



Configuring Dynamic VLAN Membership with VMPS

This chapter describes how to configure dynamic VLAN membership for ports in your network 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 major 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](#)
- [Configuration Guidelines for Dynamic Ports and VMPS, page 12-3](#)
- [Configuring VMPS, page 12-4](#)
- [Troubleshooting VMPS and Dynamic Port VLAN Membership, page 12-10](#)
- [VMPS Example, page 12-11](#)
- [Dynamic Port VLAN Membership with Auxiliary VLANs, page 12-14](#)

Understanding How VMPS Works

With VMPS, you can dynamically assign switch ports to VLANs 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 to the VMPS server, and the VMPS server begins to accept client requests. VMPS remains enabled, regardless whether you reset or power cycle the switch.

The 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 in open mode, the host receives an “access denied” response. If VMPS is in secure mode, the port is shut down and you must manually bring the port back up with the **set port** command.

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 when VMPS is in open mode. 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 the **--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 12-14 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 the VMPS server, 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).

You can use up to 50 hosts (MAC addresses) on a dynamic port if they are all authorized for the same VLAN. Each host that comes online through the port is checked against the VMPS database before the host is assigned to a VLAN.

If you move a host from one dynamic port to another, the port remains assigned to the VLAN until another MAC address changes the VLAN. You do not need to do clean up. All clean up is completed by the VMPS database.

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):

- Software release 5.1 or later releases—The Catalyst 4000 family switches support only VMPS clients.
- Software release 7.2 or later releases—The Catalyst 4000 family switches support both VMPS servers and 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 configurations.

Table 12-1 Defaults for VMPS Servers and VMPS Clients

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 min
VMPS server retry count	3 attempts
Dynamic ports	No dynamic ports configured

Configuration Guidelines for Dynamic Ports and VMPS

This section lists the guidelines and restrictions for configuring dynamic ports and VMPS:

- You must specify a primary VMPS server; you can specify up to two backup VMPS servers in your network.
- The primary VMPS server and backup VMPS servers do not communicate with each other about the VMPS database. You must enable VMPS on each server, and manually update each VMPS server when you update the VMPS database.
- 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

To configure VMPS, follow these steps:

-
- Step 1** Create the VMPS Database. See the [“Creating the VMPS Database”](#) section on page 12-4.
- Determine the MAC addresses of the hosts you want assigned to VLANs dynamically.
 - On your workstation or PC, create an ASCII text file that contains the MAC address-to-VLAN mappings.
 - Move the ASCII text file to a TFTP server so it can be downloaded to the switch.
- Step 2** On the VMPS primary and backup servers:
- Specify the location and name of the VMPS database file.
 - Enable VMPS.
- See the [“Configuring the VMPS Server”](#) section on page 12-7 for more information.
- Step 3** On the VMPS clients:
- Specify the IP addresses for the primary and backup VMSP servers.
 - Configure ports to dynamic mode.
- See the [“Configuring VMPS Clients”](#) section on page 12-7 for more information.
- Step 4** Administer and monitor VMPS as necessary. See the [“Monitoring VMPS”](#) section on page 12-9.
-

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. The example at the end of this section corresponds to the information described below.

The VMPS database can have up to five sections:

Section 1, Global settings, lists the settings for the VMPS domain name, security mode, fallback VLAN, and the policy for VMPS and VTP domain name mismatches.

- 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. If you set it to open mode, VMPS returns an access denied response for an unauthorized MAC address and returns the fallback VLAN for a MAC address not listed in the VMPS database. In secure mode, VMPS shuts down the port for a MAC address that is unauthorized or that is not listed in the VMPS database.
- (Optional) Define a fallback VLAN. Assign the fallback VLAN is assigned if the MAC addresses of the connected host is not defined in the database.

In the example at the end of this section, the VMPS domain name is WBU, the VMPS mode is set to open, the fallback VLAN is set to the VLAN default, and if the VTP domain name does match the VMPS domain name, then VMPS sends an access denied response message.

Section 2, MAC addresses, lists MAC addresses and authorized VLAN names for each MAC address.

- Enter the MAC address of each host and the VLAN name to which each should belong.
- Use the **--NONE--** keyword as the VLAN name to deny the specified host network connectivity.
- You can enter up to 21,051 MAC addresses in a VMPS database file for the Catalyst 2948G switch.

