17 Configuring Group and VLAN Policies

AutoTracker policies subdivide network traffic based on specific criteria. AutoTracker policies can be defined by port, MAC address, protocol, network address, user-defined, port binding, DHCP port, or DHCP MAC address policy. You can define multiple policies—also referred to as "rules"—for a mobile Group or an AutoTracker VLAN. A port or device is included in a mobile Group or AutoTracker VLAN if it matches any one AutoTracker rule. For example, you can define rules based on MAC address and rules based on protocol in the same mobile group or AutoTracker VLAN.

This chapter provides an overview of AutoTracker Policies as well as instructions for configuring these policies. AutoTracker policies may be applied to mobile groups (including authenticated groups) and to VLANs within standard groups. All policy types may be used with mobile groups and VLANs within standard Groups. However, only the Binding Rule may be used with authenticated groups.

♦ Note ♦

This chapter contains instructions for configuring AutoTracker policies for mobile groups or AutoTracker VLANs. Instructions for configuring groups (mobile and non-mobile) can be found in Chapter 16. More detailed overview and instructions for AutoTracker VLANs (created within non-mobile groups) can be found in Chapter 19.

AutoTracker policies enable you to control communications between end stations in your network. You define policies that determine membership in the mobile group or AutoTracker VLAN and AutoTracker automatically locates ports or devices that fit the policies and places them into the mobile group or AutoTracker VLAN.

You can define physical policies or logical policies (or combinations thereof) to determine membership. Physical policies consist of port rules: you define the members as one or more specific ports and membership is limited to the ports defined and the MAC addresses of devices connected to those ports.

Logical VLAN policies can consist of MAC address rules, protocol rules, network address rules, user-defined, or port binding rules. Ports are assigned to mobile groups or AutoTracker VLANs that have logical rules when the MPM module examines frames that originate from devices connected to the switch. If a frame is received that matches a logical rule, the source device's MAC address and the port to which the source device is connected are both made members.

The members of a mobile group or AutoTracker VLAN thus consist of source devices originating frames that fit the AutoTracker policies and the ports to which those source devices are connected.

AutoTracker Policy Types

You can define a maximum of 32 AutoTracker policies of each type per Group. There is no restriction on the number of rules you can define per AutoTracker VLAN, as long as the maximum number of policies for the Group is not exceeded. A port or device is included in a mobile group or AutoTracker VLAN if it matches any one rule.

You can define the following types of rules:

Port Policies. Port policies enable you to define membership on the basis of ports. Members of the mobile group or AutoTracker VLAN will consist of devices connected to specific ports on one switch or on multiple switches in the Group.

MAC Address Policies. MAC address policies enable you to define membership on the basis of devices' MAC addresses. This is the simplest type of rule and provides the maximum degree of control and security. Members of the mobile group or AutoTracker VLAN will consist of devices with specific MAC addresses. These devices may all be connected to one switch or they may be connected to different switches in the Group. A maximum of 1024 MAC addresses are supported per MAC address policy.

Protocol Policies. Protocol policies enable you to define membership on the basis of the protocol that devices use to communicate. All devices that communicate with the specified protocol become members of the mobile group or AutoTracker VLAN.

You can specify membership according to the following protocols: IP, IPX, AppleTalk, or DECNet. In addition, you can specify membership according to Ethernet type, source and destination SAP (service access protocol) header values, or SNAP (sub-network access protocol) type.

Network Address Policies. Network address policies enable you to define membership on the basis of network address criteria.

For example, you can specify that all IP users with a specific subnet mask be included in the mobile group or AutoTracker VLAN. Or, you can specify that all IPX users in a specific network address area using a certain encapsulation type be included.

If you define network address and port or protocol rules in the same VLAN, the network address rules will take precedence over the port and protocol rules should any conflict arise. To reverse this precedence (i.e., port and protocol rules take precedence over network address rules) you must add the following line to the switch's **mpm.cmd** file:

```
Precedence=0
```

User-Defined Policies. User-defined policies enable you to define membership on the basis of a specific pattern within a frame. All devices that originate frames containing this pattern are assigned to the mobile group or AutoTracker VLAN. The pattern is specified by defining an offset, a value, and a mask.

Port Binding Policies. A port binding policy specifies a particular device to be included in the mobile group or AutoTracker VLAN. There are six types of Port Binding Rules that can be created:

- Bind IP Address to a Port and a MAC address
- Bind MAC Address to a Protocol and a Port
- Bind Port to a Protocol
- Bind IP Address to a MAC Address
- Bind IP Address to a Port
- Bind MAC Address to a Port

You must specify a separate binding policy for each device, but you can specify an unlimited number of such policies. Binding policies take precedence over all other AutoTracker policies.

DHCP Port Policies. These policies are similar to standard port policies, but apply to switch ports to which DHCP client workstations are attached.

DHCP MAC Address Policies. These policies are similar to standard MAC address policies, but apply to the MAC addresses of DHCP client workstations only.

Defining and Configuring AutoTracker Policies

You can define AutoTracker policies by port, MAC address, protocol, network address, user definition, or port binding. You can define multiple policies for a mobile group or AutoTracker VLAN if you wish. A port or device is included in a mobile group or AutoTracker VLAN if it matches any one rule. For example, you can define rules based on ports, rules based on MAC address, and rules based on protocol in the same mobile group or AutoTracker VLAN. However, defining multiple rules is not trivial – exercise extreme care when you do so and make sure that you understand the consequences of your definitions. In most situations, it is advisable to use one of AutoTracker's predefined rules.

