

24

IEEE 802.1ak MVRP and MRP

- Prerequisites for IEEE 802.1ak MVRP and MRP, page 24-1
- Restrictions for IEEE 802.1ak MVRP and MRP, page 24-1
- Information About IEEE 802.1ak MVRP and MRP, page 24-2
- Default Settings for IEEE 802.1ak MVRP and MRP, page 24-8
- How to Configure IEEE 802.1ak MVRP and MRP, page 24-8
- Troubleshooting the MVRP Configuration, page 24-10
- Configuration Examples for IEEE 802.1ak MVRP and MRP, page 24-11

**Note**

- This feature appears in Cisco Feature navigator as “IEEE 802.1ak - MVRP and MRP.”
- For complete syntax and usage information for the commands used in this chapter, see these publications:
http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.4SY supports only Ethernet interfaces. Cisco IOS Release 15.4SY does not support any WAN features or commands.

**Tip**

For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

[Participate in the Technical Documentation Ideas forum](#)

Prerequisites for IEEE 802.1ak MVRP and MRP

None.

Restrictions for IEEE 802.1ak MVRP and MRP

- In releases where CSCta96338 is not resolved, a physical port with an MVRP configuration and enable state that differs from what is configured on a port-channel interface cannot become an active member of that EtherChannel.

Information About IEEE 802.1ak MVRP and MRP

- In releases where CSCta96338 is resolved, a physical port with an MVRP configuration and enable state that differs from what is configured on a port-channel interface can become an active member of the EtherChannel because the physical port will use the port-channel interface MVRP configuration and enable state.
- A non-Cisco device can interoperate with a Cisco device only through 802.1Q trunks.
- MVRP runs on ports where it is enabled. VTP pruning can run on ports where MVRP is not enabled.
- MVRP can be configured on both physical interfaces and EtherChannel interfaces, but is not supported on EtherChannel member ports.
- MVRP dynamic VLAN creation is not supported when the device is running in VTP server or client mode.
- MVRP and Connectivity Fault Management (CFM) can coexist but if the module does not have enough MAC address match registers to support both protocols, the MVRP ports on those modules are put in the error-disabled state. To use the ports that have been shut down, disable MVRP on the ports, and then enter **shutdown** and **no shutdown** commands.
- 802.1X authentication and authorization takes place after the port becomes active and before the Dynamic Trunking Protocol (DTP) negotiations start prior to MVRP running on the port.
- Do not enable MVRP automatic MAC address learning on edge switches that are configured with access ports. Enable MVRP automatic MAC address learning only on core switches where all the trunk interfaces are running MVRP.
- MVRP is supported only on Layer 2 trunks. MVRP is not supported on subinterfaces.

Information About IEEE 802.1ak MVRP and MRP

- [Overview, page 24-2](#)
- [Dynamic VLAN Creation, page 24-4](#)
- [MVRP Interoperability with VTP, page 24-4](#)
- [MVRP Interoperation with Non-Cisco Devices, page 24-6](#)
- [MVRP Interoperability with Other Software Features and Protocols, page 24-6](#)

