Configuring Dynamic VLAN Membership

This chapter describes how to configure dynamic port VLAN membership by using the VLAN Membership Policy Server (VMPS).

This chapter includes the following major sections:

Note For complete syntax and usage information for the switch commands used in this chapter, look at the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html

If the command is not found in the Catalyst 4500 Command Reference, it is located in the larger Cisco IOS library. Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* and related publications at this location:

http://www.cisco.com/en/US/products/ps6350/index.html

Understanding VMPS

This section includes the following subsections:

With the VMPS, you can dynamically assign switch ports to VLANs based on the source Media Access Control (MAC) address of the device connected to the port. When you move a host from a port on one switch in the network to a port on another switch in the network, that switch dynamically assigns the new port to the proper VLAN for that host.

A Catalyst 4500 series switch can be a member switch or a command switch in a cluster of switches managed as a single entity. The communication between VMPS and a member switch is managed by the command switch. In this description, the VMPS client is always the command switch.

A Catalyst 4500 series switch acts as a client to the VMPS and communicates with it by using the VLAN Query Protocol (VQP). When the VMPS receives a VQP request from a client switch, the VMPS searches its database for a MAC address-to-VLAN mapping. The server response is based on this mapping. If the server is in secure mode, the server shuts down the port when a VLAN is not allowed on it, or the server simply denies the port access to the VLAN.

In response to a request, the VMPS takes one of the following actions:

- If the assigned VLAN is restricted to a group of ports, the VMPS verifies the requesting port against this group and responds as follows:

    - If the VLAN is allowed on the port, the VMPS sends the VLAN name to the client in response.

    - If the VLAN is not allowed on the port, and the VMPS is not in secure mode, the VMPS sends an *access-denied* response.

    - If the VLAN is not allowed on the port, and the VMPS is in secure mode, the VMPS sends a *port-shutdown* response.

- If the VLAN in the database does not match the current VLAN on the port, and there are active hosts on the port, the VMPS sends an *access-denied* or a *port-shutdown* response, depending on the secure mode of the VMPS.

    If the switch receives an *access-denied* response from the VMPS, the switch continues to block traffic from the MAC address to or from the port. The switch continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new address. If the switch receives a *port-shutdown* response from the VMPS, the switch disables the port. The port must be manually reenabled by using the CLI, Cisco Visual Switch Manager (CVSM), or SNMP.

    You can also use an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons. If you enter the **none** keyword for the VLAN name, the VMPS sends an *access-denied* or *port-shutdown* response.

Entering Port Names in the VMPS

A VMPS database configuration file must use the Catalyst 4500 series convention for naming ports. For example, Fa0/5 is fixed-port number 5.

If the switch is a cluster member, the command switch adds the name of the switch before the "Fa" in the port name. For example, es3%Fa02 refers to fixed 10/100 port 2 on member switch 3. These naming conventions must be used in the VMPS database configuration file when the VMPS is configured to support a cluster.

You can configure a fallback VLAN name. If you connect a device with a MAC address that is not in the database, the VMPS sends the fallback VLAN name to the client. If you do not configure a fallback VLAN name and the MAC address does not exist in the database, the VMPS sends an *access-denied* response. If the VMPS is in secure mode, it sends a *port-shutdown* response.

Dynamic Port VLAN Membership

A dynamic (nontrunking) port can belong to only one VLAN. When the link comes up, the switch does not forward traffic to or from this port until the port is assigned to a VLAN. The source MAC address from the first packet of a new host on the dynamic port is sent to the VMPS, which attempts to match the MAC address to a VLAN in the VMPS database. If there is a match, the VMPS sends the VLAN

number for that port. If there is no match, the VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting). See the "Understanding VMPS" section on page 9-1 for a complete description of possible VMPS responses.

Multiple hosts (MAC addresses) can be active on a dynamic port if they are all in the same VLAN. If the link goes down on a dynamic port, the port returns to an isolated state and does not belong to a VLAN. Any hosts that come online through the port are checked again with the VMPS before the port is assigned to a VLAN.

Note   The VMPS shuts down a dynamic port if more than 20 hosts are active on that port.

VMPS Configuration Guidelines

The following guidelines and restrictions apply to dynamic port VLAN membership:

- You must configure the VMPS before you configure ports as dynamic.
- The communication between a cluster of switches and the VMPS is managed by the command switch and includes port-naming conventions that are different from standard port names. See "Entering Port Names in the VMPS" section on page 9-2 for the cluster-based port-naming conventions.
- When you configure a port as dynamic, the spanning-tree PortFast feature is automatically enabled for that port. The PortFast mode accelerates the process of bringing the port into the forwarding state. You can disable PortFast mode on a dynamic port.
- Secure ports cannot be dynamic ports. You must disable port security on the port before it becomes dynamic.
- Trunk ports cannot be dynamic ports, but it is possible to enter the **switchport access VLAN dynamic** command for a trunk port. In this case, the switch retains the setting and applies it if the port is later configured as an access port.

  You must turn off trunking on the port before the dynamic access setting takes effect.

- Dynamic ports cannot be network ports or monitor ports.

Note   The VTP management domain of the VMPS client and the VMPS server must match.

