27 Interswitch Protocols

This chapter describes Interswitch Protocols, which are used to discover adjacent switches, and track VLAN membership and retain mobile group information across switches. They include two new protocols and one existing protocol that is updated for release 4.0:

- Mapping Adjacency Protocol (XMAP), a new protocol used to discover the topology of OmniSwitches and OmniSwitch/Routers (Omni S/Rs)
- Group Mobility Advertisement Protocol (GMAP), a new protocol used to retain learned mobile group and protocol information
- VLAN Advertisement Protocol (VAP), an existing interswitch protocol used to exchange VLAN information between switches

The protocols are independent of each other and perform separate functions. Each protocol is described in detail in separate sections of this chapter.

Interswitch Protocol Commands

There is an Interswitch Protocol (XIP) submenu. Select **XIP** from the AutoTracker submenu, and the submenu displays as follows:

```
Command          XIP Menu
---------------  ------------------------------------------------------------------------
gmapst           Turn Group Mobility Advertisement Protocol (GMAP) ON or OFF
gmapgaptime      Set GMAP inter-message gap time in milliseconds
gmapholdtime     Set GMAP hold time interval time in minutes
gmapupdttime     Set GMAP update interval time in seconds
vlap             Turn VLAN Advertisement Protocol (VAP) ON or OFF
xmapst           Turn the Xylan Mapping Adjacency Protocol (XMAP) ON or OFF
xmapls           List adjacent switches found using the XMAP protocol
xmapdisctime     Set XMAP message interval for discovery phase in seconds
xmapcmntime      Set XMAP message interval for common phase in seconds

    Main      File      Summary  VLAN      Networking
    Interface Security  System   Services  Help
```

These commands are described in this chapter.

XMAP

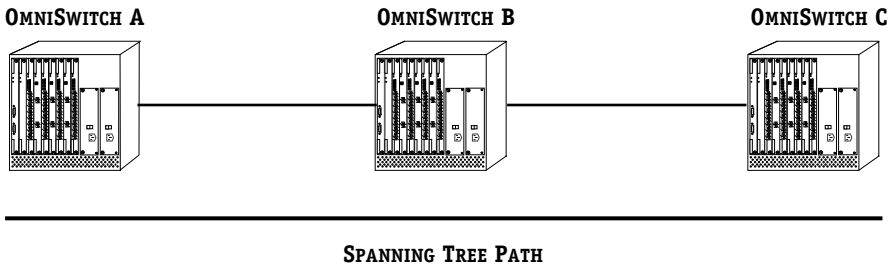
The Mapping Adjacency Protocol (XMAP) is used to discover the topology of OmniSwitches or OmniS/Rs in a particular installation. Using this protocol, each switch determines which OmniSwitches or OmniS/Rs are adjacent to it by sending and responding to Hello update packets. For the purposes of XMAP, *adjacent* switches are those that:

- have a Spanning Tree path between them
- do not have any switch between them on the Spanning Tree path that has XMAP enabled

♦ Note ♦

XMAP replaces the Adjacency Only mode of earlier versions of VAP.

In the illustration here, all switches are on the Spanning Tree path. OmniSwitch A and OmniSwitch C have XMAP enabled. OmniSwitch B does not. OmniSwitch A is adjacent to OmniSwitch C and vice versa. If OmniSwitch B enables XMAP, the adjacency changes. A would be adjacent to B, B would be adjacent to both A and C, and C would be adjacent to B.



