitor:                     supported(on)
     Remote Loopback:                  not supported
     MIB retrieval:                    not supported
     MTU Size    :                     1518
  Operational status:
     Port status:                      operational
     Loopback status:                  no loopback
     PDU revision:                     1

Remote client:
--------------
  MAC address: 409c.ba1a.5a09
  PDU revision: 1
  Vendor(oui): 40 9c ba

  Administrative configurations:
     Mode:                             active
     Unidirection:                     not supported
     Link monitor:                     supported
     Remote Loopback:                  not supported
```

```
MIB retrieval:                    not supported
MTU Size    :                     1518
```

2.4 Configuring Remote Loopback

OAM remote loopback can be used for fault localization and link performance testing. In addition, an implementation may analyze loopback frames within the OAM sublayer to determine additional information about the health of the link (i.e. determine which frames are being dropped due to link errors).

2.4.1 Topology

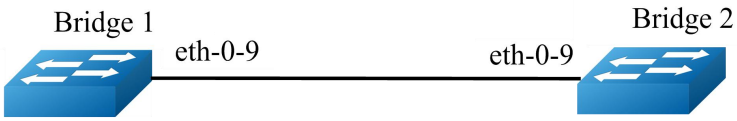


Figure 1-2 EFM Topology

2.4.2 Configuration

Bridge2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch2(config-if)# ethernet oam remote loopback supported	Enable Ethernet remote loopback on eth-0-9
Switch2(config-if)# end	Exit the Interface mode

Bridge1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch1(config-if)# ethernet oam remote loopback supported	Enable Ethernet remote loopback on eth-0-9

Switch1(config-if)# end	Exit the Interface mode
Switch1# ethernet oam remote-loopback start interface eth-0-9	Turn on remote-loopback on eth-0-9

2.4.3 Validation

An OAM entity can put its remote entity into loopback mode using a loopback control OAMPDU. In loopback mode, every frame received is transmitted back on that same port except for OAMPDUs. The periodic exchange of OAMPDUs must continue during loopback state to maintain the OAM session. Once we enable remote loopback in Bridge1, it sends out a loopback control OAMPDU with Enable remote loopback command. When Bridge2 receives it, it changes its parser state to Loopback and MUX state to discard and then sends out information OAMPDU with updated state information.

Bridge1

```
Switch1# show ethernet oam state-machine interface eth-0-9.
State Machine Details:
--------------------------------
Local OAM mode:                          Active
Local OAM enable:                         Enable
Local link status:                            OK
Local pdu status:                           ANY
Local Satisfied:                            True
Local Stable:                               True
Remote Satisfied valid:                     True
Remote Stable:                             True
Local Parser State:                         Discard
Local Multiplexer State:                     Forward
Remote Parser State:                        Loopback
Remote Multiplexer State:                   Discard
```

2.5 Configuring Link Monitoring Event

We can configure high and low threshold for link-monitoring features. We can also configure an error disable action if one of the high thresholds is exceeded.

2.5.1 Topology

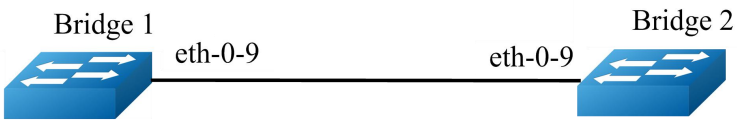


Figure 1-3 EFM Topology

2.5.2 Configuration

Bridge1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)#interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch1(config-if)# ethernet oam link-monitor supported	Enable the interface to support link monitoring. This is the default
Switch1(config-if)# ethernet oam link-monitor on	Start link monitoring
Switch1(config-if)# ethernet oam link-monitor frame threshold high 5000 low 200 window 500	Configure a high and low threshold for frame events. Specify the number of seconds to set a window period during which error frames are counted
Switch1(config-if)#ethernet oam link-monitor frame-seconds threshold high 600 low 200	Configure high and low thresholds for frame-seconds events
Switch1(config-if)#ethernet oam link-monitor high-threshold action error-disable-interface	Configure the error-disable-action that should take place on the interface when one of the high thresholds is exceeded
Switch1(config-if)# end	Exit the Interface mode

2.5.3 Validation

When link monitoring is ON and the number of errors (frame-errors, seconds-errors, or symbol period errors) exceeds the low threshold, a corresponding event notification PDU is sent. If the number of errors exceeds high threshold and a high threshold action (error-disable-interface) has been configured, the interface is disabled (shut down).

```
Switch1# show ethernet oam status interface eth-0-9
eth-0-9
General:
-------
   Mode:                                active
   PDU max rate:                        1 packets per second
   PDU min rate:                        1 packet per 1 second
   Link timeout:                        10 seconds
   High threshold action:               disable interface
   Link fault action:                   no action
   Dying gasp action:                   no action
   Critical event action:               no action
Link Monitoring:
----------------
     Status:                            supported(on)
     Frame Error:
        Window:                         500 x 100 milliseconds
        Low threshold:                  200 error frame(s)
        High threshold:                 5000 error frame(s)
        Last Window Frame Errors:       0 Frame(s)
        Total Frame Errors:             0 Frame(s)
        Total Frame Errors Events:      0 Events(s)
        Relative Timestamp of the Event:  0 x 100 milliseconds
     Frame Seconds Error:
        Window:                         1000 x 100 milliseconds
        Low threshold:                  200 error second(s)
        High threshold:                 600 error second(s)
        Last Window Frame Second Errors:  0 error second(s)
        Total Frame Second Errors:      0 error second(s)
        Total Frame Second Errors Events: 0 Events(s)
        Relative Timestamp of the Event:  0 x 100 milliseconds
```

2.6 Configuring Remote Failure Detection

An error-disable action can be configured to occur on an interface so that if any of the critical link events (link fault, dying gasp, etc.) occurs in the remote machine, the interface is shut down.

2.6.1 Topology

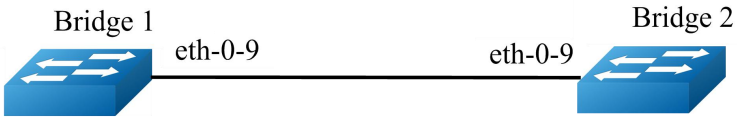


Figure 1-4 EFM Topology

2.6.2 Configuration

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch(config-if)# ethernet oam remote-failure critical-event dying-gasp link-fault action error-disable-interface	Configure the Ethernet OAM remote-failure action on eth-0-9. Configure the interface to shut down when any of the critical link events take place on the remote machine
Switch(config-if)# end	Exit the Interface mode

2.6.3 Validation

When a remote failure action (error-disable-interface) is configured in Bridge1 and when a critical link event(Link fault, dying gasp, or other critical event) occurs in Bridge2, the interface is disabled.

3 Configuring CFM

This chapter contains a complete sample Connectivity Fault Management (CFM) Protocol configuration. To see details on the commands used in this example, or to see the outputs of the validation commands, refer to the CFM Command Reference. To avoid repetition, some Common commands, like configure terminal, have not been listed under the Commands Used section.

3.1 Overview

Connectivity Fault Management provides the capability to detect, verify, isolate and notify connectivity failures on a Virtual Bridged LAN based on the protocol standard specified in IEEE 802.1ag. It provides for discovery and verification of paths through 802.1 bridges and LANs, and is part of the enhanced Operation, Administration and Management (OAM) features. CFM is designed to be transparent to the customer data transported by a network and to be capable of providing maximum fault coverage.

CFM uses standard Ethernet frames distinguished by EtherType. These CFM messages are supported:

- Continuity Check messages (CC)

  Multicast heartbeat messages exchanged periodically between MEPs that allow MEPs to discover other MEPs within a domain and allow MIPs to discover MEPs. It is used to detect loss of continuity (LOC) between any pair of MEPs.

- Loopback messages

Unicast frames transmitted by an MEP at administrator request to verify connectivity to a particular maintenance point, indicating if a destination is reachable. A loopback message is similar to an Internet Control Message Protocol (ICMP) ping message.

- Linktrace messages

  Multicast frames transmitted by an MEP at administrator request to track the path (hop-by-hop) to a destination MEP/MIP. Traceroute messages are similar in concept to UDP traceroute messages.

- Delay Measurement messages

  A MEP sends DMM with ETH-DM request information to its peer MEP and receives DMR with ETH-DM reply information from its peer MEP to carry out two-way frame delay and delay variation measurements.

  When a MEP receives 1DM frames, it will carry out one-way frame delay and delay variation measurements.

- Ethernet Locked Signal messages

  Ethernet Locked Signal function (ETH-LCK) is used to communicate the administrative locking of a server (sub) layer MEP and consequential interruption of data traffic forwarding towards the MEP expecting this traffic. It allows a MEP receiving frames with ETH-LCK information to differentiate between a defect condition and an administrative locking action at the server (sub) layer MEP.

- Ethernet client signal fail messages

  The Ethernet client signal fail function (ETH-CSF) is used by a MEP to propagate to a peer MEP the detection of a failure or defect event in an Ethernet client signal when the client itself does not support appropriate fault or defect detection or propagation mechanisms, such as ETH-CC or ETH-AIS. The ETH-CSF messages propagate in the direction from the Ethernet source-adaptation function detecting the failure or defect event to the Ethernet sink-adaptation function associated with the peer MEP. ETH-CSF is only applicable to point-to-point Ethernet transport applications.

- Ethernet Frame loss measurement message

  ETH-LM is used to collect counter values applicable for ingress and egress service frames where the counters maintain a count of transmitted and received data frames between a pair of MEPs.

  ETH-LM is performed by sending LMM with ETH-LM information to a peer MEP and similarly receiving LMR with ETH-LM information from the peer MEP.

3.2 References

IEEE 802.1ag/D8.1

3.3 Limitation

CFM is conflict with 802.1x and mirror destination on the same port. Therefore, CFM and these functions should not be configured on the same port.

3.4 Configure CC/LB/LT/AIS/DM

3.4.1 Topology

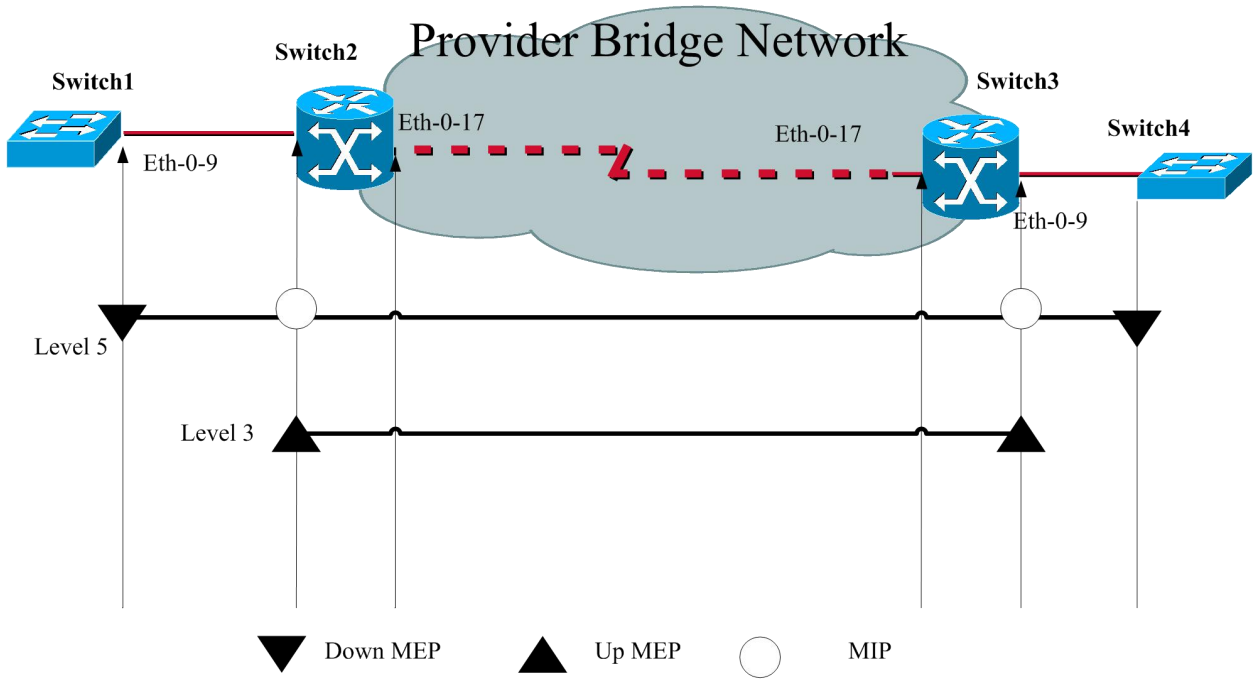


Figure 1-5 CFM Topology

3.4.2 Configurations

Switch 1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# vlan database	Enter the VLAN database
Switch1(config vlan)# vlan 30	Configure VLAN 30
Switch1(config vlan)# exit	Exit the VLAN database
Switch1(config)# ethernet cfm enable	Enable CFM globally
Switch1(config)# ethernet cfm mode y1731	Configure cfm mode
Switch1(config)# ethernet cfm domain cust level 5	Create a domain
Switch1(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch1(config-ether-cfm)# exit	Exit the CFM database
Switch1(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch1(config-if)# ethernet cfm mep down mpid 66 domain cust vlan 30 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 99 domain cust vlan 30 mac d036.4567.8009	Configure a remote maintenance end point (RMEP)
Switch1(config-if)# no shutdown	Bring up the interface
Switch1(config-if)# exit	Exit the Interface mode
Switch1(config)# ethernet cfm cc enable domain cust vlan 30	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch1(config)# ethernet cfm ais suppress alarm enable domain cust vlan 30	Suppress errors when ais packet is received and loc error
Switch1(config)# end	Exit the Configure mode

Switch 2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# vlan database	Enter the VLAN database
Switch2(config-vlan)# vlan 30	Configure VLAN 30
Switch2(config-vlan)# exit	Exit the VLAN database
Switch2(config)# ethernet cfm enable	Enable CFM globally
Switch2(config)# ethernet cfm mode y1731	Configure cfm mode
Switch2(config)# ethernet cfm domain cust level 5	Create a domain
Switch2(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch2(config-ether-cfm)# exit	Exit the CFM database
Switch2(config)# ethernet cfm domain provid level 3	Create a domain
Switch2(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch2(config-ether-cfm)# exit	Exit the CFM database
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch2(config-if)# ethernet cfm mip level 5 vlan 30	Configure a maintenance Intermediate point (MIP)
Switch2(config-if)# ethernet cfm mep up mpid 666 domain provid vlan 30 interval 1	Configure a maintenance end point (MEP)
Switch2(config-if)# ethernet cfm mep crosscheck mpid 999 domain provid vlan 30 mac 6a08.051e.bd09	Configure a remote maintenance end point (RMEP)
Switch2(config-if)# ethernet cfm ais status enable all domain provid vlan 30 level 5 multicast	Enable ais and ais parameters
Switch2(config-if)# ethernet cfm server-ais status enable level 5 interval 1	Configure ais server
Switch2(config-if)# no shutdown	Bring up the interface
Switch2(config-if)# exit	Exit the Interface mode

Switch2(config)# interface eth-0-17	Specify the interface (eth-0-17)to be configured and enter the Interface mode
Switch2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch2(config-if)# no shutdown	Bring up the interface
Switch2(config-if)# exit	Exit the Interface mode
Switch2(config)# ethernet cfm cc enable domain provid vlan 30	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch2(config)# end	Exit the Configure mode

Switch 3

Switch3# configure terminal	Enter the Configure mode
Switch3(config)# vlan database	Enter the VLAN database
Switch3(config-vlan)# vlan 30	Configure VLAN 30
Switch3(config-vlan)# exit	Exit the VLAN database
Switch3(config)# ethernet cfm enable	Enable CFM globally
Switch3(config)# ethernet cfm mode y1731	Configure cfm mode
Switch3(config)# ethernet cfm domain cust level 5	Create a domain
Switch3(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch3(config-ether-cfm)# exit	Exit the CFM database
Switch3(config)# ethernet cfm domain provid level 3	Create a domain
Switch3(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch3(config-ether-cfm)# exit	Exit the CFM database
Switch3(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode

Switch3(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch3(config-if)# ethernet cfm mip level 5 vlan 30	Configure a maintenance Intermediate point (MIP)
Switch3(config-if)# ethernet cfm mep up mpid 999 domain provid vlan 30 interval 1	Configure a maintenance end point (MEP)
Switch3(config-if)# ethernet cfm mep crosscheck mpid 666 domain provid vlan 30 mac 0e1d.a7d7.fb09	Configure a remote maintenance end point (RMEP)
Switch3(config-if)# no shutdown	Bring up the interface
Switch3(config-if)# exit	Exit the Interface mode
Switch3(config)# interface eth-0-17	Specify the interface (eth-0-17)to be configured and enter the Interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch3(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch3(config-if)# no shutdown	Bring up the interface
Switch3(config-if)# exit	Exit the Interface mode
Switch3(config)# ethernet cfm cc enable domain provid vlan 30	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch3(config)# end	Exit the Configure mode

Switch 4

Switch4# configure terminal	Enter the Configure mode
Switch4(config)# vlan database	Enter the VLAN database
Switch4(config vlan)# vlan 30	Configure VLAN 30
Switch4(config vlan)# exit	Exit the VLAN database
Switch4(config)# ethernet cfm enable	Enable CFM globally
Switch4(config)# ethernet cfm mode y1731	Configure cfm mode
Switch4(config)# ethernet cfm domain cust level 5	Create a domain

Switch4(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch4(config-ether-cfm)# exit	Exit the CFM database
Switch4(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch4(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch4(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch4(config-if)# ethernet cfm mep down mpid 99 domain cust vlan 30 interval 1	Configure a maintenance end point (MEP)
Switch4(config-if)# ethernet cfm mep crosscheck mpid 66 domain cust vlan 30 mac fa02.cdff.6a09	Configure a remote maintenance end point (RMEP)
Switch4(config-if)# no shutdown	Bring up the interface
Switch4(config-if)# exit	Exit the Interface mode
Switch4(config)# ethernet cfm cc enable domain cust vlan 30	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch4(config)# end	Exit the Configure mode

3.4.3 Validation

MEP and MIP checks

The following command gives the connectivity details of the local machine Switch1 and Switch2 for the configured domain.

```
Switch1# show ethernet cfm maintenance-points
######Local MEP:
MPID Dir  DOMAIN        L VLAN PORT     CC-Status Mac-Address    RDI  Interval
--------------------------------------------------------------------------------
66   Down cust          5 30   eth-0-9  Enabled   fa02.cdff.6a09 True 3.33ms
######Local MIP:
Level   VLAN PORT      MAC-Address
--------------------------------------
######Remote MEP:
MPID  LEVEL VLAN Remote Mac     RDI   FLAGS    STATE
------------------------------------------------------
99    5     30   d036.4567.8009 True  Learnt    UP
```

```
Switch2# show ethernet cfm maintenance-points
######Local MEP:
MPID Dir DOMAIN        LEVEL VLAN PORT     CC-Status Mac-Address    RDI
------------------------------------------------------------------------------
666  Up  provid        3     30   eth-0-9  Enabled   0e1d.a7d7.fb09 False
######Local MIP:
Level   VLAN  PORT     MAC-Address
--------------------------------------
5       30    eth-0-9  0e1d.a7d7.fb09
######Remote MEP:
MPID  LEVEL VLAN Remote Mac      RDI   FLAGS     STATE
------------------------------------------------------
999   3      30   6a08.051e.bd09  True  Learnt    UP
```

Loopback checks

Step 1 The following command is used to ping remote mep by remote mep unicast mac address.

```
Switch1# ethernet cfm loopback mac  d036.4567.8009 unicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
 Loopback completed.
 ----------------------------------
Success rate is 100 percent(1/1)
```

Step 2 The following command is used to ping remote mep by multicast mac address.

```
Switch1# ethernet cfm loopback multicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
Host MEP: 66
Number of RMEPs that replied to mcast frame = 1
LBR received from the following
  9667.bb68.f308
 success rate is  100 (1/1)
```

Step 3 The following command is used to ping remote mep by remote mep id.

```
Switch1# ethernet cfm loopback unicast rmepid 99 mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
 Loopback completed.
 ----------------------------------
 Success rate is 100 percent(1/1)
```

Step 4 The following command is used to ping mip by mip mac address:

```
Switch1# ethernet cfm loopback mac 0e1d.a7d7.fb09 unicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
 Loopback completed.
 ----------------------------------
 Success rate is 100 percent(1/1)
```

RDI checks

Before clear local mep rdi, the rdi status is as follows:

```
Switch1# show ethernet cfm maintenance-points local mep domain cust
Dir-Direction;
L-Level;
MPID Dir   DOMAIN         L VLAN PORT     CC-Status Mac-Address    RDI Interval
--------------------------------------------------------------------------------
66   Down cust           5 30   eth-0-9  Enabled   fa02.cdff.6a09 True 3.33ms
```

ERROR check

Before clear local mep errors, the errors are as follows:

```
Switch1# show ethernet cfm errors domain cust
Level Vlan MPID RemoteMac      Reason                            ServiceId
5      30   66  d036.4567.8009 errorCCMdefect: rmep not found       cst
5      30   66  d036.4567.8009 errorCCMdefect: rmep not found clear cst
Time
2011/05/27 3:19:18
2011/05/27 3:19:32
```

The following command is used to clear errors:

```
Switch1# clear ethernet cfm errors domain cust
```

After clear local mep errors, the errors are as follows:

```
Switch1# show ethernet cfm errors domain cust
Level Vlan MPID RemoteMac      Reason                            ServiceId
```

AIS check

Step 1 The following command is used to disable cc function in Switch1.

