CHAPTER 26

Monitoring Mobile Technologies

The following topics provide an overview of mobile technologies and describe how to work with mobile technologies in Prime Network Vision:

User Roles Required to Work with Mobile Technologies

This topic identifies the GUI default permission or scope security level that is required to work with the mobile technologies in Prime Network Vision. Prime Network determines whether you are authorized to perform a task as follows:

- For GUI-based tasks (tasks that do not affect elements), authorization is based on the default permission that is assigned to your user account.
- For element-based tasks (tasks that do affect elements), authorization is based on the default permission that is assigned to your account. That is, whether the element is in one of your assigned scopes and whether you meet the minimum security level for that scope.

For more information on user authorization, see the *Cisco Prime Network 3.10 Administrator Guide*.

The following tables identify the tasks that you can perform:

- Table 26-1 identifies the tasks that you can perform if a selected element **is not in** one of your assigned scopes.
- Table 26-2 identifies the tasks that you can perform if a selected element **is in** one of your assigned scopes.

By default, users with the Administrator role have access to all managed elements. To change the Administrator user scope, see the topic on device scopes in the *Cisco Prime Network 3.10 Administrator Guide*.

Table 26-1 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element Not in User's Scope

Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing GGSN properties	—	—	—	—	X
Viewing additional characteristics of a GGSN	—	—	—	—	X
Working with GGSN commands	—	—	—	—	X
Viewing GTPU properties	—	—	—	—	X
Working with GTPU commands	—	—	—	—	X
Viewing APN properties	—	—	—	—	X
Viewing additional characteristics of an APN	—	—	—	—	X
Working with APN commands	—	—	—	—	X
Viewing SAE-GW properties	—	—	—	—	X
Viewing P-GW properties	—	—	—	—	X
Working with P-GW commands	—	—	—	—	X
Viewing S-GW properties	—	—	—	—	X
Working with S-GW commands	—	—	—	—	X
Viewing GTPP properties	—	—	—	—	X
Viewing additional characteristics of a GTPP	—	—	—	—	X
Working with GTPP commands	—	—	—	—	X
Viewing EGTP properties	—	—	—	—	X
Working with EGTP commands	—	—	—	—	X
Viewing operator policies	—	—	—	—	X
Viewing APN remaps	—	—	—	—	X
Viewing APN profiles	—	—	—	—	X
Viewing additional characteristics of an APN profiles	—	—	—	—	X
Viewing active charging services (ACS)	—	—	—	—	X
Working with ACS commands	—	—	—	—	X
Viewing QCI-QoS mapping	—	—	—	—	X

Table 26-2 Default Permission/Security Level Required for Viewing GGSN, GTPU, and APN Properties - Element in User's Scope

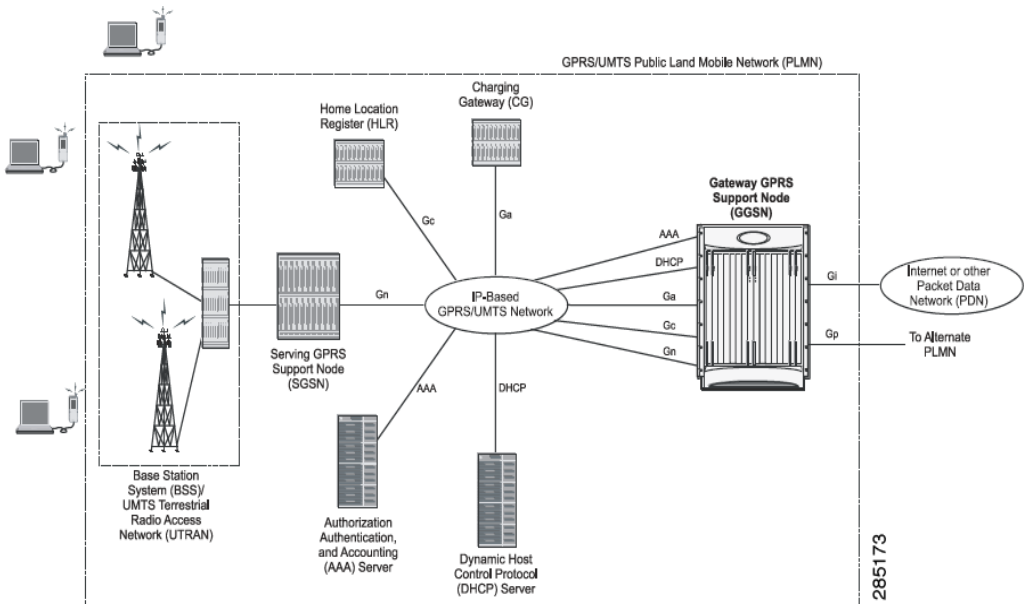
Task	Viewer	Operator	OperatorPlus	Configurator	Administrator
Viewing GGSN properties	X	X	X	X	X
Viewing additional characteristics of a GGSN	X	X	X	X	X
Working with GGSN commands	—	—	—	X	X
Viewing GTPU properties	X	X	X	X	X
Working with GTPU commands	—	—	—	X	X
Viewing APN properties	X	X	X	X	X
Viewing additional characteristics of an APN	X	X	X	X	X
Working with APN commands	—	—	—	X	X
Viewing SAE-GW properties	X	X	X	X	X
Viewing P-GW properties	X	X	X	X	X
Working with P-GW commands	—	—	—	X	X
Viewing S-GW properties	X	X	X	X	X
Working with S-GW commands	—	—	—	X	X
Viewing GTPP properties	X	X	X	X	X
Viewing additional characteristics of a GTPP	X	X	X	X	X
Working with GTPP commands	—	—	—	X	X
Viewing EGTP properties	X	X	X	X	X
Working with EGTP commands	—	—	—	X	X
Viewing operator policies	X	X	X	X	X
Viewing APN remaps	X	X	X	X	X
Viewing APN profiles	X	X	X	X	X
Viewing additional characteristics of an APN profiles	X	X	X	X	X
Viewing active charging services (ACS)	X	X	X	X	X
Working with ACS commands	—	—	—	X	X
Viewing QCI-QoS mapping	X	X	X	X	X

GPRS/UMTS Networks - An Overview

General Packet Radio Service (GPRS) and Universal Mobile Telecommunication System (UMTS) are evolutions of Global System for Mobile Communication (GSM) networks.

GPRS is a 2.5G mobile communications technology that enables mobile wireless service providers to offer their mobile subscribers packet-based data services over GSM networks. UMTS is a 3G mobile communications technology that provides wideband code division multiple access (CDMA) radio technology. Figure 26-1 shows a basic GPRS/UMTS network topology.

Figure 26-1 Basic GPRS/UMTS Network Topology



The GPRS/UMTS packet core comprises two major network elements:

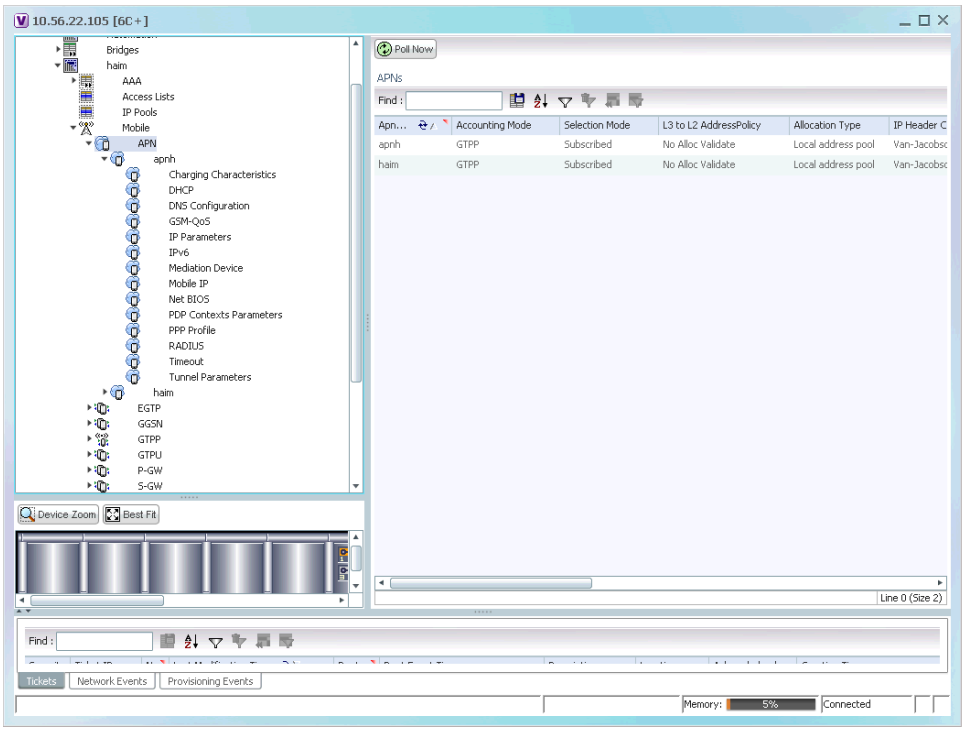
- Gateway GPRS support node (GGSN)—A gateway that provides mobile cell phone users access to a Packet Data Network (PDN) or specified private Internet Protocol (IP) networks.
- Serving GPRS support node (SGSN)—Connects the radio access network (RAN) to the GPRS/UMTS core and tunnels user sessions to the GGSN. The SGSN sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates directly with the MS and the GGSN.

