



Configuring Dynamic Port VLAN Membership with VMPS

This chapter describes how to configure dynamic port virtual LAN (VLAN) membership using the VLAN Management Policy Server (VMPS) on the Catalyst enterprise LAN switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter consists of these sections:

- [Understanding How VMPS Works, page 12-1](#)
- [VMPS and Dynamic Port Hardware and Software Requirements, page 12-2](#)
- [Default VMPS and Dynamic Port Configuration, page 12-2](#)
- [Dynamic Port VLAN Membership and VMPS Configuration Guidelines, page 12-3](#)
- [Configuring VMPS and Dynamic Port VLAN Membership, page 12-3](#)
- [Troubleshooting VMPS and Dynamic Port VLAN Membership, page 12-6](#)
- [Dynamic Port VLAN Membership with VMPS Configuration Examples, page 12-7](#)
- [Dynamic Port VLAN Membership with Auxiliary VLANs, page 12-10](#)

Understanding How VMPS Works

With VMPS, you can assign switch ports to VLANs dynamically, based on the source 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, the switch assigns the new port to the proper VLAN for that host dynamically.



Note

When you configure dynamic VLAN membership using VMPS, the default mode “open” is designed to prevent the hosts movement across dynamic vlans, where hosts are connected behind some devices (for example IP phones) without the link down in the switch port side and the assignment of VLANs for the hosts will get stuck after a host is swapped three or four times across different VLANs. The above problem can be overcome by setting the default mode to “multiple.”

When you enable VMPS, a MAC address-to-VLAN mapping database downloads from a Trivial File Transfer Protocol (TFTP) server and VMPS begins to accept client requests. If you reset or power cycle the switch, the VMPS database downloads from the TFTP server automatically and VMPS is reenabled.

VMPS opens a User Datagram Protocol (UDP) socket to communicate and listen to client requests. When the VMPS server receives a valid request from a client, it searches its database for a MAC address-to-VLAN mapping.

If the assigned VLAN is restricted to a group of ports, VMPS verifies the requesting port against this group. If the VLAN is allowed on the port, the VLAN name is returned to the client. If the VLAN is not allowed on the port and VMPS is not in secure mode, the host receives an “access denied” response. If VMPS is in secure mode, the port is shut down.

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

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

You can also make an explicit entry in the configuration table to deny access to specific MAC addresses for security reasons by specifying a **--NONE--** keyword for the VLAN name. In this case, VMPS sends an access denied or port shutdown response.

A dynamic port can belong to only one *native* VLAN in software releases prior to software release 6.2(1). With software release 6.2(1), a port can belong to a native VLAN and an auxiliary VLAN. See the “[Dynamic Port VLAN Membership with Auxiliary VLANs](#)” section on page 12-10 for complete details.

When the link comes up, a dynamic port is isolated from its static VLAN. The source MAC address from the first packet of a new host on the dynamic port is sent to VMPS, which attempts to match the MAC address to a VLAN in the VMPS database. If there is a match, VMPS provides the VLAN number to assign to the port. If there is no match, VMPS either denies the request or shuts down the port (depending on the VMPS secure mode setting).

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. Any hosts that come online through the port are checked again with VMPS before the port is assigned to a VLAN.

VMPS and Dynamic Port Hardware and Software Requirements

VMPS and dynamic port membership requires these software and hardware versions (later software versions might be required depending on the specific hardware):

- Supervisor engine software release 5.1 or later—The Catalyst 4000 family switches can function only as VMPS clients.
- VMPS-capable hardware—To determine whether a specific piece of hardware supports dynamic port VLAN membership, refer to your hardware documentation or use the **show port capabilities** command.

Default VMPS and Dynamic Port Configuration

[Table 12-1](#) shows the default VMPS client and dynamic port configuration.