The sections below provide directions for setting up each type of AutoTracker policy. Follow the directions for the policy you wish to set up.

Port Policy	See .
MAC Address Policy	See *Defining a MAC Address Policy* on page 17-6.
Protocol Policy	See *Defining a Protocol Policy* on page 17-7.
Network Address Policy	See *Defining a Network Address Policy* on page 17-9.
User-defined Policy	See *Defining Your Own Rules* on page 17-11.
Binding Policy	See *Defining a Port Binding Policy* on page 17-13.
DHCP Port Policy	See *Defining a DHCP Port Policy* on page 17-17.
DHCP MAC Address Policy	See *Defining a DHCP MAC Address Policy* on page 17-18.

Where These Procedures Start

These policy configuration sections start in the middle of a sequence of steps with the **crgp** or **modatvl** commands. During the **crgp** command prompt sequence you can configure polices for mobile groups or for VLANs within non-mobile groups. The **modatvl** command contains an option for adding policies (option #3). The procedures in these section pick up at the point after you choose to either to configure AutoTracker rules (**crgp**) or add more rules (**modatvl**).

Defining a Port Policy

After you enter the Administrative Status, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Press **<Enter>**. If this is a VLAN in a non-mobile Group refer to Chapter 17 for a detailed explanation of the two ways port policies may be configured.

2. The following prompt displays:

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

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

3. The following prompt displays:

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

   Enter the physical ports that you want included in this VLAN. You may enter multiple ports at a time. 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 LAN ports. They are only necessary when specifying logical ports used over ATM, FDDI, and Frame Relay.)

4. The following prompt displays:

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

   You can set up multiple rules for the same 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 VLAN. Follow the directions in the appropriate section to configure that rule.

   If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

   ```
   VLAN 1:2 created successfully
   ```

   You are done setting up rules.

Defining a MAC Address Policy

After you enter the Administrative Status, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Enter **2** and press **<Enter>**.
2. The following prompt displays:

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

   Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for this mobile group or AutoTracker VLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.
3. The following prompt displays:

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

   Enter the MAC addresses that you want to include in this VLAN. Separate addresses by a space. When you have entered the final MAC address, leave a space and type **save**.
4. The following prompt displays:

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

   You can set up multiple rules. Enter a **Y** here if you want to set up more rules in addition to the MAC Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

   If you enter **N**, you will receive a message, similar to the one below, indicating that the mobile group or AutoTracker VLAN was set up.

   ```
   VLAN 1:2 created successfully
   ```

   You are done setting up rules.

Defining a Protocol Policy

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Press **3** and press **<Enter>**.

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 mobile group or AutoTracker VLAN will use it to determine membership of devices. If you disable the rule, then this rule will not be used in assigning devices, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

   ```
   Select Protocol:
   1. IP
   2. IPX
   3. DECNET
   4. APPLETALK
   5. Protocol specified by ether-type
   6. Protocol specified by DSAP and SSAP
   7. Protocol specified by SNAP

   Enter protocol type (1):
   ```

   Enter the number for the protocol that will be used to define this mobile group or AutoTracker VLAN. Numbers are listed next to the protocol names. By selecting a specific protocol, you are indicating that all traffic originating from network devices using that protocol will be assigned to this mobile group or AutoTracker VLAN. You can select the IP, IPX, DECNET, and APPLETALK protocols by entering 1, 2, 3, or 4, respectively.

   ♦ Note ♦

   ARP (address resolution protocol) is included as IP. DDP (datagram delivery protocol) and AARP (AppleTalk ARP) are included as AppleTalk. DECNET is DECNET Phase IV traffic only.

   If you want to define a protocol other than IP, IPX, AppleTalk, or DECNet, you can do so by specifying an Ethernet type, or by specifying source and destination SAP (service access protocol) header values, or by specifying a SNAP (sub-network access protocol) type. The following three sections describe how to specify these protocol types. If you are not specifying one of these special protocol types, continue with Step 4 below.

Protocol Specified by Ether-Type

a. To specify a protocol by Ethernet type, enter **5** at the **Select Protocol:** menu. The following prompt displays:

Enter the Ether-type value in hex:

b. Enter the desired Ethernet type in hex. You must enter two bytes of data. For example, enter 0800 to specify IP or enter 0806 to specify ARP. All devices that use the specified Ethernet type will be members of the mobile group or AutoTracker VLAN.

c. Go on to Step 4 below.

Protocol Specified by DSAP and SSAP

a. To specify a protocol by SAP (service access protocol) header, enter **6** at the **Select Protocol:** menu. The following prompt displays:

Enter the DSAP value in hex:

b. Enter the destination service access protocol (DSAP) value in hex and press **<Enter>**. The following prompt displays:

Enter the SSAP value in hex:

c. Enter the source service access protocol (SSAP) value in hex. Each entry must consist of one byte of data. All devices that use the specified source and destination SAP types will be members of the mobile group or AutoTracker VLAN.

d. Go on to Step 4 below.