PDNs are associated with Access Point Names (APNs) configured on the system. Each APN consists of a set of parameters that dictate how subscriber authentication and IP address assignment is to be handled for that APN.

Prime Network Vision allows you to configure the mobile technologies by using commands and also view the properties configured for the mobile technologies. Figure 26-2 shows an example of the Inventory window with the mobile technology nodes/containers under the Mobile context.

From Prime Network 3.9, the mobile technologies are supported on Cisco Aggregation Service Router (ASR) 5000 series mobile gateways.

Figure 26-2 Mobile Technology Nodes in Logical Inventory



Working With GPRS/UMTS Network Technologies

The following topics explain how to work with GPRS/UMTS network technologies in Prime Network Vision:

- Working with GGSN, page 26-5
- Working with GTPU, page 26-10
- Working with APN, page 26-12
- Working with GTPP, page 26-24
- Working with EGTP, page 26-31

Working with GGSN

The GGSN works in conjunction with SGSNs within the network to perform the following functions:

- Establish and maintain subscriber Internet Protocol (IP) or Point-to-Point Protocol (PPP) type Packet Data Protocol (PDP) contexts originated by either the mobile or the network.
- Provide charging detail records (CDRs) to the charging gateway ((CG), also known as the Charging Gateway Function (CGF)).
- Route data traffic between the subscriber's Mobile Station (MS) and a PDN such as the Internet or an intranet.

In addition, to providing basic GGSN functionality as described above, the system can be configured to support Mobile IP and/or Proxy Mobile IP data applications in order to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to function as a GGSN and Foreign Agent (FA), a stand-alone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

The following topics explain how to work with GGSN in Prime Network Vision:

Viewing GGSN Properties

Prime Network Vision displays the GGSNs in a GGSN container under the Mobile node in the logical inventory. The icon used for representing GGSNs in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view GGSN properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile >** *GGSN Container*.

Prime Network Vision displays the list of GGSNs configured under the container. You can view the individual GGSN details from the table on the right pane or by choosing **Logical Inventory >** *Context* **> Mobile >** *GGSN Container* **>** *GGSN*.

Table 26-3 describes the details available for each GGSN.

Table 26-3 GGSN Properties in Logical Inventory

Field	Description
Service Name	The name of the GGSN service.
Status	The status of the GGSN service. Value could be Unknown, Running, or Down.
PLMN Policy	The PLMN policy for handling communications from SGSNs that are not configured to communicate with.
Newcall Policy	Specifies whether to accept or reject a new incoming call.
Authentication Server Timeout	The code used by the GGSN as a response message if communication with an authentication server times out. Value could be System Failure or User Authentication Failed.
Accounting Server Timeout	The code used by the GGSN as a response message if communication with an accounting server times out. Value could be System Failure or No Resouces.
GTPU	The GTPU that is associated with the GGSN and manages the GTP messages between GGSN and a radio access network equipment (RNC).
Accounting Context	The context that processes accounting for PDP contexts handled by the GGSN service.
Local IP Address	The local IP address bounded with the GGSN service.

If the GGSN is associated with SGSNs and Public Land Mobile Networks (PLMNs), you can view the details from the respective tabs for that GGSN.

Table 26-4 describes the SGSN and PLMN information associated with the GGSN.

Table 26-4 SGSN and PLMN information for a GGSN

Field	Description
SGSNs	
IP Address	The IP address of the SGSN.
Subnet Mask	The subnet mask of the SGSN.
PLMN ID	The PLMN ID associated with the SGSN.
MCC	The mobile country code (MCC) portion of the PLMN.
MNC	The mobile network code (MNC) portion of the PLMN.
PLMN Foreign	Indicates whether the SGSN belongs to a home or foreign PLMN. This field is available only if MCC and MNC are not available.
Reject Foreign Subscriber	Specifies whether to accept or reject foreign subscriber. Value could be True or False.
RAT Type	The type of radio access technology (RAT) that is used for communication.
Description	The description of the SGSN entry in the GGSN service.
PLMNs	
PLMN ID	The ID of the PLMN associated with the GGSN.
Primary	Indicates whether the PLMN ID is the primary PLMN ID for the GGSN. Value could be True or False. When multiple PLMN IDs are configured, the one configured as primary is used for the Authentication, Authorization, and Accounting (AAA) attribute.

Viewing Additional Characteristics of a GGSN

To view additional characteristics of a GGSN:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > Mobile >** *GGSN Container* **>***GGSN*.

Step 3 Expand the *GGSN* node. The following list of characteristics configured for the GGSN are displayed:

- Charging Characteristics
- Timers And QoS

Step 4 Choose **Charging Characteristics** to view the properties on the right pane. See Table 26-5 for more details on the charging characteristics configured for the GGSN.

Table 26-5 GGSN Charging Characteristics

Field	Description
Profiles	
Profile No	Type of billing. For example: • 1—Hot billing • 2—Flat billing • 4—Prepaid billing • 8—Normal billing All other profiles from 0 - 15 are customized billing types.
Buckets	Denotes container changes in the GGSN Call Detail Record (GCDR).
Prepaid	Prepaid type, which could be Prohibited or Use-rulebase-configuration.
Down Link Octets	Downlink traffic volume of the bucket.
Uplink Octets	Uplink traffic volume of the bucket.
Total Octets	Total traffic volume of the bucket.
Tariff Time Triggers	
Profile No	Type of billing.
Time1, Time2, and so on	First time-of-day time values, and so on, to close the current statistics container.
Intervals	
Profile No	Type of billing.
No. of SGSNs	Number of SGSN changes (inter-SGSN switchovers) resulting in a new Routing Area Identity (RAI) that can occur before closing an accounting record.
Interval	Normal time duration that must elapse before closing an accounting record.
Down Link Octets	Downlink traffic volume reached within the time interval.
Up Link Octets	Uplink traffic volume reached within the time interval.
Total Octets	Total traffic volume reached within the time interval.

Step 5 Under the *GGSN* node, choose **Timers and QoS** to view the properties on the right pane. See Table 26-6 for more details on the Timers and QoS parameters configured for the GGSN.

Table 26-6 GGSN Timers and QoS

Field	Description
Retransmission Timeout	Timeout, in seconds, for retransmission of GTP control packets.
Max Retransmissions	Maximum retries for transmitting GTP control packets.
Setup Timeout	Maximum time, in seconds, allowed for session setup.
Echo Interval	Echo interval, in seconds, for GTP.
Guard Interval	Interval, in seconds, for which the GGSN maintains responses sent to SGSN. This optimizes the handling of retransmitted messages.
QCI to DSCP Mapping	
QoS class index	A set of transport characteristics used to differentiate various packet flows.
DSCP	Differentiated Services Code Point (DSCP), a mechanism for classifying and managing network traffic and providing QoS.
QCI & ARP DSCP Mapping	
QoS class index	A set of transport characteristics used to differentiate various packet flows.
Allocation retention priority	The priority of allocation and retention of the service data flow. This parameter allows prioritizing allocation of resources during bearer establishment and modification. During network traffic congestions, a lower ARP flow is dropped to free up the capacity.
DSCP	A mechanism for classifying and managing network traffic and providing QoS.

GGSN Commands

The following commands can be launched from the inventory by right-clicking a GGSN and choosing *GGSN* **> Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-7 GGSN Commands

Command	Inputs Required and Notes
Create PLMN Identifier	• MCC Number • MNC Number • PLMN Type: Primary or None
Create SGSN	IP Address (IPv4/IPv 6), Mask, Description, MCC Number, MNC Number, Reject Foreign Subscriber, Disable GTPC Echo, PLMN Foreign, and RAT Type.
Delete GGSN	Click **Execute Now** to delete the GGSN.
Modify GGSN	General tab: • Delete Accounting Context Name, Accounting Context Name, Delete CC Behavior ID, CC Behavior ID, Delete GTPU, Service Name, GTPU Service Name, Delete P-GW Service Name, P-GW Service Name, Port Number, PLMN Unlisted Value
	Bind Address tab: • Delete Bind Address, Bind Address (IPv4), Max PPP PDP Context, Max Total PDP Context
	Timing Interval tab: • Retransmission Timeout, Echo Retransmission Timeout, Setup Timeout, Delete Echo Interval, Echo Interval, Dynamic, Smooth Factor, Delete Guard Interval, Guard Interval, Max Retransmission

Working with GTPU

The GGSN communicates with SGSNs on a Public Land Mobile Network (PLMN) using the GPRS Tunneling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU). GTPU is used for transferring user data in separated tunnels for each PDP context.

You can configure various parameters for a GTPU using the configuration commands in Prime Network Vision. You can view the configured parameters for a GTPU in the logical inventory.

The following topics explain how to work with GTPU in Prime Network Vision:

- Viewing GTPU Properties, page 26-10
- GTPU Commands, page 26-11

Viewing GTPU Properties

Prime Network Vision displays the GTPUs in a GTPU container under the Mobile node in the logical inventory. The icon used for representing GTPUs in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view GTPU properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile >** *GTPU Container*.

Prime Network Vision displays the list of GTPUs configured under the container. You can view the individual GTPU details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile >** *GTPU Container* **>** *GTPU*.

Table 26-8 describes the details available for each GTPU.