Table 12-1 Default VMPS Client and Dynamic Port Configuration

Feature	Default Configuration
VMPS domain server	None
VMPS reconfirm interval	60 minutes
VMPS server retry count	3 attempts
Dynamic ports	No dynamic ports configured

Dynamic Port VLAN Membership and VMPS Configuration Guidelines

These guidelines and restrictions apply to dynamic port VLAN membership:

- You cannot configure a Catalyst 4000 family switch as a VMPS server.
- You must configure VMPS before you configure ports as dynamic.
- When you configure a port as dynamic, spanning tree PortFast is enabled automatically for that port. Automatic enabling of spanning tree PortFast prevents applications on the host from timing out and entering loops caused by incorrect configurations. You can disable spanning tree PortFast mode on a dynamic port.
- If you reconfigure a port from a static port to a dynamic port on the same VLAN, the port connects immediately to that VLAN. However, VMPS checks the legality of the specific host on the dynamic port after a specified period.
- Static secure ports cannot become dynamic ports. You must turn off security on the static secure port before it can become dynamic.
- Static ports that are trunking cannot become dynamic ports. You must turn off trunking on the trunk port before changing it from static to dynamic.



Note

The VTP management domain and the management VLAN of VMPS clients and the VMPS server must be the same. For more information, see [Chapter 9, “Configuring VTP,”](#) and [Chapter 10, “Configuring VLANs.”](#)

Configuring VMPS and Dynamic Port VLAN Membership

These sections describe how to configure VMPS and define dynamic ports on clients:

- [Creating the VMPS Database, page 12-4](#)
- [Configuring VMPS, page 12-4](#)
- [Configuring Dynamic Ports on VMPS Clients, page 12-5](#)
- [Configuring Static VLAN Port Membership, page 12-6](#)

Creating the VMPS Database

To use VMPS, you first must create a VMPS database and store it on a TFTP server. The VMPS parser is line based. Start each entry in the file on a new line. Ranges are not allowed for the port numbers.



Note

For an example ASCII text VMPS database configuration file, see the [“VMPS Database Configuration File Example” section on page 12-7](#).

Follow these guidelines for creating the VMPS database file:

- Begin the configuration file with the word “VMPS,” to prevent other types of configuration files from incorrectly being read by the VMPS server.
- Define the VMPS domain—The VMPS domain should correspond to the VTP domain name configured on the switch.
- Define the security mode—VMPS can operate in open or secure mode.
- (Optional) Define a fallback VLAN—The fallback VLAN is assigned if the MAC addresses of the connected host is not defined in the database.
- Define the MAC address-to-VLAN name mappings—Enter the MAC address of each host and the VLAN to which each should belong. Use the **--NONE--** keyword as the VLAN name to deny the specified host network connectivity. A port is identified by the IP address of the switch and the module/port number of the port in the form *mod_num/port_num*.
- Define port groups—A port group is a logical group of ports. You can apply VMPS policies to individual ports or to port groups. The keyword **all-ports** specifies all the ports in the specified switch.
- Define VLAN groups—A VLAN group defines a logical group of VLANs. These logical groups define the VLAN port policies.
- Define VLAN port policies—VLAN port policies define the ports associated with a restricted VLAN. You can configure a restricted VLAN by defining the set of dynamic ports on which it can exist.

To create a VMPS database, perform this task:

	Task	Command
Step 1	Determine the MAC addresses of the hosts you want to be assigned to VLANs dynamically.	show cam
Step 2	Create an ASCII text file on your workstation or PC that contains the MAC address-to-VLAN mappings.	–
Step 3	Move the ASCII text file to a TFTP server so it can be downloaded to the switch.	–

Configuring VMPS

When you enable VMPS, the switch downloads the VMPS database from the TFTP or rcp server and begins accepting VMPS requests.

