

29 Multicast VLANs

Multicast VLANs enable you to control the flooding of multicast traffic in your network. For example, you can define a multicast VLAN for all users that want to receive CNN Newscasts or any other video feed or combination of feeds.

You define the multicast traffic to be transmitted by specifying a multicast address. You define the recipients of the multicast traffic by specifying ports and/or specific MAC addresses. The members of a multicast VLAN consist of the ports specified to **receive** the multicast traffic and the ports to which MAC address recipients are connected. Instructions for creating multicast VLANs begin on page 29-4.

Note the difference between multicast VLANs and AutoTracker VLANs. In AutoTracker VLANs, devices are assigned to VLANs by examination of the frames that **originate** from those devices. The members of an AutoTracker VLAN consist of source devices that fit the VLAN's policies and the ports to which those source devices are connected.

There are several differences between the configuration of multicast VLANs and the configuration of AutoTracker VLANs. The following is a summary of points to note when configuring multicast VLANs:

- You can not configure routing for multicast VLANs. Multicast VLANs are independent broadcast domains for multicast traffic originating from a multicast address and transmitted to one or more recipients.
- Multicast VLANs allow three rules: Port, MAC Address, and multicast policy.
- There is not a default multicast VLAN. Therefore, you can define rules for all 32 available multicast VLANs. All ports (even those that eventually become part of a multicast VLAN) start off in the standard AutoTracker default VLAN #1, but they only get assigned to a multicast VLAN if you explicitly assign them to one.
- All multicast VLANs include the multicast policy. This policy specifies the multicast address. You use the other two rules—Port and MAC Address—to define the destination of the multicast traffic.

How Devices are Assigned to Multicast VLANs

If the recipients of the multicast traffic were defined using the port rule, each specified port is then marked as a member of the multicast VLAN.

If the recipients of the multicast traffic were defined using the MAC address rule to specify the MAC addresses of the receiving devices, no action is taken until a frame is received from one of those devices. When such a frame is received, the switch learns the device, adds its MAC address to the filtering database, and marks the port on which the frame was received as a member of the multicast VLAN. Note that the MAC address does not itself become a member of the multicast VLAN, even though it is a recipient of the multicast traffic. Only ports are members of multicast VLANs.

When the switch receive multicast traffic that has an address specified as a multicast address for the multicast VLAN, the traffic is switched to the ports defined as VLAN members.

◆ Please Take Note ◆

The source port of the multicast traffic (i.e., the port through which multicast traffic enters the switch) can be a member of any Group. The source port does *not* need to be a member of the same Group as recipient ports. Note that the source port does not become a member of the multicast VLAN.

Although some leakage may occur before devices are assigned to AutoTracker VLANs, no leakage occurs in conjunction with device assignment to multicast VLANs.

◆ Please Take Note ◆

There is no default multicast VLAN. Unless you explicitly create multicast VLANs, none will exist.

Multicast VLANs and Multicast Claiming

The goal of multicast claiming and multicast VLANs is the same—to free the MPM module from processing multicast traffic. Both methods off-load multicast traffic processing to the switching modules. However, multicast VLANs can be seen as a refinement to multicast claiming.