Protocol Specified by SNAP

a. To specify a protocol by SNAP (sub-network access protocol) type, enter **7** at the **Select Protocol:** menu. The following prompt displays:

Enter the SNAP value in hex

b. Enter the desired SNAP value in hex. You must enter five bytes of data. For example, enter 0000008137 to specify IPX SNAP or enter 00000080F3 to specify AppleTalk ARP SNAP. All devices that use the specified SNAP type will be members of the mobile group or AutoTracker VLAN.

c. Go on to Step 4 below.

4. The following prompt displays:

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

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the protocol rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a Network Address Policy

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Press **4** and press **<Enter>**.

2. The following prompt displays:

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

   Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTrackerVLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

   ```
   Select the Network Protocol:
   1. IP
   2. IPX

   Enter the protocol type:
   ```

   Enter the protocol for which you want to define this network address rule. Enter a **1** for IP and a **2** for IPX. The prompts that follow are different for IP and IPX. These differences are due to the different conventions used by the protocols for network address formats. Follow the procedure below the network protocol you are setting up.

Set Up an IP Address

a. To specify an IP address, enter a **1** at the **Select the Network Protocol:** prompt.

b. The following prompt displays:

   ```
   Enter the IP address:
   ```

   Enter the IP address that you want to include in this mobile group or AutoTracker VLAN. Enter the address in dotted decimal notation or hexadecimal notation (e.g., 198.206.181.10).

c. The following prompt displays:

   ```
   Enter the IP Mask (0xffffff00):
   ```

   Enter the IP Subnet mask for this address. The default subnet mask is shown in parentheses and is automatically derived from the IP address class entered in Step b.

d. Go on to Step 4 below.

Set Up an IPX Address

a. To specify an IPX address, enter a **2** at the **Select the Network Protocol:** prompt.

b. The following prompt displays:

Enter the IPX Network Number:

Enter an IPX network number to define the network devices you want included in the mobile group or AutoTracker VLAN. IPX addresses consist of eight hex digits and you can enter a minimum of one hex digit in this field. If you enter less than eight hex digits, the system prefixes your entry with zeros to create eight digits. All devices with the specified network number will be included in the mobile group or AutoTracker VLAN.

c. The following prompt displays:

Select the IPX Network Encapsulation
1. Ethernet-II
2. IEEE 802.2 LLC
3. IEEE SNAP
4. IPX Proprietary

Enter the IPX Network Encapsulation (1):

Select the encapsulation type from the list. IPX devices do not know their network number at bootup. Typically, IPX servers assign different network numbers to devices using different encapsulation types within the same physical network. When an encapsulation type is specified here, an IPX device that does not know its network number at bootup will be assigned to the mobile group or AutoTracker VLAN as long as the device uses the encapsulation type you specify here.

d. Go on to Step 4 below.

4. The following prompt displays:

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

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the Network Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this mobile group or AutoTracker VLAN. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining Your Own Rules

A user-defined rule enables you to include all devices in the mobile group or AutoTracker VLAN that originate frames containing a specified pattern at a specified location. Each user-defined rule requires an Offset, a Value, and a Mask; you will be prompted for each of these values. The Offset specifies the location of the pattern within the frame. The Value specifies the pattern. The Mask specifies the bits that you care about within the Value pattern.

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Enter **5** and press **<Enter>**.

2. The following prompt displays:

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

   Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it controls only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

   ```
   Enter the Offset into the frame ( < 64) :
   ```

   Enter an **Offset** value, in number of bytes, to define the location where the **Value** – or pattern – is found. The offset value can be any number from 0 – 63. The first byte of the frame's MAC header is considered byte 1. An offset of 0 specifies that the pattern begins in byte 1 of the frame.

   As an example, enter an offset value of **14** if you want to specify the pattern that defines NETBIOS, because that pattern begins in the 21st byte of the frame.

4. The following prompt displays:

   ```
   Enter the value of the pattern to match:
   ```

   Enter a **Value**, in hex, to specify the pattern itself. The value can be a maximum of eight bytes. For example, enter **F0F0** to specify the pattern that identifies NETBIOS.

5. The following prompt displays:

   ```
   Enter the mask for the pattern to match:
   ```

   Enter a **Mask** value, in hex, to specify the bits within the **Value** that you care about. The mask can be a maximum of eight bytes, but must be the same length as the **Value** you entered. The mask value is ANDed with the **Value** and frames are searched for the result.

For example, if you enter **FFEF** as the value and **FFFF** as the mask:

	Hex		Binary
Value=	FFEF	=	1111 1111 1110 1111
Mask=	FFFF	=	1111 1111 1111 1111

When a bit in the mask is set to 1, the corresponding bit of the value must be literal. When a bit in the mask is set to 0, the corresponding bit in the value is ignored and can be either a 0 or a 1. In the example above, since the mask is FFFF, all bits in the value must be literal and the actual pattern searched for is the binary value 1111 1111 1110 1111. Only devices that originate frames containing this binary value beginning at the 21st byte will be included in the mobile group or AutoTracker VLAN.

As a second example, if you enter FFEF as the pattern and FFF7 as the mask:

	Hex		Binary
Value=	FFEF	=	1111 1111 1110 1111
Mask=	FFF7	=	1111 1111 1111 0111

In this example, bits 0–2 and bits 4–15 of the value must be literal, since the corresponding bits in the mask are 1s. However, since bit 3 of the mask is a 0, bit 3 of the value can be either a 0 or a 1. Therefore, in this example, two actual binary patterns are searched for:

1111 1111 1110 1111 **or** 1111 1111 1110 0111

Devices originating frames containing either one of these binary values beginning at the 21st byte of the frame will be included in the mobile group or AutoTracker VLAN.