```
Switch1(config)# no ethernet cfm cc enable domain cust vlan 30
```

Step 2 The following command is used to disable cc function in Switch3.

```
Switch3(config)# no ethernet cfm cc enable domain cust vlan 30
```

Step 3 The following command is used to check ais defect condition in Switch 2.

```
Switch2# show ethernet cfm ais mep 666 domain cust vlan 30
AIS-Status: Enabled
AIS Period: 1
Level to transmit AIS: 7
AIS Condition: No
--------------------------------------------------
   Configured defect condition     detected(yes/no)
--------------------------------------------------
   unexpected-period                 no
   unexpected-MEG level              no
   unexpected-MEP                    no
```

```
  Mismerge                        no
  LOC                             yes
```

Step 4 The following command is used to check ais reception status in Switch1.

```
Switch1# show ethernet cfm ais mep 66 domain cust vlan 30
AIS-Status: Disabled
AIS Condition: Yes
```

LinkTrace checks

The following command is used to link trace remote mep by remote mep unicast mac address.

```
Switch1# ethernet cfm linktrace mac d036.4567.8009 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
--------------------------------
Received Hops: 1
--------------------------------
TTL                          : 63
Fowarded                     : True
Terminal MEP                 : False
Relay Action                 : Rly FDB
Ingress Action               : IngOk
Ingress MAC address          : 0e1d.a7d7.fb09
Ingress Port ID Type         : ifName
Ingress Port ID              : eth-0-9
--------------------------------
Received Hops: 2
--------------------------------
TTL                          : 62
Fowarded                     : True
Terminal MEP                 : False
Relay Action                 : Rly FDB
Egress Action                : EgrOk
Egress MAC address           : 6a08.051e.bd09
Egress Port ID Type          : ifName
Egress Port ID               : eth-0-9
--------------------------------
Received Hops: 3
--------------------------------
TTL                          : 61
Fowarded                     : False
Terminal MEP                 : True
Relay Action                 : Rly Hit
Ingress Action               : IngOk
Ingress MAC address          : d036.4567.8009
Ingress Port ID Type         : ifName
Ingress Port ID              : eth-0-9
```

The following command is used to link trace remote mep by remote mep id.

```
Switch1# ethernet cfm linktrace rmepid 99 mepid 66 domain cust vlan 30
```

```
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
--------------------------------
Received Hops: 1
--------------------------------
TTL                              : 63
Fowarded                      : True
Terminal MEP                  : False
Relay Action                  : Rly FDB
Ingress Action                : IngOk
Ingress MAC address           : 0e1d.a7d7.fb09
Ingress Port ID Type          : ifName
Ingress Port ID               : eth-0-9
--------------------------------
Received Hops: 2
--------------------------------
TTL                           : 62
Fowarded                      : True
Terminal MEP                  : False
Relay Action                  : Rly FDB
Egress Action                 : EgrOk
Egress MAC address            : 6a08.051e.bd09
Egress Port ID Type           : ifName
Egress Port ID                : eth-0-9
--------------------------------
Received Hops: 3
--------------------------------
TTL                           : 61
Fowarded                      : False
Terminal MEP                  : True
Relay Action                  : Rly Hit
Ingress Action                : IngOk
Ingress MAC address           : d036.4567.8009
Ingress Port ID Type          : ifName
Ingress Port ID               : eth-0-9
```

The following command is used to link trace remote mip by remote mip unicast mac address.

```
Switch1# ethernet cfm linktrace 6a08.051e.bd09 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
--------------------------------
Received Hops: 1
--------------------------------
TTL                           : 63
Fowarded                      : True
Terminal MEP                  : False
Relay Action                  : Rly FDB
Ingress Action                : IngOk
Ingress MAC address           : 0e1d.a7d7.fb09
Ingress Port ID Type          : ifName
Ingress Port ID               : eth-0-9
--------------------------------
Received Hops: 2
--------------------------------
TTL                           : 62
```

```
Fowarded                    : False
Terminal MEP                : False
Relay Action                : Rly Hit
Egress Action               : EgrOk
Egress MAC address          : 6a08.051e.bd09
Egress Port ID Type         : ifName
Egress Port ID              : eth-0-9
```

1DM and DMM checks

The following command is used to make two way delay and delay variation measurement:

```
Switch1# ethernet cfm dmm  rmepid 99 mepid 66 count 5 domain cust vlan 30
     Delay measurement statistics:

     DMM Packets transmitted        : 5
     Valid DMR packets received     : 5

     Index      Two-way delay      Two-way delay variation
         1          4288 usec                       0 usec
         2          4312 usec                      24 usec
         3          4296 usec                      16 usec
         4          4320 usec                      24 usec
         5          4264 usec                      56 usec

     Average delay                  : 4296 usec
     Average delay variation        : 24 usec
     Best case delay                : 4264 usec
     Worst case delay               : 4320 usec
```

Before make one way delay measurement, clock timer should be synchronized. The following command is used to start sending 1dm message in Switch1:

```
Switch1#ethernet cfm 1dm rmepid 99 mepid 66 count 5 domain cust vlan 30
```

The following is 1dm test result in Switch4:

```
Switch4# show ethernet cfm delaymeasurement cache
    Remote MEP       : 66
     Remote MEP vlan  : 30
     Remote MEP level : 5
     DMM Packets transmitted         : 0
     Valid DMR packets received      : 0
     Valid 1DM packets received      : 5

     Index   One-way delay   One-way delay variation   Received Time
         1      16832 usec                    0 usec   2011/07/19 17:27:46
         2      16176 usec                  656 usec   2011/07/19 17:27:47
         3      15448 usec                  728 usec   2011/07/19 17:27:48
         4      14800 usec                  648 usec   2011/07/19 17:27:49
         5      15406 usec                  606 usec   2011/07/19 17:27:50

     Average delay                  : 15732 usec
     Average delay variation        : 527 usec
```

```
    Best case delay                 : 14800 usec
    Worst case delay                : 16832 usec
```

3.5 Configure LCK

3.5.1 Topology

Please refer to 3.3.1.

3.5.2 Configurations

Please configure MD/MA/MEP according to 3.3.2.

Configure lock enable for Switch 2.

Switch 2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch2(config-if)# ethernet cfm lck enable mep 666 domain provid vlan 30 tx-level 5 interval 1	Configure lck enable on MEP 666 and the level and interval of lck packet transmission
Switch2(config-if)# end	Exit the Interface mode

3.5.3 Validation

The following command is used to display lck status for Switch2:

```
Switch2# show ethernet cfm lck
En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
Rx-I, The period which is gotten from LCK packets
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval
------------------------------------------------------------------------
MPID Domain       VLAN En Rx-LC Rx-I Tx-Domain    Tx-I
------------------------------------------------------------------------
666  provid       30   Y  N     N/A  cust         1
```

The following command is used to display lck status for Switch2:

```
Switch1# show ethernet cfm lck
En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
Rx-I, The period which is gotten from LCK packets
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval
------------------------------------------------------------------------
MPID Domain       VLAN En Rx-LC Rx-I Tx-Domain    Tx-I
------------------------------------------------------------------------
66   cust         30   N  Y     1    N/A          N/A
```

3.6 Configure CSF

3.6.1 Topology

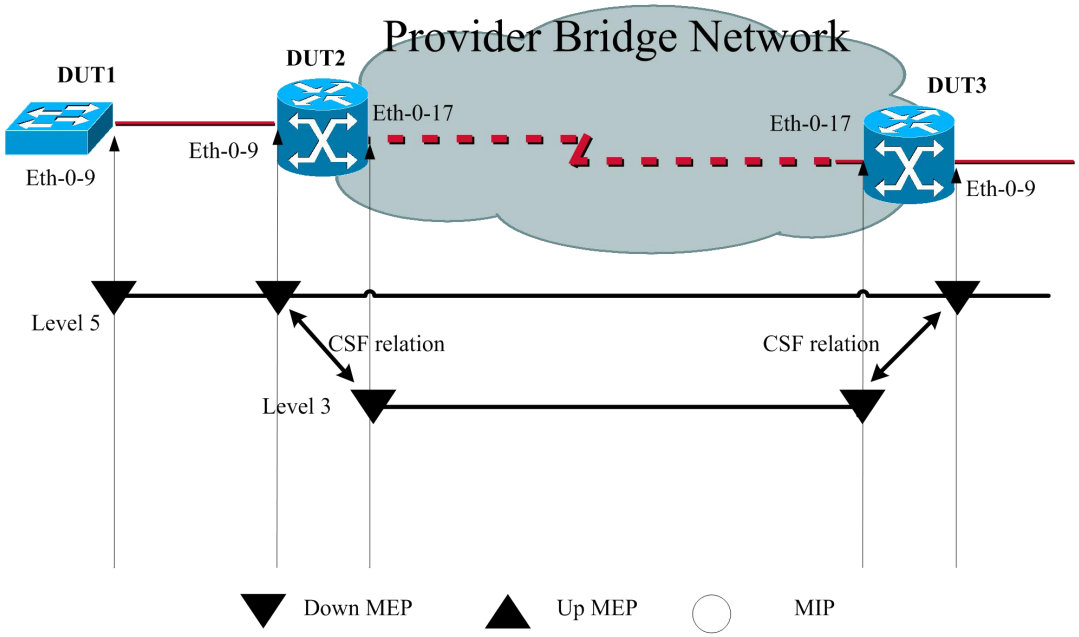


Figure 1-6 CFM CSF Topology

3.6.2 Configurations

Switch 1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# vlan database	Enter the VLAN database

Switch1(config vlan)# vlan 30	Configure VLAN 30
Switch1(config vlan)# exit	Exit the VLAN database
Switch1(config)# ethernet cfm enable	Enable CFM globally
Switch1(config)# ethernet cfm mode y1731	Configure cfm mode
Switch1(config)# ethernet cfm domain cust level 5	Create a domain
Switch1(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch1(config-ether-cfm)# exit	Exit the CFM database
Switch1(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch1(config-if)# ethernet cfm mep down mpid 66 domain cust vlan 30 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 99 domain cust vlan 30 mac d036.4567.8009	Configure a remote maintenance end point (RMEP)
Switch1(config-if)# no shutdown	Bring up the interface
Switch1(config-if)# exit	Exit the Interface mode
Switch1(config)# ethernet cfm cc enable domain cust vlan 30	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch1(config)# end	Exit the Configure mode

Switch 2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# vlan database	Enter the VLAN database
Switch2(config vlan)# vlan 20,30	Configure VLAN 20,30
Switch2(config vlan)# exit	Exit the VLAN database
Switch2(config)# ethernet cfm enable	Enable CFM globally
Switch2(config)# ethernet cfm mode y1731	Configure cfm mode
Switch2(config)# ethernet cfm domain cust level 5	Create a domain

Switch2(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch2(config)# ethernet cfm domain provid level 3	Create a domain
Switch2(config-ether-cfm)# service cst vlan 20	Define a Maintenance Association (MA) for the domain created
Switch2(config-ether-cfm)# exit	Exit the CFM database
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch2(config-if)# ethernet cfm mep down mpid 99 domain cust vlan 30 interval 1	Configure a maintenance end point (MEP)
Switch2(config-if)# ethernet cfm mep crosscheck mpid 66 domain cust vlan 30 mac fa02.cdff.6a09	Configure a remote maintenance end point (RMEP)
Switch2(config-if)# no shutdown	Bring up the interface
Switch2(config-if)# exit	Exit the Interface mode
Switch2 (config)#interface eth-0-17	Specify the interface (eth-0-17)to be configured and enter the Interface mode
Switch2 (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2 (config-if)# switchport trunk allowed vlan add 20	Enable vlan 20 on this port
Switch2 (config-if)# ethernet cfm mep down mpid 666 domain provid vlan 20 interval 1	Configure a maintenance end point (MEP)
Switch2 (config-if)# no shutdown	Bring up the interface
Switch2(config)# ethernet cfm cc enable domain cust vlan 30	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch2(config)# ethernet cfm csf client domain cust vlan 30 mepid 99 server domain provid vlan 20 mepid 666 interval 1	Configure csf relation between client mep and server mep
Switch2(config)# end	Exit the Configure mode

Switch 3

Switch3# configure terminal	Enter the Configure mode
Switch3(config)# vlan database	Enter the VLAN database
Switch3(config vlan)# vlan 20,30	Configure VLAN 20,30
Switch3(config vlan)# exit	Exit the VLAN database
Switch3(config)# ethernet cfm enable	Enable CFM globally
Switch3(config)# ethernet cfm mode y1731	Configure cfm mode
Switch3(config)# ethernet cfm domain cust level 5	Create a domain
Switch3(config-ether-cfm)# service cst vlan 30	Define a Maintenance Association (MA) for the domain created
Switch3(config)# ethernet cfm domain provid level 3	Create a domain
Switch3(config-ether-cfm)# service cst vlan 20	Define a Maintenance Association (MA) for the domain created
Switch3(config-ether-cfm)# exit	Exit the CFM database
Switch3(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch3(config-if)# switchport trunk allowed vlan add 30	Enable vlan 30 on this port
Switch3(config-if)# ethernet cfm mep down mpid 88 domain cust vlan 30 interval 1	Configure a maintenance end point (MEP)
Switch3(config-if)# no shutdown	Bring up the interface
Switch3(config-if)# exit	Exit the Interface mode
Switch3(config)#interface eth-0-17	Specify the interface (eth-0-17)to be configured and enter the Interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch3(config-if)# switchport trunk allowed vlan add 20	Enable vlan 20 on this port
Switch3(config-if)# ethernet cfm mep down mpid 999 domain provid vlan 20 interval 1	Configure a maintenance end point (MEP)
Switch3(config-if)# no shutdown	Bring up the interface
Switch3(config)# ethernet cfm cc enable domain cust vlan 30	Enable continuity check in the selected service instance (MA) instance with the configured domain

Switch3(config)# ethernet cfm csf client domain cust vlan 30 mepid 88 server domain provid vlan 20 mepid 999 interval 1	Configure csf relation between client mep and server mep
Switch3(config)# end	Exit the Configure mode

3.6.3 Validation

The following command is used to disable cc function in Switch1:

Switch1 (config)#no ethernet cfm cc enable domain cust vlan 30

For Switch 2, client MEP 99 will report loc error and trigger csf for reason los, therefore server MEP 666 will send CSF packet in interval 1 second.

The following command is used to display csf status for Swtich2:

```
Switch2# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
Tx-I, Transmit Interval
Rx-I, The period which is gotten from CSF packets
-------------------------------------------------------------------------
Client Mep                      Server Mep
MPID Cli-Domain   VLAN CTR   ECC MPID Srv-Domain   VLAN SRR   Tx-I Rx-I
-------------------------------------------------------------------------
99   cust         30   L      N   666  provid       20   N/A   1    N/A
```

For Switch3, server MEP 999 receives CSF packet and informs client MEP 99, then client MEP 88 will enter CSF condition.

The following command is used to display csf status for Switch3:

```
Switch3# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
Tx-I, Transmit Interval
Rx-I, The period which is gotten from CSF packets
-------------------------------------------------------------------------
Client Mep                      Server Mep
MPID Cli-Domain   VLAN CTR   ECC MPID Srv-Domain   VLAN SRR   Tx-I Rx-I
-------------------------------------------------------------------------
88   cust         30   N/A   Y   999  provid       20   L      1    1
```

3.7 Configure Dual-Ended LM

3.7.1 Topology

Please refer to 3.3.1.

3.7.2 Configurations

Please configure MD/MA/MEP according to 3.3.2.

Configure dual-ended lm enable for Switch1 and Switch4.

Switch 1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# ethernet cfm lm enable dual-ended domain cust vlan 30 mepid 66 all-cos cache-size 10	Configure dual-ended lm enable
Switch1(config)# end	Exit the Configure mode

Switch 4

Switch4# configure terminal	Enter the Configure mode
Switch4(config)# ethernet cfm lm enable dual-ended domain cust vlan 30 mepid 99 all-cos cache-size 10	Configure dual-ended lm enable
Switch4(config)# end	Exit the Configure mode

3.7.3 Validation

The following command is used to display lm status for Switch1:

```
Switch1# show ethernet cfm lm domain cust vlan 30 mepid 66
DOMAIN     : cust
VLAN       : 30
MEPID      : 66
Start Time : 2013/07/16 1:36:56
End Time   : 2013/07/16 1:37:07
Notes      : 1. When the difference of Tx is less than the difference of Rx,
                the node is invalid, loss and loss ratio should be "-";
             2. When loc is reported for mep, the loss should be "-" and loss
                ratio should be 100%;
```

```
             3. When calculate average loss and loss ratio, invalid or loc nodes
                will be excluded;
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio Time
--------------------------------------------------------------------------------
1     all          0        000.0000%           0         000.0000% 01:36:57
2     all          0        000.0000%           0         000.0000% 01:36:58
3     all          0        000.0000%           0         000.0000% 01:36:59
4     all          0        000.0000%           0         000.0000% 01:37:00
5     all          0        000.0000%           0         000.0000% 01:37:01
6     all          0        000.0000%           0         000.0000% 01:37:02
7     all          0        000.0000%           0         000.0000% 01:37:03
8     all          0        000.0000%           0         000.0000% 01:37:04
9     all          0        000.0000%           0         000.0000% 01:37:05
10    all          0        000.0000%           0         000.0000% 01:37:07
--------------------------------------------------------------------------------
Maximum Local-loss  : 0          Maximum Local-loss Ratio  : 000.0000%
Minimum Local-loss  : 0          Minimum Local-loss Ratio  : 000.0000%
Average Local-loss  : 0          Average Local-loss Ratio  : 000.0000%
Maximum Remote-loss : 0          Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0          Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0          Average Remote-loss Ratio : 000.0000%
```

The following command is used to display lm status for Switch4:

```
Switch4# show ethernet cfm lm domain cust vlan 30 mepid 99
DOMAIN     : cust
VLAN       : 30
MEPID      : 99
Start Time : 2013/07/16 1:37:11
End Time   : 2013/07/16 1:37:22
Notes      : 1. When the difference of Tx is less than the difference of Rx,
                the node is invalid, loss and loss ratio should be "-";
             2. When loc is reported for mep, the loss should be "-" and loss
                ratio should be 100%;
             3. When calculate average loss and loss ratio, invalid or loc nodes
                will be excluded;
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio Time
--------------------------------------------------------------------------------
1     all          0        000.0000%           0         000.0000% 01:37:12
2     all          0        000.0000%           0         000.0000% 01:37:13
3     all          0        000.0000%           0         000.0000% 01:37:14
4     all          0        000.0000%           0         000.0000% 01:37:16
5     all          0        000.0000%           0         000.0000% 01:37:17
6     all          0        000.0000%           0         000.0000% 01:37:18
7     all          0        000.0000%           0         000.0000% 01:37:19
8     all          0        000.0000%           0         000.0000% 01:37:20
9     all          0        000.0000%           0         000.0000% 01:37:21
10    all          0        000.0000%           0         000.0000% 01:37:22
--------------------------------------------------------------------------------
Maximum Local-loss  : 0          Maximum Local-loss Ratio  : 000.0000%
Minimum Local-loss  : 0          Minimum Local-loss Ratio  : 000.0000%
Average Local-loss  : 0          Average Local-loss Ratio  : 000.0000%
```

```
Maximum Remote-loss : 0          Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0          Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0          Average Remote-loss Ratio : 000.0000%
```

3.8 Configure Single-Ended LM

3.8.1 Topology

Please refer to 3.3.1.

3.8.2 Configurations

Please configure MD/MA/MEP according to 3.3.2.

Configure single-ended lm enable for Switch1 and Switch4.

Switch 1

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# ethernet cfm lm enable single-ended domain cust vlan 30 mepid 66 all-cos	Configure single-ended lm enable
Switch1(config)# end	Exit the Configure mode

Switch 2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# ethernet cfm lm enable single-ended domain cust vlan 30 mepid 99 all-cos	Configure single-ended lm enable
Switch2(config)# end	Exit the Configure mode

3.8.3 Validation

The following command is used to output lmm and display lm results for Switch1:

```
Switch1#  ethernet cfm lm single-ended domain cust vlan 30 rmepid 99 mepid 66 count 10
DOMAIN     : cust
```