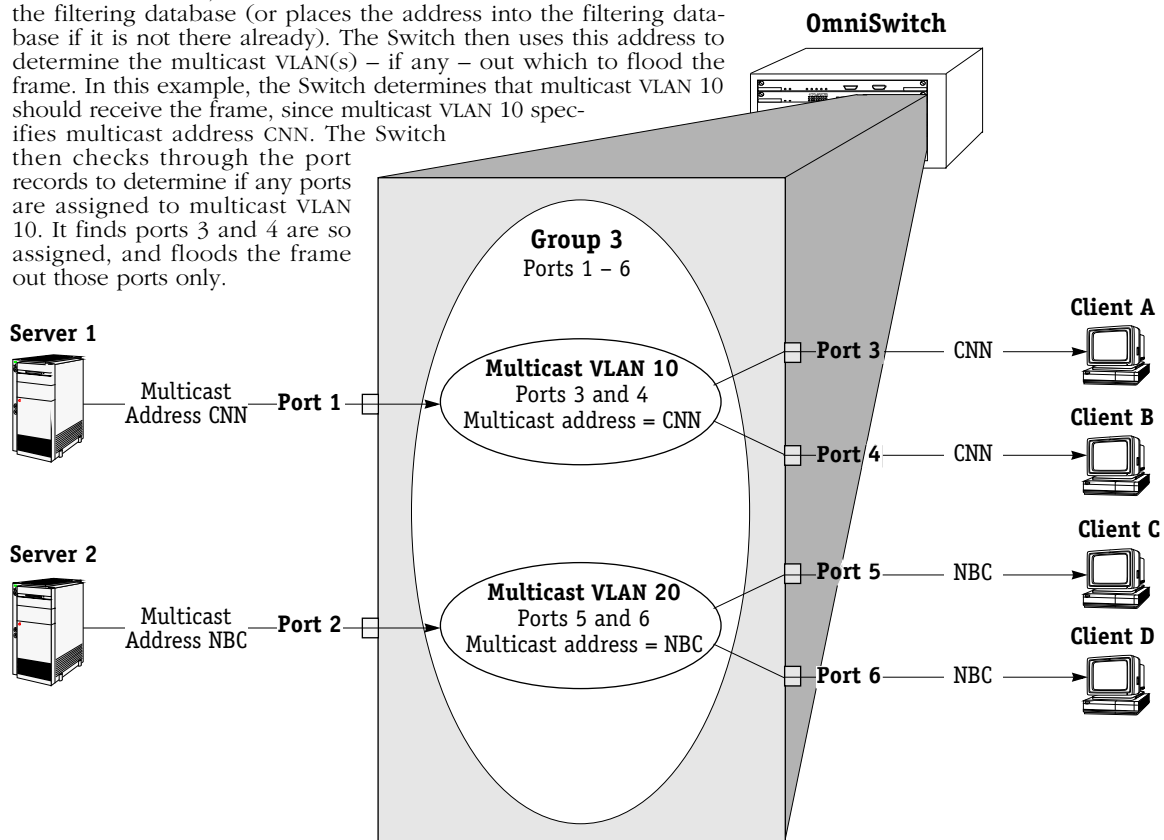
Multicast claiming claims the MAC addresses of all source devices sending multicast traffic and places those MAC addresses in the CAMs of all switching modules in a switch. Instead of claiming all multicast traffic, multicast VLANs claim only the traffic from the multicast address you specify. In addition, this multicast address is only placed in the CAMs of switching modules with destination ports that are part of the multicast VLAN.

Frame Flooding in Multicast VLANs

Multicast traffic is flooded as follows in an environment that includes multicast VLANs:

- If the destination address is a multicast address, **and**
- if the destination multicast address is in the filtering database, **and**
- if the destination multicast address is a specified multicast address for a multicast VLAN, **then** flood the traffic on all ports that have at least one multicast VLAN in common with the destination multicast address. This is illustrated below. If any of the conditions described above are untrue, the traffic is flooded as it is for normal AutoTracker VLANs.

When the Switch receives a frame with multicast destination address CNN from Server 1, the Switch locates the CNN multicast address in the filtering database (or places the address into the filtering database if it is not there already). The Switch then uses this address to determine the multicast VLAN(s) – if any – out which to flood the frame. In this example, the Switch determines that multicast VLAN 10 should receive the frame, since multicast VLAN 10 specifies multicast address CNN. The Switch then checks through the port records to determine if any ports are assigned to multicast VLAN 10. It finds ports 3 and 4 are so assigned, and floods the frame out those ports only.



For this Example, the Port Records are:

Port	VLAN Membership	MVLAN Membership
1	1	none
2	1	none
3	1	10
4	1	10
5	1	20
6	1	20

The port records show the VLAN and multicast VLAN (MVLAN) membership of each port. This table is for informational purposes only—it is not available as a UI command.