XMAP Adjacency

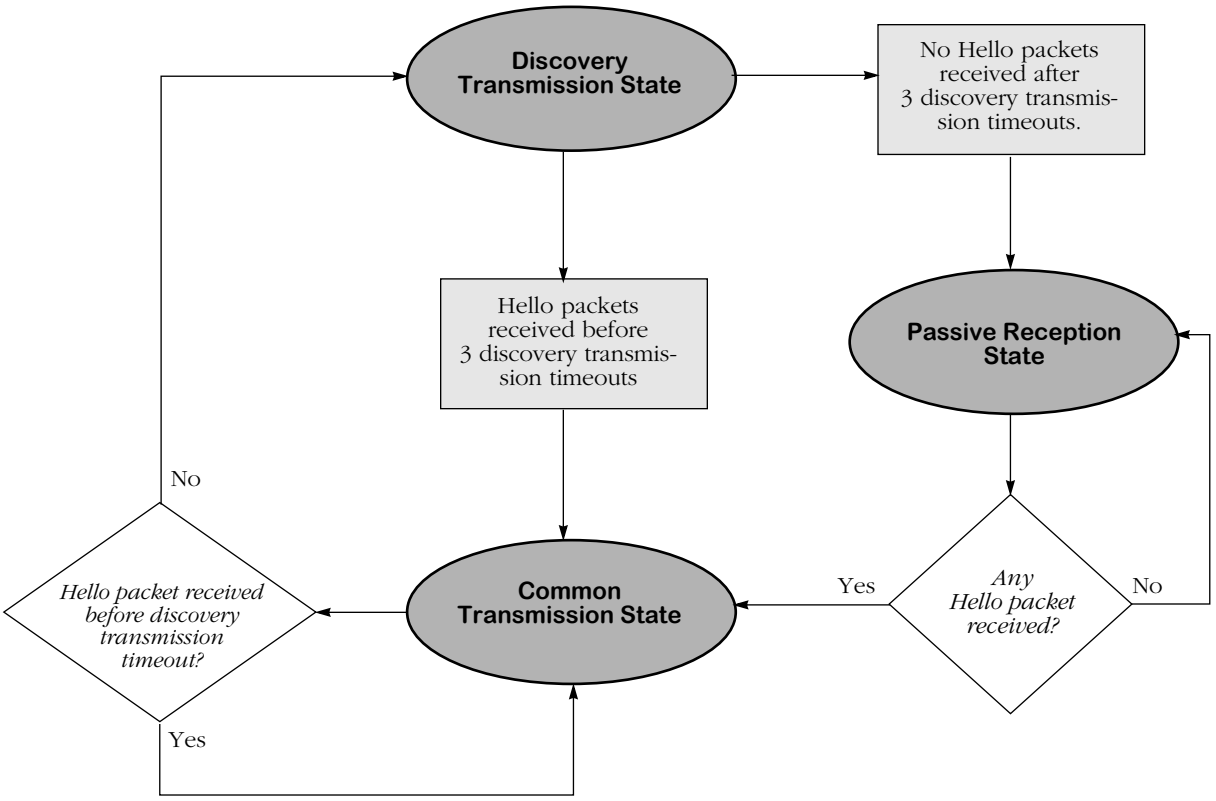
XMAP Transmission States

XMAP switch ports are either in the *discovery transmission state*, *common transmission state*, or *passive reception state*. Ports transition to these states depending on whether or not they receive Hello responses from adjacent switches.

♦ Note ♦

All Hello packet transmissions are sent to a well-known MAC address (0020DA000003).

The transmission states are illustrated here.



XMAP State Transitions

Discovery Transmission State

When XMAP is active, at startup all active switch ports are in the discovery transmission state. In this state ports send out Hello packets and wait for Hello responses. Ports send out Hello packets at a configurable interval called the *discovery transmission time*. The discovery transmission time is configurable; 30 seconds is the default. The ports send out Hello packets up to *three* timeouts of this interval trying to discover adjacent switches.

Any switch ports that receive Hello packets before three discovery transmission times expire send a Hello reply and transition to the common transmission state. Any switch ports that do not receive a Hello response before three discovery transmission times have expired are placed in the passive reception state.

Common Transmission State

In the common transmission state, ports detect adjacent switch failures or disconnects by sending Hello packets and waiting for Hello responses. Ports in this state send out Hello packets at a configurable interval (the default is 5 minutes) called the *common transmission time*. To avoid synchronization with adjacent switches, the common transmission time is jittered randomly by plus or minus ten percent.

Ports wait for Hello responses using the *discovery transmission time* (the default is 30 seconds). If Hello responses are detected within one discovery transmission time, the port remains in the common transmission state. If Hello responses are not detected within one discovery transmission time, the port reverts to the discovery state.

Passive Reception State

In the passive reception state, switch ports are in receive-only mode. Hello packets are not sent out from these ports, and there is no timer on waiting for Hello responses. If the port receives a Hello packet at any time, it enters the common transmission state and transmits a Hello packet in reply.

If a port transitions to the passive reception state, any remote switch entries for that port are deleted.

Common Transmission and Remote Switches

If an XMAP switch is connected to multiple XMAP switches via a hub, the switch sends and receives Hello traffic to and from the remote switches through the same port. If one of the remote switches stops sending Hello packets and other remote switches continue to send Hello packets, the ports in the common transmission state will remain in the common transmission state.

