IEEE 802.1ak - MVRP and MRP

First Published: November 14, 2008
Last Updated: March 6, 2009

Implementation of the IEEE 802.1ak standard allows for dynamic registration and deregistration of VLANs on ports in a VLAN bridged network. This document describes Multiple Registration Protocol (MRP) and Multiple VLAN Registration Protocol (MVRP) as implemented in accordance with the IEEE 802.1ak standard.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "Feature Information for IEEE 802.1ak - MVRP and MRP" section on page 19.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for EEE 802.1ak - MVRP and MRP

- A non-Cisco device can interoperate with a Cisco device only through .1Q trunks.
- When both MVRP and VTP pruning are enabled on the device, VTP pruning will be disabled on the dot1q trunks. All dot1q trunks are only allowed to run MVRP and talk to other MVRP participants in the network, while ISL trunks are running VTP pruning and interoperate with other Cisco devices with ISL trunks in another network.
- MVRP can be configured on both physical interfaces and Etherchannel interfaces. However, its configuration is not allowed on Etherchannel member ports.
- For simple implementation, MVRP dynamic VLAN creation feature is disallowed if the device is running in VTP server or client mode.
- MVRP and Connectivity Fault Management (CFM) can coexist but if the line card (LC) or supervisor does not have enough mac-match registers to support both protocols, the MVRP ports on those LCs are put in error disabled state. To use Layer 2 functionality, disable MVRP on those ports and configure shut/no shut.
- MVRP functionality applies only to interfaces configured for Layer 2 (switchport) functionality.
- 802.1X authentication and authorization takes place after the port becomes link-up and before the Dynamic Trunking Protocol (DTP) negotiations start prior to GVRP running on the port.
- MVRP cannot be configured and run on a sub-interface.

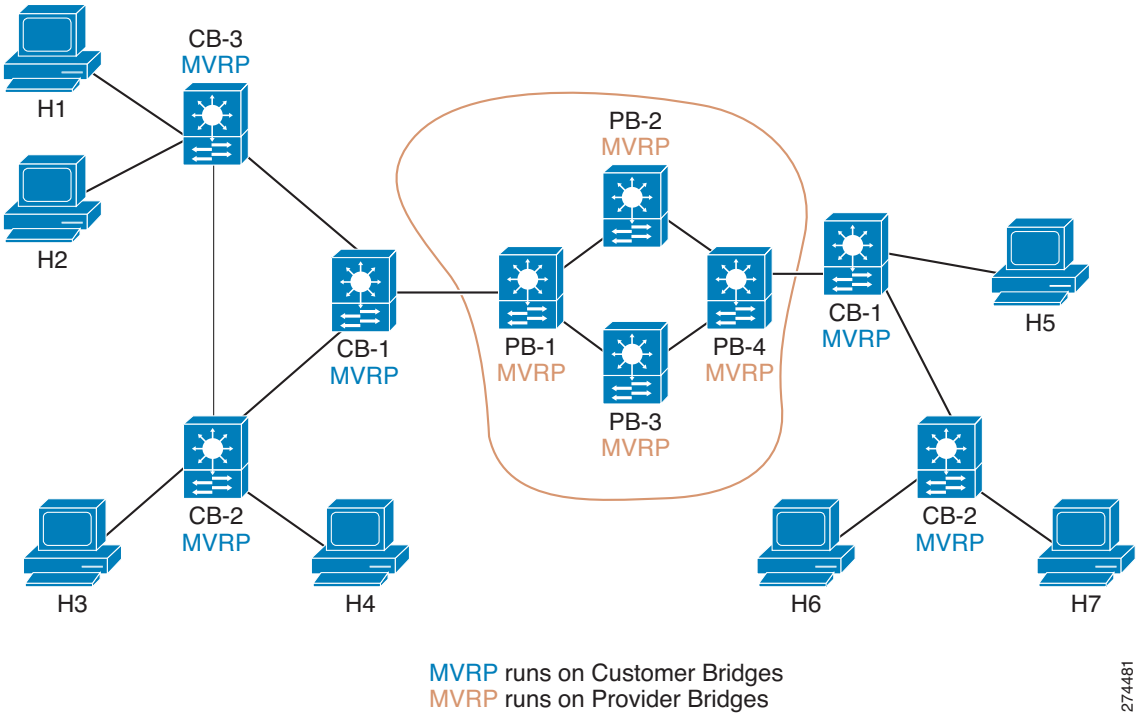
Information About EEE 802.1ak - MVRP and MRP

IEEE 802.1ak, also known as Multiple Registration Protocol (MRP), allows dynamic registration and deregistration of VLANs on ports in a VLAN bridged network. IEEE 802.1ak provides performance improvement over the GVRP and GMRP protocols with more efficient Protocol Data Units (PDUs) and protocol design. This feature implements MRP and MVRP as specified in the IEEE 802.1ak standard.