To configure VMPS, perform this task in privileged mode:

	Task	Command
Step 1	Specify the download method.	set vmps downloadmethod rcp tftp [username]
Step 2	Configure the IP address of the TFTP or rcp server on which the ASCII text VMPS database configuration file resides.	set vmps downloadserver ip_addr [filename]
Step 3	Verify the VMPS configuration.	show vmps

Configuring Dynamic Ports on VMPS Clients

To configure dynamic ports on VMPS client switches, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of the VMPS server (the switch with VMPS enabled).	set vmps server ip_addr [primary]
Step 2	Verify the VMPS server specification.	show vmps server
Step 3	Configure dynamic port VLAN membership assignment to a port.	set port membership mod_num/port_num dynamic
Step 4	Verify the dynamic port assignments.	show port [mod_num[/port_num]]

This example shows how to specify the VMPS server, verify the VMPS server specification, assign dynamic ports, and verify the configuration:

```

Console> (enable) show vmps server
VMPS domain server VMPS Status
-----
192.0.0.6
192.0.0.1      primary
192.0.0.9
Console> (enable) set port membership 3/1-3 dynamic
Ports 3/1-3 vlan assignment set to dynamic.
Spanntree port fast start option enabled for ports 3/1-3.
Console> (enable) set port membership 1/2 dynamic
Trunking port 1/2 vlan assignment cannot be set to dynamic.
Console> (enable) set port membership 2/1 dynamic
ATM LANE port 2/1 vlan assignment can not be set to dynamic.
Console> show port
Port  Name      Status  Vlan    Level  Duplex    Speed    Type
1/1      connect  dyn-3   normal  full     100     100 BASE-TX
1/2      connect  trunk   normal  half     100     100 BASE-TX
2/1      connect  trunk   normal  full     155     OC3 MMF ATM
3/1      connect  dyn-5   normal  half     10      10 BASE-T
3/2      connect  dyn-5   normal  half     10      10 BASE-T
3/3      connect  dyn-5   normal  half     10      10 BASE-T
Console> (enable)

```



Note

The **show port** command displays *dyn-* under the Vlan column of the display when it has not yet been assigned a VLAN for a port.

Configuring Static VLAN Port Membership

To return a port to static VLAN port membership, perform this task in privileged mode:

	Task	Command
Step 1	Configure static port VLAN membership assignment to a port.	set port membership <i>mod_num/port_num</i> static
Step 2	Verify the static port assignments.	show port [<i>mod_num[/port_num]</i>]

This example shows how to return a port to static VLAN port membership:

```
Console> (enable) set port membership 3/1 static
Port 3/1 vlan assignment set to static.
Console> (enable)
```

Troubleshooting VMPS and Dynamic Port VLAN Membership

These sections describe how to troubleshoot VMPS and dynamic port VLAN membership:

- [Troubleshooting VMPS, page 12-6](#)
- [Troubleshooting Dynamic Port VLAN Membership, page 12-7](#)

Troubleshooting VMPS

[Table 12-2](#) shows VMPS error messages you might see when you enter the **set vmps state enable** or the **download vmps** command.

Table 12-2 VMPS Error Messages

VMPS Error Message	Recommended Action
TFTP server IP address is not configured.	Specify the TFTP server address using the set vmps tftpserver ip_addr [filename] command.
Unable to contact the TFTP server 172.16.254.222.	Enter a static route (using the set ip route command) to the TFTP server.
File "vmeps_configuration.db" not found on the TFTP server 172.16.254.222.	Check the filename of the VMPS database configuration file on the TFTP server. Make sure the permissions are set correctly.
Enable failed due to insufficient resources.	The switch does not have sufficient resources to run the database. You can fix this problem by increasing the dynamic random-access memory (DRAM).

After VMPS successfully downloads the VMPS database configuration file, it parses the file and builds a database. When the parsing is complete, VMPS outputs statistics about the total number of lines parsed and the number of parsing errors.

To obtain more information on VMPS parsing errors, set the syslog level for VMPS to 3 using the **set logging level vmeps 3** command.