Overview

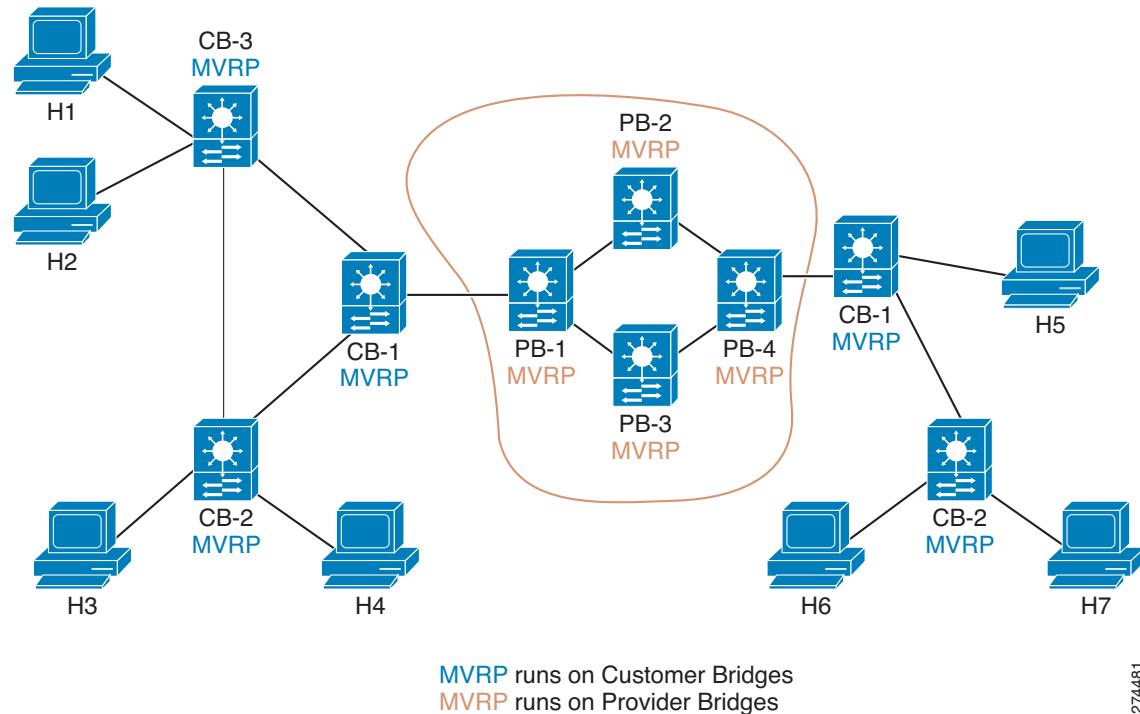
The IEEE 802.1ak Multiple VLAN Registration Protocol (MVRP) supports dynamic registration and deregistration of VLANs on ports in a VLAN bridged network. IEEE 802.1ak uses more efficient Protocol Data Units (PDUs) and protocol design to provide better performance than the Generic VLAN Registration Protocol (GARP) VLAN Registration Protocol (GVRP) and GARP Multicast Registration Protocol (GMRP) protocols.

A VLAN-bridged network usually restricts unknown unicast, multicast, and broadcast traffic to those links that the traffic uses to access the appropriate network devices. In a large network, localized topology changes can affect the service over a much larger portion of the network. IEEE 802.1ak replaces GARP with the Multiple Registration Protocol (MRP), which provides improved resource utilization and bandwidth conservation.

With the 802.1ak MRP attribute encoding scheme, MVRP only needs to send one PDU that includes the state of all 4094 VLANs on a port. MVRP also transmits Topology Change Notifications (TCNs) for individual VLANs. This is an important feature for service providers because it allows them to localize

topology changes. [Figure 24-1](#) illustrates MVRP deployed in a provider network on provider and customer bridges.

Figure 24-1 MVRP Deployed on Provider and Customer Bridges



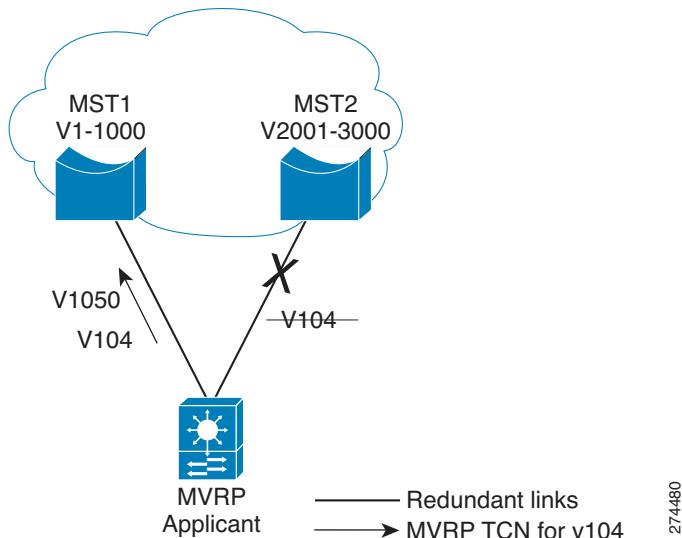
274481

Because most providers do not wish to filter traffic by destination MAC addresses, a pruning protocol like MVRP is important in a Metro Ethernet provider network, which often uses thousands of VLANs.

Figure 24-2 displays redundant links that are configured between the access switch and two distribution switches on the cloud. When the link with VLAN 104 fails over, MVRP needs to send only one TCN for VLAN 104. Without MVRP, an STP TCN would need to be sent out for the whole MST region (VLANs 1-1000), which could cause unnecessary network interruption.

STP sets the tcDetected variable to signal MVRP that MVRP must decide whether to send an MVRP TCN. MVRP can flush filtering database entries rapidly on a per-VLAN basis following a topology change because when a port receives an attribute declaration marked as new, any entries in the filtering database for that port and for that VLAN are removed.