Table 26-8 GTPU Properties in Logical Inventory

Field	Description
Service Name	The name of the GTPU service.
State	The status of the GTPU service. Status could be Unknown, Running, or Down.
Max Retransmissions	The maximum limit for GTPU echo retransmissions. Default value is 4.
Retransmission Timeout	The timeout in seconds for GTPU echo retransmissions. Default value is 5 Secs.
Echo Interval	The rate at which the GTPU echo packets are sent.
IPSEC Tunnel Idle Timeout	The IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered. Default value is 60 Secs.
Allow Error Indication	Specifies whether error indication is dropped or sent without IPSec tunnel. Default value is Disabled.
Include UDP Port Ext Hdr	Specifies whether to include an extension header in the GTPU packet for error indication messages. Default value is False.
IP Address	The list of IP addresses configured on the GTPU. The IP addresses are available only when configured for the GTPU.

GTPU Commands

The following commands can be launched from the inventory by right-clicking a GTPU and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-9 GTPU Commands

Command	Inputs Required and Notes
Create GTPU Bind IP Address	Bind IP Address Type, Bind Address (IPv4/IPv6)
Modify GTPU Bind IP Address (Right-click on an IP address in the content pane and choose **Commands > Configuration > Modify GTPU Bind IP Address**	Bind Address Type, Delete Bind Address, Bind Address (IPv4/IPv6)
Delete GTPU Bind IP Address (Right-click on an IP address in the content pane and choose **Commands > Configuration > Delete GTPU Bind IP Address**	Click **Execute Now** to delete the bind IP address.
Delete GTPU	Click **Execute Now** to delete the GTPU.
Modify GTPU	Retransmission Timeout, Echo Retransmission Timeout, Maximum Retransmission, Delete Echo Interval, Echo Interval

Working with APN

APN is the access point name that is configured in the GGSN configurations. The GGSN's APN support offers the following benefits:

- Extensive parameter configuration flexibility for the APN.
- Extensive QoS support.
- Virtual APNs to allow differentiated services within a single APN. The APN that is supplied by the mobile station is evaluated by the GGSN in conjunction with multiple configurable parameters. Then the GGSN selects an APN configuration based on the supplied APN and those configurable parameters.
- Traffic policing that governs the subscriber traffic flow if it violates or exceeds configured peak or committed data rates. The traffic policing attributes represent a QoS data rate limit configuration for both uplink and downlink directions.

Up to 1024 APNs can be configured in the GGSN. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6.

Many parameters can be configured independently for each APN on the device. They are categorized as given below:

- Accounting—Various parameters regarding accounting possibilities, such as, charging characteristics, accounting mode (RADIUS server-based accounting, GTPP-based accounting, and so on.)
- Authentication—Various parameters regarding authentication, such as, protocols used, like, Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none, default username/password, server group to use, and limit for number of PDP contexts.
- Enhanced Charging—Name of rulebase to use, which holds the enhanced charging configuration (for example, eG-CDR variations, charging rules, prepaid/postpaid options, etc.).

- IP: Method for IP address allocation (e.g., local allocation by GGSN, Mobile IP, Dynamic Host Control Protocol (DHCP), DHCP relay, etc.). IP address ranges, with or without overlapping ranges across APNs.
- Tunneling: PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the GGSN independently from the APN.
- QoS: IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

You can configure the APN parameters using Prime Network Vision. You can view the configured parameters for an APN in the logical inventory. After an APN is determined by the GGSN, the subscriber may be authenticated/authorized with an AAA server. The GGSN allows the AAA server to return Vendor Specific Attributes (VSAs) that override any or all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the GGSN during subscriber authentication/authorization.

The following topics explain how to work with APN in Prime Network Vision:

- Viewing APN Properties, page 26-13
- Viewing Additional Characteristics of an APN, page 26-18
- APN Commands, page 26-23

Viewing APN Properties

Prime Network Vision displays the APNs in an APN container under the Mobile node in the logical inventory. You can also view additional characteristics configured on the APN as explained in Viewing Additional Characteristics of an APN, page 26-18. The icon used for representing APNs in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view APN properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >***Context* **> Mobile >** *APN Container* **>***APN*.

Table 26-10 describes the information that is available for the APN. The information that is displayed depends on the configuration of the APN.

Table 26-10 APN Properties in Logical Inventory

Field	Description
APN Name	The APN name.
Accounting Mode	The accounting protocol in use in the APN. Values are GTPP (GPRS Tunneling Protocol Prime), RADIUS (Remote Authentication Dial In User Service), or None.
Selection Mode	The selection mode in use in the APN. Selection mode indicates the origin of the requested APN and whether or not the Home Location Register (HLR) has verified the user subscription.
L3 to L2 Address Policy	The layer 2 to layer 3 IP address allocation or validation policy.

Table 26-10 APN Properties in Logical Inventory (continued)

Field	Description
Allocation Type	The method by which the APN obtains IP addresses for PDP contexts.
IP Header Compression	IP packet header compression parameters for the APN.
New Call Policy	Specifies whether to accept or reject a new incoming call in case of duplicate session calls with a request for same IP address.

Step 3 To view additional details configured for the APN, use the following tabs:

- Virtual APNs—A virtual APN is a non-physical entity that represents an access point that does not itself provide direct access to a real target network. A virtual APN can be used to consolidate access to multiple, physical target networks through a single access point.
- QCI to DSCP Mapping—Shows the mapping between QoS Class Indices (QCI) to Differentiated Services Code Point (DSCP).
- QCI & ARP DSCP Mapping—Shows the mapping between QCI and Allocation/Retention Priority (ARP) to DSCP.
- QoS Downlink Traffic Policing—Shows the attributes that represent QoS data rate limit configuration for downlink direction within the APN profile.
- QoS Uplink Traffic Policing—Shows the attributes that represent QoS data rate limit configuration for uplink direction within the APN profile.

Field	Description
Virtual APNs	
Preference	Specifies the order in which the referenced APNs are compared by the system. Can be configured to any integer value from 1 (highest priority) to 1000 (lowest priority).
APN	Specifies the name of an alternative APN configured on the system that is to be used for PDP contexts with matching properties. Value can be from 1 to 62, alpha and/or numeric characters, and is not case-sensitive. It may also contain dots (.) and/or dashes (-).

Field	Description
Rule Definition	The virtual APN rule definition can be one of the following: • access-gw-address—Specifies the access gateway (SGSN/SGW/Others) address for the virtual APN. The IP address can be an IPv4 or IPv6 address in decimal notation. IPv6 also supports :: notation for the IP address. • bearer-access-service—Specifies the bearer access service name for the virtual APN. • service name—Specifies the service name. Service name is unique across all the contexts. Value is a string of size 1 to 63. • cc-profile—Specifies the APN for charging characteristics (CC) profile index. Value is an integer from 1 to 15. • Domain name—Specifies the subscriber's domain name (realm). Domain name can be from 1 to 79 alpha and/or numeric characters. • MCC—Specifies the MCC portion of the PLMN identifier. Value is an integer between 100 to 999. • MNC—Specifies the MNC portion of the PLMN identifier. Value is an integer between 100 to 999. • msisdn-range—Specifies the APN for this MSISDN range. The starting and ending values of the range is a string of size 2 to 15 with values between 00 and 999999999999999. • Rat-Type—Specifies the rat-type option, which could be gan, geran, hspa, utran, or wlan. • Roaming mode—Specifies the roaming mode, which could be Home, Visiting, or Roaming.

Field	Description
QCI to DSCP Mapping	
QoS class index	Denotes a set of transport characteristics used to differentiate various packet flows.
DSCP	Denotes a mechanism for classifying and managing network traffic and providing QoS.
QCI & ARP DSCP Mapping	
QoS class index	Denotes a set of transport characteristics used to differentiate various packet flows.
Allocation retention priority	Indicates the priority of allocation and retention of the service data flow. This parameter allows prioritizing allocation of resources during bearer establishment and modification. During network traffic congestions, a lower ARP flow is dropped to free up the capacity.
DSCP	Denotes a mechanism for classifying and managing network traffic and providing QoS.
QoS Downlink Traffic Policing	
QCI	A scalar that denotes a set of transport characteristics and used to infer nodes specific parameters that control packet forwarding treatment.
Peak Data Rate	The peak data rate allowed, in bytes, for the downlink direction and QoS traffic class.
Committed Data Rate	The committed data rate allowed, in bytes, for the downlink direction and QoS traffic class.
Negotiate Limit	Indicates whether negotiation limit is enabled or disabled for the downlink direction and Qos traffic class.
Rate Limit	Indicates whether the rate limit is enabled or disabled for the downlink direction and Qos traffic class.
Burst Size Auto Readjust	Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time of PDP activation of modification.
Burst Size Auto Readjust Duration	The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates.
Peak Burst Size (bytes)	The peak burst size allowed, in bytes, for the downlink direction and QoS class.
Guaranteed Burst Size (bytes)	The guaranteed burst size allowed, in bytes, for the downlink direction and QoS class.
Exceed Action	The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following: • Drop • Lower IP Precedence • Transmit

Field	Description
Violate Action	The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following: • Drop • Lower IP Precedence • Shape • Transmit
QoS Uplink Traffic Policing	
QCI	A scalar that denotes a set of transport characteristics and used to infer nodes specific parameters that control packet forwarding treatment.
Peak Data Rate	The peak data rate allowed, in bytes, for the uplink direction and QoS traffic class.
Committed Data Rate	The committed data rate allowed, in bytes, for the uplink direction and QoS traffic class.
Negotiate Limit	Indicates whether negotiation limit is enabled or disabled for the uplink direction and Qos traffic class.
Rate Limit	Indicates whether the rate limit is enabled or disabled for the uplink direction and Qos traffic class.
Burst Size Auto Readjust	Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time PDP.
Burst Size Auto Readjust Duration	The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates.
Peak Burst Size (bytes)	The peak burst size allowed, in bytes, for the uplink direction and QoS class.
Guaranteed Burst Size (bytes)	The guaranteed burst size allowed, in bytes, for the uplink direction and QoS class.
Exceed Action	The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following: • Drop • Lower IP Precedence • Transmit
Violate Action	The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following: • Drop • Lower IP Precedence • Shape • Transmit

Viewing Additional Characteristics of an APN

To view additional characteristics of an APN:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile >** *APN Container* **>***APN*.