In a VLAN bridged network, it is desirable to restrict unknown unicast, multicast, and broadcast traffic to those links which the traffic must use 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 MRP offering much improvement over resource utilization and conservation of bandwidth.

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 includes the transmission of a Topology Change Notification (TCN) for individual VLANs. This is an important feature for service providers because it allows them to localize topology changes. Figure 1 illustrates MVRP deployed in a provider network on provider and customer bridges.

Figure 1 MVRP Deployed on Provider and Customer Bridges

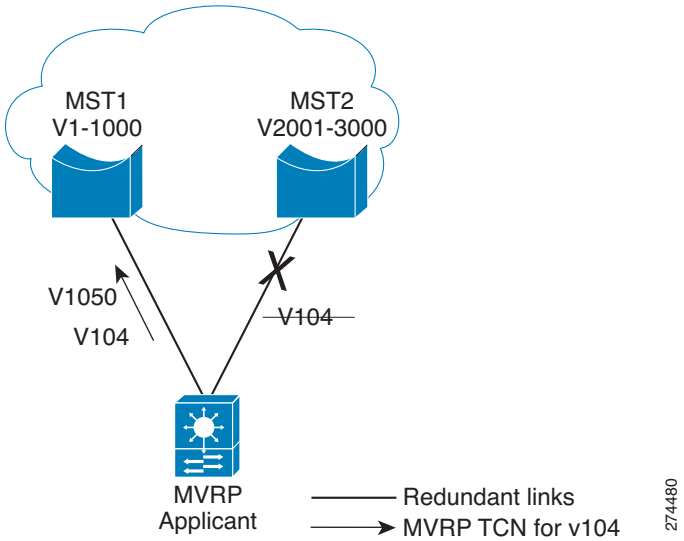


In the Metro Ethernet provider network, the use of thousands of VLANs is likely. Most providers do not wish to filter traffic by destination Mac Addresses. Hence, a pruning protocol like MVRP becomes important.

In Figure 2, redundant links are configured between the access switch and two distribution switches on the cloud. When the link with VLAN 104 fails over, MVRP need to send only one TCN for VLAN 104. Without MVRP, an STP TCN would have to be sent out for the whole MST region (VLANs1-1000), causing unnecessary network interruption.

STP sets the new variable tcDetected for MVRP to decide whether to send a New message (hence, references to MVRP TCN). When an attribute declaration marked as *new* is received on a given port, any entries in the filtering database for that port and for that VLAN are removed. This allows MVRP to flush the filtering database entries rapidly on a per-VLAN basis following a topology change.

Figure 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. MVRP dynamic VLAN creation can be enabled only when the VTP mode on the switch is set to transparent. When dynamic VLAN creation is disabled, the MVRP trunk ports can register and propagate the VLAN messages only for the existing VLANs. MVRP PDUs and MVRP messages for the non-existing 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 Other Pruning Protocols

This section discusses MVRP interoperablity with other pruning protocols.

cGVRP

The GARP VLAN Registration Protocol (GVRP) is defined in IEEE 802.1q-1998 to allow dynamic registration and deregistration of VLANs on ports. Compact GVRP (cGVRP) is a modification of GVRP that reduces the number of packets required to transmit the state of a port. In addition, cGVRP provides rapidly VLAN pruning from point-to-point links without using Leave timer or Leave All garbage collection messaging. cGVRP is the pre-standard of MVRP. Both of cGVRP and MVRP are sharing one common VLAN/PM database. Hence, they can interoperate with each other, however both MVRP and cGVRP cannot be configured and running on the same device.