The inactive switch will eventually be aged out of the switch's XMAP database because each remote switch entry has a "last seen" field that is updated when Hello packets are received. The switch checks the "last seen" field at least once every common transmission interval. Switch ports that are no longer "seen" may still retain an entry for up to three common transmission intervals. The slow aging out prevents the port from sending Hello packets right away to the inactive switch and creating additional unnecessary traffic.

Configuring XMAP

XMAP is active by default. In addition to disabling or enabling XMAP, you can view a list of adjacent switches or configure the timeout intervals for Hello packet transmission/reception.

Enabling or Disabling XMAP

To display whether or not XMAP is active or inactive, or to activate or deactivate XMAP, enter the following command:

```
xmapst
```

A screen displays similar to the following:

```
XMAP is currently ACTIVE. (a)ctivate, (d)e-activate : (a) :
```

Enter **a** or **d** to change the current state, or press **<Enter>** to keep the current value. A message similar to the following displays:

```
XMAP is ACTIVE.
```

To change the state of XMAP without displaying the current state first, enter the command with the desired value. For example:

```
xmapst d
```

A message similar to the following displays:

```
XMAP is INACTIVE.
```

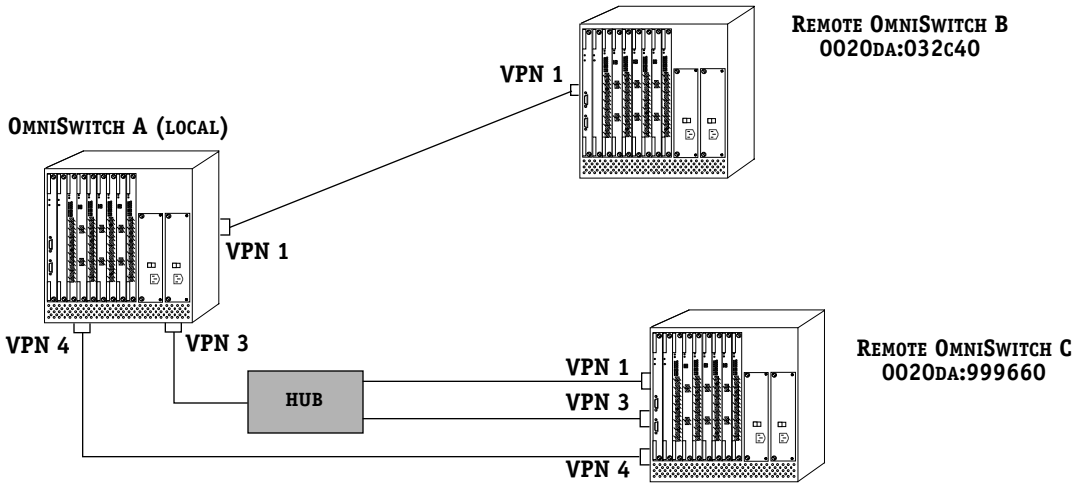
Viewing a List of Adjacent Switches

Use the **xmapls** command to view a list of adjacent switches and their associated MAC addresses, ports, groups, and IP addresses. For remote switches that stop sending Hello packets *and* are connected via a hub, entries may take up to three times the common transmission interval to age out of this table.

The example display shows three virtual ports on a local XMAP switch connected to remote virtual ports on two switches. VPN 3 is connected to a remote switch through a hub.

VPN	Rem Switch ID	Rem VPN	Pri Group	IP Addresses
1	0020da:032c40	1	2	18.1.1.1
				27.0.0.2
				192.168.10.1
				198.206.184.40
3	0020da:999660	1	2	192.168.10.1
		3	7	198.206.184.177
4	0020da:999660	4	9	192.168.10.1
				198.206.184.177

A visual illustration of these connections is shown here:



XMAP Network Example

The fields in **xmapls** table are defined as follows:

VPN. The local virtual port number which is connected to an adjacent switch.

Rem Switch ID. The MAC address of the MPM in the adjacent switch.

Rem VPN. The remote virtual port number in the adjacent switch.

Pri Group. The primary group associated with the remote port. The primary group is the group upon which Spanning Tree converges. For more information about primary groups, see Chapter 25, "Managing Groups and Ports."

IP Addresses. All IP addresses associated with the adjacent switch.