For this Example, the Filtering Database is:

MAC Address	Port	VLAN Membership	Type
CNN	n/a	10	MVLAN
NBC	n/a	20	MVLAN
Server 1	1	1	BRIDGE
Server 2	2	1	BRIDGE
Client A	3	1	BRIDGE
Client B	4	1	BRIDGE
Client C	5	1	BRIDGE
Client D	6	1	BRIDGE

The filtering database is a record of source MAC addresses, their ports of entry into the switch, and their VLAN membership. Note that the ports of entry for multicast addresses CNN and NBC are irrelevant in the filtering database. This table is for informational purposes—it is not available in the UI.

Creating Multicast VLANs

You create multicast VLANs through the AutoTracker menu options. Creating a multicast VLAN includes the following steps:

- A.** Entering basic information such as the name and number for the multicast VLAN. See *Step A. Entering Basic Information* on page 29-5 for instructions on this step.
- B.** Defining the multicast address. You define one or more multicast addresses that define the multicast stream(s) for the multicast VLAN. See *Step B. Defining the Multicast Address* on page 29-6 for instructions on this step.
- C.** Defining the recipients of multicast traffic. You may define these recipients as virtual ports or as specific MAC addresses. See *Step C. Defining the Recipients of Multicast Traffic* on page 29-7 for instructions on this step.

These steps are explained in detail below.

Step A. Entering Basic Information

1. To begin setting up a multicast VLAN type **crmctl** at any prompt.
2. The following prompt displays:

Enter the VLAN Group id for this VLAN (1):

Enter the number for the Group to which this multicast VLAN will belong. You can create up to 32 multicast VLANs and up to 31 AutoTracker VLANs in a single Group.

3. The following prompt displays:

Enter the VLAN Id for this VLAN (5):

Enter the number that will identify this multicast VLAN within the Group specified above. Up to 32 multicast VLANs may belong to the same Group. By default the system displays the next available VLAN ID number.

◆ **Note** ◆

Unlike AutoTracker VLANs, you can configure rules for the multicast VLAN #1. There is not a default multicast VLAN, so multicast VLAN #1 is treated the same as the other 31 possible multicast VLANs.

Press **<Enter>** to accept this default.

4. The following prompt displays:

Enter the new VLAN's description:

Enter a textual description that will help you identify the multicast VLAN. For example, if you know this multicast VLAN will be composed of only workstations receiving CNN news feeds, you might call the multicast VLAN "CNN MVLAN." You may use up to 30 characters for this description.

5. The following prompt displays:

Enter the Admin Status for this vlan (Enable (e) / Disable (d)):

Enter whether or not you want the Administrative Status for this multicast VLAN to be enabled or disabled. Once enabled, the switch begins using the policies you defined. A disabled multicast VLAN is still defined (name, number, policies intact), but the switch keeps the multicast VLAN disabled. The enable/disable status may be changed at a later time using the **modmctl** command.

◆ **Note** ◆

A multicast VLAN may not always be operational even when its Admin Status is enabled. A multicast VLAN's operation may be disabled by its switches because devices in the multicast VLAN cease transmitting data, among other reasons.

After you enter the administrative status, additional prompts display that allow you define the multicast address. See the next section, *Step B. Defining the Multicast Address* on page 29-6 for further instructions.

Step B. Defining the Multicast Address

The multicast address is an address that identifies a multicast traffic stream, such as CNN News.

◆ Please Take Note ◆

The source port of the multicast traffic (i.e., the port through which multicast traffic enters the switch) can be a member of any Group. The source port does *not* need to be a member of the same Group as recipient ports. Note that the source port does not become a member of the multicast VLAN.

1. After you enter the administrative status for this multicast VLAN, the following prompt displays:

Configure the Multicast Address Rule
Set Rule Admin Status to [(e)nable/(d)isable} (d):

Indicate whether you want to enable or disable this multicast Address Rule. If you enable this rule, AutoTracker will use the address to flood multicast traffic. Enter an **E** (enable) or a **D** (disable) and press **<Enter>**.

If you disable the rule, then this address will not be used to flood multicast traffic, but the parameters you set up will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule at a later time using the **modmctl** command.