Compact GVRP has two modes: Slow Compact Mode, and Fast Compact Mode. A port can be in Fast Compact Mode if it has one GVRP enabled peer on the same LAN segment, and the peer is capable of operating in Compact Mode. A port is in Slow Compact Mode if there are multiple GVRP participants on the same LAN segment operating in Compact Mode.

VTP

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 .1Q trunks and ISL trunks. A VTP-capable device is in either one of the three VTP modes: Server, Client, or Transparent.

When VTP Pruning and MVRP are both enabled globally, VTP Pruning is run on ISL trunks, and GVRP is run on .1Q trunks.

VTP in Transparent or Off Mode

When VTP is in transparent or off mode, VTP PDUs are not processed and hence VTP pruning is not supported. The device operates like a dot1q device.

Upon receiving of a MVRP Join message for a VLAN on a port, the port is transmits broadcast, multicast, and unknown unicast frames in that VLAN and adds the traffic definition to a MAP port set for that VLAN. The mapping is undone when the VLAN is no longer registered on the port.

For each and every VLAN in the local VLAN database, if there is a local association, such as, an access port, SVI, or a VTP trunk port forwarding in the VLAN, MVRP issues a Join request to each MAD instance and an MVRP Join message is sent out on each corresponding MVRP port.

Dynamic VLAN creation can be enabled in VTP transparent 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 behaves like VTP in transparent, or off, mode with the exception that dynamic VLAN creation is not allowed.

VTP in Server or Client Mode and VTP Pruning is Enabled

When MVRP and VTP are both enabled on the same device, these two protocols have to communicate and exchange pruning information. VTP pruning and MVRP are mutually exclusive and cannot be configured on the same interface, but VTP protocol with pruning disabled and MVRP can be supported on the same interface.

When VTP receives a VTP Join message on a VTP trunk, the MVRP application needs to be notified so that Join request can be posted to the state machines in the MAD instances associated with MVRP ports, and MVRP Join can be sent out on the MVRP ports to the MVRP network. When VTP pruning removes a VLAN on a VTP trunk, MVRP sends a Leave request to all the MAD instances. If the MAD instances receive a Leave request event, then a Leave or Empty message is sent out on the MVRP ports to indicate that the device is no longer interested in declaring the VLAN.

When a MVRP Join message is received on a MVRP port, in addition to propagating this event to other MVRP ports in the same MAP context, the device also notifies the VTP pruning component so that VTP pruning can send out a VTP Join message out the VTP trunk ports to the VTP network. Similarly, if MVRP learns that a VLAN is no longer declared by the neighboring devices, it needs to indicate a withdrawal event to the VTP pruning component. VTP pruning will then check if it has to continue sending VTP Join message to the VTP network.

For VLANs that are configured to be 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 dot1q trunks.

MVRP Interoperability with Other Software Features and Protocols

This section describes interoperability with protocols, both supported and unsupported in conjunction with MVRP. The following protocols are addressed:

802.1x and Port Security

802.1x authenticates and authorizes a port after it becomes *link-up*, but before DTP negotiation occurs and MVRP runs on a port. Port security also works independently of MVRP.

When MVRP is globally enabled, the mac-address auto detect and provision feature is turned on by default. This can disable MAC learning under certain scenarios. This may prevent Port Security from working properly. For example, on Port Security ports, even though the number of streams exceeds the configured maximum number of mac address, no violation will be marked because the MAC learning is disabled in L2-Mgr and hence Port Security will not know there are more streams coming into the port. Use caution when turning on automatic MAC learning (using the **mvrp mac-learning auto** command) while Port Security is configured on the interfaces.

DTP

DTP negotiates the port mode (trunk vs. non-trunk) and the trunk encapsulation type between two DTP enabled ports. After negotiation DTP may set the port to either ISL trunk, dot1Q trunk, or non trunk. DTP negotiation occurs after ports become link-up and before they become forwarding in spanning trees. If MVRP is administratively enabled on a port and the device, it should be initialized after the port is negotiated to be a .1Q trunk.

EtherChannel

When multiple dot1Q trunk ports are grouped by either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP) to become an etherchannel, the etherchannel can be configured as an MVRP participant. The physical ports in the etherchannel cannot be MVRP participants by themselves. Since an etherchannel is treated like one virtual port by STP, the MVRP application can learn the STP state change of the etherchannel just like any physical port. The MAP context is mapped to the etherchannel interface, but not to the channel member ports.

