Configuring VMPS

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table at the end of this module.

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

Prerequisites for VMPS

You should configure the VLAN Membership Policy Server (VMPS) before you configure ports as dynamic-access ports.

When you configure a port as a dynamic-access port, the spanning-tree Port Fast feature is automatically enabled for that port. The Port Fast mode accelerates the process of bringing the port into the forwarding state.

The VTP management domain of the VMPS client and the VMPS server must be the same.

Restrictions for VMPS

The following are restrictions for configuring VMPS:

- IEEE 802.1x ports cannot be configured as dynamic-access ports. If you try to enable IEEE 802.1x on a dynamic-access (VQP) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- Trunk ports cannot be dynamic-access ports, but you can enter the **switchport access vlan dynamic** interface configuration command for a trunk port. In this case, the device 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-access ports cannot be monitor ports.
- Secure ports cannot be dynamic-access ports. You must disable port security on a port before it becomes dynamic.
- Private VLAN ports cannot be dynamic-access ports
- Dynamic-access ports cannot be members of an EtherChannel group.
- Port channels cannot be configured as dynamic-access ports.
- The VLAN configured on the VMPS server should not be a voice VLAN.

Information About VMPS

Dynamic VLAN Assignments

The VLAN Query Protocol (VQP) is used to support dynamic-access ports, which are not permanently assigned to a VLAN, but give VLAN assignments based on the MAC source addresses seen on the port. Each time an unknown MAC address is seen, the device sends a VQP query to a remote VLAN Membership Policy Server (VMPS); the query includes the newly seen MAC address and the port on which it was seen. The VMPS responds with a VLAN assignment for the port. The device cannot be a VMPS server but can act as a client to the VMPS and communicate with it through VQP.

Each time the client device receives the MAC address of a new host, it sends a VQP query to the VMPS. When the VMPS receives this query, it searches its database for a MAC-address-to-VLAN mapping. The server response is based on this mapping and whether or not the server is in open or secure mode. In secure mode, the server shuts down the port when an illegal host is detected. In open mode, the server denies the host access to the port.

If the port is currently unassigned (that is, it does not yet have a VLAN assignment), the VMPS provides one of these responses:

- If the host is allowed on the port, the VMPS sends the client a vlan-assignment response containing the assigned VLAN name and allowing access to the host.
- If the host is not allowed on the port and the VMPS is in open 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 port already has a VLAN assignment, the VMPS provides one of these responses:

- If the VLAN in the database matches the current VLAN on the port, the VMPS sends an success response, allowing access to the host.
- If the VLAN in the database does not match the current VLAN on the port and active hosts exist on the port, the VMPS sends an access-denied or a port-shutdown response, depending on the secure mode of the VMPS.

If the device receives an access-denied response from the VMPS, it continues to block traffic to and from the host MAC address. The device continues to monitor the packets directed to the port and sends a query to the VMPS when it identifies a new host address. If the device receives a port-shutdown response from the VMPS, it disables the port. The port must be manually reenabled by using Network Assistant, the CLI, or SNMP.

Related Topics

Configuring Dynamic-Access Ports on VMPS Clients, on page 5
Example: VMPS Configuration, on page 11

Dynamic-Access Port VLAN Membership

A dynamic-access port can belong to only one VLAN with an ID from 1 to 4094. When the link comes up, the device does not forward traffic to or from this port until the VMPS provides the VLAN assignment. The VMPS receives the source MAC address from the first packet of a new host connected to the dynamic-access port and 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 the client device was not previously configured, it uses the domain name from the first VTP packet it receives on its trunk port from the VMPS. If the client device was previously configured, it includes its domain name in the query packet to the VMPS to obtain its VLAN number. The VMPS verifies that the domain name in the packet matches its own domain name before accepting the request and responds to the client with the assigned VLAN number for the client. If there is no match, the 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-access port if they are all in the same VLAN; however, the VMPS shuts down a dynamic-access port if more than 20 hosts are active on the port.

If the link goes down on a dynamic-access 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 through the VQP with the VMPS before the port is assigned to a VLAN.

Dynamic-access ports can be used for direct host connections, or they can connect to a network. A maximum of 20 MAC addresses are allowed per port on the device. A dynamic-access port can belong to only one VLAN at a time, but the VLAN can change over time, depending on the MAC addresses seen.

Related Topics

Configuring Dynamic-Access Ports on VMPS Clients, on page 5
Example: VMPS Configuration, on page 11

Default VMPS Client Configuration

The following table shows the default VMPS and dynamic-access port configuration on client switches.

Table 1: Default VMPS Client and Dynamic-Access Port Configuration

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

How to Configure VMPS

Entering the IP Address of the VMPS

Note If the VMPS is being defined for a cluster of switches, enter the address on the command switch.