Troubleshooting Dynamic Port VLAN Membership

A dynamic port might shut down under these circumstances:

- VMPS is in secure mode and it is illegal for the host to connect to the port. The port shuts down to prevent the host from connecting to the network.
- More than 50 active hosts reside on a dynamic port.

To reenable a shut-down dynamic port, enter the **set port enable *mod_num/port_num*** command.

Dynamic Port VLAN Membership with VMPS Configuration Examples

These sections show examples of how to configure VMPS and dynamic ports:

- [VMPS Database Configuration File Example, page 12-7](#)
- [Dynamic Port VLAN Membership Configuration Example, page 12-8](#)

VMPS Database Configuration File Example

This example shows a sample VMPS database configuration file. A VMPS database configuration file is an ASCII text file that is stored on a TFTP server accessible to the switch configured as the VMPS server.

```
!VMPS File Format, version 1.1
! Always begin the configuration file with
! the word "VMPS"
!
!vmps domain <domain-name>
! The VMPS domain must be defined.
!vmps mode {open | secure}
! The default mode is open.
!vmps fallback <vlan-name>
!vmps no-domain-req { allow | deny }
!
! The default value is allow.
vmps domain WBU
vmps mode open
vmps fallback default
vmps no-domain-req deny
!
!
!MAC Addresses
!
vmps-mac-addr
!
! address <addr> vlan-name <vlan_name>
!
address 0012.2233.4455 vlan-name hardware
address 0000.6509.a080 vlan-name hardware
address aabb.ccdd.eeff vlan-name Green
address 1223.5678.9abc vlan-name ExecStaff
address fedc.ba98.7654 vlan-name --NONE--
address fedc.ba23.1245 vlan-name Purple
!
!Port Groups
```

```

!
!vmps-port-group <group-name>
! device <device-id> { port <port-name> | all-ports }
!
vmps-port-group WiringCloset1
 device 198.92.30.32 port 3/2
 device 172.20.26.141 port 2/8
vmps-port-group "Executive Row"
 device 198.4.254.222 port 1/2
 device 198.4.254.222 port 1/3
 device 198.4.254.223 all-ports
!
!
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
vlan-name hardware
vlan-name software
!
!
!VLAN port Policies
!
!vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
! { port-group <group-name> | device <device-id> port <port-name> }
!
vmps-port-policies vlan-group Engineering
 port-group WiringCloset1
vmps-port-policies vlan-name Green
 device 198.92.30.32 port 4/8
vmps-port-policies vlan-name Purple
 device 198.4.254.22 port 1/2
 port-group "Executive Row"

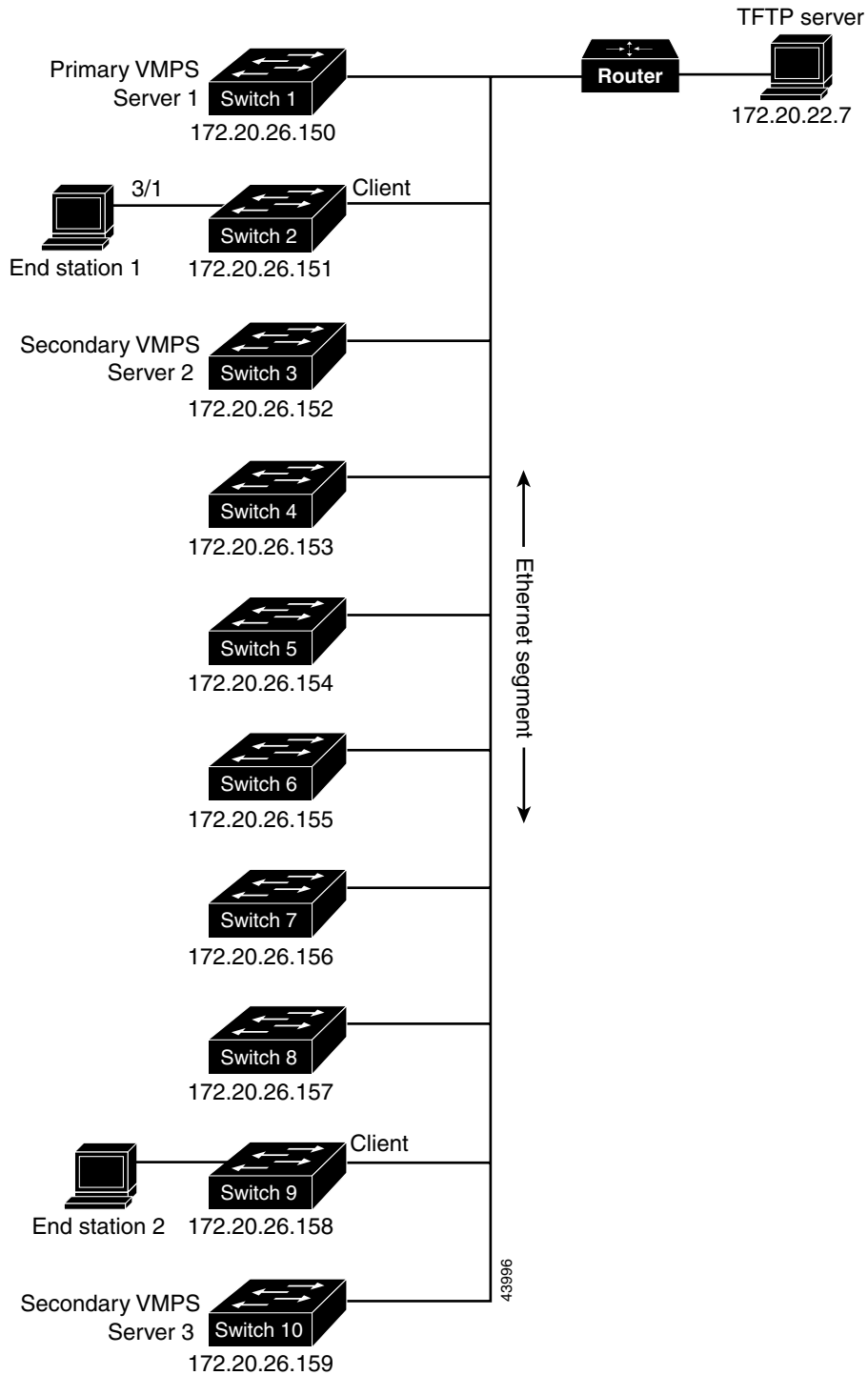
```