In the example at the end of this section, MAC addresses are listed in the MAC table. Notice that the MAC address fedc.ba98.7654 is set to **--NONE--**. This setting explicitly denies this MAC address from accessing the network.

Section 3, Port groups, lists groups of ports on various switches in your network that you want grouped together. You use these port groups when defining VLAN port policies.

- Define a port group name for each port group; then list all ports you want included in the port group.
- 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*. Ranges are not allowed for the port numbers.
- Use the **all-ports** keyword to specify all the ports in the specified switch.

The example at the end of this section has two port groups:

- **WiringCloset1** consists of the two ports: port 3/2 on the VMPS client 198.92.30.32 and port 2/8 on the VMPS client 172.20.26.141
- **Executive Row** consists of three ports: port 1/2 and 1/3 on the VMPS client 198.4.254.222, and all ports on the VMPS client 198.4.254.223

Section 4, VLAN groups, lists groups of VLANs you want to associate together. You use these VLAN groups when defining VLAN port policies.

- Define the VLAN group name; then list each VLAN name you want to include in the VLAN group.
- You can enter a maximum of 256 VLANs in a VMPS database file for the Catalyst 2948G switch.

The example at the end of this section has the VLAN group **Engineering**, which consists of the VLANs **hardware** and **software**.

Section 5, VLAN port policies, lists the VLAN port policies, which use the port groups and VLAN groups to further restrict access to the network.

- You can configure a restricted access using MAC addresses and the port groups or VLAN groups.

The example at the end of this section has three VLAN port policies specified.

- In the first VLAN port policy, the VLAN **hardware** or **software** is restricted to port 3/2 on the VMPS client 198.92.30.32 and port 2/8 on the VMPS client 172.20.23.141.
- In the second VLAN port policy, the devices specified in VLAN **Green** can connect only to port 4/8 on the VMPS client 198.92.30.32.
- In the third VLAN port policy, the devices specified in VLAN **Purple** can connect to only port 1/2 on the VMPS client 198.4.254.22 and the ports specified in the port group **Executive Row**.

This example shows a sample VMPS database configuration file:

```
!Section 1: GLOBAL SETTINGS
!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
!
!Section 2: MAC ADDRESSES
!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
!
!Section 3: PORT GROUPS
!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
!
!Section 4: VLAN GROUPS
!VLAN groups
!
!vmps-vlan-group <group-name>
! vlan-name <vlan-name>
!
vmps-vlan-group Engineering
  vlan-name hardware
  vlan-name software
!
!Section 5: VLAN PORT POLICIES
!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"

```

Configuring the VMPS Server

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

You can set one primary and up to two backup VMPS servers. The primary VMPS server and backup VMPS servers do not communicate with each other about the VMPS database. You must enable VMPS on each server and manually update each VMPS server when you update the VMPS database.

To configure a VMPS server, perform this task in privileged mode. You must complete this task for the primary and any backup VMPS servers in your network.

	Task	Command
Step 1	Specify the download method.	set vmps downloadmethod rcp tftp <i>[username]</i>
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 <i>ip_addr [filename]</i>
Step 3	Enable VMPS.	set vmps state enable
Step 4	Verify the VMPS configuration.	show vmps

This example shows how to set the VMPS database as Bldg-G.db on the TFTP server with the IP address 172.20.22.7 and enable VMPS on the switch:

```
Console> (enable) set vmps downloadmethod tftp
vmps download method : TFTP
Console> (enable) set vmps tftpserver 172.20.22.7 Bldg-G.db
IP address of the TFTP server set to 172.20.22.7
VMPS configuration filename set to Bldg-G.db
Console> (enable) set vmps state enable
Vlan Membership Policy Server enable is in progress.
Console> (enable)
```

Configuring VMPS Clients

When you configure a VMPS client, you must configure VMPS on the VMPS client before setting dynamic ports.

You cannot make trunk ports or secure ports a dynamic port. If you attempt to make a trunk port a dynamic port, VMPS disables trunking on the port to make it a dynamic port.