```
VLAN       : 30
MEPID      : 66
Start Time : 2013/07/16 1:39:38
End Time   : 2013/07/16 1:39:38
Notes      : 1. When the difference of Tx is less than the difference of Rx,
                the node is invalid, loss and loss ratio should be "-";
             2. When loc is reported for mep, the loss should be "-" and loss
                ratio should be 100%;
             3. When calculate average loss and loss ratio, invalid or loc nodes
                will be excluded;
Latest single-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio
--------------------------------------------------------------------------------
1     all          0        000.0000%           0         000.0000%
2     all          0        000.0000%           0         000.0000%
3     all          0        000.0000%           0         000.0000%
4     all          0        000.0000%           0         000.0000%
5     all          0        000.0000%           0         000.0000%
6     all          0        000.0000%           0         000.0000%
7     all          0        000.0000%           0         000.0000%
8     all          0        000.0000%           0         000.0000%
9     all          0        000.0000%           0         000.0000%
--------------------------------------------------------------------------------
Maximum Local-loss  : 0          Maximum Local-loss Ratio  : 000.0000%
Minimum Local-loss  : 0          Minimum Local-loss Ratio  : 000.0000%
Average Local-loss  : 0          Average Local-loss Ratio  : 000.0000%
Maximum Remote-loss : 0          Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0          Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0          Average Remote-loss Ratio : 000.0000%
```

3.9 Configure Test

3.9.1 Topology

Please refer to CC Topolopy.

3.9.2 Configurations

Please configure MD/MA/MEP according to CC configuration.

Configure test transmission enable on Switch1 and test reception enable on Switch4.

Switch 1

Switch1# configure terminal	Enter the Configure mode

Switch1(config)# ethernet cfm tst transmission enable domain cust vlan 30 mep 66 tx-mode continuous pattern-type random packet-size 64	Configure test transmission enable
Switch1(config)# end	Exit the Configure mode

Switch 4

Switch4# configure terminal	Enter the Configure mode
Switch4(config)# ethernet cfm tst reception enable domain cust vlan 30 mep 99	Configure test reception enable
Switch4(config)# end	Exit the Configure mode

3.9.3 Validation

The following command is used to start test transmission:

```
Switch1#  ethernet cfm tst start rate 1000 time second 1
```

The following command is used to display test information on switch1:

```
Switch1#  show ethernet cfm tst
DOMAIN           : cust
VLAN             : 30
MEPID            : 66
Transmission     : Enabled
Reception        : Disabled
Status           : Non-Running
Start Time       : 06:32:48
Predict End Time : 06:33:18
Actual End Time  : 06:33:18
Packet Type      : TST
Rate             : 1000 mbps
Packet Size      : 64 bytes
Tx Number        : 29
Tx Bytes         : 1856
Rx Number        : 0
Rx Bytes         : 0
```

The following command is used to display test information on switch4:

```
Switch4#  show ethernet cfm tst
DOMAIN           : cust
VLAN             : 30
MEPID            : 99
Transmission     : Disabled
Reception        : Enabled
```

```
Status            : Non-Running
Start Time        : null
End Time          : null
Packet Type       : null
Rate              : null
Packet Size       : null
Tx Number         : 0
Tx Bytes          : 0
Rx Number         : 29
Rx Bytes          : 1856
```

4 Configuring CPU Traffic Limit

4.1 Overview

CPU traffic limit is a useful mechanism for protecting CPU from malicious flows by injecting huge volume of PDUs into switches.

CPU traffic limit provides two-level protection for CPU. The low-level traffic limit is performed for each reason , which is realized by queue shaping of each type of PDU. The high-level traffic limit is performed for all reasons, which is realized by channel shaping at CPU channel. With this two-level protection, each PDU-to-CPU rate is limited and the overall PDU-to-CPU rate is also limited.

The word “reason”, means this type of packets will be sent to cpu for further processing. The description of all reason is as following.

Reason	Description
arp	Address Resolution Protocol
bpdu	Bridge Protocol Data Unit
dhcp	Dynamic Host Configuration Protocol
eapol	Extensible Authentication Protocol Over Lan
erps	Ethernet Ring Protection Switching
fwd-to-cpu	Packets forwarding to cpu
icmp-redirect	ICMP Redirect
igmp	IGMP/IGMP Snooping Protocol
ip-option	Packets with IP Option
ipda	IP Destination to Router-self
ldp	Label Distribution Protocol
macsa-mismatch	Port Security for source mac learned
mcast-rpf-fail	Multicast with rpf fail or first multicast packet

Reason	Description
mld	MLD/MLD Snooping Protocol
mpls-ttl-fail	Mpls Packets with ttl fail
ip-mtu-fail	Ip mtu fail
ospf	Open Shortest Path First
pim	Protocol Independent Multicast
port-security-discard	Port Security for exceeding fdb maxnum
rip	Routing Information Protocol
sflow-egress	Sampled flow at egress direction
sflow-ingress	Sampled flow at ingress direction
slow-protocol	Slow Protocol (including EFM, LACP and SYNCE)
smart-link	Smart Link Protocol
ucast-ttl-fail	Unicast Packets with ttl fail
udld	Unidirectional Link Detection Protocol
vlan-security-discard	Vlan Security for exceeding fdb maxnum
vrrp	Virtual Router Redundancy Protocol
bfd-learning	BFD learning packets

4.2 Terminology

PDU: Protocol Data Unit

4.3 Default Configuration

The default rate and class configuration for all reason is as following.

reason	rate(pps)	class	reason	rate(pps)	class
arp	640	1	mpls-ttl-fail	64	0
bpdu	64	3	ip-mtu-fail	64	0
dhcp	128	0	ospf	256	1
eapol	128	0	pim	128	1
erps	128	2	port-security-discard	128	0
fwd-to-cpu	64	0	rip	64	1
icmp-redirect	128	0	sflow-egress	128	0

reason	rate(pps)	class	reason	rate(pps)	class
igmp	128	2	sflow-ingress	128	0
ip-option	512	0	slow-protocol	128	1
ipda	1024	0	smart-link	128	2
ldp	512	1	ucast-ttl-fail	64	0
macsa-mismatch	128	0	udld	128	3
mcast-rpf-fail	128	1	vlan-security-discard	128	0
mld	128	2	vrrp	512	1
bfd-learning	128	1			

4.4 Configuration

Configure total limit rate

Switch# configure terminal	Enter the Configure mode
Switch(config)# cpu-traffic-limit total rate 3000	Set cpu traffic total limit rate

Configure individual rate

Switch# configure terminal	Enter the Configure mode
Switch(config)# cpu-traffic-limit reason rip rate 500	Set individual limit rate for RIP PDU

Configure priority class

Switch# configure terminal	Enter the Configure mode
Switch(config)# cpu-traffic-limit reason rip class 3	Modify priority class for RIP PDU

4.5 Validation Commands

To display the CPU Traffic Limit configuration, use following privileged EXEC commands.

```
Switch# show cpu traffic-limit
reason                    rate (pps)    class
dot1x-mac-bypass          64             2
```

```
bpdu                        64            3
slow-protocol               128           1
eapol                       128           0
erps                        128           2
smart-link                  128           2
udld                        128           3
loopback-detection          64            3
arp                         256           1
dhcp                        128           0
rip                         500           3
ldp                         512           1
ospf                        256           1
pim                         128           1
vrrp                        512           1
ipda                        1024          0
icmp-redirect               128           0
mcast-rpf-fail              128           1
macsa-mismatch              128           0
port-security-discard       128           0
vlan-security-discard       128           0
mtu-dontfrag                64            0
mtu-frag                    64            0
ip-mtu-fail                 64            0
ip-option                   512           0
bfd-learning                128           1
ucast-ttl-fail              64            0
mpls-ttl-fail               64            0
igmp                        128           2
sflow-ingress               128           0
sflow-egress                128           0
fwd-to-cpu                  64            0
l2protocol-tunnel           1024          0
Total rate:      3000 (pps)
```

5 Configuring G.8031

5.1 Overview

This document describes the configuration of G.8031 Ethernet Linear Protection Switching.

The goal of linear protection switching mechanism is to satisfy the requirement of fast protection switching for ethernet network. Linear protection switching means that, for one or more working transport entities, there is one protection transport entity, which is disjoint from any of working transport entities, ready for taking over the service transmission when a working transport entity failed.

To guarantee the protection switching time, for a working transport entity, its protection transport entity is always pre-configured before the failure occurs. Normally, the normal traffic will be transmitted and received on the working transport entity. The switching to protection transport entity is usually triggered by link/node failure, external commands, etc. Note that external commands are often used in transport network by operators, and they are very useful in cases of service adjustment, path maintenance, etc.

5.2 Topology

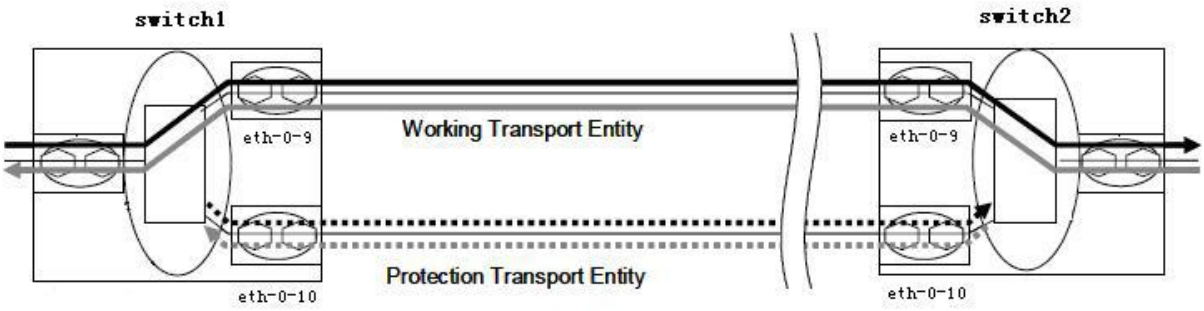


Figure 5-1 G.8031 Basic topology

5.3 Configuration

Switch1's configuration

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# vlan database	Enter the VLAN database mode
Switch1(config-vlan)# vlan 10-20	Create VLAN 10-20
Switch1(config-vlan)# exit	Exit VLAN database mode
Switch1(config)# spanning-tree mode mstp	Configure a spanning-tree mode
Switch1(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch1(config-mst)# instance 10 vlan 10-20	Create an instance of vlan
Switch1(config)# ethernet cfm enable	Enable CFM globally
Switch1(config)# ethernet cfm domain test level 5	Create a domain
Switch1(config-ether-cfm)# service test1 vlan 10	Define a Maintenance Association (MA) for the domain created
Switch1(config-ether-cfm)# service test2 vlan 11	Define a Maintenance Association (MA) for the domain created
Switch1(config-ether-cfm)# exit	Exit the CFM database
Switch1(config)# ethernet cfm cc enable domain test vlan 10	Enable continuity check in the selected service instance (MA) instance with the configured domain

Switch1(config)# ethernet cfm cc enable domain test vlan 11	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch1(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan add 10-20	Enable VLAN 10-20 on this port
Switch1 (config-if)# ethernet cfm mep down mpid 10 domain test vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 12 domain test vlan 10 mac bab3.08a4.c709	Configure a remote maintenance end point (RMEP)
Switch1(config-if)# spanning-tree port disable	Set STP disable on this port
Switch1(config-if)# exit	Exit interface mode of interface eth-0-9
Switch1(config)# interface eth-0-10	Specify the interface (eth-0-10)to be configured and enter the Interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan add 10-20	Enable VLAN 10-20 on this port
Switch1(config-if)# ethernet cfm mep down mpid 11 domain test vlan 11 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 13 domain test vlan 11 mac bab3.08a4.c70a	Configure a remote maintenance end point (RMEP)
Switch1(config-if)# spanning-tree port disable	Set STP disable on this port
Switch1(config-if)# exit	Exit interface mode of interface eth-0-10
Switch1(config)# g8031 eps-id 10 working-port eth-0-9 protection-port eth-0-10	Create a g8031 ethernet protection group and enter the g8031 config mode
Switch1(g8031-config-switching)# domain test working-service test1 protection-service test2	Associate the cfm domain and Maintenance Association (MA) with the g8031 ethernet protection group
Switch1(g8031-config-switching)# instance 10	Associate the instance with the g8031 ethernet protection group
Switch1(config-if)# exit	Exit the g8031 config mode
Switch1(config)# end	Exit the configure mode

Switch2's configuration

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# vlan database	Enter the VLAN database mode
Switch2(config-vlan)# vlan 10-20	Create VLAN 10-20
Switch2(config-vlan)# exit	Exit VLAN database mode
Switch2(config)# spanning-tree mode mstp	Configure a spanning-tree mode
Switch2(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch2(config-mst)# instance 10 vlan 10-20	Create an instance of vlan
Switch2(config)# ethernet cfm enable	Enable CFM globally
Switch2(config)# ethernet cfm domain test level 5	Create a domain
Switch2(config-ether-cfm)# service test1 vlan 10	Define a Maintenance Association (MA) for the domain created
Switch2(config-ether-cfm)# service test2 vlan 11	Define a Maintenance Association (MA) for the domain created
Switch2(config-ether-cfm)# exit	Exit the CFM database
Switch2(config)# ethernet cfm cc enable domain test vlan 10	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch2(config)# ethernet cfm cc enable domain test vlan 11	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2(config-if)# switchport trunk allowed vlan add 10-20	Enable VLAN 10-20 on this port
Switch2(config-if)# ethernet cfm mep down mpid 12 domain test vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 10 domain test vlan 10 mac bab3.08a4.c809	Configure a remote maintenance end point (RMEP)
Switch2(config-if)# spanning-tree port disable	Set STP disable on this port
Switch2(config-if)# exit	Exit interface mode of interface eth-0-9

Switch2(config)# interface eth-0-10	Specify the interface (eth-0-10)to be configured and enter the Interface mode
Switch2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2(config-if)# switchport trunk allowed vlan add 10-20	Enable VLAN 10-20 on this port
Switch2(config-if)# ethernet cfm mep down mpid 13 domain test vlan 11 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 11 domain test vlan 11 mac bab3.08a4.c80a	Configure a remote maintenance end point (RMEP)
Switch2(config-if)# spanning-tree port disable	Set STP disable on this port
Switch2(config-if)# exit	Exit interface mode of interface eth-0-10
Switch2(config)# g8031 eps-id 10 working-port eth-0-9 protection-port eth-0-10	Create a g8031 ethernet protection group and enter the g8031 config mode
Switch2(g8031-config-switching)# domain test working-service test1 protection-service test2	Associate the cfm domain and Maintenance Association (MA) with the g8031 ethernet protection group
Switch2(g8031-config-switching)# instance 10	Associate the instance with the g8031 ethernet protection group
Switch2(config-if)# exit	Exit the g8031 config mode
Switch2(config)# end	Exit the configure mode

5.4 Validation

The result of show g8031 is as follows.

```
Switch1# show g8031
Codes: ID - Group id of G.8031
       IF-W - Interface of working entity, IF-P - Interface of protection entity
       MD - Maintenance domain
       MA-W - Maintenance association of working entity
       MA-W - Maintenance association of protection entity
       CS - Current state, LS - Last state, LE - Last event, FS - Far end state
       R/B - Request signal & bridged signal, MODE - Revertive or Non-revertive
       WTR - Wait to restoren, DFOP - Failure of protocol defects
================================================================================
 ID   IF-W     IF-P     MD    MA-W  MA-P  CS    LS    LE    FS    R/B    MODE
--------------------------------------------------------------------------------
 10   eth-0-9  eth-0-10 test   test1   test2  NR    NR    NR    NR    null   REV
APS Vid - 11
Active-Path - Working
```

```
DFOP State - Not in defect mode
Protected Instance - 10
================================================================================
```