Dynamic Port VLAN Membership Configuration Example

Figure 12-1 shows a network with a VMPS server switch and VMPS client switches with dynamic ports. In this example, these assumptions apply:

- The VMPS server and the VMPS client are separate switches.
- Switch 1 is the primary VMPS server.
- Switch 3 and Switch 10 are secondary VMPS servers.
- End stations are connected to these clients:
 - Switch 2
 - Switch 9
- The database configuration file is called Bldg-G.db and is stored on a TFTP server with IP address 172.20.22.7.

Figure 12-1 Dynamic Port VLAN Membership Configuration



To configure VMPS and dynamic ports, follow these steps:

-
- Step 1** Configure the VMPS server addresses on each VMPS client:
- a. Configure the primary VMPS server IP address:

```
Console> (enable) set vmps server 172.20.26.150 primary
```
 - b. Configure the secondary VMPS server IP addresses:

```
Console> (enable) set vmps server 172.20.26.152
```

```
Console> (enable) set vmps server 172.20.26.159
```
 - c. Verify the VMPS server addresses:

```
Console> (enable) show vmps server
```
- Step 2** Configure port 3/1 on Switch 2 as dynamic:

```
Console> (enable) set port membership 3/1 dynamic
```
- Step 3** Connect End Station 2 on port 3/1. When End Station 2 sends a packet, Switch 2 sends a query to the primary VMPS server, Switch 1. Switch 1 responds with the VLAN to assign to port 3/1. Because spanning tree PortFast mode is enabled by default on dynamic ports, port 3/1 connects immediately and enters forwarding mode.
- Step 4** Repeat Steps 2 and 3 to configure the VMPS server addresses and assign dynamic ports on each VMPS client switch.
-

Dynamic Port VLAN Membership with Auxiliary VLANs



Note

This feature requires software release 6.2(1) or later releases.