Flexlink

Flexlink is a pair of switchport interfaces, one is active and the other is standby. When the active link fails, the standby interface takes over. The standby interface is set to blocking in both software and hardware. Hence, no data frames are allowed on the standby port except protocol PDUs.

MVRP must declare VLANs on STP forwarding ports but not on the blocking ports. If Flexlink is enabled, it must declare VLANs on the active ports but not on the standby ports. But when the flexlink standby port takes over the link-down active port, MVRP must be informed so that it can declare VLANs on this new active port.

High Availability

High Availability (HA) is a redundancy feature in Cisco IOS software. On platforms that support HA and State SwitchOver (SSO) and ISSU, many features and protocols my resume working in a couple of seconds after the system encounters a failure such as a crash of the active supervisor in a Catalyst 7600 switch. MVRP needs to be configured to enable user configurations, and protocol states should be synched to a standby system. If there is a failure of the active system, the MVRP in the standby system which now becomes active without a restart, has all the up-to-date VLAN registration information.

ISSU/EFSU

In-Service Software Upgrade (ISSU)/Enhanced Fast Software Upgrade (EFSU) allows for the upgrade or downgrade of software (ION) version with improved performances. It relies on the Stateful Switchover (SSO)/Nonstop Forwarding (NSF) architecture to allow different software versions on the active and standby supervisor to interact in a stateful manner. It is the intermediate phase towards ISSU/MDR for which the upgrade or downgrade will occur in a stateful manner (with the same performances as an SSO switchover). MVRP will be serviced by the ISSU client identified as ISSU_MVRP_CLIENT_ID and ISSU compliant.

L2PT

Layer 2 Protocol Tunneling (L2PT) allows Layer 2 protocol data units (PDUs), such as Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), Trunking Protocol (VLANs/VTP) (VTP) and Link Layer Discovery Protocol (LLDP) to be tunneled through a network. Without Layer 2 protocol tunneling, tunnel ports drop those protocol packets.

MVRP PDUs in Q-bridges (with 01-80-C2-00-00-21 frames) are not tunneled through the network by L2PT; only CDP, STP, VTP and LLDP PDUs are tunneled by L2PT.

MMRP

Multiple Multicast Registration Protocol (MMRP) is another dot1ak application for multicast registration protocol. MVRP and MMRP work independently and should be configured separately. MVRP and MMRP share the same MRP implementation.

REP

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol used to achieve fast reconvergence time in ring topologies aggregated by at least a pair of switches. It offers VLAN load balancing and an arbitrary number of switches can be put in a ring.

REP interface comes up in a blocked state, and, until it knows it is safe to unblock, it remains in blocked state. There are three port roles:

- Failed Port –A port with a non-operational link status.
- Alternate Port–An operational port, logically blocked for some VLANs.
- Open Port–A port forwarding traffic for all VLANs.

MVRP must declare VLANs on the Open Ports and declare non-blocking VLANs on the Alternate Ports. When the REP Alternate Port takes over the link-down Open Port, MVRP must be informed so that it can declare all VLANs on the new Open Port.

Note Running MVRP and REP together may block a port (with all VLANs being pruned on the port) and this can cause blocking of a segment port out of REP control. This can cause REP to lose control on the convergence of such a traffic. MVRP may introduce some delay for traffic recovery after REP reconvergence. You can disable MVRP to achieve fast reconvergence when REP is also used.

SPAN

Switched Port Analyzers (SPAN) work with VTP pruning ports. MVRP ports should be configured as either a SPAN source or destination port.

Switchport Blocking Unicast Traffic

The **switchport block unicast** command administratively blocks flooded traffic by disabling forwarding of unknown unicast and multicast addresses on a particular switchport interface. MVRP also prunes flooded traffic at runtime. These two features are mutually exclusive and cannot be configured on the same interface.

STP

Spanning Tree Protocol (STP) may run in one of the three STP modes: Multiple Spanning Tree (MST), Per VLAN Spanning Tree (PVST), or Rapid PVST. An STP mode range causes the forwarding ports to leave the forwarding state as STP has to reconverge. The reconvergence might cause MVRP to have its own topology changes as Join s may be received on some new forwarding ports, and Leave timers may expire on some other ports.