```
Switch2# show g8031
Codes: ID - Group id of G.8031
       IF-W - Interface of working entity, IF-P - Interface of protection entity
       MD - Maintenance domain
       MA-W - Maintenance association of working entity
       MA-W - Maintenance association of protection entity
       CS - Current state, LS - Last state, LE - Last event, FS - Far end state
       R/B - Request signal & bridged signal, MODE - Revertive or Non-revertive
       WTR - Wait to restoren, DFOP - Failure of protocol defects
================================================================================
 ID   IF-W     IF-P     MD    MA-W  MA-P  CS    LS    LE    FS    R/B    MODE
--------------------------------------------------------------------------------
 10   eth-0-9  eth-0-10 test   test1   test2  NR    NR    NR    NR    null   REV
APS Vid - 11
Active-Path - Working
DFOP State - Not in defect mode
Protected Instance - 10
================================================================================
```

6 Configuring G.8032

6.1 Overview

This document describes the configuration of G.8032 Ethernet Ring Protection Switching.

Ethernet rings can provide wide-area multipoint connectivity more economically due to their reduced number of links. Each ring node is connected to adjacent nodes participating in the same ring, using two independent links. A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port. The minimum number of nodes on a ring is two.

The fundamentals of this ring protection switching architecture are:

The principle of loop avoidance, and

The utilization of learning, forwarding, and address table mechanisms defined in the Ethernet flow forwarding function (ETH_FF).

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This particular link is called the ring protection link (RPL), and under normal conditions this link is blocked, i.e., not used for traffic. One designated node, the RPL owner, is responsible to block traffic over the RPL. Under a ring failure condition, the RPL owner is responsible to unblock the RPL, allowing the RPL to be used for traffic.

The event of a ring failure results in protection switching of the traffic. This is achieved under the control of the ETH_FF functions on all ring nodes.

An APS protocol is used to coordinate the protection actions over the ring.

6.2 Topology

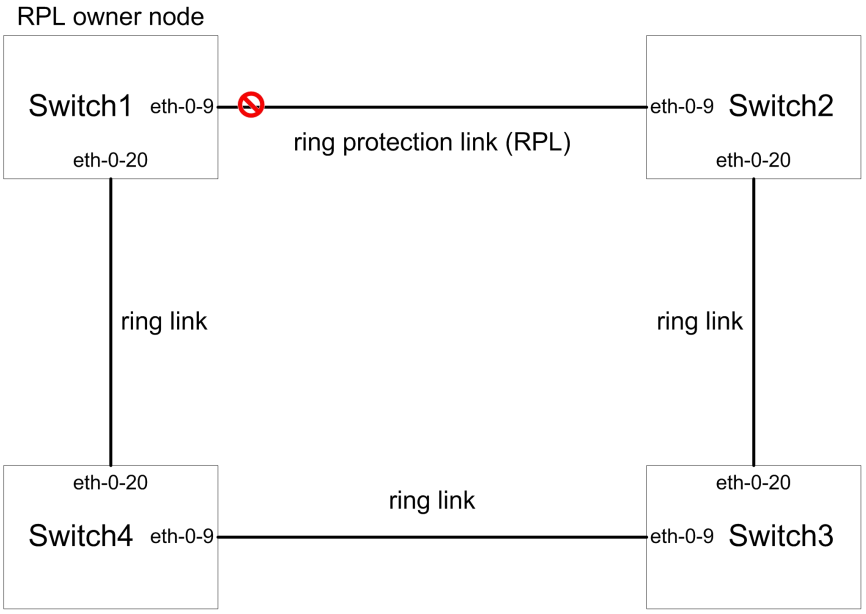


Figure 6-1 G.8032 Typical Topology

6.3 Configuration

Switch 1's configuration

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# vlan database	Enter the VLAN configure mode
Switch1(config-vlan)# vlan 10-100	Create VLAN 10-100
Switch1(config-vlan)# exit	Exit VLAN database mode
Switch1(config)# spanning-tree mode mstp	Configure a spanning-tree mode
Switch1(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch1(config-mst)# instance 1 vlan 10-99	Create an instance of vlan
Switch1(config-mst)# exit	Exit Multiple Spanning Tree configuration mode
Switch1(config)# ethernet cfm enable	Enable CFM globally
Switch1(config)# ethernet cfm domain md1 level 5	Create a domain
Switch1(config-ether-cfm)# service ma1 vlan 10	Define a Maintenance Association (MA) for the domain created

Switch1(config-ether-cfm)# exit	Exit the CFM database
Switch1(config)# ethernet cfm cc enable domain md1 vlan 10	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch1(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port
DUT (config-if)# ethernet cfm mep down mpid 109 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 209 domain md1 vlan 10 mac 08d9.94fb.f609	Configure a remote maintenance end point (RMEP)
Switch1(config-if)# spanning-tree port disable	Set STP disable on this port
Switch1(config-if)# no shutdown	Bring up the interface
Switch1(config-if)# exit	Exit interface mode of interface eth-0-9
Switch1(config)# interface eth-0-20	Specify the interface (eth-0-20) to be configured and enter the Interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port
Switch1(config-if)# ethernet cfm mep down mpid 120 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch1(config-if)# ethernet cfm mep crosscheck mpid 420 domain md1 vlan 10 mac b43a.ba34.1314	Configure a remote maintenance end point (RMEP)
Switch1(config-if)# spanning-tree port disable	Set STP disable on this port
Switch1(config-if)# no shutdown	Bring up the interface
Switch1(config-if)# exit	Exit interface mode of interface eth-0-20
Switch1(config)# g8032 ring-id 1 east-interface eth-0-9 west-interface eth-0-20	Create a g8032 ring and enter the g8032 config mode
Switch1(g8032-config-switch)# domain md1 service ma1	Associate the cfm domain and Maintenance Association (MA) with the g8032 ring
Switch1(g8032-config-switch)# instance 1	Associate the instance with the g8032 ethernet protection group

Switch1(g8032-config-switch)# control-vlan 100	Configure the RAPS message channel vlan
Switch1(g8032-config-switch)# rpl owner east-interface	Set the node as rpl owner and specify east-interface as rpl
Switch1(g8032-config-switch)# timer wait-to-restore 6	Set the wait-to-restore timer
Switch1(g8032-config-switch)# ring enable	Enable the g8032 ring
Switch1(g8032-config-mode)# exit	Exit the g8032 config mode
Switch1(config)# end	Exit the configure mode
Switch1# show g8032	Show the information of g8032

Switch 2's configuration

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# vlan database	Enter the VLAN configure mode
Switch2(config-vlan)# vlan 10-100	Create VLAN 10-100
Switch2(config-vlan)# exit	Exit VLAN database mode
Switch2(config)# spanning-tree mode mstp	Configure a spanning-tree mode
Switch2(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch2(config-mst)# instance 1 vlan 10-99	Create an instance of vlan
Switch2(config-mst)# exit	Exit Multiple Spanning Tree configuration mode
Switch2(config)# ethernet cfm enable	Enable CFM globally
Switch2(config)# ethernet cfm domain md1 level 5	Create a domain
Switch2(config-ether-cfm)# service ma1 vlan 10	Define a Maintenance Association (MA) for the domain created
Switch2(config-ether-cfm)# exit	Exit the CFM database
Switch2(config)# ethernet cfm cc enable domain md1 vlan 10	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2(config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port

Switch2(config-if)# ethernet cfm mep down mpid 209 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch2(config-if)# ethernet cfm mep crosscheck mpid 109 domain md1 vlan 10 mac fadd.f448.f909	Configure a remote maintenance end point (RMEP)
Switch2(config-if)# spanning-tree port disable	Set STP disable on this port
Switch2(config-if)# no shutdown	Bring up the interface
Switch2(config-if)# exit	Exit interface mode of interface eth-0-9
Switch2(config)# interface eth-0-20	Specify the interface (eth-0-20) to be configured and enter the Interface mode
Switch2(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch2(config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port
Switch2(config-if)# ethernet cfm mep down mpid 220 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch2(config-if)# ethernet cfm mep crosscheck mpid 320 domain md1 vlan 10 mac 481a.14e4.1814	Configure a remote maintenance end point (RMEP)
Switch2(config-if)# spanning-tree port disable	Set STP disable on this port
Switch2(config-if)# no shutdown	Bring up the interface
Switch2(config-if)# exit	Exit interface mode of interface eth-0-20
Switch2(config)# g8032 ring-id 1 east-interface eth-0-9 west-interface eth-0-20	Create a g8032 ring and enter the g8032 config mode
Switch2(g8032-config-switch)# domain md1 service ma1	Associate the cfm domain and Maintenance Association (MA) with the g8032 ring
Switch2(g8032-config-switch)# instance 1	Associate the instance with the g8031 ethernet protection group
Switch2(g8032-config-switch)# control-vlan 100	Configure the RAPS message channel vlan
Switch2(g8032-config-switch)# ring enable	Enable the g8032 ring
Switch2(g8032-config-mode)# exit	Exit the g8032 config mode
Switch2(config)# end	Exit the configure mode
Switch2# show g8032	Show the information of g8032

Switch 3's configuration

Switch3# configure terminal	Enter the Configure mode
Switch3(config)# vlan database	Enter the VLAN configure mode
Switch3(config-vlan)# vlan 10-100	Create VLAN 10-100
Switch3(config-vlan)# exit	Exit VLAN database mode
Switch3(config)# spanning-tree mode mstp	Configure a spanning-tree mode
Switch3(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch3(config-mst)# instance 1 vlan 10-99	Create an instance of vlan
Switch3(config-mst)# exit	Exit Multiple Spanning Tree configuration mode
Switch3(config)# ethernet cfm enable	Enable CFM globally
Switch3(config)# ethernet cfm domain md1 level 5	Create a domain
Switch3(config-ether-cfm)# service ma1 vlan 10	Define a Maintenance Association (MA) for the domain created
Switch3(config-ether-cfm)# exit	Exit the CFM database
Switch3(config)# ethernet cfm cc enable domain md1 vlan 10	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch3(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch3(config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port
Switch3(config-if)# ethernet cfm mep down mpid 309 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch3(config-if)# ethernet cfm mep crosscheck mpid 409 domain md1 vlan 10 mac b43a.ba34.1309	Configure a remote maintenance end point (RMEP)
Switch3(config-if)# spanning-tree port disable	Set STP disable on this port
Switch3(config-if)# no shutdown	Bring up the interface
Switch3(config-if)# exit	Exit interface mode of interface eth-0-9
Switch3(config)# interface eth-0-20	Specify the interface (eth-0-20) to be configured and enter the Interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode

Switch3 (config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port
Switch3(config-if)# ethernet cfm mep down mpid 320 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch3(config-if)# ethernet cfm mep crosscheck mpid 220 domain md1 vlan 10 mac 08d9.94fb.f614	Configure a remote maintenance end point (RMEP)
Switch3(config-if)# spanning-tree port disable	Set STP disable on this port
Switch3(config-if)# no shutdown	Bring up the interface
Switch3(config-if)# exit	Exit interface mode of interface eth-0-20
Switch3(config)# g8032 ring-id 1 east-interface eth-0-9 west-interface eth-0-20	Create a g8032 ring and enter the g8032 config mode
Switch3(g8032-config-switch)# domain md1 service ma1	Associate the cfm domain and Maintenance Association (MA) with the g8032 ring.
Switch3(g8032-config-switch)# instance 1	Associate the instance with the g8031 ethernet protection group
Switch3(g8032-config-switch)# control-vlan 100	Configure the RAPS message channel vlan.
Switch3(g8032-config-switch)# ring enable	Enable the g8032 ring
Switch3(g8032-config-mode)# exit	Exit the g8032 config mode
Switch3(config)# end	Exit the configure mode
Switch3# show g8032	Show the information of g8032

Switch 4's configuration

Switch4# configure terminal	Enter the Configure mode
Switch4(config)# vlan database	Enter the VLAN configure mode
Switch4(config-vlan)# vlan 10-100	Create VLAN 10-100
Switch4(config-vlan)# exit	Exit VLAN database mode
Switch4(config)# spanning-tree mode mstp	Configure a spanning-tree mode
Switch4(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch4(config-mst)# instance 1 vlan 10-99	Create an instance of vlan
Switch4(config-mst)# exit	Exit Multiple Spanning Tree configuration mode
Switch4(config)# ethernet cfm enable	Enable CFM globally

Switch4(config)# ethernet cfm domain md1 level 5	Create a domain
Switch4(config-ether-cfm)# service ma1 vlan 10	Define a Maintenance Association (MA) for the domain created
Switch4(config-ether-cfm)# exit	Exit the CFM database
Switch4(config)# ethernet cfm cc enable domain md1 vlan 10	Enable continuity check in the selected service instance (MA) instance with the configured domain
Switch4(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch4(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch4(config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port
Switch4(config-if)# ethernet cfm mep down mpid 409 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch4(config-if)# ethernet cfm mep crosscheck mpid 309 domain md1 vlan 10 mac 481a.14e4.1809	Configure a remote maintenance end point (RMEP)
Switch4(config-if)# spanning-tree port disable	Set STP disable on this port
Switch4(config-if)# no shutdown	Bring up the interface
Switch4(config-if)# exit	Exit interface mode of interface eth-0-9
Switch4(config)# interface eth-0-20	Specify the interface (eth-0-20) to be configured and enter the Interface mode
Switch4(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch4(config-if)# switchport trunk allowed vlan add 10-100	Enable VLAN 10-100 on this port
Switch4(config-if)# ethernet cfm mep down mpid 420 domain md1 vlan 10 interval 1	Configure a maintenance end point (MEP)
Switch4(config-if)# ethernet cfm mep crosscheck mpid 120 domain md1 vlan 10 mac fadd.f448.f914	Configure a remote maintenance end point (RMEP)
Switch4(config-if)# spanning-tree port disable	Set STP disable on this port
Switch4(config-if)# no shutdown	Bring up the interface
Switch4(config-if)# exit	Exit interface mode of interface eth-0-20
Switch4(config)# g8032 ring-id 1 east-interface eth-0-9 west-interface eth-0-20	Create a g8032 ring and enter the g8032 config mode

Switch4(g8032-config-switch)# domain md1 service ma1	Associate the cfm domain and Maintenance Association (MA) with the g8032 ring
Switch4(g8032-config-switch)# instance 1	Associate the instance with the g8031 ethernet protection group
Switch4(g8032-config-switch)# control-vlan 100	Configure the RAPS message channel vlan
Switch4(g8032-config-switch)# ring enable	Enable the g8032 ring
Switch4(g8032-config-mode)# exit	Exit the g8032 config mode
Switch4(config)# end	Exit the configure mode
Switch4# show g8032	Show the information of g8032

6.4 Validation

The result of show g8032 is as follows.

```
Switch1# show g8032
RingID  MajorRing  Current     Role       East      Status   West      Status
-------------------------------------------------------------------------------
1       N/A        Idle        Owner      eth-0-9   Blocked  eth-0-20  Forward

Control Vlan     : 100
MD Name          : md1
Service Id       : ma1
Protect Instance : 1
Current Event    : NR-RB
RPL              : east-interface
Wait-to-restore  : 06:00
Hold-off Timer   : 0 (msecs)
Guard Timer      : 500 (msecs)
-------------------------------------------------------------------------------
```

```
Switch2# show g8032
RingID  MajorRing  Current     Role       East      Status   West      Status
-------------------------------------------------------------------------------
1       N/A        Idle        Non-Owner  eth-0-9   Forward  eth-0-20  Forward

Control Vlan     : 100
MD Name          : md1
Service Id       : ma1
Protect Instance : 1
Current Event    : NR-RB
Hold-off Timer   : 0 (msecs)
Guard Timer      : 500 (msecs)
-------------------------------------------------------------------------------
```

```
Switch3# show g8032
RingID  MajorRing  Current     Role       East      Status   West      Status
-------------------------------------------------------------------------------
1       N/A        Idle        Non-Owner  eth-0-9   Forward  eth-0-20  Forward

Control Vlan     : 100
MD Name          : md1
Service Id       : ma1
Protect Instance : 1
Current Event    : NR-RB
Hold-off Timer   : 0 (msecs)
Guard Timer      : 500 (msecs)
-------------------------------------------------------------------------------
```

```
Switch4# show g8032
RingID  MajorRing  Current     Role       East      Status   West      Status
-------------------------------------------------------------------------------
1       N/A        Idle        Non-Owner  eth-0-9   Forward  eth-0-20  Forward

Control Vlan     : 100
MD Name          : md1
Service Id       : ma1
Protect Instance : 1
Current Event    : NR-RB
Hold-off Timer   : 0 (msecs)
Guard Timer      : 500 (msecs)
-------------------------------------------------------------------------------
```

7 Configuring UDLD

7.1 Overview

The Unidirectional Link Detection protocol is a light-weight protocol that can be used to detect and disable one-way connections before they create dangerous situations such as Spanning Tree loops or other protocol malfunctions.

7.2 Topology

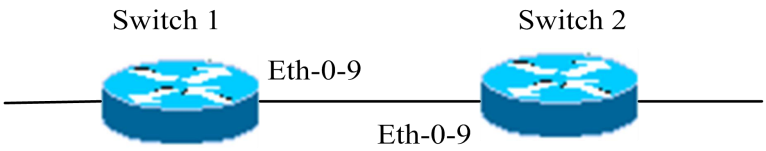


Figure 1-7 Typical topology of UDLD

7.3 Configuration

Switch 1

Enable UDLD for interface eth-0-9 of switch 1.

Switch#configure terminal	Enter the Configure mode
Switch (config)#interface eth-0-9	Enter the Interface mode
Switch (config-if)#no shutdown	Make interface up
Switch (config-if)#udld port	Enable UDLD on the interface
Switch (config-if)# exit	Exit the Interface mode
Switch (config)# udld enable	Enter UDLD globally

Switch (config)# udld message interval 10	Set UDLD message interval

Switch 2

Enable UDLD for interface eth-0-9 of switch 2.

Switch#configure terminal	Enter the Configure mode
Switch (config)#interface eth-0-9	Enter the Interface mode
Switch (config-if)#no shutdown	Make interface up
Switch (config-if)#udld port	Enable UDLD on the interface
Switch (config-if)# exit	Exit the Interface mode
Switch (config)# udld enable	Enter UDLD globally
Switch (config)# udld message interval 10	Set UDLD message interval

7.4 Validation

Switch 1

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode       : normal
Operation state : Bidirectional
Message interval: 10
Message timeout : 3

  Neighbor 1
  ---
  Device ID       : 4c7b.8510.ab00
  Port ID         : eth-0-9
  Device Name     : Switch
  Message interval: 10
  Message timeout : 3
  Link Status     : bidirectional
Expiration time : 29
```

Switch 2

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode       : normal
```

```
Operation state : Bidirectional
Message interval: 10
Message timeout : 3

  Neighbor 1
  ---
  Device ID       : 28bc.83db.8400
  Port ID         : eth-0-9
  Device Name     : Switch
  Message interval: 10
  Message timeout : 3
  Link Status     : bidirectional
  Expiration time : 23
```

8 Configuring ERPS

8.1 Overview

ERPS technology increases the availability and robustness of Ethernet rings. In the event that a fiber cut occurs, ERPS converges in less than one second, often in less than 50 milliseconds.

The main idea is described as the following. ERPS operates by declaring an ERPS domain on a single ring. On that ring domain, one switch, or node, is designated the master node, while all other nodes are designated as transit nodes. One port of the master node is designated as the master node's primary port to the ring; another port is designated as the master node's secondary port to the ring. In normal operation, the master node blocks the secondary port for all non-ERPS traffic belonging to this ERPS domain, thereby avoiding a loop in the ring. Keep-alive messages are sent by the master node in a pre-set time interval. Transit nodes in the ring domain will forward the ERPS messages. Once a link failure event occurs, the master node will detect this either by receiving the link-down message sent by the node adjacent to the failed link or by the timeout of the keep-alive message. After link failure is detected, master node will open the secondary port for data traffic to re-route the traffic.

8.2 References

The ERPS module is based on the following RFC.

RFC 3619

ERPS is a soft-state protocol. The main requirement is to enable ERPS on desired devices, and configure the ERPS information correctly for various network topologies.

This section provides ERPS configuration examples for their typical network topologies.

NOTE

For details on the commands used in the following examples, refer to the ERPS Command Reference.

8.3 Configuring ERPS for a Single-Ring Topology

Configure same ERPS domain and ring at switch 1, switch 2 and switch 3. Switch 1 is configured as ERPS master node and other two switches are configured as ERPS transit nodes. Interface agg11, which has two members called eth-0-9 and eth-0-10, is configured as primary interface at switch 1 and eth-0-13 is configured as secondary interface.

NOTE

The ports accessing an ERPS ring must be configured as trunk ports, permitting the traffic of data VLANs to pass through. If The switch is enabled stacking, the port of ERPS ring should not on slave stacking device.

The ports accessing an ERPS ring must be configured as the members of the control VLAN, allowing the ERPS packets to be sent and received.

STP on ports accessing ERPS rings must be disabled.

Only one node can be configured as master node.

Control VLAN must not be configured as Layer 3 interface.

VLAN mapping must not be enabled on the ERPS ports.

Native VLAN of a port accessing an ERPS ring must not be set as the primary control VLAN or the secondary control VLAN.

8.3.1 Topology

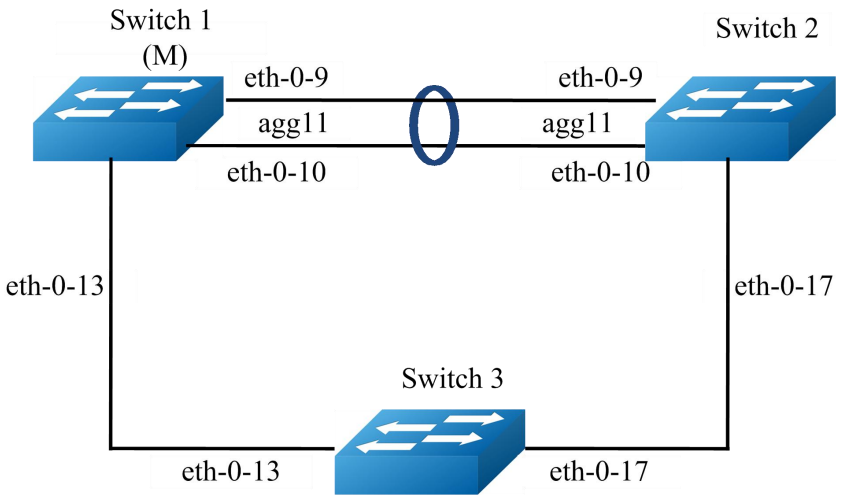


Figure 1-8 ERPS Topology

8.3.2 Configurations

Switch 1

Create VLAN for transferring ERPS control packets.

Switch# configure terminal	Enter the configure mode
Switch(config)# vlan database	Enter VLAN database mode
Switch(config-vlan)# vlan 15	Create vlan 15
Switch(config-vlan)# exit	Exit the vlan mode and enter the Configure mode

Configure interface agg11.

Switch(config)# interface eth-0-9	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port

Switch(config-if)# static-channel-group 11	Add this interface to a static channel group 11 and enable link aggregation so that it can be selected for aggregation by the local system
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode
Switch(config)# interface eth-0-10	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port
Switch(config-if)# static-channel-group 11	Add this interface to a static channel group 11 and enable link aggregation so that it can be selected for aggregation by the local system
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode
Switch(config)# interface agg11	Enter the Interface mode
Switch(config-if)# spanning-tree port disable	Disable spanning-tree on port

Configure interface eth-0-13.

Switch(config)# interface eth-0-13	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port
Switch(config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode.

Configure and enable ERPS domain.

Switch(config)# erps 11	Create erps domain with id 11
Switch(config)# erps 11 primary control vlan 15	Set vlan 15 as the primary control vlan of erps domain 11
Switch(config)# erps 11 mstp instance 0	Protect instance 0

Switch(config)# erps 11 ring 1 level primary	Create an erps primary ring 1 for domain 11
Switch(config)# erps 11 ring 1 mode master	Set node as master of ring 1 for domain 11
Switch(config)# erps 11 ring 1 primary interface agg11	Set primary interface of ring 1 for domain 11
Switch(config)# erps 11 ring 1 secondary interface eth-0-13	Set secondary interface of ring 1 for domain 11
Switch(config)# erps 11 ring 1 enable	Enable ring 1 for domain 11
Switch(config)# erps 11 enable	Enable domain 11

Switch 2

Create VLAN for transferring ERPS control packets.

Switch# configure terminal	Enter the configure mode
Switch(config)# vlan database	Enter VLAN database mode
Switch(config-vlan)# vlan 15	Create vlan 15
Switch(config-vlan)# exit	Exit the vlan mode and enter the Configure mode

Configure interface agg11.

Switch(config)# interface eth-0-9	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port
Switch(config-if)# static-channel-group 11	Add this interface to a static channel group 11 and enable link aggregation so that it can be selected for aggregation by the local system
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode
Switch(config)# interface eth-0-10	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode

Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port.
Switch(config-if)# static-channel-group 11	Add this interface to a static channel group 11 and enable link aggregation so that it can be selected for aggregation by the local system
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode
Switch(config)# interface agg11	Enter the Interface mode.
Switch(config-if)# spanning-tree port disable	Disable spanning-tree on port

Configure interface eth-0-17.

Switch(config)# interface eth-0-17	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port.
Switch(config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure and enable ERPS domain.

Switch(config)# erps 11	Create erps domain with id 11
Switch(config)# erps 11 primary control vlan 15	Set vlan 15 as the primary control vlan of erps domain 11
Switch(config)# erps 11 mstp instance 0	Protect instance 0
Switch(config)# erps 11 ring 1 level primary	Create an erps primary ring 1 for domain 11
Switch(config)# erps 11 ring 1 mode transit	Set node as transit of ring 1 for domain 11
Switch(config)# erps 11 ring 1 primary interface agg11	Set primary interface of ring 1 for domain 11
Switch(config)# erps 11 ring 1 secondary interface eth-0-17	Set secondary interface of ring 1 for domain 11
Switch(config)# erps 11 ring 1 enable	Enable ring 1 for domain 11
Switch(config)# erps 11 enable	Enable domain 11

Switch 3

Create VLAN for transferring ERPS control packets.

Switch# configure terminal	Enter the configure mode
Switch(config)# vlan database	Enter VLAN database mode
Switch(config-vlan)# vlan 15	Create vlan 15
Switch(config-vlan)# exit	Exit the vlan mode and enter the Configure mode

Configure interface eth-0-17.

Switch(config)# interface eth-0-17	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port.
Switch(config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure interface eth-0-13.

Switch(config)# interface eth-0-13	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 15	Enable VLAN 15 on this port
Switch(config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure and enable ERPS domain.

Switch(config)# erps 11	Create erps domain with id 11

Switch(config)# erps 11 primary control vlan 15	Set vlan 15 as the primary control vlan of erps domain 11
Switch(config)# erps 11 mstp instance 0	Protect instance 0
Switch(config)# erps 11 ring 1 level primary	Create an erps primary ring 1 for domain 11
Switch(config)# erps 11ring 1 mode transit	Set node as transit of ring 1 for domain 11
Switch(config)# erps 11 ring 1 primary interface eth-0-17	Set primary interface of ring 1 for domain 11
Switch(config)# erps 11 ring 1 secondary interface eth-0-13	Set secondary interface of ring 1 for domain 11
Switch(config)# erps 11 ring 1 enable	Enable ring 1 for domain 11
Switch(config)# erps 11 enable	Enable domain 11

8.3.3 Validation

Switch 1

```
Switch# show erps 11
ERPS domain ID: 11
ERPS domain name: ERPS0011
ERPS domain primary control VLAN ID: 15
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: master
ERPS ring 1 node state: complete
ERPS ring 1 primary interface name: agg11          state:unblock
ERPS ring 1 secondary interface name: eth-0-13     state:block
ERPS ring 1 stats:
Sent:
  total packets:51
  hello packets:47                    ring-up-flush-fdb packets:2
  ring-down-flush-fdb packets:2       link-down packets:0
  edge-hello packets:0                major-fault packets:0
Received:
  total packets:21
  hello packets:21                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0       link-down packets:0
  edge-hello packets:0                major-fault packets:0
```

Switch 2

