CHAPTER 3

Learning the Interface Topology and Association

Revised: July 24, 2012, OL-24162-05

Introduction

This chapter describes learning of interface topology and association of the remote cable MSO links solution.

Learning the Interface Topology

To control and report traffic in the context of a remote interface, you must map the topology in terms of the available CMTS interfaces and their associated bandwidth. This map must include keys that the SCE uses to associate subscriber traffic with specific interfaces.

The SCE learns the interface topology by retrieving the CMTS configuration by using the Simple Network Management Protocol (SNMP) and converting the configuration to a virtual links map. Virtual links are provisioned to the relevant SCEs.

VLM queries the CMTS device and learns the upstream and downstream channels, their names, and their rates. VLM supports multiple primary channels for each wideband group. For primary channels within a wideband group, VLM queries the CMTS for resource allocation that is reserved for legacy modems.

For downstream channels, VLM obtains the mapping information of the channels to wideband groups. For the wideband channels, VLM extracts the:

- Wideband to narrowband mapping to detect a primary channel
- Wideband name from the Interface MIB
- Mapping of channels that belong to the wideband group and their rates to calculate the wideband rate

The parameters for the primary and secondary channels include:

- PIR
- CIR

Table 3-1 lists the parameters and their values for primary and secondary channels and the dynamic AGCs.

Table 3-1 Parameter Values

Parameters	Values for Primary Channels	Values for Secondary Channels	Values for Dynamic AGC
PIR	The values are extracted from the interface rate of the primary channel of the wideband.	The values are extracted from the total rate of the wideband channel.	The values are extracted from the total rate of the wideband channel.
CIR	The values are calculated from the CMTS configurations.	CIR = 0	CIR = 0

Learning the Interface Association

Interface association awareness is achieved through DHCP integration. The CMTS IP (specifically, the Relay-Agent IP, or giaddr) is part of the DHCP dialog and upstream and downstream interface IDs are included in the **Relay-Agen**t option (for example, option 82 [encoded in suboption 1, the circuit ID]). This information allows the SCE to uniquely identify upstream and downstream interfaces to which a subscriber is mapped, even in cases in which more than one CMTS is connected to an SCE.

The Cisco Subscriber Manager learns the interfaces automatically from the CMTSs and provisions the Vlinks to the Cisco SCE on the following events:

- Each configured device query interval
- Manual device query
- Re-sync with Cisco SCE
- Applying policy on Cisco SCE
- Cisco Subscriber Manager restart
- Cisco Subscriber Manager load configuration
- Cisco SCE reload

During these events, the Cisco Subscriber Manager creates new Vlinks learnt from the CMTSs, updates the existing Vlinks if the SM observed any changes, and removes the unwanted Vlinks to make sure that the SM has synchronized completely with the CMTS interfaces to reserve the unused Vlinks for the new interfaces. During this process, the Cisco Subscriber Manager removes all Vlinks created directly in an SCE using CLI or any other source without the knowledge of the Cisco Subscriber Manager.

Note If multiple CMTS devices connected to an SCE have the same SNMP SysName, the VLM fails to identify the duplication and this results in unpredictable behavior.

The SCE DHCP sniffer LEG extracts the CMTS IP and reports it to the Subscriber Manager, which performs the appropriate virtual-link association, allowing the SCE to manage the traffic correctly.

Wideband channels are associated with three AGCs in a two-level hierarchy and the cable modems are mapped to their respective AGCs. For information on the AGC mapping, see the "Bandwidth Control Enhancements" section on page 2-4 and the "Mapping of Cable Modems Through DHCP Sniffing" section on page 2-11.

Dynamic giaddr Learning

When the VLM queries the CMTS device, it reads all the IP addresses from the CMTS device IP table and creates the mapping table that is used to map IP addresses to the CMTS device to which they are related. Many of the IP addresses that are read from the CMTS device are not used by subscribers, which can cause the mapping table to become too large and unmanageable. To prevent this, the VLM dynamically selects and releases the giaddr values from the IP table. VLM ignores IP addresses that starts with 127 because these IP addresses are considered as the loop back IP addresses.