UDLR

Unidirectional link routing (UDLR) limits frames in one direction and MVRP is a two-way communication protocol. Hence, UDLR and MVRP are mutually exclusive and cannot be configured on the same port.

VLANs with MVRP

This section discusses topics related to VLANs with MVRP.

VLAN Mapping

VLAN Mapping, also known as VLAN translation, maps 802.1q frames from the original VLAN (the VLAN indicated in the 802.1q tag in the frames) to a different VLAN on a device. In other words, it is a *translated* VLAN. If VLAN Mapping is enabled, MVRP translates the original VLAN IDs in the coming MVRP PDUs to the translated VLAN ids and then processes the request. Similarly, before MVRP sends PDUs out to a port, it inserts the original VLAN IDs in the PDUs, if VLAN Mapping is enabled on the port.

VLAN Mapping is an expensive operation to support on MVRP because it requires a lookup for each VLAN coming in with the MVRP PDU, and another lookup when the MVRP PDU is sent out.

All VLAN Tagging

All VLAN tagging, also known as, Native VLAN tagging, causes the frames sent in the native VLAN of the dot1q trunk ports to be encapsulated with a dot1q tag. Other MVRP participants on the LAN may not be able to accept tagged MVRP PDUs and can cause network issues. You should design your network carefully when both MVRP and Native VLAN tagging are configured.

Private VLANs

Private VLANs provide Layer 2 isolation between ports within the same private VLAN. There are three types of private VLAN ports:

- **Promiscuous**—A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.
- **Isolated**— An isolated port is a host port that belongs to an isolated secondary VLAN. It has complete Layer 2 separation from other ports within the same private VLAN except for the promiscuous port. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports.
- **Community**—A community port is a host port that belongs to a community secondary VLAN. Community ports communicate among themselves and with their promiscuous ports. These interfaces are isolated at Layer 2 from all other interfaces in other communities or isolated ports within their private VLAN.

Note MVRP and private VLAN porta are mutually exclusive. MVRP should declare both the primary VLAN and secondary VLANs of a private VLAN host port or promiscuous port.

VTP

VTP version 3 expands the range of VLANs that can be created and removed via VTP. VTP Pruning is available for VLANs 1 - 1005 only.

How to Configure MVRP

MVRP can be configured on the entire switch or on specific interface. MVRP is operational on an interface only if it is administratively enabled both globally and at the interface level. Only when MVRP is operational on an interface can MVRP PDUs be transmitted out of the interface, and other MVRP-related operations be effective. The interface must be a forwarding dot1q trunk. The following tasks are included:

- Enabling MVRP, page 10
- Enabling Automatic Detection of MAC Addresses, page 12
- Enabling MVRP Dynamic VLAN Creation, page 12
- Changing the MVRP Registrar State, page 13

Enabling MVRP

When MVRP is enabled globally, it is operational on 802.1q trunk ports only. To be enabled on an interface, it must be configured on the specific interface. To enable MVRP, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mvrp global**
4. **interface** *type number*
5. **exit**
6. **mvrp global**
7. **interface** *type number*
8. **exit**
9. **mvrp global**
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mvrp global** **Example:** `Router(config)# mvrp global`	Configures global MVRP and enables MVRP on all .1Q trunks.
Step 4	**interface** *type number* **Example:** `Router(config)# interface FastEthernnet 2/1`	Specifies and interface and enters interface configuration mode. • Enter an interface type and interface number.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 6	**mvrp global** **Example:** `Router(config)# mvrp global`	Enables MVRP on the interface.
Step 7	**interface** *type number* **Example:** `Router(config)# interface FastEthernnet 2/2`	Specifies an interface and enters interface configuration mode. • Enter an interface type and interface number.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 9	**mvrp global** **Example:** `Router(config)# mvrp global`	Enables MVRP on the interface.
Step 10	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Enabling Automatic Detection of MAC Addresses

You can enable automatic detection of (and provisioning for) MAC addresses globally on the switch. MVRP automatic detection of MAC addresses is disabled by default. To enable MVRP automatic detection of MAC addresses on VLANs, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mvrp mac-learning auto**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mvrp mac-learning auto** **Example:** `Router(config)# gvrp mac-learning auto`	Enables learning of MAC entries.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits privileged EXEC mode.