2. The following prompt displays:

Enter the Multicast addresses (AABBCC:DDEEFF) in Canonical format
(Enter save to end):

Enter one or more multicast addresses, separated by spaces. The address must be a multicast address. If you enter too many characters, the system truncates the address. The switch will flood all traffic from the address(es) you specify here to the ports and/or MAC addresses you define as recipients in Step C.

All multicast MAC addresses must consist of 12 hex digits. In all valid multicast addresses, the least significant bit of the most significant byte is set to 1. Addresses with this bit unset will be rejected.

Most Significant Byte

x x x x x x x 1



least significant bit
must be set to 1

Structure of Multicast Address

When you have entered the final MAC address, leave a space and type **save** and press **<Enter>**.

Next, a menu displays prompting you to select the rules governing membership in this multicast VLAN. Go on to the next section, *Step C. Defining the Recipients of Multicast Traffic* on page 29-7 to continue setting up this multicast VLAN.

Step C. Defining the Recipients of Multicast Traffic

You can define the recipients of multicast traffic by virtual port or MAC address. You define these recipients as policies for this multicast VLAN. The available policies for recipients are Port and MAC Address. You can use both rules within a single multicast VLAN. For example, you might want to flood multicast traffic to all devices attached to one switch port, but only a few devices attached to other switch ports. In this case, you could use a Port rule for the devices on the port where all devices receive the multicast traffic, and then the MAC address rule to flood multicast traffic only to specific devices attached to the other ports on the switch.

Follow the directions in one of the following sections for the rule type you want to define.

Defining Recipients By Port

After you define the multicast address, the following menu displays:

Select rule type:

1. Port Rule
2. MAC Address Rule
3. Multicast Address Rule

Enter rule type (1):

1. Press **<Return>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable this rule. Type **e** to enable or **d** to disable. If you enable the rule, the multicast VLAN will use it to determine membership of devices. If you disable the rule, then this rule will not be used in assigning devices to this multicast VLAN, but the parameters you set up for the multicast VLAN will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule at a later time using the **modmcvl** command.

3. The following prompt displays:

Enter the list of port in Slot/Int/Service/Instance format:

Enter the ports that you want to receive multicast traffic for this multicast VLAN. You may enter multiple ports at a time. You can include a total of 255 ports per switch in a port-based multicast VLAN. Use the <slot>/<port> format. For example, to include port 7 from the module in slot 2, you would enter 2/7. (The service and instance numbers are not necessary for specifying physical ports. They are only necessary when specifying logical or virtual ports, which normally only differ from physical ports in more complex configurations, such as ATM LAN Emulation.)

4. The following prompt displays:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same multicast VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this multicast VLAN. If you enter **N**, you will receive a message, similar to the one below, indicating that the multicast VLAN was set up.

VLAN 3:23 created successfully

5. If you are done setting up rules for this multicast VLAN, then your multicast VLAN is set up. You can monitor activity on these multicast VLANs through other AutoTracker commands. See later sections in this chapter for information on these commands.

Defining Recipients By MAC Address

After you define the multicast address, the following menu displays:

Select rule type:

- 1. Port Rule**
- 2. MAC Address Rule**
- 3. Multicast Address Rule**

Enter rule type (1):

1. Press **2** and **<Return>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable this rule. Type **e** to enable or **d** to disable. If you enable the rule, the multicast VLAN will use it to determine membership of devices. If you disable the rule, then this rule will not be used in assigning devices to this multicast VLAN, but the parameters you set up for the multicast VLAN will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule at a later time using the **modmcvl** command.

3. The following prompt displays:

Enter the list of MAC addresses (Enter save to end):

Enter the MAC addresses that you want to receive multicast traffic for this multicast VLAN. Separate addresses by a space. When you have entered the final MAC address, leave a space and type **save**.

4. The following prompt will display:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same multicast VLAN. Enter a **Y** here if you want to set up more rules in addition to the port rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this multicast VLAN. If you enter **N**, you will receive a message, similar to the one below, indicating that the multicast VLAN was set up.

VLAN 3:24 created successfully

5. If you are done setting up rules for this multicast VLAN, then your multicast VLAN is set up. You can monitor activity on these multicast VLANs through other AutoTracker commands. See later sections in this chapter for information on these commands.