```
Switch#show erps 11
ERPS domain ID: 11
ERPS domain name: ERPS0011
```

```
ERPS domain primary control VLAN ID: 15
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: agg11          state:unblock
ERPS ring 1 secondary interface name: eth-0-17     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:114
  hello packets:113                  ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
```

Switch 3

```
Switch# show erps 11
ERPS domain ID: 11
ERPS domain name: ERPS0011
ERPS domain primary control VLAN ID: 15
ERPS domain sub control VLAN ID: 0
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: eth-0-17       state:unblock
ERPS ring 1 secondary interface name: eth-0-13     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:130
  hello packets:129                  ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
```

8.4 Configuring a Intersecting-Ring Topology

Configure same ERPS domain at switch 1, switch 2, switch 3 and switch 4. Switch 1, switch 2 and switch 3 consist of ERPS primary ring 1 while switch 2, switch3 and switch 4 consist of ERPS sub ring 2. Switch 1 is configured as ERPS ring 1 master node and other two switches are configured as ERPS transit nodes while switch 4 is configured as ERPS ring 2 master node. In addition switch 2 is configured as edge node and switch 3 is configured as assistant-edge node.

The ports accessing an ERPS ring must be configured as trunk ports, permitting the traffic of data VLANs to pass through.

The ports accessing an ERPS ring must be configured as the members of the control VLAN, allowing the ERPS packets to be sent and received.

STP on ports accessing ERPS rings must be disabled.

Only one primary ring is allowed to be configured for each domain.

The edge/assistant-edge node of the sub rings must be the intersecting nodes for two rings.

The edge/assistant-edge node of the sub rings must be transit node.

The common interface must be the intersecting interface for two rings.

The edge interface must belong to only one sub ring.

Primary and sub rings must only be coexisted in edge/assistant nodes.

Primary ring must be Created and enabled prior to sub rings.

Sub rings must be disabled and removed before primary ring.

One switch can only work as master node for a ring and transit node for the other rings within the same domain.

8.4.1 Topology

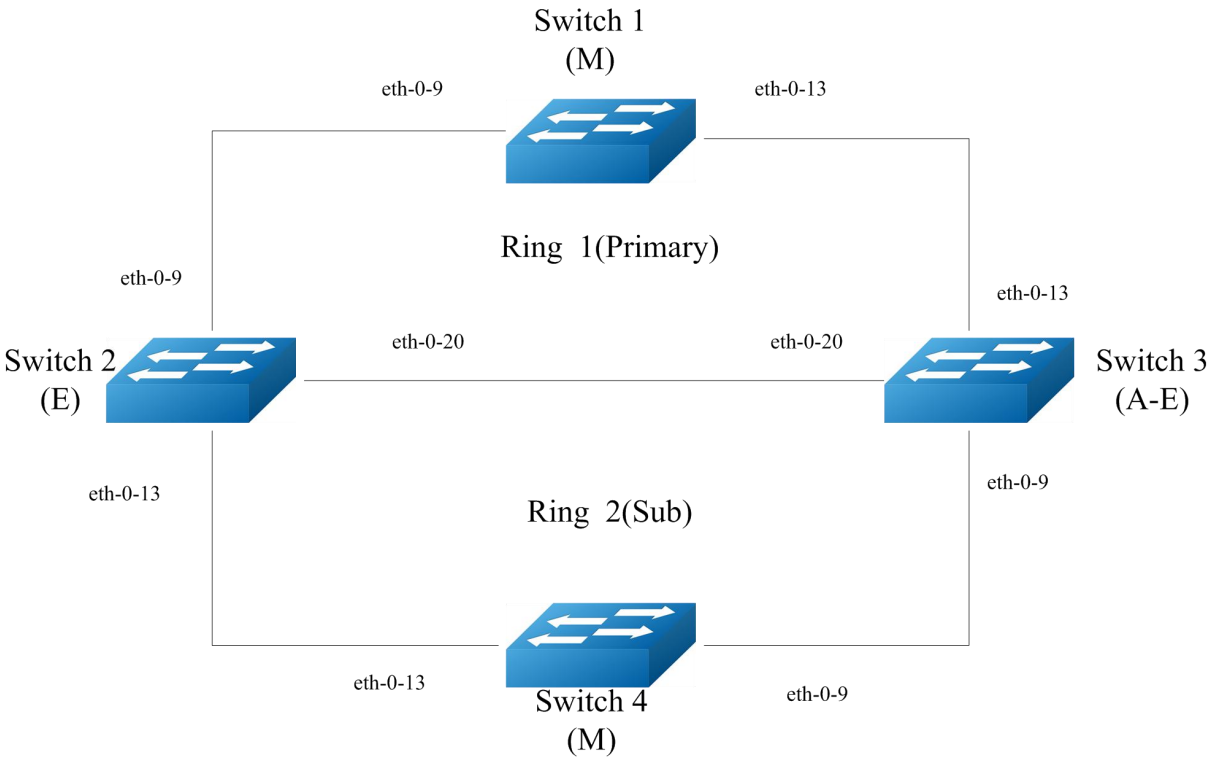


Figure 1-9 Single-Domain Intersecting-Ring Topology

8.4.2 Configurations

Switch 1

Create VLANs for transferring ERPS control packets.

Switch# configure terminal	Enter the configure mode
Switch(config)# vlan database	Enter VLAN database mode
Switch(config-vlan)# vlan 11,12	Create vlan 11, 12
Switch(config-vlan)# exit	Exit the vlan mode and enter the Configure mode

Configure interface eth-0-9.

Switch(config)# interface eth-0-9	Enter the Interface mode

Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch(config-if)# switchport trunk allowed vlan add 11,12	Enable VLAN 11, 12 on this port
Switch(config-if)# spanning-tree port disable	Disable spanning-tree on por
Switch(config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure interface eth-0-13.

Switch(config)# interface eth-0-13	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 11,12	Enable VLAN 11, 12 on this port
Switch (config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure and enable ERPS domain.

Switch (config)# erps 1	Create erps domain with id 1
Switch (config)# erps 1 primary control vlan 11	Set vlan 11 as the primary control vlan of erps domain 1
Switch (config)# erps 1 sub control vlan 12	Set vlan 12 as the sub control vlan of erps domain 1
Switch(config)# erps 1 mstp instance 0	Protect instance 0
Switch (config)# erps 1 ring 1 level primary	Create an erps primary ring 1 for domain 1
Switch (config)# erps 1 ring 1 mode master	Set node as master of ring 1 for domain 1
Switch (config)# erps 1 ring 1 primary interface eth-0-9	Set primary interface of ring 1 for domain 1
Switch (config)# erps 1 ring 1 secondary interface eth-0-13	Set secondary interface of ring 1 for domain 1
Switch (config)# erps 1 ring 1 enable	Enable ring 1 for domain 1
Switch (config)# erps 1 enable	Enable domain 1

Switch 2

Create VLANs for transferring ERPS control packets.

Switch# configure terminal	Enter the configure mode
Switch (config)# vlan database	Enter VLAN database mode
Switch (config-vlan)# vlan 11,12	Create vlan 11, 12
Switch (config-vlan)# exit	Exit the vlan mode and enter the Configure mode

Configure interface eth-0-9.

Switch (config)# interface eth-0-9	Enter the Interface mode
Switch (config-if)# no shutdown	Turn up the interface
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 11,12	Enable VLAN 11, 12 on this port
Switch (config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure interface eth-0-20.

Switch(config)# interface eth-0-20	Enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 11,12	Enable VLAN 11, 12 on this port
Switch (config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch (config-vlan) # exit	Exit the interface mode and enter the Configure mode

Configure interface eth-0-13.

Switch (config)# interface eth-0-13	Enter the Interface mode
Switch (config-if)# no shutdown	Turn up the interface
Switch (config-if)# spanning-tree port disable	Disable spanning tree
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 12	Enable VLAN 12 on this port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure and enable ERPS domain.

Switch (config)# erps 1	Create erps domain with id 1
Switch (config)# erps 1 primary control vlan 11	Set vlan 11 as the primary control vlan of erps domain 1
Switch (config)# erps 1 sub control vlan 12	Set vlan 11 as the sub control vlan of erps domain 1
Switch(config)# erps 1 mstp instance 0	Protect instance 0
Switch (config)# erps 1 ring 1 level primary	Create an erps primary ring 1 for domain 1
Switch (config)# erps 1 ring 1 mode transit	Set node as transit of ring 1 for domain 1
Switch (config)# erps 1 ring 1 primary interface eth-0-9	Set primary interface of ring 1 for domain 1
Switch (config)# erps 1 ring 1 secondary interface eth-0-20	Set secondary interface of ring 1 for domain 1
Switch (config)# erps 1 ring 1 enable	Enable ring 1 for domain 1
Switch (config)# erps 1 ring 2 level sub	Create an erps sub ring 2 for domain 1
Switch (config)# erps 1 ring 2 edge-mode edge	Set edge-mode of ring 2 for domain 1
Switch (config)# erps 1 ring 2 edge interface eth-0-13	Set edge interface of ring 2 for domain 1
Switch (config)# erps 1 ring 2 common interface eth-0-20	Set common interface of ring 2 for domain 1
Switch (config)# erps 1 ring 2 srpt disable	Disable sprit of ring 2 for domain 1
Switch (config)# erps 1 ring 2 enable	Enable ring 2 for domain 1
Switch (config)# erps 1 enable	Enable domain 1

Switch 3

Create VLANs for transferring ERPS control packets.

Switch# configure terminal	Enter the configure mode
Switch (config)# vlan database	Enter VLAN database mode
Switch (config-vlan)# vlan 11,12	Create vlan 11, 12
Switch (config-vlan)# exit	Exit the vlan mode and enter the Configure mode

Configure interface eth-0-9.

Switch (config)# interface eth-0-9	Enter the Interface mode
Switch (config-if)# no shutdown	Turn up the interface
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 12	Enable VLAN 12 on this port
Switch (config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure interface eth-0-20.

Switch (config)# interface eth-0-20	Enter the Interface mode
Switch (config-if)# no shutdown	Turn up the interface
Switch (config-if)# spanning-tree port disable	Disable spanning tree
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 11,12	Enable VLAN 11, 12 on this port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure interface eth-0-13.

Switch (config)# interface eth-0-13	Enter the Interface mode
Switch (config-if)# no shutdown	Turn up the interface
Switch (config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 11,12	Enable VLAN 11, 12 on this port
Switch (config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure and enable ERPS domain

Switch (config)# erps 1	Create erps domain with id 1
Switch (config)# erps 1 primary control vlan 11	Set vlan 11 as the primary control vlan of erps domain 1
Switch (config)# erps 1 sub control vlan 12	Set vlan 11 as the sub control vlan of erps domain 1
Switch(config)# erps 1 mstp instance 0	Protect instance 0
Switch (config)# erps 1 ring 1 level primary	Create an erps primary ring 1 for domain 1
Switch (config)# erps 1 ring 1 mode transit	Set node as transit of ring 1 for domain 1
Switch (config)# erps 1 ring 1 primary interface eth-0-13	Set primary interface of ring 1 for domain 1
Switch (config)# erps 1 ring 1 secondary interface eth-0-20	Set secondary interface of ring 1 for domain 1
Switch (config)# erps 1 ring 1 enable	Enable ring 1 for domain 1
Switch (config)# erps 1 ring 2 level sub	Set level sub of ring 2 for domain 1
Switch (config)# erps 1 ring 2 edge-mode assistant-edge	Set edge-mode of ring 2 for domain 1
Switch (config)# erps 1 ring 2 edge interface eth-0-9	Set edge interface of ring 2 for domain 1
Switch (config)# erps 1 ring 2 common interface eth-0-20	Set common interface of ring 2 for domain 1
Switch (config)# erps 1 ring 2 enable	Enable ring 2 for domain 1
Switch (config)# erps 1 enable	Enable domain 1

Switch 4

Create VLANs for transferring ERPS control packets.

Switch# configure terminal	Enter the configure mode
Switch (config)# vlan database	Enter VLAN database mode
Switch (config-vlan)# vlan 12	Create vlan 12
Switch (config-vlan)# exit	Exit the vlan mode and enter the Configure mode

Configure interface eth-0-9

Switch (config)# interface eth-0-9	Enter the Interface mode
Switch (config-if)# no shutdown	Turn up the interface
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 12	Enable VLAN 12 on this port
Switch (config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure interface eth-0-13

Switch (config)# interface eth-0-13	Enter the Interface mode
Switch (config-if)# no shutdown	Turn up the interface
Switch (config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch (config-if)# switchport trunk allowed vlan add 12	Enable VLAN 12 on this port
Switch (config-if)# spanning-tree port disable	Disable spanning-tree on port
Switch (config-vlan)# exit	Exit the interface mode and enter the Configure mode

Configure and enable ERPS domain.

Switch (config)# erps 1	Create erps domain with id 1
Switch (config)# erps 1 sub control vlan 12	Set vlan 12 as the sub control vlan of erps domain 1
Switch(config)# erps 1 mstp instance 0	Protect instance 0
Switch (config)# erps 1 ring 2 level sub	Create an erps sub ring 2 for domain 1
Switch (config)# erps 1 ring 2 mode master	Set node as master of ring 2 for domain 1
Switch (config)# erps 1 ring 2 primary interface eth-0-9	Set primary interface of ring 2 for domain 1
Switch (config)# erps 1 ring 2 secondary interface eth-0-13	Set secondary interface of ring 2 for domain 1
Switch (config)# erps 1 ring 2 enable	Enable ring 2 for domain 1
Switch (config)# erps 1 enable	Enable domain 1

8.4.3 Validation

Switch 1

```
Switch # show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain primary control VLAN ID: 11
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: master
ERPS ring 1 node state: complete
ERPS ring 1 primary interface name: eth-0-9        state:unblock
ERPS ring 1 secondary interface name: eth-0-13     state:block
ERPS ring 1 stats:
Sent:
  total packets:1310
  hello packets:1303                ring-up-flush-fdb packets:3
  ring-down-flush-fdb packets:4     link-down packets:0
  edge-hello packets:0              major-fault packets:0
Received:
  total packets:921
  hello packets:921                 ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0     link-down packets:0
  edge-hello packets:0              major-fault packets:0
```

Switch 2

```
Switch # show erps 1
```

```
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain primary control VLAN ID: 11
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: eth-0-9        state:unblock
ERPS ring 1 secondary interface name: eth-0-20     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:988
  hello packets:985                  ring-up-flush-fdb packets:2
  ring-down-flush-fdb packets:1      link-down packets:0
  edge-hello packets:0               major-fault packets:0
ERPS ring ID: 2
ERPS ring level: sub
ERPS ring 2 node mode: transit
ERPS ring 2 edge node mode: edge
ERPS ring 2 node state: link up
ERPS ring 2 edge interface name: eth-0-13       state: unblock
ERPS ring 2 common interface name: eth-0-20     state: unblock
EPRS ring 2 SRPT is disabled
ERPS ring 2 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:858
  hello packets:856                  ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:1      link-down packets:0
  edge-hello packets:0               major-fault packets:0
```

Switch 3

```
Switch # show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain primary control VLAN ID: 11
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS ring ID: 1
ERPS ring level: primary
ERPS ring 1 node mode: transit
```

```
ERPS ring 1 node state: link up
ERPS ring 1 primary interface name: eth-0-13       state:unblock
ERPS ring 1 secondary interface name: eth-0-20     state:unblock
ERPS ring 1 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:645
  hello packets:644                  ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
ERPS ring ID: 2
ERPS ring level: sub
ERPS ring 2 node mode: transit
ERPS ring 2 edge node mode: assistant edge
ERPS ring 2 node state: link up
ERPS ring 2 edge interface name: eth-0-9        state: unblock
ERPS ring 2 common interface name: eth-0-20     state: unblock
ERPS ring 2 stats:
Sent:
  total packets:0
  hello packets:0                    ring-up-flush-fdb packets:0
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
  total packets:645
  hello packets:644                  ring-up-flush-fdb packets:1
  ring-down-flush-fdb packets:0      link-down packets:0
  edge-hello packets:0               major-fault packets:0
```

Switch 4

```
Switch# show erps 1
ERPS domain ID: 1
ERPS domain name: ERPS001
ERPS domain primary control VLAN ID: 0
ERPS domain sub control VLAN ID: 12
ERPS domain hello timer interval: 1 second(s)
ERPS domain fail timer interval: 3 second(s)
ERPS ring ID: 2
ERPS ring level: sub
ERPS ring 2 node mode: master
ERPS ring 2 node state: complete
ERPS ring 2 primary interface name: eth-0-9        state:unblock
ERPS ring 2 secondary interface name: eth-0-13     state:block
ERPS ring 2 stats:
Sent:
  total packets:814
  hello packets:810                  ring-up-flush-fdb packets:2
  ring-down-flush-fdb packets:2      link-down packets:0
  edge-hello packets:0               major-fault packets:0
Received:
```

```
total packets:774
hello packets:774                    ring-up-flush-fdb packets:0
ring-down-flush-fdb packets:0        link-down packets:0
edge-hello packets:0                 major-fault packets:0
```

9 Configuring Smart Link

9.1 Overview

The Smart Link is a simple but practical technology of fast link protection. It is a solution specific to dual uplink networking to fulfill redundancy and fast migration of active and standby links.

Every smart-link group is included a pair of a layer 2 interfaces where one interface is configured to act as a standby to the other. The feature provides an alternative solution to the STP. Users can disable STP and still retain basic link redundancy. The feature also support load-balancing so than both interfaces simultaneously forward the traffic.

9.2 Topology

The following figure is a typical smart-link application. The Switch1 and Switch2 are configured smart-link group. Switch3, Switch4 and Switch5 are configured smart-link flush receiver.

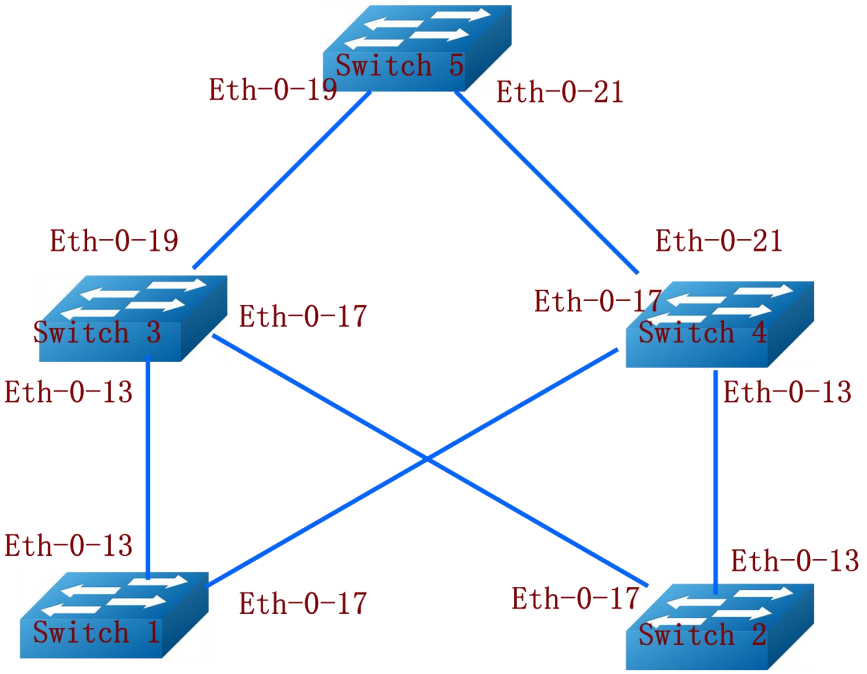


Figure 1-10 Smart-Link Typical Topology

9.3 Configuration

To configure smart-link group, some configuration should be configured before it.

- VLANs should be configured.
- MSTP instance should be configured.
- Spanning-tree should be disabled in the interface.
- About above configurations, please see the related references.

Switch 1

Switch1# configure terminal	Enter globle configuration mode
Switch1(config)# vlan database	Enter VLAN database
Switch1(config- vlan)# vlan 2-20	Configure VLAN 2-20
Switch1(config- vlan)# exit	Exit VLAN database
Switch1(config)# spanning-tree mode mstp	Configure a spanning-tree mode

Switch1(config)# spanning-tree mst configuration	Enter the Multiple Spanning Tree configuration mode
Switch1(config-mst)# instance 1 vlan 1	Create an instance of vlan
Switch1(config-mst)# instance 2 vlan 2	Create an instance of vlan
Switch1(config-mst)# instance 3 vlan 3	Create an instance of vlan
Switch1(config-mst)# exit	Exit the Multiple Spanning Tree configuration mode
Switch1(config)# interface eth-0-13	To enter interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan all	Enable all Vlan on this port
Switch1(config-if)# spanning-tree port disable	Set STP disable on this port
Switch1(config-if)# no shutdown	Turn up the interface
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# interface eth-0-17	To enter interface mode
Switch1(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch1(config-if)# switchport trunk allowed vlan all	Enable all Vlan on this port
Switch1(config-if)# no shutdown	Turn up the interface
Switch1(config-if)# spanning-tree port disable	Set STP disable on this port
Switch1(config-if)# exit	Exit interface mode
Switch1(config)# smart-link group 1	Create smart-link group and enter smart-link group configuration mode
Switch1(config-smlk-group)# interface eth-0-13 master	Add master interface. The interface should be physical (i.e. eth-0-1) or aggregator (i.e. agg1) switch interface
Switch1(config-smlk-group)# interface eth-0-17 slave	Add slave interface. The interface should be physical (i.e. eth-0-2) or aggregator (i.e. agg2) switch interface
Switch1(config-smlk-group)# protected mstp instance 1	Set protected MSTP instance to the smart-link group
Switch1(config-smlk-group)# protected mstp instance 2	Set protected MSTP instance to the smart-link group
Switch1(config-smlk-group)# protected mstp instance 3	Set protected MSTP instance to the smart-link group
Switch1(config-smlk-group)# load-balance instance 3	Enable load-balance on Instance

Switch1(config-smlk-group)# restore time 40	(optional) Set restore time of the smart-link group. The range of restore-time is 30 to 1200 seconds
Switch1(config-smlk-group)# restore enable	(optional) Enable the restoring feature of the smart-link group. If load-balancing instance is configured, this feature is recommended strongly
Switch1(config-smlk-group)# flush send control-vlan 10 password simple test	(optional)Set the flush packet sender in the smart-link group. Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose. PASSWORD is simple password of the flush packet, and the length is 1 to 15
Switch1(config-smlk-group)# group enable	Enable the smart-link group
Switch1(config-smlk-group)# end	Exit smart-link mode

Configuration of Switch 2 is the same with Switch 1.

Switch 3

Switch3# configure terminal	Enter globle configuration mode
Switch3(config)# interface eth-0-13	To enter interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch3(config-if)# no shutdown	Turn up the interface
Switch3(config-if)# switchport trunk allowed vlan all	Enable all Vlan on this port
Switch3(config-if)# smart-link flush receive control-vlan 10 password simple test	(optional)Set the flush packet sender in the smart-link group. Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose. PASSWORD is simple password of the flush packet, and the length is 1 to 15
Switch3(config-if)# exit	Exit interface mode
Switch3(config)# interface eth-0-17	To enter interface mode
Switch3(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode

Switch3(config-if)# switchport trunk allowed vlan all	Enable all Vlan on this port
Switch3(config-if)# no shutdown	Turn up the interface
Switch3(config-if)# smart-link flush receive control-vlan 10 password simple test	(optional)Set the flush packet sender in the smart-link group. Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose. PASSWORD is simple password of the flush packet, and the length is 1 to 15
Switch3 (config-if)# exit	Exit interface mode

Configuration of Switch 4 is the same with Switch 3.

Switch 5

Switch5# configure terminal	Enter globle configuration mode
Switch5(config)# interface eth-0-19	To enter interface mode
Switch5(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch5(config-if)# switchport trunk allowed vlan all	Enable all Vlan on this port
Switch5(config-if)# no shutdown	Turn up the interface
Switch5(config-if)# smart-link flush receive control-vlan 10 password simple test	(optional)Set the flush packet sender in the smart-link group. Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose. PASSWORD is simple password of the flush packet, and the length is 1 to 15
Switch5(config-if)# exit	Exit interface mode
Switch5(config)# interface eth-0-21	To enter interface mode
Switch5(config-if)# switchport mode trunk	Set the switching characteristics of this interface to trunk mode
Switch5(config-if)# no shutdown	Turn up the interface
Switch5(config-if)# switchport trunk allowed vlan all	Enable all Vlan on this port

smart-link flush receive control-vlan 10 password simple test	(optional)Set the flush packet sender in the smart-link group. Mac address-table should be updated when a master (forwarding) link goes down and the slave link begins forwarding traffic. Flush packet is used for this purpose. PASSWORD is simple password of the flush packet, and the length is 1 to 15
Switch5(config-if)# exit	Exitinterface mode
Switch5(config)# no smart-link relay enable	Disable the relay function

9.4 Validation

Switch 1