Before you begin

You must first enter the IP address of the server to configure the switch as a client.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vmps server** *ipaddress* **primary**
4. **vmps server** *ipaddress*
5. **end**
6. **show vmps**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Switch# configure terminal`	
Step 3	**vmps server** *ipaddress* **primary** **Example:** `Switch(config)# vmps server 10.1.2.3 primary`	Enters the IP address of the device acting as the primary VMPS server.
Step 4	**vmps server** *ipaddress* **Example:** `Switch(config)# vmps server 10.3.4.5`	(Optional) Enters the IP address of the device acting as a secondary VMPS server. You can enter up to three secondary server addresses.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 6	**show vmps** **Example:** `Switch# show vmps`	Verifies your entries in the *VMPS Domain Server* field of the display.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuring Dynamic-Access Ports on VMPS Clients

Caution Dynamic-access port VLAN membership is for end stations or hubs connected to end stations. Connecting dynamic-access ports to other switches can cause a loss of connectivity.

If you are configuring a port on a cluster member device as a dynamic-access port, first use the **rcommand** privileged EXEC command to log in to the cluster member device.

Before you begin

You must have IP connectivity to the VMPS for dynamic-access ports to work. You can test for IP connectivity by pinging the IP address of the VMPS and verifying that you get a response.

Note To return an interface to its default configuration, use the **default interface** *interface-id* interface configuration command. To return an interface to its default switchport mode (dynamic auto), use the **no switchport mode** interface configuration command. To reset the access mode to the default VLAN for the device, use the **no switchport access vlan** interface configuration command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode access**
5. **switchport access vlan dynamic**
6. **end**
7. **show interfaces** *interface-id* **switchport**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Switch(config)# interface gigabitethernet 0/1`	Specifies the device port that is connected to the end station, and enters interface configuration mode.
Step 4	**switchport mode access** **Example:** `Switch(config-if)# switchport mode access`	Sets the port to access mode.
Step 5	**switchport access vlan dynamic** **Example:**	Configures the port as eligible for dynamic VLAN membership.

	Command or Action	Purpose
	`Switch(config-if)# switchport access vlan dynamic`	The dynamic-access port must be connected to an end station.
Step 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 7	**show interfaces** *interface-id* **switchport** **Example:** `Switch# show interfaces gigabitethernet 0/1 switchport`	Verifies your entries in the *Operational Mode* field of the display.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Dynamic VLAN Assignments, on page 2
Dynamic-Access Port VLAN Membership, on page 3
Example: VMPS Configuration, on page 11

Reconfirming VLAN Memberships

This task confirms the dynamic-access port VLAN membership assignments that the device has received from the VMPS.

SUMMARY STEPS

1. **enable**
2. **vmps reconfirm**
3. **show vmps**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**vmps reconfirm** **Example:** `Switch# vmps reconfirm`	Reconfirms dynamic-access port VLAN membership.
Step 3	**show vmps** **Example:** `Switch# show vmps`	Verifies the dynamic VLAN reconfirmation status.

Changing the Reconfirmation Interval

VMPS clients periodically reconfirm the VLAN membership information received from the VMPS. You can set the number of minutes after which reconfirmation occurs.

Note If you are configuring a member device in a cluster, this parameter must be equal to or greater than the reconfirmation setting on the command device. You also must first use the **rcommand** privileged EXEC command to log in to the member device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vmps reconfirm** *minutes*
4. **end**
5. **show vmps**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**vmps reconfirm** *minutes* **Example:** `Switch(config)# vmps reconfirm 90`	Sets the number of minutes between reconfirmations of the dynamic VLAN membership. The range is 1 to 120. The default is 60 minutes.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vmps** **Example:** `Switch# show vmps`	Verifies the dynamic VLAN reconfirmation status in the *Reconfirm Interval* field of the display.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Changing the Retry Count

Follow these steps to change the number of times that the device attempts to contact the VMPS before querying the next server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vmps retry** *count*
4. **end**
5. **show vmps**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**vmps retry** *count* **Example:** `Switch(config)# vmps retry 5`	Changes the retry count. The retry range is 1 to 10; the default is 3.
Step 4	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode.
Step 5	**show vmps** **Example:** `Switch# show vmps`	Verifies your entry in the *Server Retry Count* field of the display.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Troubleshooting Dynamic-Access Port VLAN Membership

Problem The VMPS shuts down a dynamic-access port under these conditions:

- **Problem** The VMPS is in secure mode, and it does not allow the host to connect to the port. The VMPS shuts down the port to prevent the host from connecting to the network.
- **Problem** More than 20 active hosts reside on a dynamic-access port.

Solution To reenable a disabled dynamic-access port, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

Monitoring the VMPS

You can display information about the VMPS by using the **show vmps** privileged EXEC command. The device displays this information about the VMPS:

- VMPS VQP Version—The version of VQP used to communicate with the VMPS. The device queries the VMPS that is using VQP Version 1.
- Reconfirm Interval—The number of minutes the device 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 device starts to query the secondary VMPS.
- VMPS domain server—The IP address of the configured VLAN membership policy servers. The device 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. A reconfirmation attempt can occur automatically when the reconfirmation interval expires, or you can force it by entering the **vmps reconfirm** privileged EXEC command or its Network Assistant or SNMP equivalent.