When a subscriber logs in, the CMTS device appends the giaddr to the DHCP transaction. For a giaddr that is new to the DHCP LEG (or an existing giaddr that was not used during previous logins):

- If the login giaddr value is known to the VLM (related to one of the CMTS devices), the VLM updates the DHCP LEG with the policy mapping table related to the login giaddr value.

- If the login giaddr value is unknown to VLM (if the IP is not related to any device in the VLM), the VLM opens the SNMP connection using the login giaddr value as an IP address, and queries the SNMP connection to get the device host-name (sysName OID):
  - If a device exists with the same host-name, it indicates that a new IP was added to the device:
- The VLM queries the device to learn the new updates
- The VLM updates the policy mappings based on the query output and updates the LEG
- Login operations continue on the device
  - If the device host-name is invalid, it indicates one of these causes:
- Device is not configured as expected (sysName MIB value is not set).
- Device was not intended to be part of the VLM solution.
- Subscriber is logged in without a virtual link policy mapping.
  - If the device host name is valid, the name is new to the VLM, and the dynamic device feature is enabled:
- VLM creates a new device by using the device host-name.
- Login operations using the same giaddr value are blocked by the LEG.
- VLM starts querying the new device and updates its policy mappings accordingly.
- Login operations continue on the device.

  From Service Control Application for Broadband Release 3.6.5, for a static device configuration, you can disable learning new giaddr during login. After you disable learning new giaddr, if the Subscriber Manager identifies that the relay agent does not belong to any known CMTS, the SM continues to log in instead of doing a query. During periodic queries, the SM continues to learn new giaddrs. To disable learning new giaddr during login, set enable_dynamic_giaddrs_learning to false.
- For giaddr that is known to the DHCP LEG (or an existing giaddr that was in use during the previous logins):
  - If the policy mappings are found, a subscriber is created by using the policy mappings.
  - During a login operation, if the policy mappings are not found:
- All login operations related to the device that belongs to the giaddr are put on hold by the DHCP LEG.
- Based on the giaddr value received from DHCP, the VLM identifies the device associated with the giaddr, and queries the device.
- After the query is completed, the policy mappings are updated in the LEG.

Note When the VLM queries a device, all login operations of the affected device are stored in a queue. After completing the query operations, the login process resumes and there is no loss of login operations. Each subscriber is logged in with their respective mappings.

- VLM defines a lease time for each dynamic giaddr. If no further login operations occur during the lease time period:
  - VLM removes the giaddr from its list of giaddr values.
  - IP value is no longer a giaddr in the CMTS device (when performing **p3vlink --show-device -d** <*device*>, the giaddr attribute does not contain the removed IP).
  - LEG removes the entries from the mapping table that are related to the giaddr.

  - For each subscriber, the VLM checks if the subscriber giaddr custom property is the same as the removed giaddr and if so, changes the property to be the IP address of the CMTS device.

    This example shows the current details of a subscriber:

```
p3subs --show -s lynn_jones
Name:           lynn_jones
Domain:         subscribers
Mappings:
        IP: 1.1.1.13/32
Properties:
        downVlinkId=7    Name=device1_1_Cmts8/1-downstream1
        upVlinkId=4      Name=device1_1_Cmts8/1-upstream1
Custom Properties:
        giaddr=1.1.1.1
Command terminated successfully

If the IP address 1.1.1.1 is the removed giaddr and 2.2.2.2 is the CMTS device IP
address, the result of the lease time operation is as follows:
p3subs --show -s lynn_jones

Name:           lynn_jones
Domain:         subscribers
Mappings:
        IP: 1.1.1.13/32
Properties:
        downVlinkId=7    Name=device1_1_Cmts8/1-downstream1
        upVlinkId=4      Name=device1_1_Cmts8/1-upstream1
Custom Properties:
        giaddr=2.2.2.2
Command terminated successfully
```