Modifying Multicast VLANs

After you set up a multicast VLAN you can modify its Admin Status, description, rules, and the Admin Status of each of the rules. You use the **modmcvl** command to modify a multicast VLAN as follows:

modmcvl <Group Number>:<VLAN Number>

You must specify the Group and multicast VLAN number and they must be separated by a colon. For example, to modify multicast VLAN 2 in Group 2, you would specify:

modmcvl 2:2

After entering a valid **modmcvl** command, a screen similar to the following sample displays:

```

VLAN    2 : 2 is defined as:
  1.      Description      = MVLAN 2
  2.      Admin Status    = Enabled
  3.      Rule Definition
          Rule Num   Rule Type   Rule Status
            1        Port Rule   Enabled
            2        Multicast Rule Enabled

Available options:
  1.      Set VLAN Admin Status
  2.      Set VLAN Description
  3.      Add more rules
  4.      Delete a rule
  5.      Set rule Admin Status
  6.      Quit

Option =

```

The first half of the display shows the current configuration of this multicast VLAN. For example, this sample shows multicast VLAN 2 in Group 2 with a description, "MVLAN 2." The multicast VLAN is Enabled and a Port Rule has been set up and it is enabled.

The second half of the display shows a list of the multicast VLAN attributes you can modify. You can modify basic information such as the Admin Status and Description. You can also add rules, delete rules, and enable or disable a rule. To modify an attribute, enter the number next to the option you want to modify and press **<Enter>**.

The following sections describe each of the six Available Options for the **modmcvl** command.

Changing a VLAN's Admin Status

1. At the **Option=** prompt enter a **1** and press **<Enter>**.
2. The following prompt displays:

Set Admin Status to ((e)nable/((d)isable):

Type an **e** to enable the multicast VLAN or a **d** to disable it. An enabled VLAN starts using policies to direct data flow. A disabled multicast VLAN is saved, but can not become active.

The system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing a **6**.

Changing a VLAN's Description

1. At the **Option=** prompt enter a **2** and press **<Enter>**.
2. The following prompt displays:

Enter a new description:

Type in the revised description for this multicast VLAN. The description can be up to 30 characters long. Press **<Enter>** when you have completed the new description.

The system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing an **6**.

Adding More Policies for This VLAN

1. At the **Option=** prompt enter a **3** and press **<Enter>**.
2. The following menu displays:

Select rule type:

1. Port Rule
2. MAC Address Rule
3. Multicast Address Rule

Enter rule type (1):

This is the same menu used by the **crmcvl** command. This menu has three options, some of which contain multiple branching options. This menu is documented fully in the section, *Step C. Defining the Recipients of Multicast Traffic* on page 29-7. Please consult this section for information on this menu.

When have entered all new rule types, the system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing an **6**.

Deleting A Policy for This VLAN

1. At the **Option=** prompt enter a **4** and press **<Enter>**.
2. The following menu displays:

Enter rule number to delete:

The rule number is listed with other information on the multicast VLAN just after you entered the **modmcvl** command. Find the number corresponding to the rule you want to delete and enter it at this prompt and press **<Enter>**. The rule is deleted and the system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing a **6**.

Changing the Admin Status for a VLAN Policy

1. At the **Option=** prompt enter a **5** and press **<Enter>**.
2. The following menu displays:

Enter rule number:

The rule number is listed with other information on the multicast VLAN just after you entered the **modmcvl** command. Find the number corresponding to the rule you want to change and enter it at this prompt and press **<Enter>**.

3. The following menu displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Type an **e** to enable this rule or a **d** to disable it. If the rule is enabled, the multicast VLAN will start using the rule criteria to segment data traffic.

The system returns to the **Available Options** menu. You can modify more attributes for this multicast VLAN, or quit modifying the multicast VLAN by typing a **6**.

Deleting a Multicast VLAN

You can delete a multicast VLAN. When you delete a multicast VLAN, multicast traffic is no longer flooded to the recipients you defined. Follow these steps to delete a multicast VLAN.

