



Configuring Dynamic Port VLAN Membership with VMPS



Note

Catalyst 6000 family switches support VMPS client only. You must have a Catalyst 5000 family switch as the VMPS server to configure dynamic port VLAN membership. VMPS server configuration is included in this chapter as a convenience; **all VMPS server configuration must be performed on the Catalyst 5000 family switch.**

This chapter describes how to configure dynamic port VLAN membership using the VMPS.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6000 Family Command Reference* publication.

This chapter consists of these sections:

- Understanding How VMPS Works, page 12-1
- 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 12-8
- Dynamic Port VLAN Membership with VMPS Configuration Examples, page 12-9

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.

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 VLAN at a time. 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.

Default VMPS and Dynamic Port Configuration

Table 12-1 shows the default VMPS and dynamic port configuration.

Table 12-1 Default VMPS and Dynamic Port Configuration

Feature	Default Configuration
VMPS server	
VMPS enable state	Disabled
VMPS management domain	Null
VMPS TFTP server	None
VMPS database configuration filename	<i>vmpls-config-database.1</i>
VMPS fallback VLAN	Null
VMPS secure mode	Open
VMPS no domain requests	Allow
VMPS Client	
VMPS domain server	None
VMPS reconfirm interval	60 minutes

Table 12-1 Default VMPS and Dynamic Port Configuration (continued)

Feature	Default Configuration
VMPS server retry count	3
Dynamic ports	No dynamic ports configured

Dynamic Port VLAN Membership and VMPS Configuration Guidelines


Note

This section applies to VMPS server configuration on the Catalyst 5000 family switch only.

These guidelines and restrictions apply to dynamic port VLAN membership:

- 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 certain 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 8, “Configuring VTP;” and Chapter 9, “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 12-5
- Configuring Dynamic Ports on VMPS Clients, page 12-5
- Administering and Monitoring VMPS, page 12-6
- Configuring Static VLAN Port Membership, page 12-7

Creating the VMPS Database


Note

This section applies to VMPS server configuration on the Catalyst 5000 family switch only.

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 12-9.

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



Note This section applies to VMPS server configuration on the Catalyst 5000 family switch only.

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

To configure VMPS, perform this task in privileged mode:

	Task	Command
Step 1	Specify the download method.	<code>set vmps downloadmethod rcp tftp [username]</code>
Step 2	Configure the IP address of the TFTP or rcp server on which the ASCII text VMPS database configuration file resides.	<code>set vmps tftpserver ip_addr [filename]</code>
Step 3	Enable VMPS.	<code>set vmps state enable</code>
Step 4	Verify the VMPS configuration.	<code>show vmps</code>

This example shows how to enable VMPS on the switch:

```
Console> (enable) set vmps state enable
Vlan Membership Policy Server enable is in progress.
Console> (enable)
```

To disable VMPS, perform this task in privileged mode:

	Task	Command
Step 1	Disable VMPS.	<code>set vmps state disable</code>
Step 2	Verify that VMPS is disabled.	<code>show vmps</code>

This example shows how to disable VMPS on the switch:

```
Console> (enable) set vmps state disable
All the VMPS configuration information will be lost and the resources released on
disable.
Do you want to continue (y/n/[n]): y
Vlan Membership Policy Server disabled.
Console> (enable)
```

Configuring Dynamic Ports on VMPS Clients



Note This section applies to VMPS client configuration on the Catalyst 5000 family switch only.

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 <i>ip_addr</i> [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 <i>mod_num/port_num</i> dynamic
Step 4	Verify the dynamic port assignments.	show port [<i>mod_num[/port_num]</i>]



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.

Administering and Monitoring VMPS

To show information about MAC address-to-VLAN mappings, perform one of these tasks in privileged mode:

Task (performed on Catalyst 5000 family switch only)	Command
<ul style="list-style-type: none"> Show the VLAN to which a MAC address is mapped in the database. 	show vmps mac [<i>mac_address</i>]
<ul style="list-style-type: none"> Show the MAC addresses that are mapped to a VLAN in the database. 	show vmps vlan [<i>vlan_name</i>]
<ul style="list-style-type: none"> Show ports belonging to a restricted VLAN. 	show vmps vlanports [<i>vlan_name</i>]

To show VMPS statistics, perform this task in privileged mode:

Task	Command
Show VMPS statistics.	show vmps statistics

To clear VMPS statistics, perform this task in privileged mode:

Task	Command
Clear VMPS statistics.	clear vmps statistics

To clear a VMPS server entry, perform this task in privileged mode:

Task (performed on Catalyst 5000 family switch only)	Command
Clear a VMPS server entry.	clear vmps server <i>ip_addr</i>

To reconfirm the dynamic port VLAN membership assignments, perform this task in privileged mode:

	Task	Command
Step 1	Reconfirm dynamic port VLAN membership.	reconfirm vmps
Step 2	Verify the dynamic VLAN reconfirmation status.	show dvlan statistics

This example shows how to reconfirm dynamic port VLAN membership assignments:

```
Console> (enable) reconfirm vmps
reconfirm process started
Use 'show dvlan statistics' to see reconfirm status
Console> (enable)
```

To download the VMPS database manually (to download a changed database configuration file or retry after a failed download attempt), perform this task in privileged mode:

	Task (performed on Catalyst 5000 family switch only)	Command
Step 1	Download the VMPS database from the TFTP server, or specify a different VMPS database configuration file.	download vmps
Step 2	Verify the VMPS database configuration file.	show vmps

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</i> [/ <i>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 12-8
- Troubleshooting Dynamic Port VLAN Membership, page 12-8

Troubleshooting VMPS



Note

This section applies to troubleshooting the VMPS server configuration on the Catalyst 5000 family switch only.

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 command, set vmps tftpserver ip_addr [filename] .
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 "vmpls_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 vmpls 3** command.



Note

For more information on system error messages, refer to the *System Message Guide—Catalyst 6000 Family, Catalyst 5000 Family, and Catalyst 4000 Family, Catalyst 2926G Series, Catalyst 2948G, and Catalyst 2980G*.

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 12-9
- Dynamic Port VLAN Membership Configuration Example, page 12-10

VMPS Database Configuration File Example



Note

This example applies to the VMPS server configuration on the Catalyst 5000 family switch only.

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. A summary of the configuration example follows:

- The security mode is open.
- The default is used for the fallback VLAN.
- MAC address-to-VLAN name mappings—The MAC address of each host and the VLAN to which each host belongs is defined.
- Port groups are defined.
- VLAN groups are defined.
- VLAN port policies are defined for the ports associated with restricted VLANs.

```

vmps domain vtp-domain
vmps mode open
vmps fallback default
vmps no-domain-req deny

vmps-mac-addr
address 0000.7777.0001 vlan-name qa
address 0000.7777.0002 vlan-name qa
address 0000.7777.0003 vlan-name swe
address 0000.7777.0004 vlan-name swe
address 0000.7777.0005 vlan-name inside
address 0000.7777.0006 vlan-name inside
address 0000.7777.0007 vlan-name outside
address 0000.7777.0008 vlan-name outside

vmps-port-group portgroup1
device 192.168.1.2 port 3/13
device 192.168.1.2 port 3/14
device 192.168.2.2 port 3/9
device 192.168.2.2 port 3/10

vmps-vlan-group engineering
vlan-name qa
vlan-name swe

vmps-port-policies vlan-group engineering
port-group portgroup1