Figure 24-2 MVRP TCN Application



Dynamic VLAN Creation

Virtual Trunking Protocol (VTP) is a Cisco proprietary protocol that distributes VLAN configuration information across multiple devices within a VTP domain. When VTP is running on MVRP-aware devices, all of the VLANs allowed on the Cisco bridged LAN segments are determined by VTP.

Only the VTP transparent mode supports MVRP dynamic VLAN creation. When dynamic VLAN creation is disabled, the MVRP trunk ports can register and propagate the VLAN messages only for existing VLANs. MVRP PDUs and MVRP messages for the nonexistent VLANs are discarded.

For a switch to be configured in full compliance with the MVRP standard, the switch VTP mode must be transparent and MVRP dynamic VLAN creation must be enabled.

MVRP Interoperability with VTP

- [Overview, page 24-5](#)
- [VTP in Transparent or Off Mode, page 24-5](#)
- [VTP in Server or Client Mode and VTP Pruning is Disabled, page 24-5](#)
- [VTP in Server or Client Mode and VTP Pruning is Enabled, page 24-5](#)

Overview

The VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that distributes VLAN configuration information across multiple devices within a VTP domain. VTP pruning is an extension of VTP. It has its own Join message that can be exchanged with VTP PDUs. VTP PDUs can be transmitted on both 802.1Q trunks and ISL trunks. A VTP-capable device is in one of the VTP modes: server, client, transparent, or off.

When VTP Pruning and MVRP are both enabled globally, MVRP runs on trunks where it is enabled and VTP Pruning runs on other trunks. MVRP or VTP pruning can be enabled on a trunk, but not both.

VTP in Transparent or Off Mode

When VTP is in transparent or off mode, VTP pruning is not supported and VTP PDUs are not processed.

When a port receives an MVRP join message for a VLAN, the port transmits broadcast, multicast, and unknown unicast frames in that VLAN and adds the traffic definition to the MRP Attribute Propagation (MAP) port configured for that VLAN. The mapping is removed when the VLAN is no longer registered on the port.

For each interface that is forwarding in each VLAN, MVRP issues a join request to each MRP Attribute Declaration (MAD) instance and an MVRP Join message is sent out on each corresponding MVRP port.

MVRP dynamic VLAN creation can be enabled in VTP transparent or off mode. If it is enabled and the VLAN registered by a join message does not exist in the VLAN database in the device, then the VLAN will be created.

VTP in Server or Client Mode and VTP Pruning is Disabled

MVRP functions like VTP in transparent or off mode, except that MVRP dynamic VLAN creation is not allowed.

VTP in Server or Client Mode and VTP Pruning is Enabled

MVRP and VTP with pruning disabled can be supported on the same port and these two protocols need to communicate and exchange pruning information.

When VTP receives a VTP join message on a VTP trunk, MVRP is notified so that join request can be posted to the MVRP port MAD instances, and MVRP join messages are sent out on the MVRP ports to the MVRP network.

When VTP pruning removes a VLAN from a VTP trunk, MVRP sends a leave request to all the MAD instances and the MAD instances send a leave or empty message from the MVRP ports to indicate that the VLAN is not configured on the device.

When an MVRP port receives an MVRP join message, MVRP propagates the event to other MVRP ports in the same MAP context, and notifies VTP so that VTP pruning can send a VTP join message from the VTP trunk ports.

If MVRP learns that a VLAN is no longer declared by the neighboring devices, MVRP sends a withdrawal event to VTP and then VTP pruning verifies that it should continue sending VTP join messages.

For VLANs that are configured as VTP pruning non-eligible on the VTP trunks, the VTP pruning state variables are set to joined for the VLANs. MVRP join requests are sent to those VLANs through the MVRP ports.

MVRP Interoperation with Non-Cisco Devices

Non-Cisco devices can interoperate with a Cisco device only through 802.1q trunks.

MVRP Interoperability with Other Software Features and Protocols

- [802.1x and Port Security, page 24-6](#)
- [DTP, page 24-6](#)
- [EtherChannel, page 24-7](#)
- [Flex Links, page 24-7](#)
- [High Availability, page 24-7](#)
- [ISSU and eFSU, page 24-7](#)
- [L2PT, page 24-7](#)
- [SPAN, page 24-7](#)
- [Unknown Unicast and Multicast Flood Control, page 24-7](#)
- [STP, page 24-7](#)
- [UDLR, page 24-7](#)
- [VLANs with MVRP, page 24-8](#)

802.1x and Port Security

802.1x authenticates and authorizes a port after it transitions to the link-up state, but before DTP negotiation occurs and MVRP runs on a port. Port security works independently of MVRP.