Configuring the Discovery Transmission Time

The discovery transmission time is used in both the discovery transmission state *and* the common transmission state to determine how long the port will wait for Hello packets. For ports in the discovery transmission state, this timer is also used as the interval between sending out Hello packets.

♦ Note ♦

Ports in the common transmission state send out Hello packets based on the common transmission time as described in the next section.

Use the **xmapdisctime** command to view or update the discovery transmission time.

To view the current discovery transmission time, enter the following command:

```
xmapdisctime
```

A message similar to the following displays:

```
XMAP Discovery Phase Timeout Interval is 30 seconds.
```

To change the interval, enter the command with the desired value (any value between 1 and 65535). For example:

```
xmapdisctime 20
```

A message similar to the following displays:

```
XMAP Discovery Phase Timeout Interval is 20 seconds.
```

Configuring the Common Transmission Time

Use the **xmapcmntime** command to view or change the time between sending Hello update packets in the common transmission state. (This timer is only used in the common transmission state.) A switch sends an update for a port just before or after the common transmission time expires.

♦ Note ♦

The switches avoid synchronization by jittering the common transmission time by plus or minus ten percent of the configured value. For example, if the default common transmission time is used (300 seconds), the jitter is plus or minus 30 seconds.

When a Hello packet is received from an adjacent switch before the common transmission time expires, the switch sends a Hello reply and restarts the common transmission timer.

To view the current common transmission time, enter the following:

```
xmapcmntime
```

A message similar to the following displays:

```
XMAP Common Phase Timeout Interval is 300 seconds.
```

To change the interval, enter the command with the desired value (the value must be between 1 and 65535):

```
xmapcmntime 200
```

A message similar to the following displays:

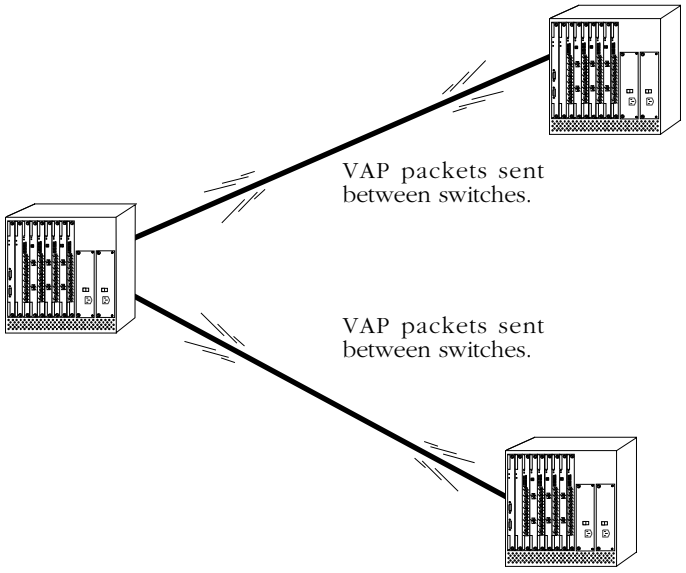
```
XMAP Common Phase Timeout Interval is 200 seconds.
```

VLAN Advertisement Protocol (VAP)

The VLAN Advertisement Protocol (VAP) is an interswitch protocol that keeps the VLAN membership databases stored on switches in sync and enables the auto-discovery of network nodes. VAP is useful when you want all VLANs to communicate over a backbone, but do not want locally connected devices to receive all backbone traffic.

In order for a switch to participate in VAP exchanges, VAP must be enabled through a software configuration command. The switch does not need to have attached devices that are a part of all groups and VLANs for which VAP information is exchanged; however, all groups and VLANs must be defined on each switch.

Each switch in a network maintains an AutoTracker database. This database is built by observing traffic that matches user-configured policies. The VAP protocol reads this database on all switches and then advertises entries in the database to all other switches in the network.



VAP Exchanges Between Switches

VAP updates nodes on any new entries in AutoTracker databases every 60 seconds.

VAP also stores information in its own database. Currently this information is used by SNMP-based network management software. The database contains information on VLAN membership; it maps each learned MAC address to a group and to any associated VLANs. This database can contain information on up to 40,000 MAC addresses.

VAP and Port Policies

One of the main purposes of VAP is to advertise the connectivity of devices attached to the switch via AutoTracker port policies. VAP eliminates the need to apply port policies to backbones to ensure that connectivity is established and maintained. When you use port policies, all devices heard through a port will become a member of the VLAN. Using port policies across backbones is not efficient because all devices learned over the backbone would be placed in the same VLAN since they would be attached to the same port.