1. Type **rmmcvl** followed by the Group number, a colon (:), and the multicast VLAN number that you want to delete. For example to delete multicast VLAN 2 in Group 3, you would type:

rmmcvl 3:2

2. The following prompt displays:

Delete VLAN 3:2 ? (n):

Enter a **y** and press **<Enter>** to complete the deletion of the multicast VLAN. A message display confirming the deletion.

VLAN 3:2 deleted

Modifying a Multicast Address Policy

After you create a multicast VLAN, you can modify the multicast address policy by adding more addresses through the **modmcvl** command. However, you can not add an existing multicast address. Follow the steps outlined in *Modifying Multicast VLANs* on page 29-9 and the steps for *Adding More Policies for This VLAN* on page 29-10. Continue with the procedure below.

The following menu displays:

Select rule type:

- 1. Port Rule**
- 2. MAC Address Rule**
- 3. Multicast Address Rule**

Enter rule type (1):

1. Press **3** and **<Return>**.
2. The following prompt displays:

Set Rule Admin Status to ((e)nable/(d)isable):

Indicate whether or not you want to enable this rule. Type **e** to enable or **d** to disable. If you disable the rule, then the multicast addresses you enter will not be used to flood traffic, but the parameters you set up for the multicast VLAN will be saved. This Admin Status is different from the Admin Status for the multicast VLAN as it controls only this specific rule. You can enable or disable the rule at a later time using the **modmcvl** command.

3. The following prompt displays:

Enter the list of MAC addresses (Enter save to end):

Enter one or more multicast addresses. Separate addresses by a space. When you have entered the final multicast address, leave a space and type **save**.

4. The following prompt will display:

Configure more rules for this vlan (y/n):

You can set up multiple rules for the same multicast VLAN. Enter a **Y** here if you want to set up more rules in addition to the multicast address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this multicast VLAN. If you enter **N**, you will receive a message, similar to the one below, indicating that the multicast VLAN was set up.

VLAN 3:24 created successfully

Viewing Multicast VLANs

You can view the current status of all multicast VLANs in the switch using the **mcvl** command. Type **mcvl** and a table similar to the following displays:

VLAN Group :	VLAN Id	VLAN Description	Admin Status	Operational Status
3:	5	MVLAN 5	Enabled	Active
3:	11	MVLAN 11	Enabled	Inactive
3:	12	MVLAN 12	Enabled	Inactive
3:	22	MVLAN 22	Enabled	Active
3:	23	MVLAN 23	Enabled	Active
3:	24	MVLAN 24	Enabled	Inactive
3:	25	MVLAN 25	Enabled	Inactive
3:	26	MVLAN 26	Enabled	Inactive
3:	27	MVLAN 27	Enabled	Inactive
3:	31	MVLAN 31	Enabled	Inactive
3:	32	MVLAN 32	Enabled	Inactive

VLAN Group. The Group to which this multicast VLAN is assigned. The Group is specified when first creating a multicast VLAN.

VLAN ID. An identification number that you assigned when you created this multicast VLAN.

VLAN Description. A textual description that you entered to describe a multicast VLAN when you created or modified it through **crmcvl** or **modmcvl**. This description is limited to 30 characters.

Admin Status. A multicast VLAN can be enabled or disabled. You enable or disable a multicast VLAN when you create or modify it. If the multicast VLAN is enabled, AutoTracker floods multicast traffic to the recipients you specified when setting up the multicast VLAN. If the multicast VLAN is disabled, the multicast traffic is not flooded as you specified; however, the parameters you set up for the multicast VLAN are saved.

Oper Status. The multicast VLAN is shown as active or inactive. In order for an enabled multicast VLAN to become “active” it must be able to assign a switch port to the multicast VLAN. If the port rule is used for a multicast VLAN, then the multicast VLAN automatically becomes active. If you defined multicast traffic recipients by MAC address only, then a frame destined for a defined MAC address must first be received by a switch port before the multicast VLAN is active. An active multicast VLAN requires the following:

- Admin Status must be enabled.
- A port must be assigned to the multicast VLAN through either a port-based rule or by a device transmitting data that matches the multicast VLAN policy.