Step 3 Expand the *APN* node. The following list of characteristics configured for the APN are displayed:

- Charging Characteristics—Charging characteristics configured on the APN for different subscribers.
- DHCP—Dynamic Host Control Protocol (DHCP) parameter configured, if the APN supports dynamic address assignment for PDP contexts.
- GSM-QoS—Represents the negotiated QoS attribute reliability class based on the configuration provided for service data unit (SDU) error ratio and residual bit error rate (BER) attributes in the APN.
- IP Parameters—Represents the APN parameters related to IP.
- IPv6—Represents IPv6 configurations and related services for the APN.
- Mediation Device—Represents the mediation device used by the APN for communication with the subscriber.
- Mobile IP—Represents mobile IP configuration of the APN.
- Net BIOS—Represents the NetBIOS server configuration used by the APN.
- PDP Contexts Parameters—Represents the PDP contexts supported by the APN.
- PPP Profile—Represents the PPP profile used by the APN.
- RADIUS—Represents the APN parameters related to communication with the RADIUS server.
- Timeout—Represents the timeout parameters of the APN.
- Tunnel Parameters—Represents the parameters configured for tunneling between the GGSN and an external gateway for the APN.
- DNS Configuration—Represents the Domain Name System (DNS) settings configured on the APN.

Step 4 Click each of one of these characteristics to view its properties on the right pane. See Table 26-11 for more details on the properties of each characteristics configured for the APN.

Table 26-11 APN Characteristics

Field	Description
Charging Characteristics	
Home Bit Behavior	The behavior bit for charging a home subscriber.
Home Profile	The profile index for a home subscriber.
Roaming Bit Behavior	The behavior bit for charging a roaming subscriber.
Roaming Profile	The profile index for a roaming subscriber.
Visiting Bit Behavior	The behavior bit for charging a visiting subscriber.
Visiting Profile	The profile index for a visiting subscriber.
All Bit Behavior	The behavior bit for charging all subscribers. This value is used only if all subscribers are configured to use the same charging characteristics. This value is overridden by the behavior bit set for a subscriber type.
All Profile	The profile index for all subscribers.
Use GGSN	The type of the subscriber using the charging characteristics configured on the APN. Value could be Home, Roaming, Visitor, or None. None indicates that the subscriber is using the charging characteristics from the SGSN.
Use RADIUS Returned	Specifies whether the GGSN accepts charging characteristics returned from the RADIUS server for all subscribers for the APN. Value could be True or False.
DHCP	
Lease Expiration Policy	The action taken when leases for IP addresses assigned to PDP contexts that are facilitated by the APN, are about to expire. For example, auto renew.
GSM-QoS	
SDU Error Ratio Code	The SDU error ratio code based on which the negotiation of QoS attribute reliability class needs to be configured on the APN. Value is an integer between the range 1 and 7. Each code has an assigned value.
Residual BER Code	The residual bit error rate (BER) based on which the negotiation of QoS attribute reliability class needs to be configured on the APN. This value is specified if the SDU error ratio code is 1, 2, 3, or 7. Residual BER code is an integer in the range 1 and 9. Each code has an assigned value.
IP Parameters	
In Access Group	The name of the IPv4/IPv6 access group for the APN when configured for inbound traffic.
Out Access Group	The name of the IPv4/IPv6 access group for the APN when configured for outbound traffic.
Local Address	The static local IP address assigned to the APN.
Next Hop Gateway Address	The IP address of the next hop gateway for the APN. This parameter is available only if it is configured on the APN.

Table 26-11 APN Characteristics (continued)

Field	Description
Is Discard Enabled	Specifies whether multicast discard is enabled or disabled. Value could be True or False.
IPv6	
Inbound Access Group Name	The name of the IPv6 access group for the APN when configured for inbound traffic.
Outbound Access Group Name	The name of the IPv6 access group for the APN when configured for outbound traffic.
Router Advertisement Interval	The time interval (in milliseconds) the initial IPv6 router advertisement is sent to the mobile node. Value is an integer in the range 100 and 16,000. Smaller the advertisement interval greater is the chance of the router being discovered quickly.
Router Advertisement Number	The number of initial IPv6 router advertisements sent to the mobile node. Value is an integer in the range of 1 and 16.
Prefix Pool Name	The name of the IPv6 address prefix pool configured for the subscriber. You can configure upto a maximum of four pools per subscriber.
Egress Address Filtering	Specifies whether filtering of packets not meant for the mobile interface, is enabled or disabled.
Mediation Device	
Mediation Accounting Enabled	Indicates whether mediation accounting is enabled or disabled.
No Early PDUs	Indicates whether protocol data units (PDUs) must be delayed or not until a response to the GGSN's accounting start request is received from the mediation device. If No Early PDUs is ‘true’, the chassis does not send any uplink or downlink data from or to a MS, until it receives a command from the mediation device.
No Interims	Indicates whether radius interim updates are sent to the mediation device or not for the APN for radius accounting.
Delay GTP Response	Indicates whether the GTP response must be delayed or not. If this value is ‘true’, the GTP response is delayed and is sent to the SGSN only if the AAA server is up. If the value is ‘false’, the subscriber will be connected to the SGSN even if the AAA server is down.
Mobile IP	
Home Agent	The IP address of the home agent (HA) used by the current APN to facilitate subscriber mobile IP sessions.
Mobile Node Home Agent SPI	The mobile node Security Parameter Index (SPI) configured for the APN. Value is an integer between 256 and 4294967295.
Mobile Node Home Agent Hash Algorithm	The encryption algorithm used (if any) by the APN for security.
Mobile Node AAA Removal Indication	Specifies whether the system is configured to remove various information elements when relaying registration request (RRQ) messages to HA. Value could be Enabled or Disabled.
Net BIOS	
Primary NBNS Address	Primary service address of the NetBIOS server.

Table 26-11 APN Characteristics (continued)

Field	Description
Secondary NBNS Address	Secondary service address of the NetBIOS server.
PDP Contexts Parameters	
Total Contexts	The total number of primary and secondary PDP contexts that can be supported by the APN. Value is an integer between 1 and 4,000,000.
PDP Type	The type of the PDP contexts supported by the APN.
Primary Contexts	The status of the primary contexts of the APN.
PPP Profile	
Data Compression Protocols	The compression protocol used by the APN for compression of data packets.
Keep Alive	The frequency (in seconds) of sending the Link Control Protocol (LCP) keep alive messages. A value zero denotes that the keep alive messages are disabled completely.
Data Compression Mode	The compression mode used by the compression protocol which could be: • Normal—Packets are compressed using the packet history. • Stateless—Each packet is compressed individually.
MTU (bytes)	The maximum transmission unit (MTU) for packets accessing the APN.
Min. Compression Size (bytes)	The smallest packet to which compression may be applied.
RADIUS	
RADIUS Group	The Authentication, Authorization, and Accounting (AAA) group name for the subscriber. If no group is set, the value is displayed as Default.
RADIUS Secondary Group	The secondary AAA group for the APN. If no group is set, the value is displayed as None.
Returned Framed IP Address Policy	The policy which indicates whether to accept or reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and when the MS does not supply an IP address.
Timeout	
Absolute	Absolute timeout of a session, in seconds, for the APN.
Idle	Maximum duration, in seconds, after which the system considers the session as dormant or idle and invokes the long duration timer action.
Long Duration	Maximum duration, in seconds, before the system automatically reports or terminates the session. This is the maximum duration before the specified timeout action is activated for the session.
Long Duration Inactivity	Maximum duration, in seconds, before the session is marked as dormant.
Emergency Inactivity	Timeout duration, in seconds, to check inactivity on the emergency session.
Idle Activity Downlink State	Indicates whether the system must ignore the downlink traffic to consider as activity for idle-timeout. Only uplink packets will be able to reset the idle-timeout.

Table 26-11 APN Characteristics (continued)

Field	Description
MBMS Bearer Absolute	Maximum time a Multimedia Broadcast and Multicast Server (MBMS) bearer can exist in active or idle state.
MBMS Bearer Idle	Maximum time an MBMS bearer context can be idle.
MBMS UE Absolute	Session timeout value for the MBMS user equipment.
IPv6 Init Solicit Wait	IPv6 initial router solicit wait timeout.
Long Duration Action Type	The action taken on long duration sessions. For example, the system performs any of the following actions: • Detects a long duration session and sends an SNMP trap and CORBA notification. • Disconnects the session after sending an SNMP trap and CORBA notification. • Suppresses the SNMP trap and CORBA notification after detecting and disconnecting long duration session.
Tunnel Parameters	
Address Policy	The address allocation / validation policy for all tunneled calls except Layer 2 Tunneling Protocol (L2TP) calls.
Peer Load Balancing	The algorithm that defines how the tunnel peers are selected by the APN when multiple peers are configured in the APN.
DNS Configuration	
Primary DNS Address	The primary DNS server for the APN.
Secondary DNS Address	The secondary DNS server for the APN.