```
Switch1# show smart-link group 1
Smart-link group 1 information:
 The smart-link group was enabled.
 ============================================================
 Auto-restore:
   state       time            count    Last-time
   enabled      40               0      N/A
 ============================================================
 Protected instance: 1  2  3
 Load balance instance: 3
 Flush sender , Control-vlan ID: 10    Password:test
 ============================================================
 INTERFACE:
 Role   Member    DownCount Last-Down-Time  FlushCount Last-Flush-Time
 MASTER eth-0-13    0       N/A                  0     N/A
 SLAVE  eth-0-17    0       N/A                  0     N/A
 ============================================================
 Instance states in the member interfaces:
   A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
 Map-instance-ID   MASTER(eth-0-13)    SLAVE(eth-0-17)
       1              A                  B
       2              A                  B
       3              B                  A
```

Switch 2

```
Switch2# show smart-link group 1
Smart-link group 1 information:
 The smart-link group was enabled.
 ============================================================
 Auto-restore:
   state       time            count    Last-time
```

```
  enabled      40               0      N/A
============================================================
Protected instance: 1  2  3
Load balance instance: 3
Flush sender , Control-vlan ID: 10    Password:test
============================================================
INTERFACE:
Role   Member    DownCount Last-Down-Time  FlushCount Last-Flush-Time
MASTER eth-0-13    0       N/A                  0     N/A
SLAVE  eth-0-17    0       N/A                  0     N/A
============================================================
Instance states in the member interfaces:
  A - ACTIVE ,   B -BLOCK  , D-The interface is link-down
Map-instance-ID   MASTER(eth-0-13)    SLAVE(eth-0-17)
      1              A                  B
      2              A                  B
      3              B                  A
```

Switch 3

```
Switch3# show smart-link
 Relay smart-link flush packet is enabled
 Smart-link flush receiver interface:
    eth-0-13   control-vlan:10   password:test
    eth-0-17   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

Switch 4

```
Switch4# show smart-link
 Relay smart-link flush packet is enabled
 Smart-link flush receiver interface:
    eth-0-13   control-vlan:10   password:test
    eth-0-17   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

Switch 5

```
Switch5# show smart-link
 Relay smart-link flush packet is disabled
 Smart-link flush receiver interface:
    eth-0-21   control-vlan:10   password: test
    eth-0-19   control-vlan:10   password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
 Smart link Group Number is 0.
```

10 Configuring Monitor Link

10.1 Overview

Monitor Link is a port collaboration function. Monitor Link usually works together with Layer 2 topology protocols. The idea is to monitor the states of uplink ports and adapt the up/down state of downlink ports to the up/down state of uplink ports, triggering link switchover on the downstream switch in time.

10.2 Topology

This chapter will descript how to configure Monitor link group.

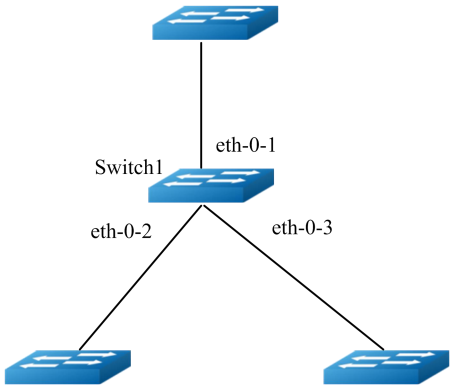


Figure 1-11 Configure monitor link

10.3 Configuration

Switch1#configure terminal	Enter the Configure mode
Switch1(config)# interface range eth-0-1 - 3	Enter the Interface range mode
Switch1(config-if-range)# no shutdown	Configure the port up

Switch1(config-if-range)# exit	Exit the Interface range mode and enter the Configure mode
Switch1(config)# monitor-link group 1	Create monitor link group 1.
Switch1(config-mtlk-group)# monitor-link uplink interface eth-0-1	Configure eth0-0-1 as uplink of monitor link group
Switch1(config-mtlk-group)# monitor-link downlink interface eth-0-2	Configure eth0-0-2 as downlink of monitor link group
Switch1(config-mtlk-group)# monitor-link downlink interface eth-0-3	Configure eth0-0-3 as downlink of monitor link group
Switch1(config-mtlk-group)# end	Exit the monitor link config mode and enter the Configure mode

10.4 Validation

```
Switch1# show monitor-link group
Group Id: 1
Monitor link status: UP
Role     Member   Last-up-time     Last-down-time          upcount   downcount
UpLk 1   eth-0-1  2011/07/15,02:07:31  2011/07/15,02:07:31     2         1
DwLk 1   eth-0-2  2011/07/15,02:07:34  2011/07/15,02:07:31     1         1
DwLk 2   eth-0-3  N/A                      N/A                        0         0
```

11 Configuring VRRP

11.1 Overview

This chapter provides an overview of Virtual Router Redundancy Protocol (VRRP) and its implementation.

VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

11.2 References

The VRRP module is based on:

RFC 3768 (VRRP): Knight, S., et.al "Virtual Router Redundancy Protocol (VRRP)"

11.3 Terminology

- **Backup Router**: VRRP router that back up an IP address. It assumes forwarding responsibility for the virtual IP address if the Master fails.
- **Critical IP**: The IP address that the VRRP router send/receive messages on for a particular session.
- **IP Address Owner**: The VRRP Router that has the virtual router's IP address (es) as real interface address (es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, etc.

- **Master Router**: The VRRP router that owns the IP address (i.e., is being backed up), and which is the default router for forwarding for that IP address.
- **Virtual IP**: The IP address back up by a VRRP session.
- **Virtual Router**: A router managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP addresses across a common LAN. A VRRP Router might backup one or more virtual routers.
- **VRRP Router**: A router runs the Virtual Router Redundancy Protocol. It might participate in one or more virtual routers.

11.4 VRRP Process

Typically, end hosts are connected to the enterprise network through a single router (first hop router) that is in the same Local Area Network (LAN) segment. The most popular method of configuration for the end hosts is to statically configure this router as their default gateway. This minimizes configuration and processing overhead. The main problem with this configuration method is that it produces a single point of failure if this first hop router fails.

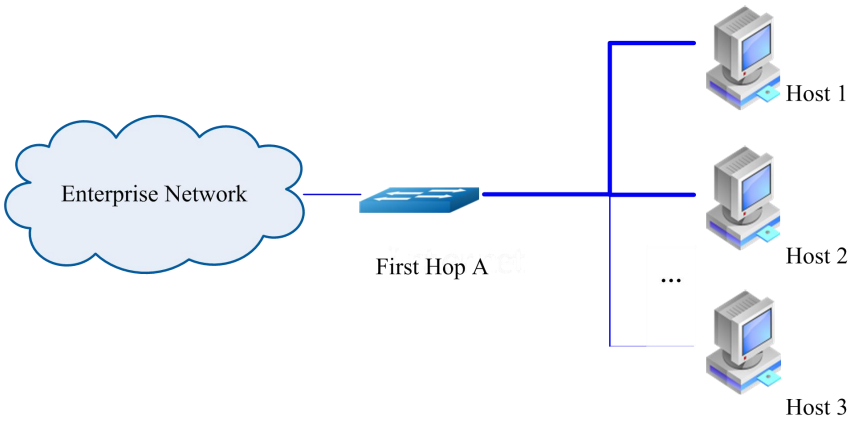


Figure 11-1 VRRP Process

The Virtual Router Redundancy Protocol attempts to solve this problem by introducing the concept of a virtual router, composed of two or more VRRP routers on the same subnet. The concept of a virtual IP address is also introduced, which is the address that end hosts configure as their default gateway. Only one router (called the master) forward packets on the behalf of

this IP address. In the event that the Master router fails, one of the other routers (Backup) assumes forwarding responsibility for it.

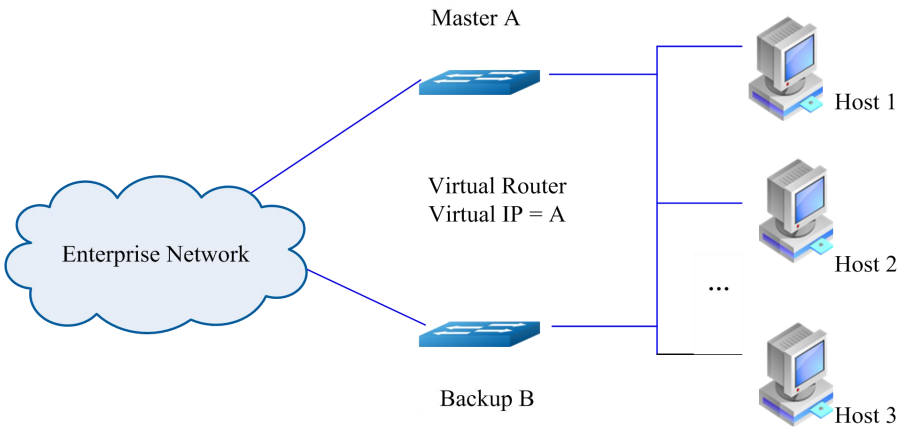


Figure 11-2 VRRP Protocol

At first glance, the configuration outlined in might not seem very useful, as it doubles the cost and leaves one router idle at all times. This, however, can be avoided by creating two virtual routers and splitting the traffic between them.

11.5 Limitations

MD5 authentication is not yet supported for VRRP.

11.6 Configuring VRRP (One Virtual Router)

In this configuration the end-hosts install a default route to the IP address of virtual router 1(VRID = 1) and both routers R1 and R2 run VRRP. R1 is configured to be the Master for virtual router 1 (VRID = 1) and R2 as a Backup for virtual router 1. If R1 fails, R2 will take over virtual router 1 and its IP addresses, and provide uninterrupted service for the hosts. Configuring only one virtual router, doubles the cost and leaves R2 idle at all times.

11.6.1 Topology

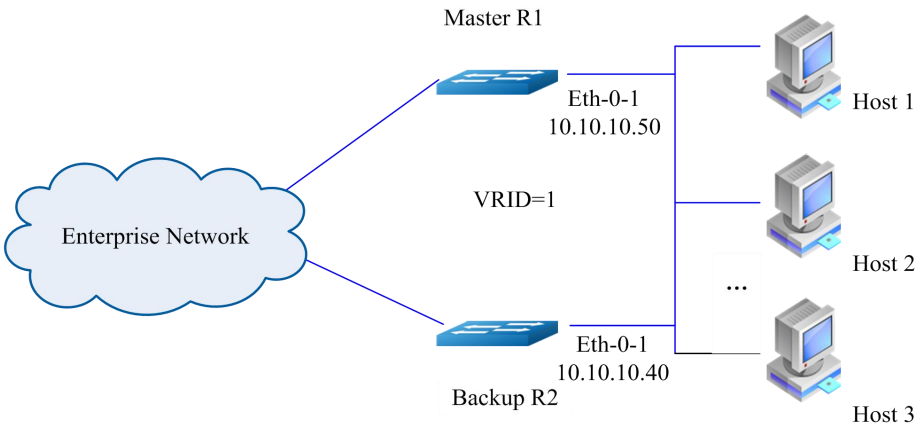


Figure 11-3 One VRRP Router

11.6.2 Configuration

R1

Switch # configure terminal	Enter the Configure mode.
Switch (config)#interface eth-0-1	Enters the interface configuration mode
Switch (config-if)#no switchport	Configure to layer3 interface
Switch (config-if)#ip address 10.10.10.50/24	Configure the IP address
Switch (config-if)#exit	Exit the interface configuration mode
Switch (config)#router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session.
Switch (config-router)#virtual-ip 10.10.10.50	Set the virtual IP address for the VRRP session.
Switch (config-router)#interface eth-0-1	Specify the physical interface that will participate in virtual routing.
Switch (config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable
Switch (config-router)# advertisement-interval 5	Configure the advertisement interval to 5 seconds.
Switch (config-router)# bfd 10.10.10.40	Configure the bfd session for VRRP instance
Switch (config-router)# enable	Enable the VRRP session on the router.

R2

Switch # configure terminal	Enter the Configure mode.
Switch (config)#interface eth-0-1	Enters the interface configuration mode
Switch (config-if)#no switchport	Configure to layer3 interface
Switch (config-if)#ip address 10.10.10.40/24	Configure the IP address
Switch (config-if)#exit	Exit the interface configuration mode
Switch (config)#router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session.
Switch (config-router)#virtual-ip 10.10.10.50	Set the virtual IP address for the VRRP session.
Switch (config-router)#interface eth-0-1	Specify the physical interface that will participate in virtual routing.
Switch (config-router)#priority 200	Configure the priority to 200 (less than 255) as R2 is the Backup router.
Switch (config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable
Switch (config-router)#advertisement-interval 5	Configure the advertisement interval to 5 seconds.
Switch (config-router)# bfd 10.10.10.50	Configure the bfd session for VRRP instance
Switch (config-router)# enable	Enable the VRRP session on the router.

11.7 Configuring VRRP (Two Virtual Router)

In the one virtual router example earlier, R2 is not backed up by R1. This example illustrates how to backup R2 by configuring a second virtual router.

In this configuration, R1 and R2 are two virtual routers and the hosts split their traffic between R1 and R2. R1 and R2 function as backups for each other.

11.7.1 Topology

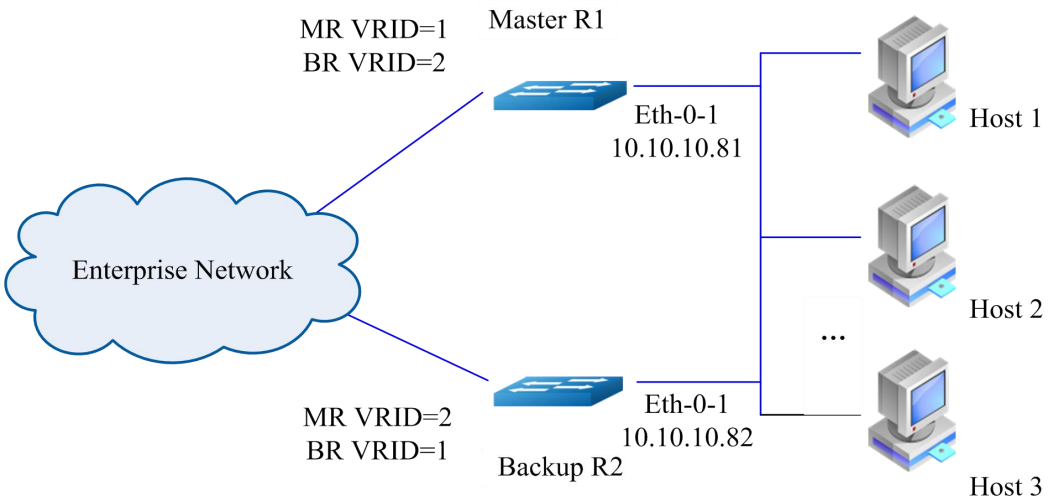


Figure 1-12 Two Virtual Router

11.7.2 Configuration

R1

Switch# configure terminal	Enter the Configure mode
Switch (config)# interface eth-0-1	Enters the interface configuration mode
Switch (config-if)# no switchport	Configure to layer3 interface
Switch (config-if)# ip address 10.10.10.81/24	Configure the IP address
Switch (config-if)# exit	Exit the interface configuration mode
Switch (config)# router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session
Switch (config-router)# virtual-ip 10.10.10.81	Set the virtual IP address for the VRRP session
Switch (config-router)# interface eth-0-1	Specify the physical interface that will participate in virtual routing
Switch (config-router)# preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable

Switch (config-router)# advertisement-interval 5	Configure the advertisement interval to 5 seconds
Switch (config-router)# enable	Enable the VRRP session 1 on the router
Switch (config-router)# exit	Exit Router mode and enter the Configure mode
Switch (config)# router vrrp 2	Create a new VRRP session on the router and specify the VRID for the session
Switch (config-router)# virtual-ip 10.10.10.82	Set the virtual IP address for the VRRP session
Switch (config-router)# interface eth-0-1	Specify the physical interface that will participate in virtual routing
Switch (config-router)# priority 200	Configure the priority to 200 (less than 255) as R1 is the Backup router
Switch (config-router)# preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable
Switch (config-router)# advertisement-interval 5	Configure the advertisement interval to 5 seconds
Switch (config-router)# bfd 10.10.10.82	Configure the bfd session for VRRP instance
Switch (config-router)# enable	Enable the VRRP session 2 on the router

R2

Switch# configure terminal	Enter the Configure mode
Switch (config)# interface eth-0-1	Enters the interface configuration mode
Switch (config-if)# no switchport	Configure to layer3 interface
Switch (config-if)# ip address 10.10.10.82/24	Configure the IP address
Switch (config-if)# exit	Exit the interface configuration mode
Switch (config)# router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session
Switch (config-router)# virtual-ip 10.10.10.81	Set the virtual IP address for the VRRP session
Switch (config-router)# interface eth-0-1	Specify the physical interface that will participate in virtual routing
Switch (config-router)# priority 200	Configure the priority to 200 (less than 255) as R2 is the Backup router

Switch (config-router)# preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable
Switch (config-router)# advertisement-interval 5	Configure the advertisement interval to 5 seconds
Switch (config-router)# enable	Enable the VRRP session 1 on the router
Switch (config-router)# exit	Exit Router mode and enter the Configure mode
Switch (config)# router vrrp 2	Create a new VRRP session on the router and specify the VRID for the session
Switch (config-router)# virtual-ip 10.10.10.82	Set the virtual IP address for the VRRP session
Switch (config-router)# interface eth-0-1	Specify the physical interface that will participate in virtual routing
Switch (config-router)# preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable
Switch (config-router)# advertisement-interval 5	Configure the advertisement interval to 5 seconds
Switch (config-router)# bfd 10.10.10.81	Configure the bfd session for VRRP instance
Switch (config-router)# enable	Enable the VRRP session 2 on the router

11.7.3 Validation

The following outputs on R1 and R2 display the complete configuration for each session on R1 and R2. In session one R1 is the master router and in session 2 R2 is the master router.