For this reason, port policies should not be used to interconnect switches because these policies classify MAC addresses on VLANs. Backbone ports should be left in the default VLAN, and only learned devices should be segregated into VLANs by port policies.

There are two types of port policies (or rules), regular port rules and port forwarding rules. Only one can be active at a time. The type of port rule is determined by a command line in the **mpm.cmd** or **mpx.cmd** file. See *Port Policy Functionality* in Chapter 28, "Managing AutoTracker VLANs," for a detailed explanation of the two port rules settings.

Regular port policy places frames received on a particular port into a VLAN; VLAN membership is based on the port. The current version of VAP supports regular port rules only.

If you set up VAP in its full mode (VLAN membership exchanges and auto-discovery), the switch will automatically set the port policy to *regular* mode.

♦ Note ♦

Earlier versions of VAP include an Adjacency Only mode. If an earlier version of VAP is running on the switch in Adjacency Only mode, when new code is loaded and the switch is rebooted, VAP will be set to off. If an earlier version of VAP is set to Full mode, VAP remains in Full mode when the new code is loaded and the switch is rebooted.

Configuring VAP

There are two settings for the VLAN advertisement protocol, off or full mode. These modes are defined as follows:

- *Full mode*—VLAN membership information exchanged between switches and auto-discovery of network nodes is enabled. This option automatically sets the port policy to regular mode.
- *Off*—Disables VAP exchanges. Nodes will not be auto-discovered and VLAN information will not be exchanged between switches.

To change the VAP mode, at a UI command prompt, enter **vlap** and select the mode in which you want VAP to run. A screen similar to the following displays:

```
The VLAN advertisement protocol is currently not running
To change the mode type: F - full mode, O - off : ( ) :
```

Or, enter the **vlap** command with the desired mode. For example:

```
vlap f
```

A message similar to the following displays:

```
The VLAN advertisement protocol is currently running.
```

The new mode takes effect immediately. You do not need to reboot the switch.

GMAP

The Group Mobility Advertisement Protocol (GMAP) enables workstation users to move from port to port among interconnected switches and still retain all learned mobile group and protocol information. Using GMAP the switch sends a complete list of learned MAC addresses and associated group/protocol information to all interconnected switches in the network. Update and retention times are configurable. A switch that receives a GMAP update packet updates its internal GMAP tables and queries the forwarding database to make any necessary updates.

At startup time and for three successive update intervals, GMAP sends update packets on all virtual ports that are active non-leaf ports (that is, ports that are running Spanning Tree). GMAP packets are sent using the VAP multicast address. After startup and three transmissions, interval packets will only be sent on virtual ports that are active and are known to have an OmniSwitch or OmniS/R running GMAP connected to them.

GMAP will send updates only for MAC addresses that are learned on leaf ports (ports that are not running Spanning Tree). It does not advertise MAC addresses for groups assigned by authentication, and it does not advertise group 1 entries or nonmobile group entries. If conflicting information is received for a MAC address, the last packet received for that address will take precedence.

When AutoTracker learns a new MAC address on a leaf port it attempts to assign it to a mobile group. It consults GMAP tables and any appropriate group membership entries are added to the forwarding database.

GMAP Updating Rules

Upon receiving a packet, GMAP updates its internal tables and queries the forwarding database. When GMAP reviews the forwarding database to update it with new information, it uses the following rules:

- GMAP will only update information for leaf ports.
- GMAP does not add a new MAC address to a port.
- GMAP will only overwrite group 1 entries. If there is no group 1 entry, it will add a new entry, provided that it will not create a conflict with existing entries in the forwarding database.
- GMAP will not add an entry for an authenticated group.
- GMAP will not add an entry that is in conflict or potential conflict with a binding rule. A potential conflict would be a binding rule that requires the IP address be known for the MAC address. GMAP does not have access to IP information.
- GMAP will not add an entry for a group/protocol pair when there is an existing entry for that protocol on the requested port.
- When GMAP finds an entry for the desired group already on the switch but not on the requested port, it will move it to the requested port.
- When GMAP finds an entry with the appropriate group but a protocol value of 0 (indicating all protocols), it will update the protocol value in that entry to that in its database.