This is an example of output for the **show vmps** privileged EXEC command:

```
Switch# show vmps
VQP Client Status:
--------------------
VMPS VQP Version:   1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server: 172.20.128.86 (primary, current)
                    172.20.128.87

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

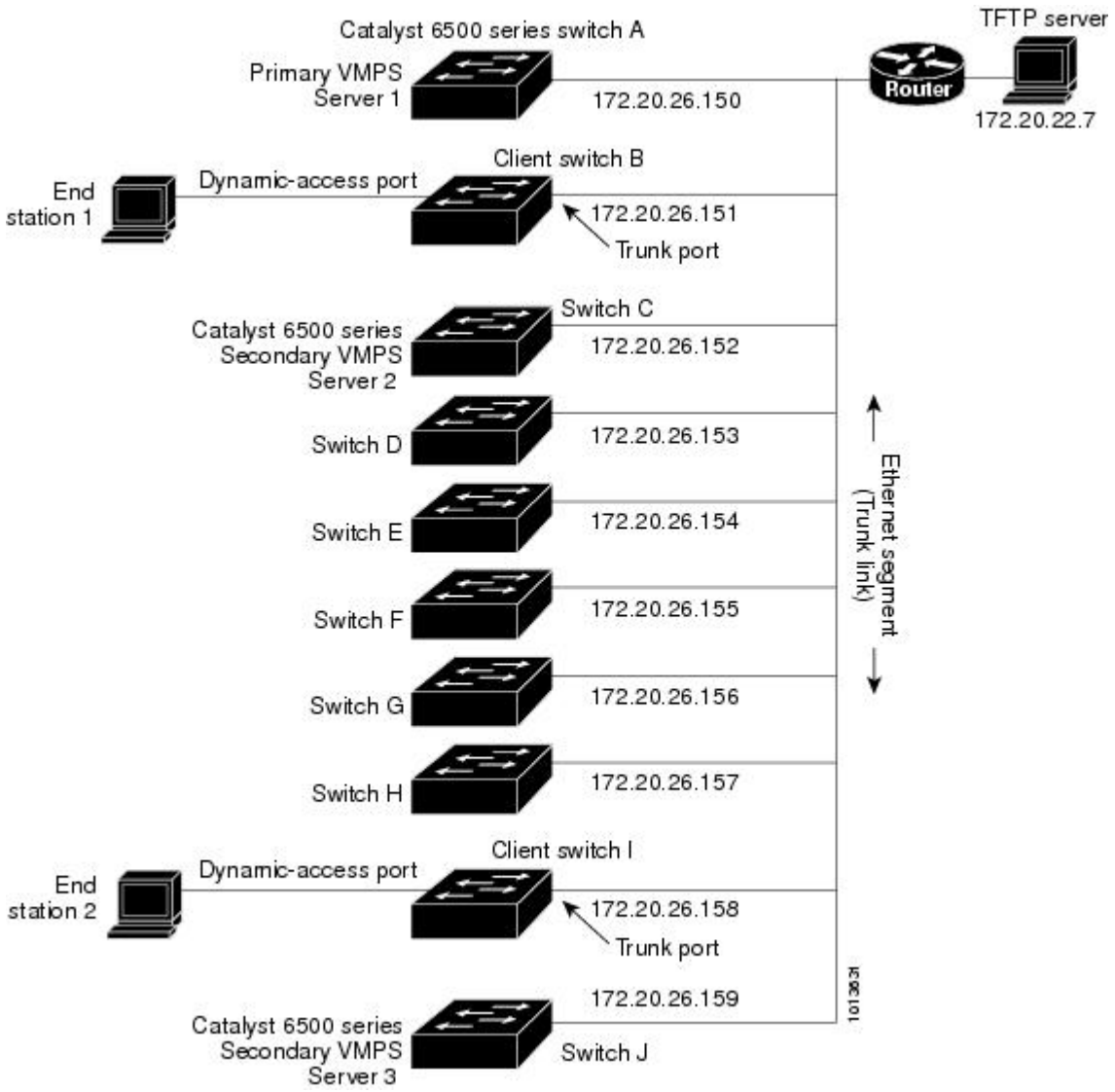
Configuration Example for VMPS

Example: VMPS Configuration

Figure 1: Dynamic Port VLAN Membership Configuration

This network has a VMPS server switch and VMPS client switches with dynamic-access ports with this configuration:

- The VMPS server and the VMPS client are separate switches.
- The Catalyst 6500 series Switch A is the primary VMPS server.
- The Catalyst 6500 series Switch C and Switch J are secondary VMPS servers.
- End stations are connected to the clients, Switch B and Switch I.
- The database configuration file is stored on the TFTP server with the IP address 172.20.22.7.



Related Topics

Configuring Dynamic-Access Ports on VMPS Clients, on page 5
Dynamic VLAN Assignments, on page 2
Dynamic-Access Port VLAN Membership, on page 3

Where to Go Next

You can configure the following:

- VTP
- VLANs
- VLAN Trunking

- Private VLANs
- Voice VLANs