```
R1# show vrrp 1
VRID <1>
 State               : Initialize(Interface down)
 Virtual IP          : 10.10.10.81(IP owner)
 Interface           : eth-0-1
 VMAC                : 0000.5e00.0101
 VRF                 : Default
 Advt timer          : 5 second(s)
 Preempt mode        : TRUE
 Conf pri            : Unset          Run pri    : 255
 Master router ip    : Unknown
 Master priority     : Unknown
 Master advt timer   : Unknown
 Master down timer   : Unknown
 Preempt delay       : 0 second(s)
 Learn master mode   : FALSE
```

```
R1#show vrrp 2
VRID <2>
 State               : Initialize(Interface down)
 Virtual IP          : 10.10.10.82(Not IP owner)
 Interface           : eth-0-1
 VMAC                : 0000.5e00.0102
 VRF                 : Default
 Advt timer          : 5 second(s)
 Preempt mode        : TRUE
 Conf pri            : 200            Run pri    : 200
 Master router ip    : Unknown
 Master priority     : Unknown
 Master advt timer   : Unknown
 Master down timer   : Unknown
 Preempt delay       : 0 second(s)
 Learn master mode   : FALSE
```

11.8 VRRP Circuit Failover

The need for VRRP Circuit Failover arose because VRRPv2 was unable to track the gateway interface status. The VRRP Circuit Failover feature provides a dynamic failover of an entire circuit in the event that one member of the group fails. It introduces the concept of a circuit, where two or more Virtual Routers on a single system can be grouped. In the event that a failure occurs and one of the Virtual Routers performs the Master to Backup transition, the other Virtual Routers in the group are notified and are forced into the Master to Backup transition, so that both incoming and outgoing packets are routed through the same gateway router, eliminating the problem for Firewall/NAT environments.

The following scenario explains this feature.

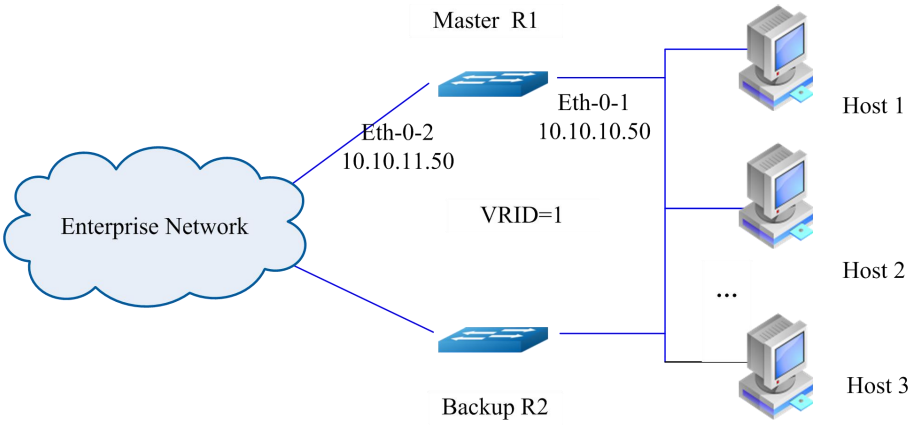
To configure VRRP Circuit Failover, each circuit is configured to have a corresponding priority-delta value, which is passed to VRRP when a failure occurs. The priority of each Virtual Router on the circuit is decremented by the priority delta value causing the VR Master to VR Backup transition.

In this example, two routers R1 and R2 are configured as backup routers with different priorities. The priority-delta value is configured to be greater than the difference of both the priorities. R1 is configured to have a priority of 100 and R2 has a priority of 90. R1 with a greater priority is the Virtual Router Master. The priority-delta value is 20, greater than 10 (100 minus 90). On R1 when the external interface eth1 fails, the priority of R1 becomes 80

(100 minus 20). Since R2 has a greater priority (90) than R1, R2 becomes the VR Master and routing of packages continues without interruption.

When this VR Backup (R1) is up again, it regains its original priority (100) and becomes the VR Master again.

11.8.1 Topology



11.8.2 Configuration

R1

Switch# configure terminal	Enter the Configure mode.
Switch (config)# interface eth-0-1	Enters the interface configuration mode
Switch (config-if)# no switchport	Configure to layer3 interface
Switch (config-if)# ip address 10.10.10.50/24	Configure the IP address
Switch (config-if)# exit	Exit the interface configuration mode
Switch (config)# interface eth-0-2	Enters the interface configuration mode
Switch (config-if)# no switchport	Configure to layer3 interface
Switch (config-if)# ip address 10.10.11.50/24	Configure the IP address
Switch (config-if)# exit	Exit the interface configuration mode
Switch (config)# track 10 interface eth-0-2 linkstate	Create an track object to monitor the link state of interface eth-0-2
Switch (config)# router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session.
Switch (config-router)# virtual-ip 10.10.10.1	Set the virtual IP address for the VRRP session.

Switch (config-router)# interface eth-0-1	Specify the physical interface that will participate in virtual routing.
Switch (config-router)# preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable
Switch (config-router)# advertisement-interval 5	Configure the advertisement interval to 5 seconds.
Switch (config-router)# priority 100	Configure the priority 100.
Switch (config-router)# track 1 decrement 20	Configure the priority-delta value to be 20. In case of failover, this priority-delta value is subtracted from the current VR Master
Switch (config-router)# enable	Enable the VRRP session on the router

R2

Switch # configure terminal	Enter the Configure mode
Switch (config)# interface eth-0-1	Enters the interface configuration mode
Switch (config-if)# no switchport	Configure to layer3 interface
Switch (config-if)# ip address 10.10.10.40/24	Configure the IP address
Switch (config-if)# exit	Exit the interface configuration mode
Switch (config)# router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session
Switch (config-router)# virtual-ip 10.10.10.1	Set the virtual IP address for the VRRP session.
Switch (config-router)# interface eth-0-1	Specify the physical interface that will participate in virtual routing
Switch (config-router)# preempt-mode true	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable
Switch (config-router)# advertisement-interval 5	Configure the advertisement interval to 5 seconds
Switch (config-router)# priority 90	Configure the priority 90
Switch (config-router)# enable	Enable the VRRP session on the router

Currently, only one interface is supported in a circuit Failover for a VRRP session.

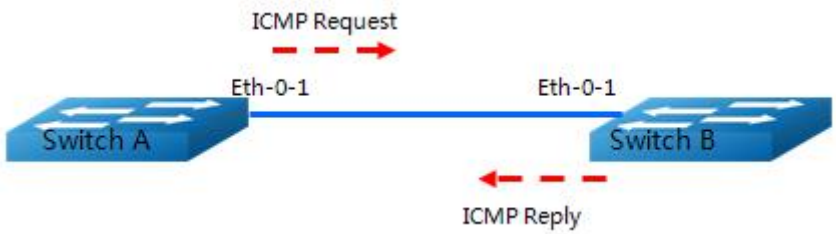
12 Configuring VRRP Remote Tracking

12.1 Configuring IP SLA

12.1.1 Overview

IP SLA (Service Level Agreement) is a network performance measurement and diagnostics tool that uses active monitoring. Active monitoring is the generation of traffic in a reliable and predictable manner to measure network performance. Every IP SLA operation maintains an operation return-code value. This return code is interpreted by the tracking process. The return code can return OK, Over Threshold, and several other return codes. Different operations can have different return-code values, so only values common to all operation types are used. In IP SLA, use icmp echo to check state or reachability of a route.

12.1.2 Topology



12.1.3 Configuring Interface With VRF

Configuring the ICMP echo.

Beginning in privileged EXEC mode, follow these steps to configure the ICMP echo.

Switch A

Switch#configure terminal	Enter the Configure mode.
Switch(config)# ip vrf vpn1	Create an vrf or enters vrf configuration mode.
Switch(config-vrf)# exit	Exit the vrf mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip vrf forwarding vpn1	Config vpn1 forward via eth-0-1
Switch(config-if)# ip address 192.168.0.2/24	Config ip address 192.168.0.2
Switch(config)# ip sla monitor 1	Create an IP SLA entry or enters IP SLA monitor configuration mode.
Switch(config-ipsla)# type echo protocol ipIcmpEcho 192.168.0.1	Defines an Echo operation with icmp packet and enters destination ip address or hostname.
Switch(config-ipsla)#frequency 10	(Optional)Configure the IP SLA entry parameters: Sets the rate at which a specified IP SLA operation repeats.
Switch(config-ipsla)#timeout 5	(Optional)Configure the IP SLA entry parameters: Sets the amount of time an IP SLA operation waits for a response from its request packet.
Switch(config-ipsla)#threshold 1	(Optional)Configure the IP SLA entry parameters: Sets the upper threshold value for calculating network monitoring statistics created by an IP SLA operation.
Switch(config-ipsla)#vrf vpn1	(Optional)Configure the IP SLA entry parameters: To use IP SLA operations in VPNs.
Switch(config-ipsla)#exit	Exit the IP SLA mode.
Switch(config)# ip sla monitor schedule 1	Enable an IP SLA entry
Switch(config)#exit	Exit the Configure mode.

Switch B

Switch#configure terminal	Enter the Configure mode.
Switch(config)# ip vrf vpn1	Create an vrf or enters vrf configuration mode.
Switch(config-vrf)# exit	Exit the vrf mode

Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip vrf forwarding vpn1	Config vpn1 forward via eth-0-1
Switch(config-if)# ip address 192.168.0.1/24	Config ip address 192.168.0.1

12.1.4 Validation

To display the ICMP echo configuration, use the show ip sla monitor privileged EXEC command.

```
Switch# show ip sla monitor 1
Entry 1
    Type                : Echo
    Admin state          : Enable
    Destination address  : 192.168.0.1
    Frequency            : 10 seconds
    Timeout              : 5 seconds
    Threshold            : 5 seconds
    Running Frequency    : 3 seconds
    Vrf                  : vpn1
    Return code          : OK
```

```
Switch# ping vrf vpn1 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.645 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.640 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.631 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.631 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.696 ms
```

12.1.5 Configuring Interface Without VRF

Switch A

Switch#configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip address 192.168.0.2/24	Config ip address 192.168.0.2
Switch(config)# ip sla monitor 1	Create an IP SLA entry or enters IP SLA monitor configuration mode.
Switch(config-ipsla)# type echo protocol ipIcmpEcho 192.168.0.1	Defines an Echo operation with icmp packet and enters destination ip address or hostname.

Switch(config-ipsla)#frequency 10	(Optional)Configure the IP SLA entry parameters: Sets the rate at which a specified IP SLA operation repeats.
Switch(config-ipsla)#timeout 5	(Optional)Configure the IP SLA entry parameters: Sets the amount of time an IP SLA operation waits for a response from its request packet.
Switch(config-ipsla)#threshold 1	(Optional)Configure the IP SLA entry parameters: Sets the upper threshold value for calculating network monitoring statistics created by an IP SLA operation.
Switch(config-ipsla)#exit	Exit the IP SLA mode.
Switch(config)# ip sla monitor schedule 1	Enable an IP SLA entry
Switch(config)#exit	Exit the Configure mode.

Switch B

Switch#configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip address 192.168.0.1/24	Config ip address 192.168.0.1

12.1.6 Validation

To display the ICMP echo configuration, use the show ip sla monitor privileged EXEC command.

```
Switch# show ip sla monitor
Entry 1
    Type                 : Echo
    Admin state          : Enable
    Destination address  : 192.168.0.1
    Frequency            : 10 seconds
    Timeout              : 5 seconds
    Threshold            : 5 seconds
    Running Frequency    : 8 seconds
Return code          : OK
```

```
Switch# ping 192.168.0.1
```

```
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.846 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.643 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.978 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.640 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.704 ms
```

Switch B

Switch#configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)#shutdown	Shutdown port

```
Switch# show ip sla monitor
Entry 1
    Type                 : Echo
    Admin state          : Enable
    Destination address  : 192.168.0.1
    Frequency            : 10 seconds
    Timeout              : 5 seconds
    Threshold            : 5 seconds
    Running Frequency    : 9 seconds
    Running Timeout      : 4 seconds
    Running Threshold    : 4 seconds
Return code          : Timeout
```

12.1.7 Configuring Remote Interface VIA IP Route

Switch A

Switch# configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip address 192.168.0.2/24	Config ip address 192.168.0.2
Switch(config)# ip sla monitor 2	Create an IP SLA entry or enters IP SLA monitor configuration mode.
Switch(config-ipsla)# type echo protocol ipIcmpEcho 1.1.1.1	Defines an Echo operation with icmp packet and enters destination ip address or hostname.
Switch(config-ipsla)# frequency 10	(Optional)Configure the IP SLA entry parameters: Sets the rate at which a specified IP SLA operation repeats.

Switch(config-ipsla)# timeout 5	(Optional)Configure the IP SLA entry parameters: Sets the amount of time an IP SLA operation waits for a response from its request packet.
Switch(config-ipsla)# threshold 1	(Optional)Configure the IP SLA entry parameters: Sets the upper threshold value for calculating network monitoring statistics created by an IP SLA operation.
Switch(config-ipsla)# exit	Exit the IP SLA mode.
Switch(config)# ip sla monitor schedule 2	Enable an IP SLA entry
Switch(config)# exit	Exit the Configure mode.

12.1.8 Validation

To display the ICMP echo configuration, use the show ip sla monitor privileged EXEC command.

```
Switch# show ip sla monitor 2
Entry 2
    Type                  : Echo
    Admin state           : Enable
    Destination address   : 1.1.1.1
    Frequency             : 10 seconds
    Timeout               : 5 seconds
    Threshold             : 5 seconds
    Running Frequency     : 1 seconds
    Return code           : Unreachable
Switch# ping 1.1.1.1
connect: Network is unreachable
```

Switch A

Command	Description
Switch# configure terminal	Enter the Configure mode.
Switch(config)# ip route 1.1.1.1/32 192.168.0.1	Set ip static route

```
Switch# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.661 ms
```

```
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=0.762 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=64 time=0.942 ms
```

```
Switch# show ip sla monitor 2
Entry 2
    Type                  : Echo
    Admin state           : Enable
    Destination address   : 1.1.1.1
    Frequency             : 10 seconds
    Timeout               : 5 seconds
    Threshold             : 5 seconds
    Running Frequency     : 8 seconds
    Return code           : OK
```

12.2 Configuring TRACK

12.2.1 Overview

Before the introduction of track feature, the VRRP had a simple tracking mechanism that allowed you to track the interface link state only. If the link state of the interface went down, the VRRP priority of the router was reduced, allowing another VRRP router with a higher priority to become active. The Track feature separates the tracking mechanism from VRRP and creates a separate standalone tracking process that can be used by other processes in future. This feature allows tracking of other objects in addition to the interface link state. VRRP can now register its interest in tracking objects and then be notified when the tracked object changes state. TRACK is a separate standalone tracking process that can be used by other processes as well as VRRP. This feature allows tracking of other objects in addition to the interface link state.

12.2.2 Configuring the track interface linkstate

Topology

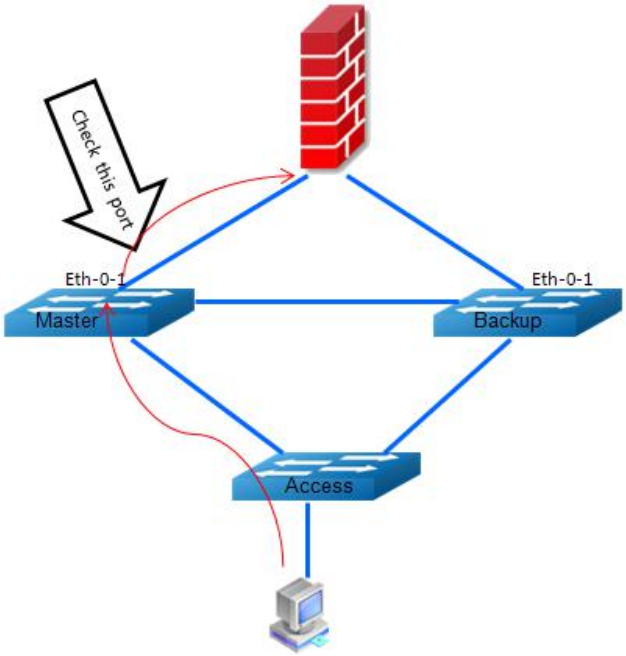


Figure 12-1 VRRP track topology

Configuration

Beginning in privileged EXEC mode, follow these steps to configure the track interface linkstate.

Switch# configure terminal	Enter the Configure mode
Switch(config)# track 1 interface eth-0-1 linkstate	Create a track object and track the state of an interface
Switch(config-track)# delay up 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from down to up
Switch(config-track)# delay down 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from up to down
Switch(config-track)# exit	Exit the track mode

Switch(config)# exit	Exit the Configure mode

Validation

To display the track interface linkstate configuration, use the show track privileged EXEC command.

```
DUT#show track
Track 2
    Type                    : Interface Link state
    Interface               : eth-0-1
    State                   : down
    Delay up                : 30 seconds
Delay down                  : 30 seconds
```

12.2.3 Configuring the track bfd

Topology

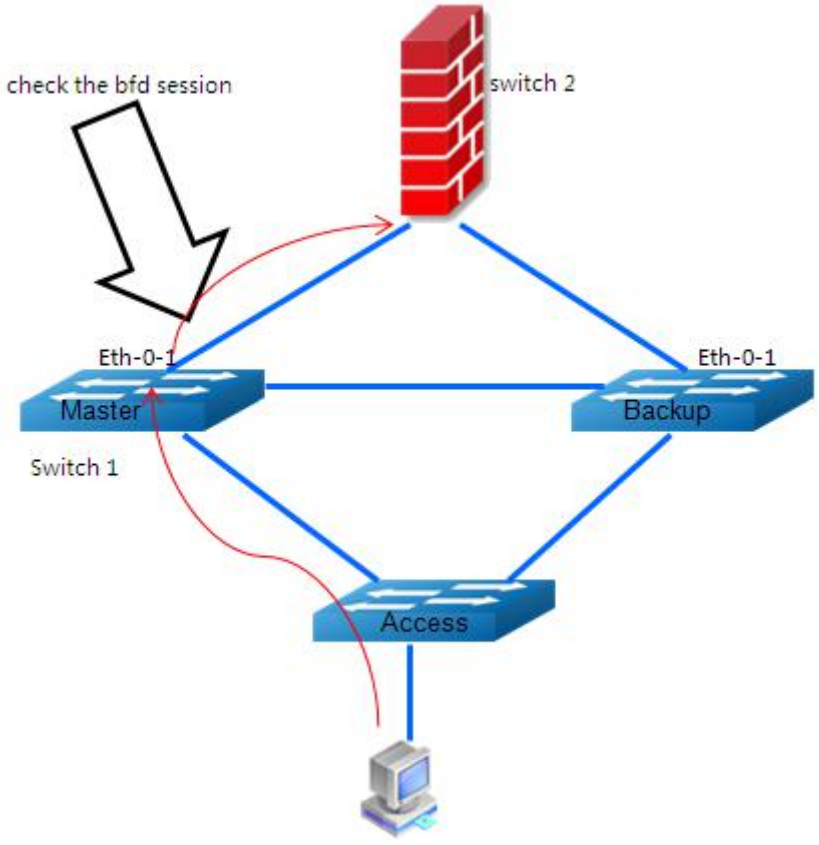


Figure 12-2 VRRP track topology

Configuration

Beginning in privileged EXEC mode, follow these steps to configure the track bfd.

Configuration of switch1

Switch1# configure terminal	Enter the Configure mode
Switch 1(config)# interface eth-0-1	Enter the Interface mode
Switch 1(config-if)# no switchport	Set the interface as routed port
Switch 1(config-if)# no shutdown	Set the interface state up
Switch 1(config-if)# ip address 9.9.9.1/24	Set the ip address of the interface
Switch 1(config-if)# quit	Exit the interface mode
Switch1(config)# track 1 bfd source interface eth-0-1 destination 9.9.9.2	Create a track object and track the state of bfd session
Switch1(config-track)# delay up 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from down to up
Switch1(config-track)# delay down 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from up to down
Switch1(config-track)# exit	Exit the track mode
Switch1(config)# exit	Exit the Configure mode

Configuration of switch2

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# interface eth-0-1	Enter the Interface mode
Switch2(config-if)# no switchport	Set the interface as routed port
Switch2(config-if)# no shutdown	Set the interface state up
Switch2(config-if)# ip address 9.9.9.2/24	Set the ip address of the interface
Switch2(config-if)# quit	Exit the interface mode
Switch2(config)# track 1 bfd source interface eth-0-1 destination 9.9.9.1	Create a track object and track the state of bfd session
Switch1(config-track)# delay up 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from down to up

Switch1(config-track)# delay down 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from up to down
Switch1(config-track)# exit	Exit the track mode
Switch1(config)# exit	Exit the Configure mode

Validation

To display the track bfd configuration, use the show track privileged EXEC command.

Switch #show track

```
Switch1 # show track
Track 1
    Type                : BFD state
    Source interface    : eth-0-1
    Destination IP      : 9.9.9.2
    BFD Local discr     : 1
    State               : up

Switch2 # show track
Track 1
    Type                : BFD state
    Source interface    : eth-0-1
    Destination IP      : 9.9.9.1
    BFD Local discr     : 1
    State               : up
```

12.2.4 Configuring Track RTR Reachability

Topology

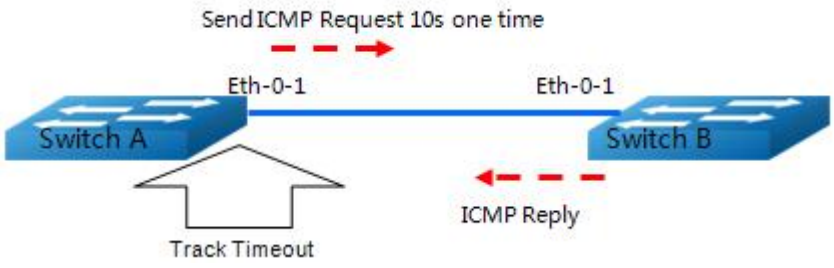


Figure 1-1 Track rtr reachability

Configuration

Beginning in privileged EXEC mode, follow these steps to configure the track rtr reachability.

Switch A

Switch# configure terminal	Enter the Configure mode
Switch(config)# track 1 rtr 1 reachability	Create a track object and track the state of an ip sla entry. When the state of ip sla entry is OK or Over threshold, track object state is up; otherwise track object state is down.
Switch(config-track)# delay up 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from down to up
Switch(config-track)# delay down 30	(Optional)Configure the track object parameters to specify a period of time (in seconds) to delay when object state is turned from up to down.
Switch(config-track)# exit	Exit the track mode
Switch(config)# exit	Exit the Configure mode
Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip address 192.168.0.2/24	Config ip address 192.168.0.2
Switch(config)# ip sla monitor 1	Create an IP SLA entry or enters IP SLA monitor configuration mode
Switch(config-ipsla)# type echo protocol ipIcmpEcho 192.168.0.1	Defines an Echo operation with icmp packet and enters destination ip address or hostname
Switch(config-ipsla)#frequency 10	(Optional)Configure the IP SLA entry parameters: Sets the rate at which a specified IP SLA operation repeats
Switch(config-ipsla)# timeout 5	(Optional)Configure the IP SLA entry parameters: Sets the amount of time an IP SLA operation waits for a response from its request packet
Switch(config-ipsla)# threshold 1	(Optional)Configure the IP SLA entry parameters: Sets the upper threshold value for calculating network monitoring statistics created by an IP SLA operation
Switch(config-ipsla)# exit	Exit the IP SLA mode

Switch(config)# ip sla monitor schedule 1	Enable an IP SLA entry
Switch(config)# exit	Exit the Configure mode

Switch B

Switch# configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip address 192.168.0.1/24	Config ip address 192.168.0.1

Validation

To display the track rtr reachability configuration, use the show track privileged EXEC command.