6. The following prompt displays:

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

You can set up multiple rules for the same mobile group or AutoTracker VLAN. Enter a **Y** here if you want to set up more rules in addition to the Network Address rule specified here. If you enter **Y**, you will be prompted for the next rule that you want to set up on this mobile group or AutoTracker VLAN. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 1:2 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a Port Binding Policy

Port binding polices require devices to match two or three criteria. The criteria can be one of six combinations:

1. The device can attach to a specific switch port *and* use a specific MAC address *and* use a specific protocol (IP or IPX).
2. The device can attach to a specific switch port *and* use a specific MAC address *and* use a specific IP network address
3. The device can attach to a specific switch port *and* use a specific protocol (IP or IPX)
4. The device can use a specific IP address *and* use a specific MAC address
5. The device can use a specific port *and* a specific IP address
6. The device can use a specific port *and* a specific MAC address.

A device must match all values in the criteria set.

Port binding policies have two additional features. First, if a policy violation is detected, an SNMP trap is generated to alert the network manager which rule was violated. Secondly, if you attempt to configure a port binding rule that creates a conflict with another binding rule, an error message is generated to alert the user of the problem.

For example, if a port binding rule is created with a policy that links IP address 1.1.1.1 and MAC address aabbcc:ddeeff, and you attempt to create a port binding rule for the same IP address with a policy that links it to port 3/1, an error message will appear as shown:

This IP address has already been assigned to a different rule

In this example the second port binding rule is not created because the purpose of the first rule is to provide mobility for the IP address 1.1.1.1 (i.e., it is not restricted to a port), while the second rule specifically limits the mobility of IP address 1.1.1.1 to port 3/1.

A general rule for port binding policies is that once an address has been assigned (MAC or IP), it cannot be assigned to another policy until it is removed from the first policy. The following table is a reference for policy conflicts:

Limitations for Port Policies

	IP Address	MAC Address	Port	Protocol
IP Address	N/A	IP and MAC address cannot be used again	IP address cannot be used again	N/A
MAC Address	IP and MAC address cannot be used again	N/A	MAC address cannot be used again	MAC address cannot be used again
Port	IP address cannot be used again	MAC address cannot be used again	N/A	None
Protocol	N/A	MAC address cannot be used again	None	N/A

After you indicate you want to set up rules for this mobile Group or AutoTracker VLAN (using the **cratvl** command), the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Enter a 6 and press **<Enter>**.

2. The following prompt displays:

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

   Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it applies only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

   ```
   Please select one of the following bindings:
   1. Bind IP Address to a Port and a MAC Address.
   2. Bind MAC Address to a Protocol and a Port
   3. Bind Port to a Protocol
   4. Bind IP Address to a MAC Address
   5. Bind IP Address to a Port
   6. Bind MAC Address to a Port
   Enter the type of binding (1) :
   ```

   Enter the type of binding you want to use for this policy. Each binding policy specifies a particular device to be included in the mobile group or AutoTracker VLAN. Therefore, you must set up a separate binding policy for each device you want included in this mobile Group or AutoTracker VLAN.

   You can bind a device's IP address to a switch port and a MAC address (select option 1), bind a device's MAC address to a protocol and a switch port (select option 2), bind a switch port to a specific protocol (select option 3), bind an IP address to a MAC address (select option 4), bind an IP address to a switch port (select option 5), or bind a MAC address to a switch port (select option 6).

   ♦ Note ♦

   It is important to remember the line number of the binding policy you chose in order to follow the correct sequence for the remainder of these steps.

   If you select option 1, 2, 3, 5, or 6, go to step 4. If you select option 4, go to step 5.

4. The following prompt displays:

Enter the port in the form of slot/interface:

Enter the switch port to which this device must be attached. If the device is not attached to this port, it will not be included in this mobile Group or AutoTracker VLAN. You should first enter the slot for the module, then a slash (*/*), then the port number.

If you selected binding policy 1 or 5, then continue with step 5. If you selected binding policy 2 or 6, then continue with step 6. If you selected binding policy 3, then continue on with step 7.

5. The following prompt displays:

Enter the IP address:

Enter the IP address for the device. If the device does not have this IP address, it will not be included in this mobile Group or AutoTracker VLAN.

If you selected binding policy 1 or 4, continue with step 6. If you selected binding policy 5, continue with step 8.

6. The following prompt displays:

Enter the Canonical MAC address in AABBCC:DDEEFF format:

Enter the MAC address for the device. If the device does not have this MAC address, it will not be included in this mobile Group or AutoTracker VLAN.

If you selected binding policy 1, 4, or 6, then continue with step 8. If you selected binding policy 2, then continue with step 7.

7. The following prompt displays:

Select Protocol:
1. IP
2. IPX
3. DECNET
4. APPLETALK
5. Protocol specified by ether-type
6. Protocol specified by DSAP and SSAP
7. Protocol specified by SNAP

Enter protocol type (1):

Enter the number for the protocol that will be used to define this binding policy. Numbers are listed next to the protocol names. By selecting a specific protocol, you are indicating that a device with the MAC address you specified previously that are attached to the switch port you specified previously, and with traffic using this protocol will be assigned to this mobile group or AutoTracker VLAN. You can select the IP, IPX, DECNET, and APPLETALK protocols by entering 1, 2, 3, or 4, respectively.