APN Commands

The following commands can be launched from the inventory by right-clicking an APN and choosing **Commands > Configuration**. Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-12 APN Commands

Command	Inputs Required and Notes
Create QoS to DSCP Mapping	QCI Attribute, DSCP Value
Create Virtual APN	Virtual APN Reference, Virtual APN Name, Virtual APN Optional Parameters, Access Gateway Address (IPV4/IPV6), Bearer Access Service Name, CC Profile Index, Domain Name, MCC Number, MNC Number, MSISDN Start Range, MSISDN End Range, RAT Type, Roaming Mode
Delete APN	Click **Execute Now** to delete the APN.

Table 26-12 APN Commands (continued)

Command	Inputs Required and Notes
Modify APN	General tab: Selection Mode, Accounting Mode, Authentication Type, Authentication Protocol Priority, Bearer Control Mode, Delete Home Agent IP Address, Home Agent IP Address (IPV4)
	PDP Context tab: Primary Contexts, Total Contexts, PDP Type, Delete Destination Context Name, Destination Context Name
	Charging Characteristics tab: Delete CC SGSN Type, CC SGSN Type, Home Behavior, Home Profile Bit, Roaming Behavior, Roaming Profile Bit, Visiting Behavior, Visiting Profile Bit
	Timeout tab: Delete Timeout Type, Timeout Type, Absolute Duration, Emergency Inactivity Duration, Idle Duration, Long Duration, Long Duration Inactivity Time, Long Duration Action Type, Long Duration Disconnection Type
	IP tab: IP Address Allocation Method, DHCP Proxy: Allow Deferred, DHCP Proxy: Allow User Specified, DHCP Proxy: Prefer DHCP Options, DHCP Relay: Allow User Specified, Local: Allow Deferred, Local: Allow User Specified, No Dynamic: Allow Deferred, No Dynamic: Allow User Specified, Delete IP Pool Name, IP Pool Name
	IPV6 tab: Delete IPV6 Pool Name, IPV6 Pool Name, Delete IPV6 DNS Type, IPV6 DNS Type, IPV6 DNS Address (IPV6), IPV6 Advertisement Interval, IPV6 Number of Advertisements
	AAA/DNS tab: Delete AAA Type, AAA Type, AAA Group Name, AAA Secondary Group Name, Delete DNS Type, DNS Type, DNS IP Address(IPV4)
	GTPP Group tab: Delete GTPP Group, GTPP Group Name, Accounting Context Name
	Miscellaneous tab: Source Violation Type, Drop Limit, Delete Restriction Value, Restriction Value

Working with GTPP

GPRS Tunneling Protocol Prime (GTPP) is used for communicating accounting messages to CGs. Enhanced Charging Service (ECS) supports different accounting and charging interfaces for prepaid and postpaid charging and record generation. GTPP accounting in ECS allows the collection of counters for different types of data traffic including the data in a GGSN CDR (G-CDR) that is sent to the CGF.

GTPP performs the following functions:

- Transfers CDRs between the Charging Data Function (CDF) and CGF.
- Redirects CDRs to another CGF.
- Advertises to peers about its CDR transfer capability; for example, after a period of service down time.
- Prevents duplicate CDRs that might arise during redundancy operations. The CDR duplication prevention function is carried out by marking potentially duplicated CDR packets, and delegating the final duplicate deletion task to a CGF or the billing domain, instead of handling the possible duplicates solely by GTPP messaging.

Prime Network provides support on gathering the GTPP accounting setup details that are configured in the mobile gateway for transferring the different types of CDRs from charging agent to a GTPP server or accounting server.

GTPP is configured within the accounting context of an APN and is also used by GGSN, P-GW, and S-GW to transmit CDRs to CGF.

The following topics provide details on how to work with GTPP in Prime Network Vision:

- Viewing GTPP Properties, page 26-25
- Viewing Additional Characteristics of a GTPP, page 26-26
- GTPP Commands, page 26-30

Viewing GTPP Properties

Prime Network Vision displays the GTPPs in a GTPP container under the Mobile node in the logical inventory. The icon used for representing GTPPs in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view GTPP properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile >** *GTPP Container*.

Prime Network Vision displays the list of GTPP groups configured under the container. You can view the individual GTPP group details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile >** *GTPP Container* **>** *GTPP Group*.

Table 26-13 describes the details available for each GTPP group.

Table 26-13 GTPP Properties in Logical Inventory

Field	Description
Group Name	Name of the GTPP group.
CDR Storage Mode	Storage mode for CDRs, which could be Local or Remote.
CDR Timeout	Maximum amount of time the system waits for a response from the CGF before assuming the packet is lost.
CDR Max Retries	Number of times the system attempts to a CGF that is not responding.
Max CDR Size (bytes)	Maximum payload size of the GTPP packet.
Max CDR Wait Time	Maximum payload size of the GTPP packet. The payload includes the CDR and the GTPP header.
Max CDRs in Message	Maximum number of CDRs allowed in a single packet.
Recover Files Sequence Number	Indicates whether recovery of file sequence number is enabled or not. If enabled, everytime the machine is rebooted, the file sequence number continues from the last sequence number.
Data Request Start Sequence Number	The starting sequence number to be used in the GTPP data record transfer (DRT) record.
Start File Sequence Number	Starting value of the file sequence number.
Source Port Validation	Indicates whether port checking is enabled or disabled for node alive/echo/redirection requests from the CGF.
Dictionary	Dictionary supported by the GTPP group.
Accounting Server	
Group	GTPP group, in which the accounting server is configured.
Context Name	Name of the context, in which the CGF is configured.
Primary Accounting Server Address	IPv4 or IPv6 address of the CGF.
Port	UDP port over which the GGSN communicates with the CGF.
State	Status of the CGF, which could be Active or Inactive.
Priority	Relative priority of the CGF. This priority determines which CGF server to send the accounting data to.

Viewing Additional Characteristics of a GTPP

To view additional characteristics of a GTPP:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile >** *GTPP Container* **>***GTPP*.

Step 3 Expand the GTPP node. The following list of characteristics configured for the GGSN are displayed:

- Accounting Server Failure Detection—Attributes of the CGF accounting server within the GTPP server group.
- CDR Attributes Indicator—Indicates whether associated attributes are enabled or disabled for CDR generation.
- CDR Triggers—Attributes that trigger CDR generation.
- Charging Agent— IP address and port of the system interface within the current context used to communicate with the CGF or the GTPP Storage Server (GSS).
- EGCDR Data Generation Configuration—Attributes that represent the GTPP eG-CDR data generation configuration.
- Local Storage—Storage server information, if CDR storage mode is Local.
- MBMS CDR Triggers—Attributes that trigger the MBMS CDR generation.
- Storage Server—Configuration information for the GTPP backup storage server.

Step 4 Click each of one of these characteristics to view its properties on the right pane. See Table 26-14 for more details on the properties of each characteristics configured for the GTPP.

Table 26-14 GTPP Characteristics

Field	Description
Accounting Server Failure Detection	
Detect Dead Server Consecutive Failures	Number of failures that could occur before marking a CGF as dead (down).
Dead Server Suppress CDRs	Indicates whether suppression of CDRs is enabled or disabled when the GTPP server is detected as dead or unreachable.
Dead Time	Maximum duration, in seconds, before marking a CGF as dead on consecutive failures.
Echo Timeout	The amount of time that must elapse before the system attempts to communicate with a CGF that was previously unreachable.
Echo Max Retries	Number of times the system attempts to communicate with a GTPP backup storage server that is not responding.
Redirection Allowed	Indicates whether redirection of CDRs is allowed or not, when the primary CGF is unavailable.
Duplicate Hold Time Minutes	Number of minutes to hold on to CDRs that may be duplicates, when the primary CGF is down.

Table 26-14 GTPP Characteristics (continued)

Field	Description
CDR Attributes Indicator	
Indicators	Indicates whether the following CDR attributes are enabled or not: • PDP Type • PDP Address • Dynamic Flag • Diagnostics • Node ID • Charging Characteristic Selection Mode • Local Record Sequence Number • MSISDN • PLMN ID • PGW PLMN ID • IMEI • RAT • User Location Information • List of Service Data • Served MNAI • Start Time • Stop Time • PDN Connection ID • Served PDP PDN Address Extension • Duration
CDR Triggers	
Triggers	Indicates whether the following CDR triggers are enabled or not: • Volume Limit • Time Limit • Tariff Time Change • Serving Node Change Limit • Intra SGSN Group Change • Inter PLMN SGSN Change • EGCDR Max LOSDV Limit • QOS Change • RAT Change • MS Timezone Change • Direct Tunnel

Table 26-14 GTPP Characteristics (continued)

Field	Description
Charging Agent	
IP Address	IP address of the charging agent.
Port	Port of the charging agent.
EGCDR Data Generation Configuration	
Service Interval	The volume octet counts for the generation of the interim eG-CDRs to service data flow container in flow-based charging (FBC).
Service Idle Timeout	Time interval, in seconds, to close the eG-CDR, if the minimum time duration thresholds for service data flow containers are satisfied in FBC.
Delete Service Thresholds	Configured threshold in eG-CDR to be deleted in the service.
Include All LOSDVs	Indicates whether all content IDs are included in the final eG-CDR or not.
LOSDV Max Containers	Maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR.
LOTDV Max Containers	Maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR.
Closing Cause Unique	Indicates whether the same closing cause needs to be included for multiple final eG-CDRs or not.
Local Storage	
File Format	File format to store CDRs.
File Compression	Type of compression used on CDR files stored locally. None indicates that file compression is disabled.
File Rotation Time Interval	Time duration, in seconds, after which CDR file rotation happens.
File Rotation Volume Limit (MB)	Volume of CDR file, in MB, after which CDR file rotation happens.
File Rotation CDR Count	Number of CDRs to include in a CDR file after which CDR file rotation happens.
Force File Rotation by Time Interval	Indicates whether file rotation is forced or not. If this is enabled, the system is forced to do a file rotation at specified interval, even if there are no CDRs generated.
Purge Processed Files	Indicates whether processed files must be processed or not.
MBMS CDR Triggers	
Interval	Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions are satisfied: • Down link traffic volume is reached within the time interval • Tariff time based trigger occurred within the time interval • Data volume (uplink and downlink) bucket trigger occurred within the time interval
Buckets	Total number of data buckets configured for MBMS CDR trigger service.
Storage Server	

Table 26-14 GTPP Characteristics (continued)

Field	Description
IP Address	IP address of the backup storage server.
Port	UDP port number over which the GGSN communicates with the backup storage server.
Timeout	Maximum amount of time, in seconds, the system waits for a response from the GTPP backup storage server before assuming the packet is lost.
Max Retries	Number of times the system attempts to communicate with a GTPP backup storage server that is not responding.