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

	Task	Command
Step 1	Specify the IP address for the primary VMPS server.	set vmps server <i>ip_addr [primary]</i>
Step 2	(Optional) Specify the IP address for the backup VMPS server(s).	set vmps server <i>ip_addr</i>
Step 3	Verify the VMPS server specification.	show vmps server
Step 4	Configure ports on the switch to dynamic mode.	set port membership <i>mod_num/port_num</i> dynamic
Step 5	Verify the dynamic port assignments.	show port <i>[mod_num[/port_num]]</i>

This example shows how to specify the primary VMPS server and two backup VMPS servers, and verify the VMPS server specification:

```
Console> (enable) set vmps server 192.0.0.1 primary
192.0.0.1 added to VMPS table as primary domain server.
Console> (enable) set vmps server 192.0.0.6
192.0.0.6 added to VMPS table as backup domain server.
Console> (enable) set vmps server 192.0.0.9
192.0.0.9 added to VMPS table as backup domain server.
```

```
Console> (enable) show vmps server
```

```
VMPS Client Status:
-----
VMPS VQP Version:      1
Reconfirm Interval:    60 min
Server Retry Count:    3
VMPS domain server:    192.0.0.1 (primary)
                       192.0.0.6
                       192.0.0.9
```

This example sets ports 1 to 3 on module 3 to dynamic mode, disables trunking port 1 on module 2 to make it a dynamic port, and verifies the port configuration:

```
Console> (enable) set port membership 3/1-3 dynamic
Ports 3/1-3 vlan assignment set to dynamic.
Console> (enable) set port membership 2/1 dynamic
Spantree port fast start option enabled for ports 2/1.
Trunk mode set to off for ports 2/1.
Console> show port
Port  Name      Status  Vlan   Level  Duplex  Speed  Type
1/1      connect trunk  normal full    100    100 BASE-TX
1/2      connect trunk  normal half    100    100 BASE-TX
2/1      connect dyn   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- in the Vlan column of the display when a VLAN has not been assigned to a port.

Monitoring VMPS

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

Task	Command
Show the VLAN to which a MAC address is mapped in the database.	show vmps mac <i>[mac_address]</i>
Show the MAC addresses that are mapped to a VLAN in the database.	show vmps vlan <i>vlan_name</i>
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

Maintaining VMPS

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

Task	Command
Clear VMPS statistics.	clear vmps statistics

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

Task	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 and refresh the existing VMPS database, perform this task in privileged mode. If you are updating the VMPS database, you need to download the VMPS database to the primary and backup VMPS servers.

	Task	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

To disable VMPS on the VMPS server, perform this task in privileged mode. When you disable the VMPS server, any active dynamic ports in the network will retain the VLAN until the host releases the VLAN or disconnects from the port.

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

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 Static Ports

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

	Task	Command
Step 1	Configure to static mode.	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 port 1 on module 3 to static mode:

```
Console> (enable) set port membership 3/1 static
Port 3/1 vlan assignment set to static.
Spantree port fast start option set to default for ports 3/1.
Console> (enable)
```

Troubleshooting VMPS and Dynamic Port VLAN Membership

The next two sections describe how to troubleshoot VMPS and dynamic port VLAN membership.

Troubleshooting VMPS

Table 12-2 shows the VMPS error messages that 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 "vmps_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. Verify that the permissions are set correctly.
Failed to download VMPS configuration file. Out of memory.	The VMPS database file might have more than 256 different VLANs specified. Reduce the number of VLANs that are used in the file.
Download aborted. File size larger than download buffer	The VMPS database file is longer than 21051 lines. If possible, shorten the file.

After VMPS successfully downloads the VMPS database configuration file, it parses the existing file on the VMPS server and builds a database. When the parsing is complete, VMPS displays 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 vmps** command.

Troubleshooting Dynamic Ports

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 dynamic port that has been shut down, enter the **set port enable** command.

When you move a PC from a hub connected to the switch to a direct port on the VMPS client, both ports remain assigned to the same VLAN.

The VMPS query and response messages are multicast packets with a destination address of 01000CCCCCD.

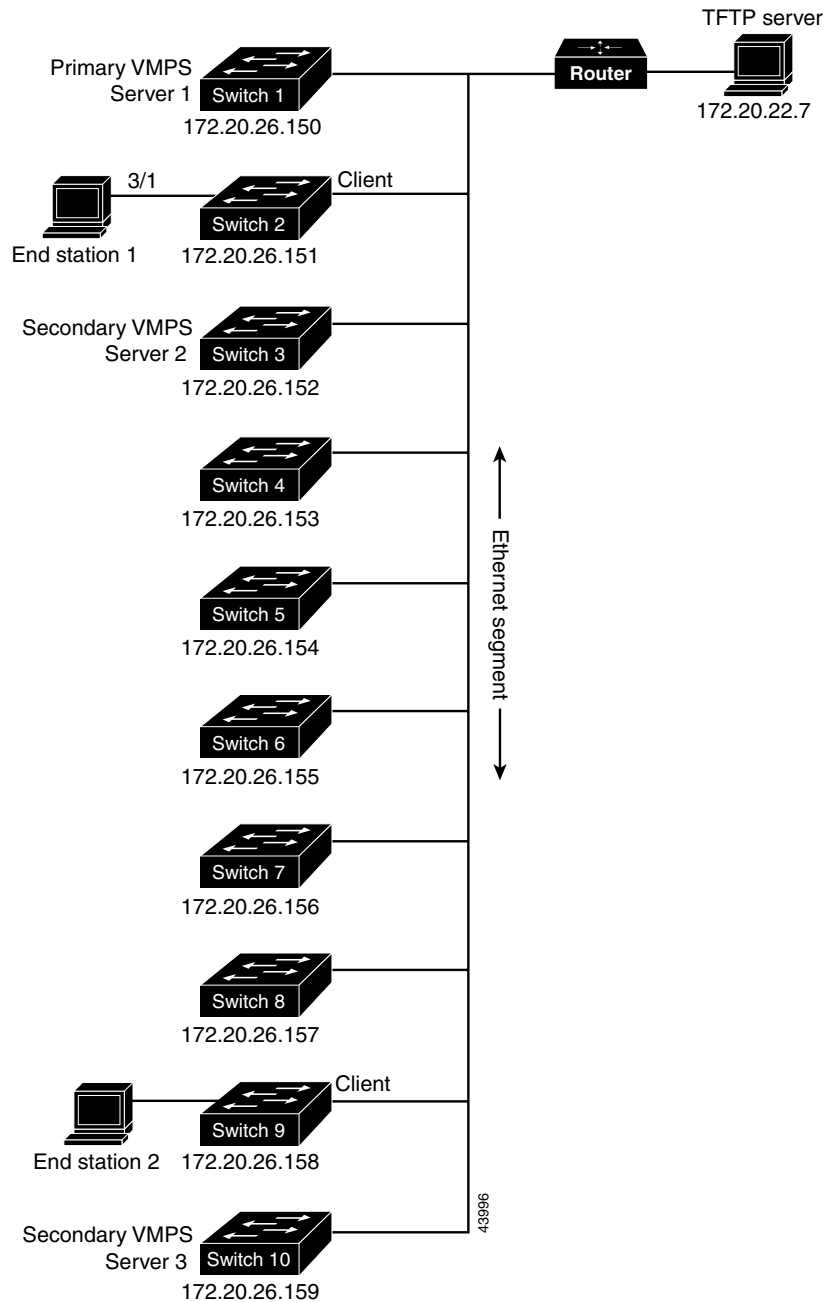
VMPS Example

Figure 12-1 shows a network with a VMPS server switch, two backup VMPS servers, and VMPS client switches with dynamic ports. In this example, the following 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 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 Switch 2 and Switch 3 as backup VMPS servers.

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

```
Console> (enable) set vmps tftpserver 172.20.26.152 Bldg-G.db
```

- b. Enable VMPS:

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

- c. Repeat Steps a and b for switch 3.

After you enter these commands, the file **Bldg-G.db** is downloaded to each switch.

Step 3 Configure the VMPS server addresses on each VMPS client.

- a. Configure the IP address for the primary VMPS server:

```
Console> (enable) set vmps server 172.20.26.150 primary
```

- b. Configure the IP addresses for the backup VMPS servers:

```
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 4 Configure port 3/1 on Switch 2 as dynamic.

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

Step 5 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 a message to assign port 3/1 to the VLAN specified in the VMPS database. Because spanning tree PortFast mode is enabled by default on dynamic ports, port 3/1 connects immediately and enters forwarding mode.

Step 6 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

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 release 6.2(1) and later releases, 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)

Configuration Guidelines

This section lists the guidelines and restrictions for configuring dynamic port VLAN membership for auxiliary VLANs:

- Read the “[Configuration Guidelines for Dynamic Ports and VMPS](#)” section on page 12-3 before you begin the configuration.
- 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 “[VMPS Example](#)” section on page 12-11 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.

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)
```