- When a CMTS device reboots, the CMTS allocates new ifIndex values for the interfaces, specifically when the downstream ifIndex values are changed and the VLM mappings are no longer synchronized. The VLM monitors the upstream and downstream parameters of option 82 and compares the values against the mapping tables. If a mismatch is found in the DHCP transaction parameters, VLM initiates a synchronization process with the CMTS device. During this process:
  - DHCP transactions of the affected CMTS device are placed on hold. The VLM buffer can store 100,000 DHCP events per CMTS.
  - LEG queues up the subscriber login request.
  - On completion of device query operation, the VLM notifies the LEG.
  - LEG removes the stored messages in the queue and restarts the login operation.
  - DHCP transactions of any newly detected CMTS device are stored in the queue until VLM queries the new CMTS information.

Managing Control and Reporting

SCE virtual links emulate the physical interfaces of the CMTSs and the VLM provisions the links with the bandwidth required to control the traffic:

1. For each CMTS physical interface (either upstream or downstream), the VLM creates a virtual link on the SCE.
2. VLM maps traffic that travels from a subscriber that is associated with this interface to the virtual link.
3. To create the proper association of subscribers to virtual links, the VLM creates a mapping between the DHCP information (CMTS-ID, upstream-ID, downstream-ID) and the virtual link IDs.
   - VLM creates a channel and an upstream virtual link for every upstream-ID on a CMTS.
   - VLM creates a legacy channel or wideband and legacy channels for a downstream virtual link for every downstream-ID on a CMTS.

Subscriber management logic is required to associate subscribers with their upstream and downstream virtual links based on the attributes that the DHCP LEG extracts from the DHCP traffic.

For a downstream virtual link, the Subscriber Manager login determines if the subscriber is associated with legacy or wideband cable modems. Depending on the modem types, subscribers are mapped either to wideband or legacy (primary) channels:

- Subscribers with wideband cable modems are mapped to the wideband channel beneath the VLink.
- Subscribers with legacy modems are mapped to legacy channels beneath the VLink.

In addition to the virtual links association, the subscriber is also assigned a package. In terms of bandwidth management, you can use only schemes that use one virtual-link-controller per direction; therefore, you should design the bandwidth controller architecture (committed information rate, peak information rate, and assurance level) accordingly.

VLM Device Learning—Limitations

These limitations are applicable to the VLM device learning feature:

- The VLM device learning does not support static bandwidth sharing if the wideband channel or bonding group is configured by using the **no cable dynamic-bw-sharing** command.
- The VLM device learning does not support overlapping same set of channels under a MAC domain.
- The VLM device learning does not support channels and bonding groups that overlap across MAC domains.
- The VLM device learning does not learn Dynamic Bonding Group configuration.
- While learning the RF channel width of a wideband, the Cisco Subscriber Manager checks for the entPhysicalName of the card. The Cisco Subscriber Manager expects the entPhysicalName value to be in the format *SPA bay <slot>/<subslot>* or *Cable<slot>/<subslot>-RF<rf-port>,* or includes *3GX60*. Based on the card type, the interface descriptor (ifDescr) is derived. You can change the default format of the ifDescr value in the Vlink configuration file vlink.cfg. For the ifDescr matching, the port information must be in the format *<slot/subslot/port>,* in the same order and as a single string. The channel number can be any where based on the format configured in the vlink.cfg file.
- The VLM device learning may fail if there is an overlap of the IP address learned from ipAddrTable across all configured CMTS. The IP address overlapping between CMTS is usually observed in MPLS VPN based network deployments where virtual routing and forwarding (VRF) is used.
- The VLM device learning feature does not support modular or integrated interfaces that are directly associated to a Mac domain; it only supports interfaces associated through a bonding group.