♦ Note ♦

ARP (address resolution protocol) is included as IP. DDP (datagram delivery protocol) and AARP (AppleTalk ARP) are included as AppleTalk. DECNET is DECNET Phase IV traffic only.

If you want to define a protocol other than IP, IPX, AppleTalk, or DECNet, you can do so by specifying an Ethernet type, or by specifying source and destination SAP (service access protocol) header values, or by specifying a SNAP (sub-network access protocol) type. The following three sections describe how to specify these protocol types. If you are not specifying one of these special protocol types, continue with Step 8 below.

Protocol Specified by Ether-Type

a. To specify a protocol by Ethernet type, enter **5** at the **Select Protocol:** menu. The following prompt displays:

Enter the Ether-type value in hex:

b. Enter the desired Ethernet type in hex. You must enter two bytes of data. For example, enter 0800 to specify IP or enter 0806 to specify ARP. All devices that use the specified Ethernet type will be members of the mobile group or AutoTracker VLAN.

c. Go on to Step 8 below.

Protocol Specified by DSAP and SSAP

a. To specify a protocol by SAP (service access protocol) header, enter **6** at the **Select Protocol:** menu. The following prompt displays:

Enter the DSAP value in hex:

b. Enter the destination service access protocol (DSAP) value in hex and press **<Enter>**. The following prompt displays:

Enter the SSAP value in hex:

c. Enter the source service access protocol (SSAP) value in hex. Each entry must consist of one byte of data. All devices that use the specified source and destination SAP types will be members of the mobile group or AutoTracker VLAN.

d. Go on to Step 8 below.

Protocol Specified by SNAP

a. To specify a protocol by SNAP (sub-network access protocol) type, enter **7** at the **Select Protocol:** menu. The following prompt displays:

Enter the SNAP value in hex

b. Enter the desired SNAP value in hex. You must enter five bytes of data. For example, enter 0000008137 to specify IPX SNAP or enter 00000080F3 to specify AppleTalk ARP SNAP. All devices that use the specified SNAP type will be members of the mobile group or AutoTracker VLAN.

c. Go on to Step 8 below.

8. The following prompt displays:

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

You can set up more devices for this binding policy group. Enter a **Y** here if you want to set up more devices. If you enter **Y**, you will be prompted for the next rule that you want to set up. Follow the directions in the appropriate section to configure that rule.

If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

VLAN 2:1 created successfully

You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a DHCP Port Policy

DHCP port polices simplify network configurations requiring DHCP clients and servers to be in the same mobile group or AutoTracker VLAN. You can see how DHCP port policies were used in an application example on page 17-23.

DHCP port policies differ fundamentally from standard port policies. In a standard port policy, the port is placed in the mobile group or AutoTracker VLAN as soon as the port rule is configured; no traffic on the port is required. A DHCP port rule *requires* traffic on the port in the form of a DHCP request packet before the port gains membership.

After you indicate you want to set up rules for this mobile Group or AutoTracker VLAN, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Enter a 7 and press **<Enter>**.

2. The following prompt displays:

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

   Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it applies only to this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

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

   Enter the physical switch ports that you want included in this mobile Group or AutoTracker VLAN. You may enter multiple ports at a time. 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 LAN ports. They are only necessary when specifying logical ports used over Frame Relay.)

4. The following prompt displays:

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

   You can set up multiple rules for the same mobile group or AutoTracker 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. Follow the directions in the appropriate section to configure that rule. If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

   ```
   VLAN 1:2 created successfully
   ```

   You are done setting up rules for this mobile group or AutoTracker VLAN.

Defining a DHCP MAC Address Policy

You can see how DHCP MAC address policies were used in an application example on page 17-23.

After you enter the Administrative Status for this mobile group or AutoTracker VLAN, the following menu displays:

```
Select rule type:
1. Port Rule
2. MAC Address Rule
3. Protocol Rule
4. Network Address Rule
5. User Defined Rule
6. Binding Rule
7. DHCP PORT Rule
8. DHCP MAC Rule

Enter rule type (1):
```

1. Enter **8** and press **<Enter>**.

2. The following prompt displays:

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

   Indicate whether or not you want to enable the Administrative Status for this rule. Type **e** to enable or **d** to disable. If you enable the rule, the switch will use it to determine membership of devices. If you disable the rule, then the switch will not use this rule, but the parameters you set up will be saved. The Admin Status for a Policy is different from the Admin Status for the mobile group or AutoTracker VLAN as it applies only this specific rule. You can enable or disable the rule at a later time using the **modatvl** command.

3. The following prompt displays:

   ```
   Enter the list of MAC addresses (AABBCC:DDEEFF) in Canonical format
   (Enter save to end):
   ```

   Enter the MAC addresses that you want to include in this mobile group or AutoTracker VLAN. Separate addresses by a space. When you have entered the final MAC address, leave a space and type **save**.

4. The following prompt displays:

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

   You can set up multiple rules for the same mobile group or AutoTracker 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. Follow the directions in the appropriate section to configure that rule.

   If you enter **N**, you will receive a message, similar to the one below, indicating that the VLAN was set up.

   ```
   VLAN 1:2 created successfully
   ```

   You are done setting up rules for this mobile group or AutoTracker VLAN.