Viewing Multicast VLAN Policies

You can view the current multicast VLAN policies and their status using the **vimcrl** command. Type **vimcrl** and a Policy Configuration Table displays similar to the following:

VLAN Group :	VLAN Id	Rule Num	Rule Type	Rule Status	Rule Definition
3:	5	1	PORT RULE	Disabled	2/7/Brg/1
3:	5	2	MCAST	Disabled	072467:0034ab
3:	22	1	PORT RULE	Enabled	2/7/Brg/1
3:	22	2	MCAST	Enabled	080027:0135de1
3:	23	1	PORT RULE	Enabled	2/7/Brg/1
3:	23	2	MCAST	Enabled	050034:000017
3:	24	1	MAC RULE	Enabled	082008:003002
					082009:803728
3:	24	2	MCAST	Enabled	053967:0126af5

VLAN Group. The Group to which this multicast VLAN is assigned. The Group is specified when first creating a multicast VLAN.

VLAN ID. An identification number that you assigned when you created this multicast VLAN.

Rule Num. The number for this rule within the multicast VLAN definition. Each rule defined for a multicast VLAN is numbered sequentially in the order of creation. The rule number is needed when you want to modify or delete a rule definition.

Rule Type. The type of multicast VLAN rule. For multicast VLANs, the rule type can be PORT RULE, MAC RULE, or MUCICAST RULE. Each multicast VLAN by definition will contain a multicast rule. The multicast rule defines the multicast address. In addition, the multicast VLAN contains either a Port-based rule, MAC address rule, or both a Port and MAC address rule. The Port and MAC address rules define the recipients of multicast traffic.

Rule Status. Indicates whether the rule for this row is Enabled or Disabled. If the rule is enabled, then the switch is using the rule definition to determine multicast traffic flooding. If Disabled, then the switch is not using this rule to regulate multicast traffic flow. Note that this Rule Status is different from the Admin Status for the multicast VLAN since it controls only this specific rule within this specific multicast VLAN. You can enable or disable the rule using the **modmcvl** command.

Rule Definition. Details of this rule. For a Port Rule, this column lists the virtual interface for the Port that is a recipient of the multicast traffic as

<slot>/<port>/<service>/<instance>

For example, the port defined for the first row in the table applies to the first bridge instance on port 7 on the module in slot 2 of the switch. For a MAC address rule, this column lists the MAC address for the recipient of the multicast traffic. For a multicast Rule, this column lists the multicast address.

Viewing the Virtual Interface of Multicast VLANs

You can view the multicast VLAN membership of each virtual interface in the switch. In most cases the virtual interface is the same as a virtual port. However, when multiple services are set up for a virtual port, then each service may be split into one or more instances.

Type **vimcvi** and a Virtual Interface Table displays similar to the one that follows. You can also specify just the slot and port number to narrow the range of ports displayed.

Virtual Interface VLAN Membership

Slot/Intf/Service/Instance				Group	Member of VLAN#
1	/1	/Rtr	/1	1	1
1	/1	/Rtr	/2	3	23
1	/1	/Rtr	/3	3	24
2	/1	/Brg	/1	1	23
2	/7	/Brg	/1	1	22
4	/1	/Brg	/1	1	24
5	/1	/Brg	/1	1	22

Slot/Intf/Service/Instance. Specifies the virtual interface for which multicast VLAN information will be displayed. The **Slot** is the physical slot location to which the virtual interface maps. The **Intf** is the physical port to which the virtual interface maps. The **Service** is the service type for this interface. The service type may be a Router (**Rtr**), Bridge (**Brg**), Classical IP (**CIP**), FDDI Trunk (**Trk**), or an 802.10 Trunk (**T10**). **Instance** is the specific instance of this service type. These different instances are identified numerically. The first instance of a service type belonging to a physical port is identified as 1, the second instance is identified as 2, etc.

Group. The Group to which this virtual interface is assigned. The Group is specified when first creating a multicast VLAN.

Member of VLAN #. The multicast VLANs to which this virtual interface belongs. An interface may belong to more than one multicast VLAN. For example, if you set up a multicast VLAN for CNN News and another for NBC News, you may want certain ports to receive both multicast traffic streams.