```

```

vmmps-port-policies vlan-name qa
device 192.168.1.2 port 3/13
device 192.168.2.2 port 3/9
vmmps-port-policies vlan-name swe
device 192.168.1.2 port 3/14
device 192.168.2.2 port 3/10

vmmps-port-group portgroup2
device 192.168.1.2 port 3/15
device 192.168.1.2 port 3/16
device 192.168.2.2 port 3/11
device 192.168.2.2 port 3/12

vmmps-vlan-group sales
vlan-name inside
vlan-name outside

vmmps-port-policies vlan-group sales
port-group portgroup2

vmmps-port-policies vlan-name inside
device 192.168.1.2 port 3/15
device 192.168.2.2 port 3/11

vmmps-port-policies vlan-name outside
device 192.168.1.2 port 3/16
device 192.168.2.2 port 3/12
device 192.168.1.3 port 9/48

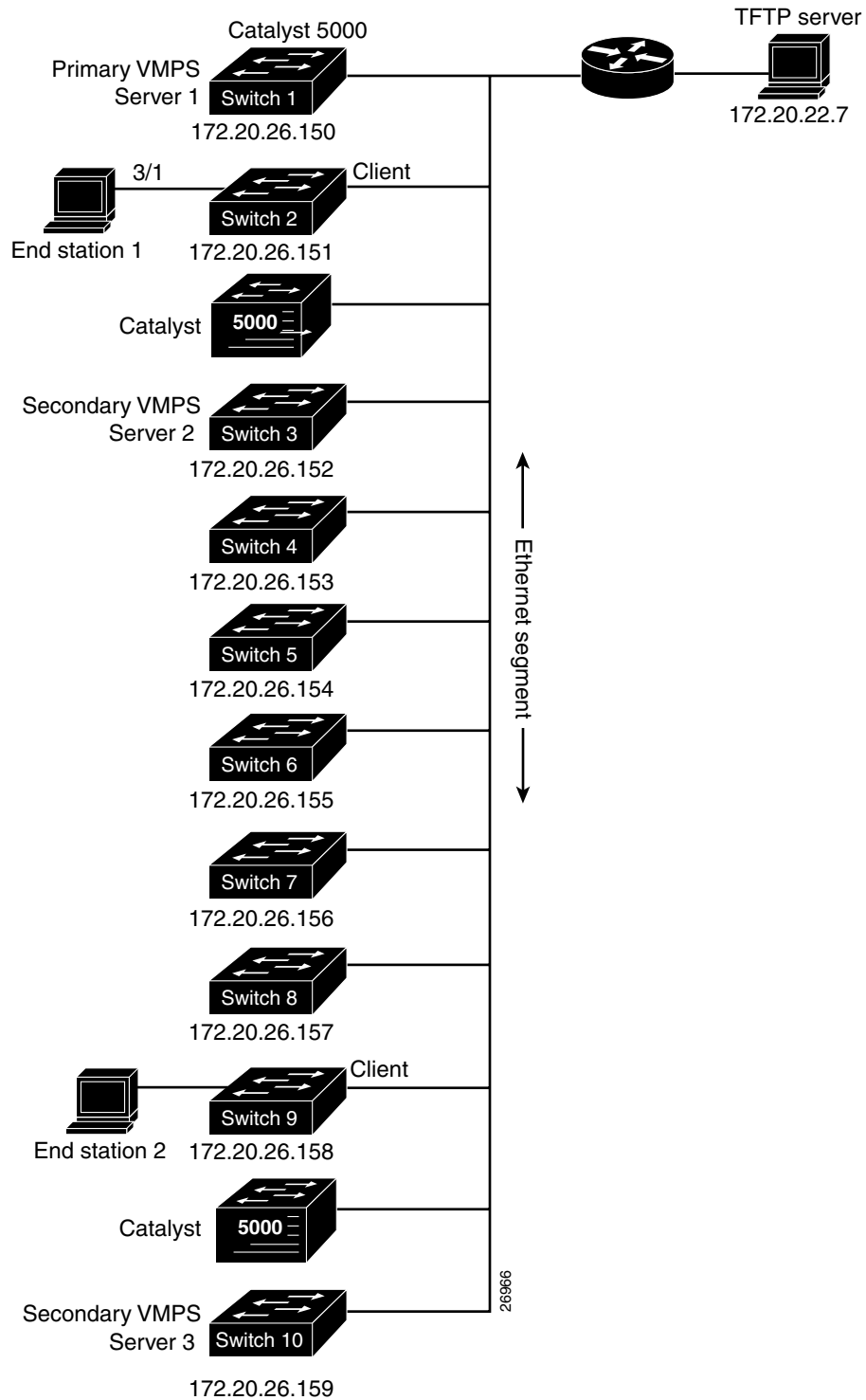
```

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



Use this procedure to configure VMPS and dynamic ports on the Catalyst 5000 family switch only:

Step 1 Configure Switch 1 as the primary VMPS server:

- a. Configure the IP address of the TFTP server on which the ASCII file resides:

```
Console> (enable) set vmps tftpserver 172.20.22.7 Bldg-G.db
```

- b. Enable VMPS:

```
Console> (enable) set vmps state enable
```

After entering these commands, the file Bldg-G.db is downloaded to Switch 1. Switch 1 becomes the VMPS server.

Step 2 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 3 Configure port 3/1 on Switch 2 as dynamic:

```
Console> (enable) set port membership 3/1 dynamic
```

Step 4 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 5 Repeat Steps 2 and 3 to configure the VMPS server addresses and assign dynamic ports on each VMPS client switch.