Viewing Mobile Groups and AutoTracker VLANs

You can view the current status of all mobile groups or AutoTracker VLANs in the switch using the **atvl** command. Enter **atvl** and a table similar to the following displays.

VLAN Group :	VLAN Id	VLAN Description	Admin Status	Operational Status
6		New Mobile Group 6	Enabled	Active
8		New Mobile Group 8	Enabled	Active

VLAN Group. The Group to which this AutoTracker VLAN is assigned. The Group is specified when first creating an AutoTracker VLAN.

VLAN ID. An identification number that you assigned when you created this VLAN. A value will not display in this column for mobile groups.

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

Admin Status. The Administrative Status for the VLAN may be enabled or disabled. You enable or disable the Administrative Status for a VLAN when you create or modify it. If the VLAN is enabled, the switch will use the policies you configured to filter traffic to the devices in this VLAN. If you disable the rule, then policies will not be used, but the parameters you set up for the VLAN will be saved.

Oper Status. The VLAN is shown as **Active** or **Inactive**. In order for an enabled VLAN to become "active" it must be able to assign a switch port to the VLAN. If the port rule is used for a VLAN, then the VLAN automatically becomes active. If any other rule is used (MAC address, protocol, etc.), then a frame matching the VLAN rule must first be received by a switch port before the VLAN is active. So, an Active VLAN requires the following:

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

Viewing Policy Configurations

Typing **viatrl** brings up the Policy Configuration Table, which shows the policies defined for the mobile Group or VLAN specified.

VLAN Group :	VLAN Id	Rule Num	Rule Type	Rule Status	Rule Definition
3:	5	1	PORT RULE	Disabled	2/7/Brg/1
3:	11	1	NET ADDR RULE	Enabled	IPX Addr = 11223344
					IPX Encapsulation = Ethernet
3:	12	1	NET ADDR RULE	Enabled	DECNET Area = 13579
3:	22	1	PORT RULE	Enabled	2/7/Brg/1
3:	23	1	PORT RULE	Enabled	2/7/Brg/1
3:	24	1	MAC RULE	Enabled	082008:003002
					082009:803728
3:	25	1	PROTOCOL RULE	Enabled	Protocol = IP
3:	26	1	NET ADDR RULE	Enabled	IP Addr = 131.1.2.3
					IP Mask = 255.255.0.0
3:	27	1	USER RULE	Enabled	Offset = 64
					Length = 2
					Value = FFFF
					Mask = FFFF
3:	31	1	PROTOCOL RULE	Enabled	Protocol = IP
3:	32	1	NET ADDR RULE	Enabled	IPX Addr = 00000001
					IPX Encapsulation = Ethernet

VLAN Group. The Group to which this AutoTracker VLAN is assigned. The Group number is specified when first creating the VLAN.

VLAN ID. An identification number that you assigned when you created this virtual LAN. A value will not display in this column for mobile groups.

Rule Num. The number of the policy within the VLAN definition. Each rule defined for a 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 VLAN policy. The Rule Type can be a port policy (PORT RULE), MAC Address policy (MAC RULE), network address policy (NET ADDR RULE), Protocol policy (PROTOCOL RULE), a user-defined policy (USER RULE), port-binding policy (BIND RULE), DHCP Port policy (DHCP PORT RULE), or a DHCP MAC address policy (DHCP MAC RULE). You set up VLAN policies when you create or modify the VLAN.

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

Rule Definition. Details of this rule. For a Port Rule, this column lists the virtual interface for the Port included in the VLAN 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 device in the VLAN. For a Network Address Rule, the column will list the address (IP or IPX) and the IP Mask (IP) or the Encapsulation type (IPX). For a Protocol policy, the column list the protocol used to determine membership. And in a User-Defined rule, the offset, length, value, and mask are listed.

Viewing Virtual Ports' Group/VLAN Membership

You can view the VLAN membership of each virtual interface in the switch. For physical LAN ports, the virtual interface is the same as a virtual port. However, when multiple services are set up for a physical port, then each service has a virtual port.

Type **vivl** 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#
2 /1 /Brg /1	1	1
2 /2 /Brg /1	1	1
2 /3 /Brg /1	1	1
2 /4 /Brg /1	1	1
2 /5 /Brg /1	1	1
2 /6 /Brg /1	1	1
2 /7 /Brg /1	1	1 22
2 /8 /Brg /1	1	1
2 /9 /Brg /1	1	1
2 /10 /Brg /1	1	1
2 /11 /Brg /1	1	1
2 /12 /Brg /1	1	1

Slot/Intf/Service/Instance. Specifies the virtual interface for which AutoTracker 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 an AutoTracker VLAN.

Member of VLAN #. The AutoTracker VLANs to which this virtual interface belongs. An interface may belong to more than one VLAN. For example, a port may contain devices using the IP Protocol and could match the Port policy of one AutoTracker VLAN and the Protocol policy of another AutoTracker VLAN. Also, physical ports always remain members of the default VLAN #1.

View VLAN Membership of MAC Devices

The **fwtvl** command displays a table of learned MAC addresses and the VLAN membership of those MAC addresses. Follow these steps to view this table.