Note

When MVRP is globally enabled, the MVRP MAC address auto detect and provision feature is disabled by default (**mvrp mac-learning auto**). In some situations, MVRP MAC address auto detect and provision can disable MAC address learning and prevent correct port security operation. For example, on ports where port security is configured, when the number of streams exceeds the configured maximum number of MAC addresses, no port security violation occurs because MAC address learning is disabled, which prevents updates to port security about the streams coming into the port. To avoid incorrect port security operation, use caution when enabling the MVRP MAC address auto detect and provision feature on ports where port security is configured.

DTP

DTP negotiation occurs after ports transition to the link-up state and before transition to the forwarding state. If MVRP is administratively enabled globally and enabled on a port, it becomes operational when the port starts trunking.

EtherChannel

An EtherChannel port-channel interface can be configured as an MVRP participant. The EtherChannel member ports cannot be MVRP participants. MVRP learns the STP state of EtherChannel port-channel interfaces. The MAP context applies to the EtherChannel port-channel interfaces, but not to the EtherChannel member ports.

Flex Links

MVRP declares VLANs on STP forwarding ports but not on ports in the blocking state. On flex links ports, MVRP declares VLANs on the active ports but not on the standby ports. When a standby port takes over and an active port transitions to the link-down state, MVRP declares the VLANs on the newly active port.

High Availability

State Switchover (SSO) and ISSU supports MVRP.

ISSU and eFSU

Enhanced Fast Software Upgrade (EFSU) is an enhanced software upgrade procedure. MVRP is serviced by the ISSU client identified as ISSU_MVRP_CLIENT_ID.

L2PT

Layer 2 Protocol Tunneling (L2PT) does not support MVRP PDUs on 802.1Q tunnel ports.

SPAN

MVRP ports can be configured as either Switched Port Analyzer (SPAN) sources or destinations.

Unknown Unicast and Multicast Flood Control

MVRP and the Unknown Unicast and Multicast Flood Control feature, configured with the **switchport block** command, cannot be configured on the same port.

STP

An STP mode change causes forwarding ports to leave the forwarding state until STP reconverges in the newly configured mode. The reconvergence might cause an MVRP topology change because join messages might be received on different forwarding ports, and leave timers might expire on other ports.

UDLR

MVRP and unidirectional link routing (UDLR) cannot be configured on the same port.

■ Default Settings for IEEE 802.1ak MVRP and MRP

- [VLAN Translation, page 24-8](#)
- [802.1Q Native VLAN Tagging, page 24-8](#)
- [Private VLANs, page 24-8](#)

VLAN Translation

VLAN translation and MVRP cannot be configured on the same port.

802.1Q Native VLAN Tagging

Other MVRP participants might not be able to accept tagged MVRP PDUs in the 802.1Q native VLAN. Compatibility between MVRP and 802.1Q native VLAN tagging depends on the specific network configuration.

Private VLANs

Private VLAN ports cannot support MVRP.

Default Settings for IEEE 802.1ak MVRP and MRP

None.

How to Configure IEEE 802.1ak MVRP and MRP

- [Enabling MVRP, page 24-8](#)
- [Enabling Automatic Detection of MAC Addresses, page 24-9](#)
- [Enabling MVRP Dynamic VLAN Creation, page 24-9](#)
- [Changing the MVRP Registrar State, page 24-10](#)

Enabling MVRP

MVRP must be enabled globally and on trunk ports. To enable MVRP, perform this task:

	Command or Action	Purpose
Step 1	Router> enable	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# mvrp global	Globally enables MVRP.

Command or Action	Purpose
Step 4 Router(config)# interface type number	Specifies a trunk port and enters interface configuration mode.
Step 5 Router(config-if)# mvrp	Enables MVRP on the interface. Note If MVRP is not successfully enabled on the port, the port is put in the errdisabled state. Enter the no mvrp command on the interface or the no mvrp global command to clear the errdisabled state.

This example shows how to enable MVRP globally and on an interface:

```
Router> enable
Router# configure terminal
Router(config)# mvrp global
Router(config)# interface FastEthernet 2/1
Router(config-if)# mvrp
```

Enabling Automatic Detection of MAC Addresses

MVRP automatic detection of MAC addresses is disabled by default. To enable MVRP automatic detection of MAC addresses on VLANs, perform this task:

Command or Action	Purpose
Step 1 Router> enable	Enables privileged EXEC mode (enter your password if prompted).
Step 2 Router# configure terminal	Enters global configuration mode.
Step 3 Router(config)# mvrp mac-learning auto	Enables MAC address learning.