Default VMPS Configuration

Table 9-1 shows the default VMPS and dynamic port configuration on client switches.

Table 9-1   Default VMPS Client and Dynamic Port Configuration

Feature	Default Configuration
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3
Dynamic ports	None configured

Configuring Dynamic VLAN Membership

These subsections describe how to configure a switch as a VMPS client and configure its ports for dynamic VLAN membership.

The following topics are included:

Entering the IP Address of the VMPS

To configure the switch as a client, you must enter the IP address of the Catalyst 4500 series switch or the other device acting as the VMPS.

To define a VMPS for a cluster of switches, perform this task:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(config)# **vmps server** *ipaddress* **primary**	Enters the IP address of the switch acting as the primary VMPS server.
Step 3	Switch(config)# **vmps server** *ipaddress*	Enters the IP address for the switch acting as a secondary VMPS server.
Step 4	Switch(config)# **end**	Returns to privileged EXEC mode.
Step 5	Switch# **show vmps**	Verifies the VMPS server entry.

This example shows how to enter the primary and backup VMPS devices:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# vmps server 172.20.128.179 primary
Switch(config)# vmps server 172.20.128.178
Switch(config)# end

Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.179 (primary, current)
                    172.20.128.178

Reconfirmation status
---------------------
VMPS Action:        No Dynamic Port
```

Configuring Dynamic Ports on VMPS Clients

To configure dynamic ports on the VMPS client switches, perform this task:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(config)# **interface** *interface*	Enters interface configuration mode and the port to be configured.
Step 3	Switch(config-if)# **switchport mode access**	Sets the port to access mode.
Step 4	Switch(config-if)# **switchport access vlan dynamic**	Configures the port as eligible for dynamic VLAN access.
Step 5	Switch(config-if)# **end**	Returns to privileged EXEC mode.
Step 6	Switch# **show interface** *interface* **switchport**	Verifies the entry.

This example shows how to configure a port as a dynamic access port and then verify the entry:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fa0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan dynamic
Switch(config-if)# end

Switch# show interface fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative mode: dynamic access
Operational Mode: dynamic access
Administrative Trunking Encapsulation: isl
Operational Trunking Encapsulation: isl
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: NONE
```

Administering and Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** command in mode privileged EXEC.

The switch displays the following information about the VMPS:

VMPS VQP Version	The version of VQP used to communicate with the VMPS. The switch queries the VMPS using version 1 of VQP.
Reconfirm Interval	The number of minutes the switch waits before reconfirming the VLAN-to-MAC-address assignments.
Server Retry Count	The number of times VQP resends a query to the VMPS. If no response is received after this many tries, the switch starts to query the secondary VMPS.
VMPS domain server	The IP address of the configured VLAN membership policy servers. The switch currently sends queries to the one marked *current*. The one marked *primary* is the primary server.
VMPS Action	The result of the most-recent reconfirmation attempt. This can happen automatically when the reconfirmation interval expired, or you can force it by entering the privileged EXEC **vmps reconfirm** command or its CVSM or SNMP equivalent.

The following example shows how to display VMPS information. You can enter this information on a command or member switch:

```
Switch# show vmps
VQP Client Status:
-------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
---------------------
VMPS Action:        other

The following example shows how to display VMPS statistics:
Switch# show vmps statistics
VMPS Client Statistics
----------------------
VQP  Queries:             0
VQP  Responses:           0
VMPS Changes:             0
VQP  Shutdowns:           0
VQP  Denied:              0
VQP  Wrong Domain:        0
VQP  Wrong Version:       0
VQP  Insufficient Resource: 0
```

Note Refer to the *Catalyst 4500 Series Switch Cisco IOS Command Reference* for details on the VMPS statistics.

Configuring the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the interval at which the reconfirmation will occur.

To configure the reconfirmation interval, perform this task:

	Command	Purpose
Step 1	Switch# **configure terminal**	Enters global configuration mode.
Step 2	Switch(config)# **vmps reconfirm** *minutes*	Enters the number of minutes between reconfirmations of the dynamic VLAN membership.
Step 3	Switch(config)# **end**	Returns to privileged EXEC mode.
Step 4	Switch# **show vmps**	Verifies the dynamic VLAN reconfirmation status.

This example shows how to change the reconfirmation interval to 60 minutes and verify the change by displaying the VMPS information:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# vmps reconfirm 60
Switch(config)# end

Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 10
VMPS domain server: 172.20.130.50 (primary, current)

Reconfirmation status
--------------------
VMPS Action:         No Host
```

Reconfirming VLAN Memberships

To confirm the dynamic port VLAN membership assignments that the switch has received from the VMPS, perform this task in privileged EXEC mode:

	Command	Purpose
Step 1	Switch(config)# **vmps reconfirm**	Reconfirms dynamic port VLAN membership.
Step 2	Switch# **show vmps**	Verifies the dynamic VLAN reconfirmation status.

Troubleshooting Dynamic Port VLAN Membership

The VMPS shuts down a dynamic port under these conditions:

- The VMPS is in secure mode, and it will not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.

- More than 20 active hosts reside on a dynamic port.

  To reenable a shut-down dynamic port, enter the **no shutdown** command in interface configuration mode.