GTPP Commands

The following commands can be launched from the inventory by right-clicking a GTPP and choosing **Commands > Configuration** or **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-15 GTPP Commands

Command Type	Command	Inputs Required and Notes
Configuration	**Create CGF**	Server Address (IPV4), Server Port, Server Priority, Server Max
	Create Storage Server	IP Address (IPV4), Port Number, Max Retries, Timeout, Mode Type
	Modify Storage Server (*GTPP Container* > *GTPP Group* > **Storage Server**)	Max Retries, Timeout, Mode Type
	Delete Storage Server (*GTPP Container* > *GTPP Group* > **Storage Server**)	Click **Execute Now** to delete the storage server.
	Delete CGF	Server Address (IPV4), Server Port Click **Execute Now** to delete the CGF.
	Delete GTPP	Click **Execute Now** to delete the GTPP.
	Modify CGF	Server Address (IPV4), Server Port, Server Priority, Server Max
	Modify GTPP	Dictionary, Transport Layer Protocols, Delete Accounting Type, Accounting Type, RAT Generation Type
Show	**Show CGF**	Click **Execute Now** to view the CGF.

Working with EGTP

Evolved GPRS Tunneling Protocol (EGTP) formulates the primary bearer plane protocol within an LTE / EPC architecture. It provides support for tunnel management including handover procedures within and across LTE networks.

This topic contains the following sections:

Viewing EGTP Properties

Prime Network Vision displays the EGTPs in an EGTP container under the Mobile node in the logical inventory. The icon used for representing EGTPs in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view EGTP properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > *Context* > **Mobile** > *EGTP Container*.

Prime Network Vision displays the list of EGTPs configured under the container. You can view the individual EGTP details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile >** *EGTP Container* **>** *EGTP*.

Table 26-16 describes the details available for each EGTP.

Table 26-16 EGTP Properties in Logical Inventory

Field	Description
Service Name	Name of the EGTP service.
Status	Status of the EGTP service.
Message Validation Mode	Mode of message validation for the EGTP service.
Interface Type	Interface type for the EGTP service.
Restart Counter	Restart counter value for the EGTP service.
GTPC Retransmission Timeout	Control packet retransmission timeout for the EGTP service.
GTPC Max Request Retransmissions	Maximum number of request retransmissions for the EGTP service.
GTPC IP QoS DSCP Value	The IP QoS DSCP value for the EGTP service.
GTPC Echo	Indicates whether GTPC echo is configured for the EGTP service or not.
GTPC Echo Interval	GTPC echo interval for the EGTP service.
GTPC Echo Mode	GTPC echo mode, which could be Dynamic or Default.
GTPC Smooth Factor	Smooth factor used in the dynamic echo timer for the EGTP service.

EGTP Commands

The following commands can be launched from the inventory by right-clicking an EGTP and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-17 EGTP Commands

Command Type	Command	Inputs Required and Notes
Configuration	**Modify EGTP**	General tab: Delete GTPU Service, GTPU Service, Interface, Validation Mode GTPC Attributes tab: Retransmission Timeout, Echo Retransmission Timeout, Maximum Retries, Delete Echo Interval, Echo Interval, Dynamic Echo Timer, Smooth Factor, IP QoS DSCP, Delete Bind Address, Bind Address Type, Bind Address, Delete Path Failure Detection Policy, Path Failure Detection Policy
	Delete EGTP	Click **Execute Now** to delete the EGTP.

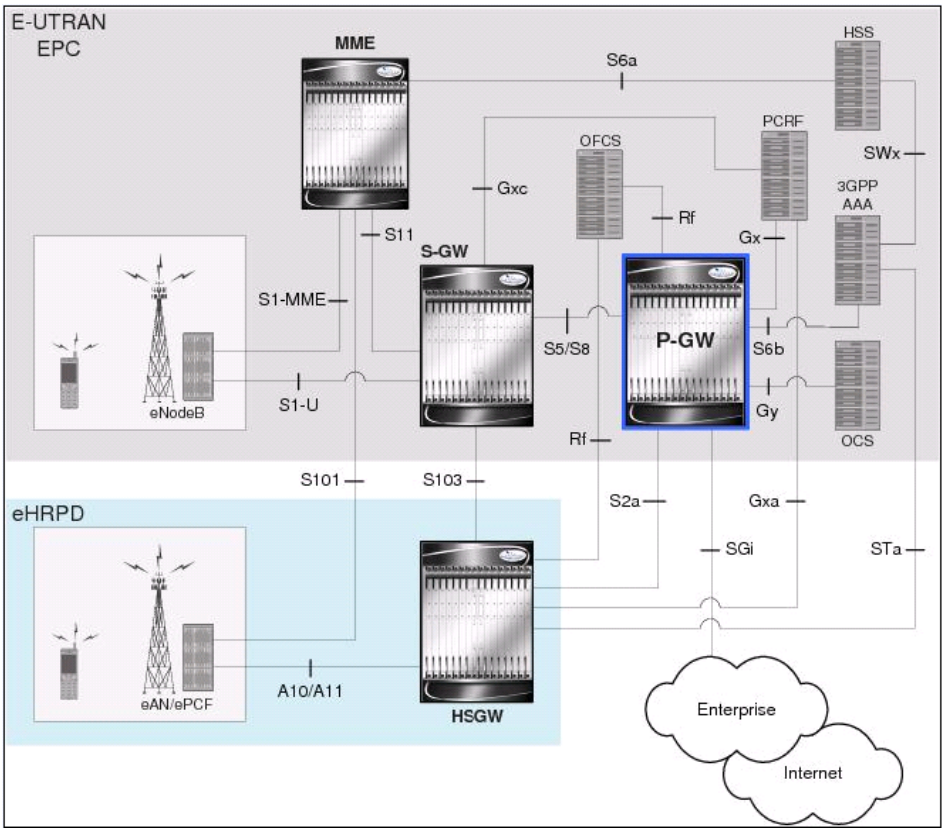
LTE Networks - An Overview

Long Term Evolution (LTE) is the latest step in moving forward from the cellular 3G services, such as GSM to UMTS to HSPA to LTE or CDMA to LTE. LTE is based on standards developed by the Third Generation Partnership Project (3GPP). LTE may also be referred more formally as Evolved UMTS Terrestrial Radio Access Network (E-UTRAN). Following are the main objectives of an LTE network.

- Increased downlink and uplink peak data rates
- Scalable bandwidth
- Improved spectral efficiency
- All IP network

Figure 26-3 provides the topology of a basic LTE network.

Figure 26-3 Basic LTE Network Topology



Working with LTE Network Technologies

The E-UTRAN uses a simplified single node architecture consisting of the eNodeBs (E-UTRAN Node B). The eNB communicates with the Evolved Packet Core (EPC) using the S1 interface, specifically with the Mobility Management Entity (MME) and Serving Gateway (S-GW) using S1-U interface. The PDN Gateway (P-GW0 provides connectivity to the external packet data networks.

Following sections provide more details on these services and their support in Prime Network:

- Monitoring SAE-GW, page 26-34
- Working with PDN-Gateway, page 26-36
- Working with Serving Gateway, page 26-38
- Viewing QCI-QoS Mapping, page 26-40

Monitoring SAE-GW

Systems Architecture Evolution (SAE) has a flat all-IP architecture with separation of control plane and user plane traffic. The main component of SAE architecture is the Evolved Packet Core (EPC), also known as SAE Core. The EPC serves as an equivalent to GPRS networks by using its subcomponents Mobility Management Entities (MMEs), Serving Gateway (S-GW), and PDN Gateway (P-GW).

Mobility Management Entity (MME)

MME is the key control node for a Long Term Evolution (LTE) access network. It is responsible for idle mode User Equipment (UE) tracking and paging procedure including retransmissions. It is involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW for a UE at the initial attach and at time of intra-LTE handover involving Core Network (CN) node relocation. The MME also provides the control plane function for mobility between LTE and 2G/3G access networks with the S3 interface terminating at the MME from the SGSN.

Serving Gateway (S-GW)

The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies. For idle state UEs, the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, such as parameters of the IP bearer service, network internal routing information, and so on. It also performs replication of the user traffic in case of lawful interception.