This example shows how to enable automatic MAC address learning:

```
Router> enable
Router# configure terminal
Router(config)# mvrp mac-learning auto
```

Enabling MVRP Dynamic VLAN Creation

To enable MVRP dynamic VLAN creation, perform this task:

Command or Action	Purpose
Step 1 Router> enable	Enables privileged EXEC mode (enter your password if prompted).
Step 2 Router# configure terminal	Enters global configuration mode.
Step 3 Router(config)# vtp mode transparent	Sets VTP mode to transparent. Note Required for MVRP dynamic VLAN creation.
Step 4 Router(config)# mvrp vlan creation	Enables MVRP dynamic VLAN creation.

This example shows how to enable MVRP dynamic VLAN creation:

Troubleshooting the MVRP Configuration

```
Router> enable
Router# configure terminal
Router(config)# vtp mode transparent
Router(config)# mvrp vlan create
```

Changing the MVRP Registrar State

The MRP protocol allows one participant per application in an end station, and one per application per port in a bridge. To set the MVRP registrar state, perform this task:

	Command or Action	Purpose
Step 1	Router> enable	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# configure terminal	Enters global configuration mode.
Step 3	Router(config)# interface type number	Specifies and interface and enters interface configuration mode.
Step 4	Router(config-if)# mvrp registration [normal fixed forbidden]	Registers MVRP with the MAD instance.

This example shows how to set the MVRP registrar state to normal:

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 2/1
Router(config-if)# mvrp registration normal
```

Troubleshooting the MVRP Configuration

Use the **show mvrp summary** and **show mvrp interface** commands to display configuration information and interface states, and the **debug mvrp** command to enable all or a limited set of output messages related to an interface.

To troubleshoot the MVRP configuration, perform this task:

	Command or Action	Purpose
Step 1	Router> enable	Enables privileged EXEC mode (enter your password if prompted).
Step 2	Router# show mvrp summary	Displays the MVRP configuration.
Step 3	Router# show mvrp interface interface-type port/slot	Displays the MVRP interface states for the specified interface.
Step 4	Router# debug mvrp	Displays MVRP debugging information.
Step 5	Router# clear mvrp statistics	Clears MVRP statistics on all interfaces.

The following is sample output from the **show mvrp summary** command. This command can be used to display the MVRP configuration at the device level.

```
Router# show mvrp summary
```

```
MVRP global state      : enabled
MVRP VLAN creation   : disabled
VLANs created via MVRP : 20-45, 3001-3050
Learning disabled on VLANs : none
```

The following is sample output from the **show mvrp interface** command. This command can be used to display MVRP interface details of the administrative and operational MVRP states of all or one particular trunk port in the device.

```
Router# show mvrp interface

Port      Status    Registrar State
Fa3/1     off       normal

Port      Join Timeout  Leave Timeout  Leaveall Timeout
Fa3/1     201        600            700           1000

Port      Vlans Declared
Fa3/1     none

Port      Vlans Registered
Fa3/1     none

Port      Vlans Registered and in Spanning Tree Forwarding State
Fa3/1     none
```

Configuration Examples for IEEE 802.1ak MVRP and MRP

- [Enabling MVRP, page 24-11](#)
- [Enabling MVRP Automatic Detection of MAC Addresses, page 24-11](#)
- [Enabling Dynamic VLAN Creation, page 24-12](#)
- [Changing the MVRP Registrar State, page 24-12](#)

Enabling MVRP

The following example shows how to enable MVRP:

```
Router> enable
Router# configure terminal
Router(config)# mvrp global
Router(config)# interface fastethernet2/1
Router(config-if)# mvrp
```

Enabling MVRP Automatic Detection of MAC Addresses

The following example shows how to enable MAC address learning:

```
Router> enable
Router# configure terminal
Router(config)# mvrp mac-learning auto
```

Enabling Dynamic VLAN Creation

The following example shows how to enable dynamic VLAN creation:

```
Router> enable
Router# configure terminal
Router(config)# vtp mode transparent
Router(config)# mvrp vlan create
```

Changing the MVRP Registrar State

The following example shows how to change the MVRP registrar state:

```
Router> enable
Router# configure terminal
Router(config)# mvrp registration normal
```



Tip For additional information about Cisco Catalyst 6500 Series Switches (including configuration examples and troubleshooting information), see the documents listed on this page:

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

Participate in the [Technical Documentation Ideas forum](#)