Configuring GMAP

GMAP is inactive by default. In addition to enabling and disabling GMAP, you can configure the time between packet transmissions (when multiple packets are required for an update), the time between updates, and the length of time GMAP will retain its current information.

Enabling and Disabling GMAP

Use the **gmapst** command to display or change the state of GMAP. A prompt similar to the following displays:

```
GMAP is currently INACTIVE. (a)ctivate, (d)e-activate: (d)
```

Enter **a** or **d** or press **<Enter>** to keep the current value. A message similar to the following displays:

```
GMAP is ACTIVE.
```

To change the state of GMAP without displaying the current state first, enter the command with the desired value. For example:

```
gmapst d
```

The following message displays:

```
GMAP is INACTIVE.
```

Configuring the Gap Time

Use the **gmapgaptime** command to display or change the interpacket gap time used when multiple packets are required for an update. When there are many MAC addresses on mobile ports, more than one GMAP packet is required for an update. Typically the gap time does not have to be changed, but you may want to modify it if traffic spikes are occurring in the network.

To view the current gap time, enter the following command:

```
gmapgaptime
```

A message similar to the following displays:

```
GMAP Gap Time is 133 milliseconds.
```

To change the gap time, enter the command with the desired value (any value between 0 and 65535). For example:

```
gmapgaptime 100
```

A message displays similar to the following:

```
GMAP Gap Time is 100 milliseconds.
```

The switch approximates the gap time because its internal clock does not use milliseconds. For any value shorter than one second, the switch uses 1/60 second increments called “ticks.” The default for gap time is 8 ticks or approximately 133 milliseconds. Any value you enter will be rounded to the nearest tick.

Configuring the Interpacket Update Time

Use the **gmapupdtime** command to display or change the time between sending updates.

♦ Note ♦

The switches avoid synchronization by jittering the update time by plus or minus one quarter of the configured interval. For example, if the default of 300 seconds is used, the jitter is plus or minus 75 seconds.

To view the current update time, enter the following:

```
gmapupdttime
```

A message similar to the following displays:

```
GMAP Update Time is 300 seconds.
```

To change the update time, enter the command and the desired time (any value between 1 and 65535). For example:

```
gmapupdttime 100
```

A message similar to the following displays:

```
GMAP Update Time is 100 seconds.
```

Configuring the Hold Time

Use the **gmapholdtime** command to display or change the length of time for which GMAP will retain information it has learned.

To view the current hold time, enter the following:

```
gmapholdtime
```

A message similar to the following displays:

```
GMAP Hold Time is 4320 minutes.
```

The default is 4320 minutes (72 hours). To change the current hold time, enter the command followed by the desired value (any value between 1 and 65535). For example:

```
gmapholdtime 2880
```

A message similar to the following displays:

```
GMAP Hold Time is 2880 minutes.
```

Displaying GMAP Statistics by MAC Address

To display GMAP statistics for all MAC addresses, use the **gmapls** command. The screen displays similar to the following:

```
GMAP Table
==================
  MAC Address     Protocol    Group   Src Switch ID          Flags          Timeout(sec)
-----------------------  -------------  -----------  ------------------------  -----------------  --------------------
000502:C07F11      1809B        12   0020DA:ECC770  00:00:00:00          3536
                     800        12   0020DA:ECC770  00:00:00:00          3536
00105A:1873B9      1809B        12   0020DA:ECC770  00:00:00:00          3536
                     800        23   0020DA:ECC770  00:00:00:00          3536
```

To limit the display, specify the MAC address. For example:

```
gmapls 00105A:C07F11
```

Fields in this table are defined as follows:

MAC Address. The MAC address of the local end station.

Group. The group(s) to which the MAC address belongs.

Protocol. The protocol associated with the group on the switch from which the information was received. Protocol values are defined as follows:

- e0e0 or ffff — IPX over 802.3
- 8137 — IPX over Ethernet II
- 18137 — IPX over SNAP
- 28137 — any IPX encapsulation
- 800 — IP
- 809b — AppleTalk
- 1809b — AppleTalk over SNAP
- 6003 — DECNET

Src Switch ID. The MAC address of the switch from which the entry was received.

Flags. The first two bytes are not used. The third byte displays the AutoTracker flags associated with the entry on the source switch. The last byte displays the router flags associated with this entry on the source switch.

Timeout (sec). The number of seconds remaining until this entry is deleted (unless another GMAP message is received and then the entry is refreshed).