For more information, see Working with Serving Gateway, page 26-38.

PDN Gateway (P-GW)

The P-GW provides connectivity from the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. Another key role of the P-GW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2.

For more information, see Working with PDN-Gateway, page 26-36.

Running S-GW and P-GW services together as a SAE-GW provides the following benefits:

- Higher capacity—For a UE with one PDN connection that is passing through standalone S-GW and P-GW services consumes 2 license units because both S-GW and P-GW services account for it separately. SAE-GW as a single node consumes only one license unit for the same, thus increasing the capacity.
- Cohesive configuration—Configuration and management of SAE-GW as a node is simpler to follow and logical to explain.

See Viewing SAE-GW Properties, page 26-35 for details on how to view SAE-GW properties in Prime Network Vision.

Viewing SAE-GW Properties

Prime Network Vision displays the SAE-GWs in a SAE-GW container under the Mobile node in the logical inventory. The icon used for representing SAE-GW in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view SAE-GW properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory** > *Context* > **Mobile** > *SAE-GW Container*.

Prime Network Vision displays the list of SAE-GW services configured under the container. You can view the individual SAE-GW service details from the table on the right pane or by choosing **Logical Inventory** > *Context* > **Mobile** > *SAE-GW* Container > *SAE-GW*.

Table 26-18 describes the details available for each SAE-GW.

Table 26-18 SAE-GW Properties in Logical Inventory

Field	Description
Service Name	Name of the SAE-GW service.
Service ID	ID of the SAE-GW service.
Status	Status of the SAE-GW service.
P-GW Service	The P-GW service associated with the SAE-GW.
S-GW Service	The S-GW service associated with the SAE-GW.
New Call Policy	Specifies if the new call related behavior of SAE-GW service is enabled or disabled, when duplicate sessions with same IP address request is received.

Working with PDN-Gateway

PDN Gateway (P-GW) is the node that terminates the SGi interface towards the PDN. If a user equipment (UE) is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides connectivity to the UE to external packet data networks by being the point of exit and entry of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple PDNs.

The P-GW facilitates policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. The features of P-GW include:

- Integration of multiple core network functions in a single node
- Multiple instances of P-GW can enable call localization and local breakout
- High performance across all parameters like, signaling, throughput, density, and latency
- Integrated in-line services
- Support for enhanced content charging, content filtering with blacklisting, dynamic network-based traffic optimization, application detection and optimization, stateful firewall, NAT translation, and lawful intercept
- High-availability helps to ensure subscriber satisfaction

The following topics explain how to work with P-GW in Prime Network Vision:

- Viewing P-GW Properties, page 26-36
- P-GW Commands, page 26-37

Viewing P-GW Properties

Prime Network Vision displays the P-GWs in a P-GW container under the Mobile node in the logical inventory. The icon used for representing P-GW in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view P-GW properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile >** *P-GW Container.*

Prime Network Vision displays the list of P-GW services configured under the container. You can view the individual P-GW service details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile >** *P-GW* Container **>** *P-GW.*

Table 26-19 describes the details available for each P-GW.

Table 26-19 P-GW Properties in Logical Inventory

Field	Description
Service Name	Name of the P-GW service.
Service Status	Status of the P-GW service.
EGTP Service	Evolved GPRS Tunneling Protocol (EGTP) service associated with the P-GW. EGTP provides tunneling support for the P-GW.
GGSN Service	GGSN service associated with the P-GW.
LMA Service	Local Mobility Anchor (LMA) that facilitates proxy mobile IP on the P-GW.
QCI QoS Mapping Table Name	Table name of QoS class indices that enfore QoS parameters.
New Call Policy	Specifies if the new call related behavior of P-GW service is enabled or disabled, when duplicate sessions with same IP address request is received.
Session Delete Delay Timeout	Duration, in seconds, to retain a session before terminating it.
SAE-GW Service	Systems Architecture Evolution (SAE) gateway service associated with the P-GW.

Step 3 If the P-GW is associated with PLMNs, you can view the details of the PLMNs on clicking the specified P-GW.

P-GW Commands

The following commands can be launched from the inventory by right-clicking a P-GW and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-20 P-GW Commands

Command	Inputs Required and Notes
Create P-GW PLMN	MCC Number, MNC Number, PLMN Type
Delete P-GW	Click **Execute Now** to delete the P-GW.

Table 26-20 P-GW Commands

Command	Inputs Required and Notes
Modify P-GW	General tab: Delete Associate Service, Associate Service Name, Accociate Service Type, Delete QCI-QoS Mapping Name, QCI-QoS Mapping Name, Delete New Call Policy, New Call Policy, Delete Session DeleteDelay, Session Delete Delay, Session Delay Timeout
	FQDN tab: Delete FQDN, FQDN Host Name, Realm Name

Working with Serving Gateway

In a Long Term Evolution (LTE) / Systems Architecture Evolution (SAE) network, a Serving Gateway (S-GW) acts as a demarcation point between the Radio Access Network (RAN) and core network, and manages user plane mobility. It serves as the mobility anchor when terminals move across areas served by different eNode-B elements in Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), as well as across other 3GPP radio networks such as GSM EDGE Radio Access Network(GERAN) and UTRAN. S-GW buffers downlink packets and initiates network-triggered service request procedures. Other functions include lawful interception, packet routing and forwarding, transport level packet marking in the uplink and the downlink, accounting support for per user, and inter-operator charging. The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNode-B handovers and as the anchor for mobility between LTE and other 3GPP technologies.

For idle state user equipment (UE), the S-GW terminates the downlink data path and triggers paging when downlink data arrives for the UE. It manages and stores UE contexts, such as parameters of the IP bearer service, network internal routing information, and so on. It also performs replication of the user traffic in case of lawful interception.

The following topics provide details on how to work with S-GWs in Prime Network Vision:

- Viewing S-GW Properties, page 26-38
- S-GW Commands, page 26-40

Viewing S-GW Properties

Prime Network Vision displays the S-GWs in a S-GW container under the Mobile node in the logical inventory. The icon used for representing S-GW in the logical inventory is explained in Logical Inventory Icons, page A-6.

To view S-GW properties:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory >** *Context* **> Mobile >** *S-GW Container.*

Prime Network Vision displays the list of S-GW services configured under the container. You can view the individual S-GW service details from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile >** *S-GW* Container **>** *S-GW.*

Table 26-21 describes the details available for each S-GW.

Table 26-21 S-GW Properties in Logical Inventory

Field	Description
Service Name	Name of the S-GW service.
Service Status	Status of the S-GW service.
Accounting Context	Name of the context configured on the system that processes accounting for service requests handled by the S-GW service.
Accounting GTPP Group	Name of the accounting GTPP group associated with the S-GW service. This will hold the configured GTPP server group (for GTPP servers redundancy) on a S-GW service for CGF accounting functionality.
Accounting Mode	Accounting protocol, which could be GTPP or Radius-Diameter.
Egress Protocol	Egress protocol used for the S-GW service, which could be GTP, GTP-PMIP, or PMIP.
Ingress EGTP Service	Ingress EGTP service associated with the S-GW. EGTP provides tunneling support for the S-GW.
Egress Context	Context used for S-GW service egress.
Egress ETGP Service	Ingress EGTP service associated with the S-GW. EGTP provides tunneling support for the S-GW.
Egress Mag Service	Mobile Access Gateway (MAG) egress service through calls are routed to the S-GW.
IMS Authorization Service	IMS authorization service associated with the S-GW.
Accounting Policy	Accounting policy configured for the S-GW.
New Call Policy	Specifies if the new call related behavior of S-GW service is enabled or disabled, when duplicate sessions with same IP address request is received.
QCI QoS Mapping Table	Table name of QoS class indices that enfore QoS parameters.
SAE GW Service	Systems Architecture Evolution (SAE) gateway service associated with the S-GW.

Step 3 If the S-GW is associated with PLMNs, you can view the PLMN entries on clicking the specified S-GW.

S-GW Commands

The following commands can be launched from the inventory by right-clicking an S-W and choosing **Commands > Configuration.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-22 S-GW Commands

Command	Inputs Required and Notes
Create S-GW PLMN	MCC Number, MNC Number, PLMN Type
Delete S-GW	Click Execute Now to delete the P-GW.
Modify S-GW	General tab: Accounting Mode, Delete Accounting Context Name, Accounting Context Name, Gtpp Group Name, Delete QCI-QoS Mapping Name, QCI-QoS Mapping Name, Egress Protocol, Delete Egress Context Name, Egress Context Name, Delete EGTP Service Name, EGTP Service Name, Delete MAG Service Name, MAG Service Name, Delete Ingress EGTP Service Name, Ingress EGTP Service Name, Delete Accounting Policy Name, Accounting Policy Name, Delete IMS Authorization Service Name, IMS Authorization Service Name, Delete New Call Policy, New Call Policy

Viewing QCI-QoS Mapping

The QoS Class Index (QCI) to QoS mapping configuration mode is used to map QCIs to enforceable QoS parameters. Mapping can occur between the RAN and the S-GW, the MME, and/or the P-GW in an LTE network or between the RAN and the eHRPD Serving Gateway (HSGW) in an eHRPD network. This is a global configuration. These maps can be imported by P-gateway and S-gateway to enforce these parameters on upstream/downstream traffic.

Prime Network Vision displays the QCI-QoS mapping information under the Mobile node in the logical inventory. See Figure 26-4.