1. Enter **fwtvl**.
2. The following prompt displays:

   Enter Slot/Interface (return for all ports) :

   Enter the slot and port for which you want to view MAC Address/VLAN information. You can also press **<Enter>** to view information on all ports in the switch.
3. The following message and prompt displays:

   Total number of MAC addresses learned for Group 1: 4
   Maximum number of entries to display [20]) :

   The top line displays the number of MAC addresses learned on this switch. This number indicates the potential number of entries you can display in the Learned MAC Address Table. The second line allows you to indicate how many of these MAC addresses you want to display. Enter the number of MAC entries you want to display or press **<Enter>** to select the default in brackets [20].
4. The Learned MAC Address/VLAN Membership Table displays as follows:

MAC Address	Slot/Intf/Service/Instance	AT VLAN Membership
0020DA:05F623	2/ /1 /Brg 1	1
0020DA:021533	2/ /1 /Brg 1	1
0020DA:0205B3	2/ /1 /Brg 1	1
0020DA:06BAD3	2/ /1 /Brg 1	1
0020DA:05F610	2/ /1 /Brg 1	1

MAC Address. The MAC address for which virtual interface and VLAN membership information will be displayed.

Slot/Intf/Service/Instance. Specifies the virtual port for which AutoTracker VLAN information will be displayed. The **Slot** is the physical slot location to which the MAC address maps. The **Intf** is the physical port to which the MAC address maps. The **Service** is the service type for this MAC address. The service type may be a Router (**Rtr**) or Bridge (**Brg**). **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.

AT VLAN Membership. The AutoTracker VLANs to which this MAC Address belongs. An MAC address may belong to more than one VLAN. For example, let's say a MAC device runs on an IPX network. It could be included in a MAC Address policy for one AutoTracker VLAN and the IPX Protocol Policy of another VLAN.

Application Example: DHCP Policies

This application example shows how Dynamic Host Configuration Protocol (DHCP) port and MAC address policies can be used in a DHCP-based network. DHCP is built on a client-server model in which a designated DHCP server allocates network addresses and delivers configuration parameters to dynamically configured clients.

Since DHCP clients initially have no IP address, placement of these clients in an AutoTracker VLAN presents a problem. AutoTracker determines VLAN membership by looking at traffic from source devices. Since the first traffic transmitted from a source DHCP client does not contain the actual address for the client (because the server has not allocated the address yet), the client may not be placed in the same VLAN as its server.

Before the introduction of DHCP port and MAC address rules, various strategies were deployed to use DHCP with Groups and VLANs. Typically these strategies involved IP protocol and network rules along with Bootp relay functionality. (See Chapter 21 for some application examples of these strategies.) These solutions required that all DHCP clients in a particular mobile group or VLAN be grouped together through a common IP policy.

DHCP port and MAC address rules simplify the configuration of DHCP networks. Instead of relying on IP-based policies to group all DHCP clients in the same network as a DHCP server, you can manually place each individual DHCP client in the VLAN or mobile group of your choice. DHCP port and MAC address policies operate the same way as standard port and MAC address policies except these new rules have been enhanced for use with DHCP clients.

The VLANs

This application example contains three (3) AutoTracker VLANs within a single non-mobile group. These VLANs are called Test, Production, and Branch.

The Test VLAN connects to the main network, the Production VLAN, through an external router. This VLAN is intended to be self-contained such that copies of it could be made and attached to the Production VLAN in the same way this VLAN does. The Test VLAN contains its own DHCP server and DHCP clients. The clients gain membership to the VLAN through DHCP port rules.

The Production VLAN carries most of the traffic in this network. It does not contain a DHCP server, but does contain DHCP clients that gain membership through DHCP port rules. Two external routers connect this VLAN to the Test VLAN and a Branch VLAN. One of the external routers—the one connected to the Branch VLAN—has Bootp relay functionality enabled. It is through this router that the DHCP clients in the Production VLAN access the DHCP server in the Branch VLAN.

The Branch VLAN contains a number of DHCP client stations and its own DHCP server. The DHCP clients gain membership to the VLAN through both DHCP port and MAC address rules. The DHCP server allocates IP addresses to all clients in this VLAN as well as the DHCP clients in the Production VLAN.

DHCP Servers and Clients

DHCP clients must be able to communicate with a DHCP server at initialization. The most reliable way to ensure this communication is for the server and its associated clients to share the same VLAN or mobile group. However, if the network configuration does not lend itself to this solution (as the Production VLAN does not in this application example), then the server and clients can communicate through a router with Bootp relay enabled.

The DHCP servers and clients in this example are either in the same VLAN or are connected through a router with Bootp relay. All clients in the Test VLAN receive IP addresses from the server in their VLAN (Server 1). Likewise, all clients in the Branch VLAN receive IP addresses from their local server (Server 2). The DHCP clients in the Production VLAN do not have a local DHCP server, so they must rely on the Bootp relay functionality in external Router 2 to obtain their IP addresses from the DHCP server in the Branch VLAN.