```
Switch# show track
Track 1
    Type                    : Response Time Reporter(RTR) Reachability
    RTR entry number      : 1
    State                     : up
    Delay up                : 30 seconds
Delay down                : 30 seconds
```

12.2.5 Configuring Track RTR State

Topology

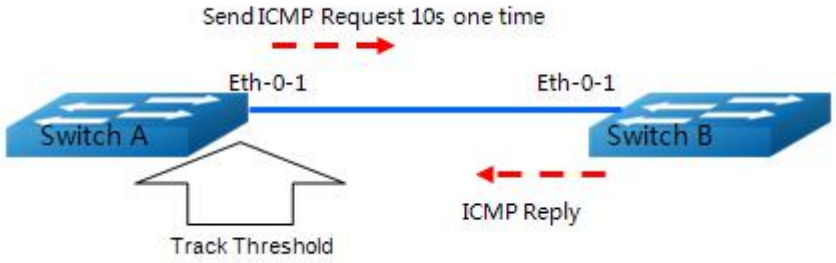


Figure 1-2 Track rtr state

Configuration

Beginning in privileged EXEC mode, follow these steps to configure the track rtr state.

Switch A

Switch#configure terminal	Enter the Configure mode.
Switch(config)# track 1 rtr 1 state	Create a track object and track the state of an ip sla entry When the state of ip sla entry is OK , track object state is up; otherwise track object state is down.
Switch(config-track)# delay up 30	(Optional)Configure the track object parameters: specify a period of time (in seconds) to delay when object state is turned from down to up
Switch(config-track)# delay down 30	(Optional)Configure the track object parameters: specify a period of time (in seconds) to delay when object state is turned from up to down.
Switch(config-track)#exit	Exit the track mode
Switch(config)#exit	Exit the Configure mode
Switch#configure terminal	Enter the Configure mode.
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip address 192.168.0.2/24	Config ip address 192.168.0.2
Switch(config)# ip sla monitor 1	Create an IP SLA entry or enters IP SLA monitor configuration mode
Switch(config-ipsla)# type echo protocol ipIcmpEcho 192.168.0.1	Defines an Echo operation with icmp packet and enters destination ip address or hostname.
Switch(config-ipsla)#frequency 10	(Optional)Configure the IP SLA entry parameters: Sets the rate at which a specified IP SLA operation repeats
Switch(config-ipsla)#timeout 5	(Optional)Configure the IP SLA entry parameters: Sets the amount of time an IP SLA operation waits for a response from its request packet.
Switch(config-ipsla)#threshold 1	(Optional)Configure the IP SLA entry parameters: Sets the upper threshold value for calculating network monitoring statistics created by an IP SLA operation.
Switch(config-ipsla)#exit	Exit the IP SLA mode.
Switch(config)# ip sla monitor schedule 1	Enable an IP SLA entry

Switch(config)#exit	Exit the Configure mode

Switch B

Switch# configure terminal	Enter the Configure mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ip address 192.168.0.1/24	Config ip address 192.168.0.1

Validation

To display the track rtr state configuration, use the show track privileged EXEC command.

Switch#show track

```
Track 1
    Type                    : Response Time Reporter(RTR) State
    RTR entry number      : 1
    State                   : up
    Delay up                : 30 seconds
Delay down                  : 30 seconds
```

12.3 Configuring VRRP TRACK

12.3.1 Topology

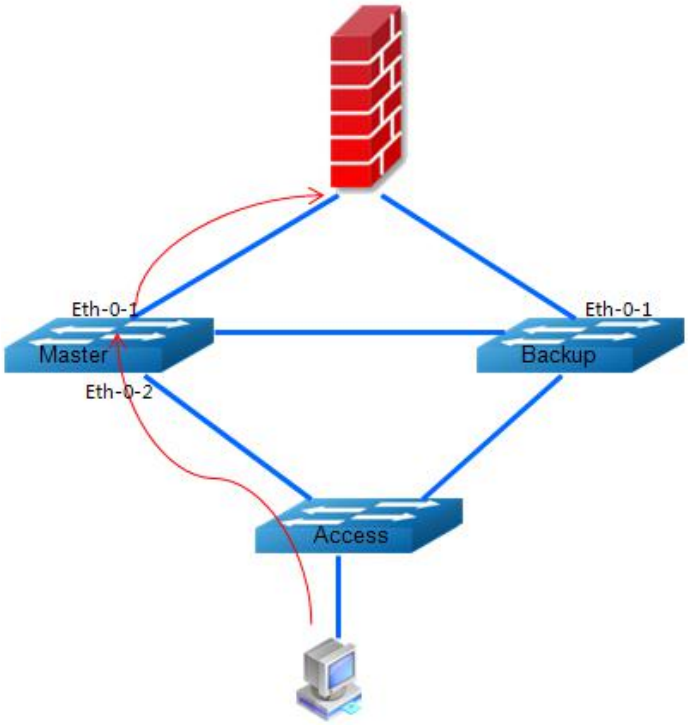


Figure 1-3 VRRP TRACK

12.3.2 Configuration

Beginning in privileged EXEC mode, follow these steps to configure the vrrp track.

Switch# configure terminal	Enter the Configure mode
Switch(config)# track 1 interface eth-0-1 linkstate	Configure the track linkstate object
Switch(config-track)# exit	Exit the track mode
Switch(config)# router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session
Switch(config-router)# track 1 decrement 30	Track an object in vrrp process, object id is 1, Priority delta is 30
Switch(config-router)# exit	Exit the router mode
Switch(config)# exit	Exit the Configure mode

12.3.3 Validation

To display the vrrp track configuration, use the show vrrp privileged EXEC command.

```
Switch# show vrrp
VRID <1>
 State              : Master
 Virtual IP          : 172.16.10.100(Not IP owner)
 Interface           : eth-0-2
 VMAC                 : 0000.5e00.0101
 Advt timer         : 1
 Preempt mode      : TRUE
 Auth type          : NONE
 Conf pri           : Unset          Run pri    : 70
 Track Object       : 1
 Delta pri           : 30
 Master router ip     : 172.16.10.1
 Master priority      : 70
 Master advt timer    : 1
 Master down timer   : 4
 Learn master mode   : FALSE
```

13 Configuring IP BFD

13.1 Overview

An increasingly important feature of networking equipment is the rapid detection of communication failures between adjacent systems, in order to more quickly establish alternative paths. Detection can come fairly quickly in certain circumstances when data link hardware comes into play (such as Synchronous Optical Network (SONET) alarms). However, there are media that do not provide this kind of signaling (such as Ethernet), and some media may not detect certain kinds of failures in the path, for example, failing interfaces or forwarding engine components.

Networks use relatively slow "Hello" mechanisms, usually in routing protocols, to detect failures when there is no hardware signaling to help out. The time to detect failures (“Detection Times”) available in the existing protocols is no better than a second, which is far too long for some applications and represents a great deal of lost data at gigabit rates. Furthermore, routing protocol Hellos are of no help when those routing protocols are not in use, and the semantics of detection are subtly different -- they detect a failure in the path between the two routing protocol engines.

The goal of Bidirectional Forwarding Detection (BFD) is to provide low-overhead, short-duration detection of failures in the path between adjacent forwarding engines, including the interfaces, data link(s), and, to the extent possible, the forwarding engines themselves.

An additional goal is to provide a single mechanism that can be used for aliveness detection over any media, at any protocol layer, with a wide range of Detection Times and overhead, to avoid a proliferation of different methods.

13.2 Limitation

If ethernet CFM mep is configured on an physical port and CFM LM is enabled, at the same time, IP BFD is configured on an vlan interface and the former physical port is a member of the vlan, IP BFD can't work normally. If CFM LM is disabled, IP BFD can work normally.

13.3 Topology

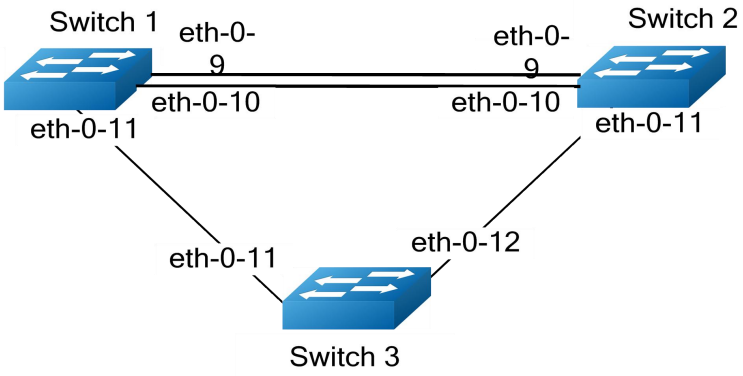


Figure 13-1 IP BFD basic topology for single-hop session

13.4 Configuration

This topo and configuration is for 3 BFD sessions.

One is based on static route, one is based on ospf， the other is based on vrrp.

Switch1's configuration

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch1(config-if)# no switchport	Set the interface as routed port
Switch1(config-if)# no shutdown	Set the interface state up
Switch1(config-if)# ip address 9.9.9.1/24	Set the IPv4 address for this interface
Switch1(config-if)# bfd interval mintx 1 minrx 1 multiplier 3	Set the BFD transmit interval, receive interval and detect multiplier
Switch1(config-if)# exit	Exit interface mode of interface eth-0-9
Switch1(config)# interface eth-0-10	Specify the interface (eth-0-10)to be configured and enter the Interface mode

Switch1(config-if)# no switchport	Set the interface as routed port
Switch1(config-if)# no shutdown	Set the interface state up
Switch1(config-if)# ip address 10.10.10.1/24	Set the IPv4 address for this interface
Switch1(config-if)# bfd interval mintx 2 minrx 2 multiplier 3	Set the BFD transmit interval, receive interval and detect multiplier
Switch1(config-if)# ip ospf bfd	Set BFD for ospf enable
Switch1(config-if)# exit	Exit interface mode of interface eth-0-10
Switch1(config)# router ospf	Enter the router ospf mode
Switch1 (config-router)# network 10.10.10.0/24 area 0	Set the ospf network
Switch1 (config-router)# exit	Exit the router ospf mode
Switch1 (config)#interface eth-0-11	Enters the interface configuration mode
Switch1 (config-if)#no switchport	Configure to layer3 interface
Switch1 (config-if)#ip address 11.11.11.1/24	Configure the IP address
Switch1 (config-if)#exit	Exit the interface configuration mode
Switch1 (config)#router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session.
Switch1 (config-router)#virtual-ip 11.11.11.100	Set the virtual IP address for the VRRP session.
Switch (config-router)#interface eth-0-11	Specify the physical interface that will participate in virtual routing.
Switch1 (config-router)# bfd 11.11.11.2	Configure the bfd session for VRRP instance
Switch1 (config-router)# enable	Enable the VRRP session on the router.
Switch1(config)# bdf.test peer-ip 9.9.9.2 interface eth-0-9 auto	Create a bdf session
Switch1(config)# ip route 1.1.1.0/24 9.9.9.2 bfd	Configure a static route and bind IP BFD session for the static route
Switch1(config)# end	Exit the configure mode

Switch2's configuration

Switch2# configure terminal	Enter the Configure mode
Switch2(config)# interface eth-0-9	Specify the interface (eth-0-9)to be configured and enter the Interface mode
Switch2(config-if)# no switchport	Set the interface as routed port
Switch2(config-if)# no shutdown	Set the interface state up
Switch2(config-if)# ip address 9.9.9.2/24	Set the IPv4 address for this interface

Switch2(config-if)# bfd interval mintx 1 minrx 1 multiplier 3	Set the BFD transmit interval, receive interval and detect multiplier
Switch2(config-if)# exit	Exit interface mode of interface eth-0-9
Switch2(config)# interface eth-0-10	Specify the interface (eth-0-10)to be configured and enter the Interface mode
Switch2(config-if)# no switchport	Set the interface as routed port
Switch2(config-if)# no shutdown	Set the interface state up
Switch2(config-if)# ip address 10.10.10.2/24	Set the IPv4 address for this interface
Switch2(config-if)# bfd interval mintx 2 minrx 2 multiplier 3	Set the BFD transmit interval, receive interval and detect multiplier
Switch2(config-if)# ip ospf bfd	Set BFD for ospf enable
Switch2(config-if)# exit	Exit interface mode of interface eth-0-10
Switch2(config)# router ospf	Enter the router ospf mode
Switch2 (config-router)# network 10.10.10.0/24 area 0	Set the ospf network
Switch2 (config-router)# exit	Exit the router ospf mode
Switch 2(config)#interface eth-0-11	Enters the interface configuration mode
Switch 2(config-if)#no switchport	Configure to layer3 interface
Switch2 (config-if)#ip address 11.11.11.2/24	Configure the IP address
Switch2 (config-if)#exit	Exit the interface configuration mode
Switch 2(config)#router vrrp 1	Create a new VRRP session on the router and specify the VRID for the session.
Switch2 (config-router)#virtual-ip 11.11.11.100	Set the virtual IP address for the VRRP session.
Switch2 (config-router)#interface eth-0-11	Specify the physical interface that will participate in virtual routing.
Switch2 (config-router)# bfd 11.11.11.1	Configure the bfd session for VRRP instance
Switch2 (config-router)# enable	Enable the VRRP session on the router.
Switch1(config)# bdf.test peer-ip 9.9.9.1 interface eth-0-9 auto	Create a bfd session
Switch2(config)# ip route 2.2.2.0/24 9.9.9.1 bfd	Configure a static route and bind IP BFD session for the static route
Switch2(config)# end	Exit the configure mode

Switch3's configuration

Switch3# configure terminal	Enter the Configure mode
Switch3(config)# interface eth-0-11	Specify the interface (eth-0-11)to be configured and enter the Interface mode

Switch3(config-if)# no shutdown	Set the interface state up
Switch 3(config-if)#exit	Exit the interface configuration mode
Switch3(config)# interface eth-0-12	Specify the interface (eth-0-12)to be configured and enter the Interface mode
Switch3(config-if)# no shutdown	Set the interface state up
Switch 3(config-if)#exit	Exit the interface configuration mode

13.5 Validation

The result of show bfd session is as follows.

```
Switch1# show bfd session
abbreviation:
LD: local Discriminator.    RD: Discriminator
S: single hop session.    M: multi hop session.
A: Admin down.    D:down.    I:init.    U:up.
=====================================================
LD   RD   TYPE ST   UP-Time    Remote-Addr
1    1    S    U    00:01:05   9.9.9.2/32
2    2    S    U    00:00:25   10.10.10.2/32
3    3    S    U    00:00:25   11.11.11.2/32

Number of Sessions:    3
```

```
Switch2# show bfd session
abbreviation:
LD: local Discriminator.    RD: Discriminator
S: single hop session.    M: multi hop session.
A: Admin down.    D:down.    I:init.    U:up.
=====================================================
LD   RD   TYPE ST   UP-Time    Remote-Addr
1    1    S    U    00:01:27   9.9.9.1/32
2    2    S    U    00:00:46   10.10.10.1/32
3    3    S    U    00:00:25   11.11.11.3/32
Number of Sessions:    3
```

14 Configuring VARP

14.1 Overview

Virtual ARP (VARP) allows multiple switches to simultaneously route packets with the same destination MAC address. Each switch is configured with the same virtual MAC address for the the VLAN interfaces configured with a virtual IP address. In MLAG configurations, VARP is preferred over VRRP because VARP working on active-active mode without traffic traverse peer link.

For ARP and GARP requests to virtual IP address, VARP will use the virtual MAC address. The virtual MAC address is only for inbound packets and never used in the source field of outbound packets.

14.2 Topology

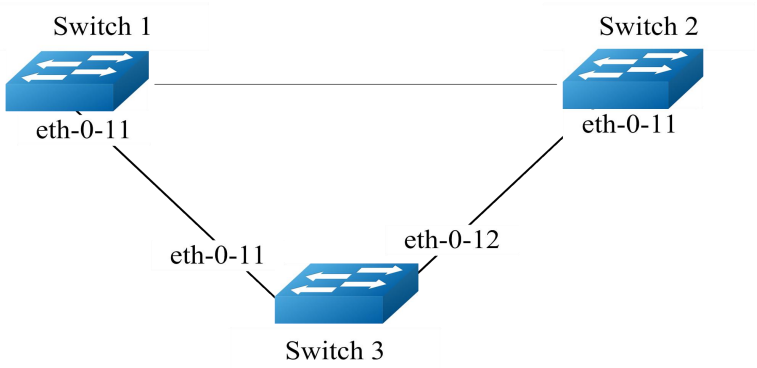


Figure 14-1 VARP & MLAG topology

14.3 Configuration

This topo and configuration is for VARP function.

Switch1's configuration

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# ip virtual-router mac a.a.a	Specify the virtual MAC address
Switch1(config)# vlan database	Enter the VLAN Configure mode
Switch1(config-vlan)# vlan 2	Create VLAN 2
Switch1(config-vlan)# exit	Exit the VLAN Configure mode
Switch1(config)# interface eth-0-11	Enter interface mode of interface eth-0-11
Switch1(config-if)# switchport access vlan 2	Add this interface to VLAN 2
Switch1(config-if)# no shutdown	Set the interface state up
Switch1(config-if)# interface vlan 2	Enter interface mode of interface vlan2
Switch1(config-if)# ip address 10.10.10.1/24	Set the IPv4 address for this interface
Switch1(config-if)# ip virtual-router address 10.10.10.254	Set the virtual IP address for this interfac
Switch1(config-if)# end	Exit the interface configure mode

Switch2's configuration

Switch1# configure terminal	Enter the Configure mode
Switch1(config)# ip virtual-router mac a.a.a	Specify the virtual MAC address
Switch1(config)# vlan database	Enter the VLAN Configure mode
Switch1(config-vlan)# vlan 2	Create VLAN 2
Switch1(config-vlan)# exit	Exit the VLAN Configure mode
Switch1(config)# interface eth-0-11	Enter interface mode of interface eth-0-11
Switch1(config-if)# switchport access vlan 2	Add this interface to VLAN 2
Switch1(config-if)# no shutdown	Set the interface state up
Switch1(config-if)# interface vlan 2	Enter interface mode of interface vlan2
Switch1(config-if)# ip address 10.10.10.2/24	Set the IPv4 address for this interface
Switch1(config-if)# ip virtual-router address 10.10.10.254	Set the virtual IP address for this interfac
Switch1(config-if)# end	Exit the interface configure mode

14.4 Validation

The result of show arp entry is as follows.

```
Switch1# show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    10.10.10.1             -   cef0.12da.8100  vlan2
 Internet    10.10.10.254           -   000a.000a.000a  vlan2
```

```
Switch2#  show ip arp
 Protocol    Address          Age (min)  Hardware Addr   Interface
 Internet    10.10.10.2             -   66d1.4c26.e100  vlan2
 Internet    10.10.10.254           -   000a.000a.000a  vlan2
```