This section describes how to configure a dynamic port to belong to two VLANs—a native VLAN and an auxiliary VLAN. This section uses the following terminology:

- Auxiliary VLAN—Separate VLAN for IP phones
- Native VLAN—Traditional VLAN for data
- Auxiliary VLAN ID—VLAN ID of an auxiliary VLAN
- Native VLAN ID—VLAN ID of a native VLAN

Prior to software release 6.2(1), dynamic ports could only belong to one VLAN. You could not enable the dynamic port VLAN feature on ports that carried a native VLAN and an auxiliary VLAN.

With software releases 6.2(1) and later, the dynamic ports can belong to two VLANs. The switch port configured for connecting an IP phone can have separate VLANs configured for carrying:

- Voice traffic to and from the IP phone (auxiliary VLAN)
- Data traffic to and from the PC connected to the switch through the *access port* of the IP phone (native VLAN)

**Note**

For detailed information on auxiliary VLANs and Cisco voice-over-IP networks, refer to the "Configuring a Voice-over-IP Network" chapter in the *Catalyst 6000 Family Software Configuration Guide*.

Configuration Guidelines

These guidelines and restrictions apply to configuring dynamic port VLAN membership for auxiliary VLANs:

- Configuration of the native VLAN ID is dynamic for the PC connected to the access port of the IP phone. Configuration of the auxiliary VLAN ID is not dynamic, you need to configure it manually. As you manually configure the auxiliary VLAN ID, the VMPS server is queried for packets coming from the PC, but not for packets coming from the IP phone.
- All packets except CDP packets from the IP phone are tagged with the auxiliary VLAN ID. All such tagged packets are considered to be packets from the phone, and all other packets are considered to be packets from the PC.
- When configuring the auxiliary VLAN ID with untagged frames, you need to configure the VMPS server with the IP phone's MAC address (see the "[Dynamic Port VLAN Membership with VMPS Configuration Examples](#)" section on page 12-7 for information on configuring VMPS).
- For dynamic ports, the auxiliary VLAN ID cannot be the same as the native VLAN ID assigned by VMPS for the dynamic port.
- Read the "[Dynamic Port VLAN Membership and VMPS Configuration Guidelines](#)" section on page 12-3 prior to doing any port configuration.

Configuring Dynamic Port VLAN Membership with Auxiliary VLANs

This example shows how to add voice ports to auxiliary VLANs and specify an encapsulation type:

```

Console> (enable) set port auxiliaryvlan 5/9 222
Auxiliaryvlan 222 configuration successful.
AuxiliaryVlan AuxVlanStatus Mod/Ports
-----
222          active          5/9
Console> (enable)

Console> (enable) set port auxiliaryvlan 5/9 untagged
Port 2/48 allows the connected device send and receive untagged packets and without 802.1p
priority.
Console> (enable)

```

This example shows how to specify port 5/9 as a dynamic port:

```

Console> (enable) set port membership 5/9 dynamic
Warning: Auxiliary Vlan set to dot1p|untagged on dynamic port. VMPS will be queried for IP
phones.
Port 5/9 vlan assignment set to dynamic.
Spantree port fast start option enabled for ports 5/9.
Console> (enable)

```

This example shows that the auxiliary VLAN ID specified cannot be the same as the native VLAN ID:

```
Console> (enable) set port auxiliaryvlan 5/10 223
Auxiliary vlan cannot be set to 223 as PVID=223.
Console> (enable)
```