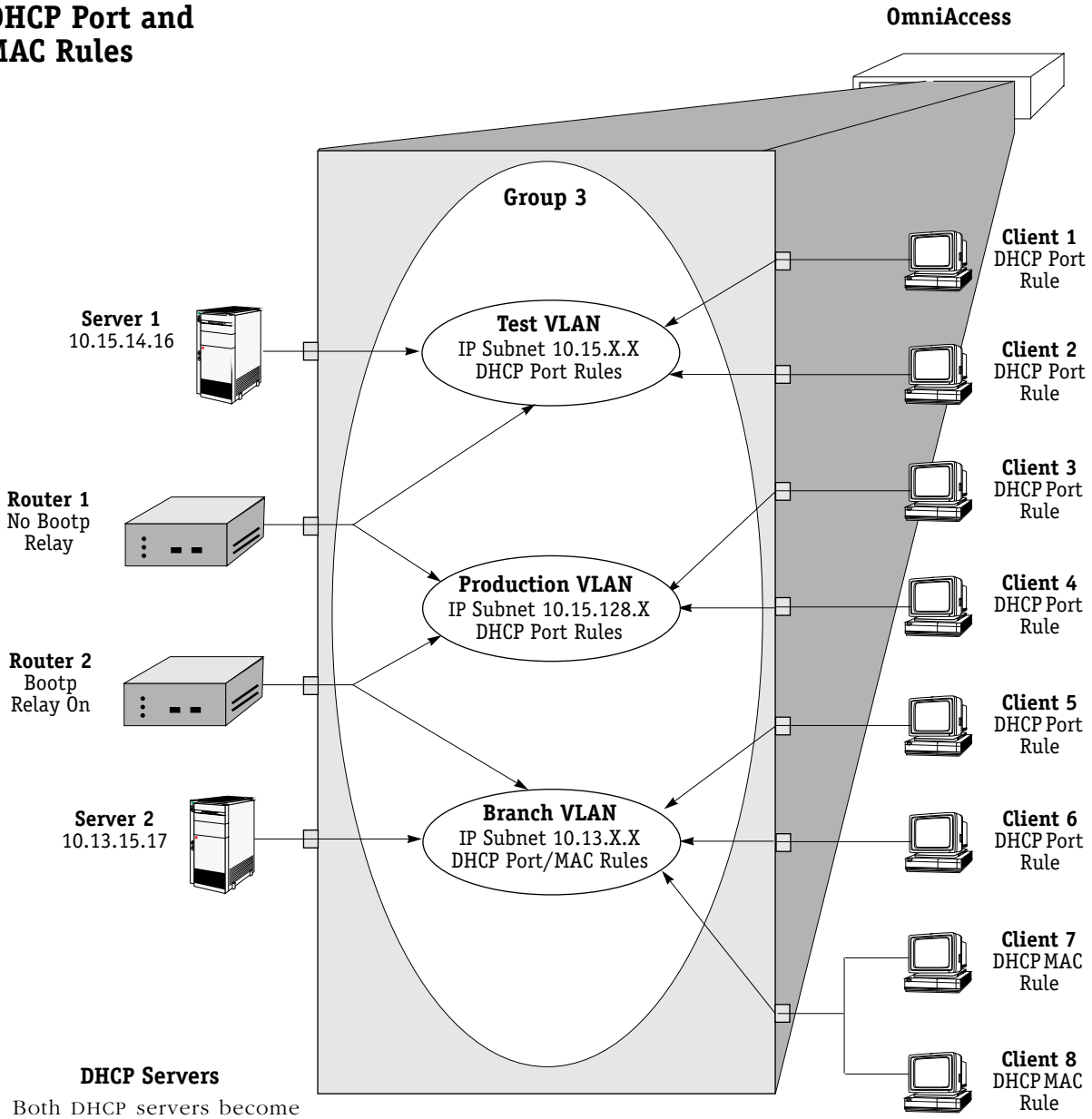
Both DHCP servers gain membership to their VLANs through IP network address policies.

The following table summarizes the VLAN architecture and policies for all devices in this network configuration. The diagram on the following page illustrates this network configuration.

Devices and VLAN Membership

Device	VLAN Membership	Policy Used/Router Role
DHCP Server 1	Test VLAN	IP subnetwork rule=10.15.X.X
DHCP Server 2	Branch VLAN	IP subnetwork rule=10.13.X.X
External Router 1	Test VLAN Production VLAN	Connects Test VLAN to Production VLAN
External Router 2	Production VLAN Branch VLAN	Bootp relay provides access to DHCP server in Branch VLAN for clients in Production VLAN.
DHCP Client 1	Test VLAN	DHCP Port Rule
DHCP Client 2	Test VLAN	DHCP Port Rule
DHCP Client 3	Production VLAN	DHCP Port Rule
DHCP Client 4	Production VLAN	DHCP Port Rule
DHCP Client 5	Branch VLAN	DHCP Port Rule
DHCP Client 6	Branch VLAN	DHCP Port Rule
DHCP Client 7	Branch VLAN	DHCP MAC Address Rule
DHCP Client 8	Branch VLAN	DHCP MAC Address Rule

DHCP Port and MAC Rules



DHCP Servers

Both DHCP servers become members in their respective VLANs via IP subnet rules.

Routers

Router 1 provides connectivity between the Test VLAN and the Production VLAN. It does not have Bootp functionality enabled so it cannot connect DHCP servers and clients from different VLANs.

Router 2 connects the Production VLAN and the Branch VLAN. With Bootp relay enabled, this router can provide connectivity between the DHCP server in the Branch VLAN and the DHCP clients in the Production VLAN.

DHCP Clients

Clients 1 to 6 are assigned to their respective VLANs through DHCP port rules. Clients 3 and 4 are not in a VLAN with a DHCP server so they must rely on the server in the Branch VLAN for initial addressing information. Clients 7 and 8 share a port with other devices, so they are assigned to the Branch VLAN via DHCP MAC address rules.