Enabling MVRP Dynamic VLAN Creation

VLANs can be created dynamically when MVRP is enabled. This can be done only if VTP is in transparent mode. To enable an MVRP dynamic VLAN, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vtp mode transparent**
4. **mvrp vlan creation**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**vtp mode transparent** **Example:** `Router(config)# vtp mode transparent`	Sets VTP mode to transparent.
Step 4	**mvrp vlan creation** **Example:** `Router(config)# gvrp vlan create`	Enables a dynamic VLAN creation when MRVP is configured.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Changing the MVRP Registrar State

You can set the registrar in an MRP Attribute Declaration (MAD) instance associated with an interface to one of three possible states. An MRP-aware device can be in one of the following participant states:

- Active Participants–participants that have sent a message or messages to make a declaration to register.
- Passive Participants–require registration, but have not had to declare the attribute to register, and will not have to explicitly deregister.
- Observer–does not require registration, but tracks the attribute's registration in case it does require registration and becomes a passive participant.

The MRP protocol allows one participant per application in an end station, and one per application per port in a bridge.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mvrp registration** [**normal | fixed | forbidden**]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mvrp registration** [**normal** | **fixed** | **forbidden**] **Example:** `Router(config)# mvrp registration normal`	Registers MVRP with the MAD instance.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode.

Troubleshooting the MVRP Configuration

Perform this task to troubleshoot 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.

SUMMARY STEPS

1. **enable**
2. **show mvrp summary**
3. **show mvrp interface** *interface-type port/slot*
4. **debug mvrp [all | config | error | event | ha | packets | switch]**
5. **clear mvrp statistics**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show mvrp summary** **Example:** `Router# show mvrp summary`	Displays the MVRP configuration.
Step 3	**show mvrp interface** *interface-type port/slot* **Example:** `Router# show mvrp interface fastethernet0/0`	Displays the MVRP interface states for the specified interface. • Enter the interface type and port/slot number.
Step 4	**debug gvrp** **Example:** `Router# debug gvrp`	Displays GVRP debugging information.
Step 5	**clear mvrp statistics** **Example:** `Router# clear mvrp statistics`	Clears MVRP statistics on all interfaces.
Step 6	**end** **Example:** `Router# end`	Exits privileged EXEC mode.

Example

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 IEEE 802.1q 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

This section provides the following configuration examples:

Enabling MVRP: Example

The following example shows how to enable MVRP.

```
Router> enable
Router# configure terminal
Router(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on 802.1q trunk ports only.
Router(config)# interface fastethernet2/1
Router(config-if)# exit
Router(config)# mvrp global
Router(config)# interface fastethernet2/2
Router(config-if)# exit
Router(config)# mvrp global
Router(config)# end
```

Enabling Automatic Detection of MAC Addresses: Example

The following example shows how to enable the automatic detection of MAC addresses.

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

Enabling Dynamic VLAN Creation: Example

The following example shows how to enable dynamic VLAN creation.

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

Changing the MVRP Registrar State: Example

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

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

Additional References

The following sections provide references related to the IEEE 802.1ak - MVRP and MRP feature.

Related Documents

Related Topic	Document Title
IP LAN switching commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS LAN Switching Services Command Reference*
Information about cGVRP	"cGRVP" module

Standards

Standard	Title
IEEE 802.1ak	*Multiple Registration Protocol*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IEEE 802.1ak - MVRP and MRP

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 IEEE 802.1ak - MVRP and MRP

Feature Name	Releases	Feature Information
IEEE 802.1ak - MVRP and MRP	12.2(33)SXI	Implementation of the IEEE 802.1ak standard allows for dynamic registration and deregistration of VLANs on ports in a VLAN bridged network. This document describes Multiple Registration Protocol (MRP) and Multiple VLAN Registration Protocol (MVRP) as specified in the IEEE 802.1ak standard. MVRP and MRP are intended to replace the GVRP and GARP protocols specified in earlier versions of the IEEE 802.1Q standard. The following commands were introduced or modified to support this feature: **clear mvrp statistics, debug mrp, debug mvrp, mvrp global, mvrp mac-learning, mvrp registration, mvrp timer**, **mvrp vlan creation, show mvrp interface, show mvrp module, show mvrp summary.**