Note QCI-QoS mapping is applicable only for the ‘local’ context in the logical inventory.

To view QCI-QoS mapping:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > QCI-QoS Mapping**.

Prime Network Vision displays the list of QCI-QoS mapping records configured under the container. You can view the individual record from the table on the right pane or by choosing **Logical Inventory >***Context* **> Mobile > QCI-QoS Mapping >** *Mapping Name.*

Table 26-23 describes the QCI-QoS mapping details.

Table 26-23 QCI-QoS Mapping

Field	Description
Mapping Name	Name of the QCI-QoS mapping record.
QCI-QoS Mapping Table	
QCI Number	QCI number.
QCI Type	QCI type.
Uplink	DSCP marking to be used for encapsulation and UDP for uplink traffic
Downlink	DSCP marking to be used for encapsulation and UDP for downlink traffic
Max Packet Delay	Maximum packet delay, in milliseconds, that can be applied to the data.
Max Error Rate	Maximum error loss rate of non congestion related packet loss.
Delay Class	Packet delay.
Precedence Class	Indicates packet precedence.
Reliability Class	Indicates packet reliability.
Traffic Policing Interval	Traffic policing interval.

Viewing Operator Policies, APN Remaps, and APN Profiles

Operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It can also be used to control the behavior of visiting subscribers in roaming scenarios, enforcing roaming agreements, and providing a measure of local protection against foreign subscribers.

An operator policy associates APNs, APN profiles, an APN remap table, and a call-control profile to ranges of International Mobile Subscriber Identities (IMSIs). These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements, such as DNS servers and HSSs.

Note Operator policies and APN profiles are applicable only for the ‘local’ context in the logical inventory.

The following topics explain how to view operator policies, APN remaps, and APN profiles in Prime Network Vision:

- Viewing Operator Policies, page 26-42
- Viewing APN Remaps, page 26-44
- Viewing APN Profiles, page 26-46

Viewing Operator Policies

Operator policies provide an operator with a range of control to manage the services, facilities, and privileges available to subscribers. By configuring the various components of an operator policy, the operator fine tunes any desired restrictions or limitations needed to control call handling and this can be done for a group of callers within a defined IMSI range or per subscriber.

Besides enhancing operator control through configuration, the operator policy feature minimizes configuration by drastically reducing the number of configuration lines needed. Operator policy maximizes configurations by breaking them into the following reusable components that can be shared across IMSI ranges or subscribers:

- Call-control profiles
- IMEI profiles (SGSN only)
- APN profiles
- APN remap tables
- Operator policies
- IMSI ranges

To view operator policies in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Policy > Operator Policies**

Prime Network Vision displays the list of operator policies configured under the container. You can view the individual policy details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Policy > Operator Policies >** *Policy*.

Table 26-24 describes the details available for each operator policy.

If an operator policy is configured with IMEI ranges and APN entries, the details are displayed in the respective tabs IMEI Ranges and APN Entries on the content pane.

Table 26-24 Operator Policies in Logical Inventory

Field	Description
Name	Name of the operator policy.
Description	Description of the operator policy.
Call Control Profile Name	Name of the call control profile associated with the operator policy.

Table 26-24 Operator Policies in Logical Inventory (continued)

Field	Description
Call Control Validity	Indicates whether the call control profile name associated with the operator policy is valid or is not created yet (invalid).
APN Remap Table Name	Name of the APN remap table associated with the operator policy.
APN Remap Table Validity	Indicates whether the APN remap table name associated with the operator policy is valid or is not created yet (invalid).
Default APN Profile Name	Name of the default APN profile associated with the operator policy.
Default APN Profile Validity	Indicates whether the default APN profile name associated with the operator policy is valid or is not created yet (invalid).
IMEI Ranges	
Start Range	The starting number in the range of IMEI profiles.
To Range	The ending number in the range of IMEI profiles.
Software Version	Software version to fine tune the IMEI definition.
Profile Name	Name of the IMEI profile associated with the IMEI range. Displays ‘None’, if no profile is associated with the range.
Validity	Validity of the IMEI profile.
APN Entries	
NI	APN network identifier.
NI APN Profile	Name of the APN profile associated with the network identifier. An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied.
NI APN Profile Validity	Indicates whether the NI APN profile associated with the operator policy is valid or is not created yet (invalid).
OI	APN operator identifier.
OI APN Profile	Name of the APN profile associated with the operator identifier. An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied.
OI APN Profile	Indicates whether the OI APN profile associated with the operator policy is valid or is not created yet (invalid).

Viewing APN Remaps

An APN remap tables allow an operator to override an APN specified by a user, or the APN selected during the normal APN selection procedure, as specified by 3GPP TS 23.060. This level of control enables operators to deal with situations such as:

- An APN is provided in the activation request that does not match with any of the subscribed APNs; either a different APN was entered or the APN could have been misspelled. In such situations, the SGSN rejects the activation request. It is possible to correct the APN, creating a valid name so that the activation request is not rejected.
- In some cases, an operator might want to force certain devices or users to use a specific APN. For example, a set of mobile users may need to be directed to a specific APN. In such situations, the operator needs to override the selected APN.

An APN remap table group is a set of APN-handling configurations that may be applicable to one or more subscribers. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN remap table are applied. For example, an APN remap table allows configuration of the following:

- APN aliasing—Maps incoming APN to a different APN, based on partial string match (MME and SGSN) or matching charging characteristic (SGSN only).
- Wildcard APN—Allows APN to be provided by the SGSN, when wildcard subscription is present and the user has not requested an APN.
- Default APN—Allows a configured default APN to be used, when the requested APN cannot be used.

APN remap tables are configured with commands in the APN Remap Table configuration mode. A single APN remap table can be associated with multiple operator policies, but an operator policy can only be associated with a single APN remap table.

To view APN remap properties in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > > Profile > APN Remaps**

Prime Network Vision displays the list of APN remaps configured under the container. You can view the individual APN remap details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Profile > APN Remaps >** *APN Remap*.

Table 26-25 describes the details available for each APN remap.

If an APN remap is configured with charging characteristics and NI and OI entries, the details are displayed in the respective tabs Charging Characteristics and Network And Operator Identifier Entries on the content pane.

Table 26-25 APN Remap Properties in Logical Inventory

Field	Description
Name	Name of the APN remap.
Description	Description of the APN remap.
APN When No APN Requested	APN network identifier that will be used when no APN is requested.

Table 26-25 APN Remap Properties in Logical Inventory (continued)

Field	Description
Wildcard APN for IPv4	Wildcard APN included in the subscriber record, with PDP type as IPv4 context.
Wildcard APN for IPv6	Wildcard APN included in the subscriber record, with PDP type as IPv6 context.
Wildcard APN for IPv4v6	Wildcard APN included in the subscriber record, with PDP type as both IPv4 and IPv6 contexts.
Wildcard APN for PPP	Wildcard APN included in the subscriber record, with PDP type as PPP context.
Charging Characteristics	
Profile Index	Profile index in charging characteristics.
Behavior Bit Value	Behavior bit in charging characteristics.
APN For Overriding	Name of the APN profile that the charging characteristic attributes must be applied to, to generate CDRs.
Network And Operator Identifier Entries	
Requested NI	The old network identifier that is being mapped for replacement.
Mapped to NI	The new network identifier.
NI Wildcard Replace String	When a wildcard character is included in the old APN network identifier, this parameter identifies the information to replace the wildcard in the new APN network identifier.
Requested OI	The old operator identifier that is being mapped for replacement.
Mapped to OI	The new operator identifier.
OI MNC Replace String	When a wildcard character is included in the MNC portion of the old APN operator identifier, this parameter identifies the information to replace the wildcard in the new APN operator identifier.
OI MCC Replace String	When a wildcard character is included in the MCC portion of the old APN operator identifier, this parameter identifies the information to replace the wildcard in the new APN operator identifier.

Step 3 If a default APN is configured for the remap, click the **Default APN** node under the APN remap. You can view the following details on the content pane.

Table 26-26 Default APN Properties in Logical Inventory

Field	Description
Default APN Name	Name of the default APN.
Use Default APN When No APN is Requested	Indicates whether the configured default APN can be used or not, if there is no APN in the request.
Use Default APN When DNS Query Fails	Indicates whether the configured default APN can be used or not, if DNS query fails.
Fallback APN to Use	A fallback APN to be used when the configured default APN is not present in the subscription, so that activation does not fail.
Fallback APN in First Subscription	Indicates whether APN from the first subscription record must be used, when the configured default APN is not available.
Use APN From Single Subscription Record	Indicates whether APN from the subscription record must be used, if it is the only record available and the normal APN selection fails.

Viewing APN Profiles

APN Profile defines a set of parameters controlling the SGSN or MME behavior, when a specific APN is received or no APN is received in a request. An APN profile is a key element in the Operator Policy feature. An APN profile is not used or valid unless it is associated with an APN and this association is specified in an operator policy.

Essentially, an APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, then the set of commands in the associated APN profile will be applied. The same APN profile can be associated with multiple APNs and multiple operator policies.

An APN profile groups a set of APN-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile are applied. For example:

- Enable or disable a direct tunnel (DT) per APN (SGSN).
- Define charging characters for calls associated with a specific APN.
- Identify a specific GGSN to be used for calls associated with a specific APN (SGSN).
- Define various quality of service (QoS) parameters to be applied to calls associated with a specific APN.
- Restrict or allow PDP context activation on the basis of access type for calls associated with a specific APN.

A single APN profile can be associated with multiple operator policies.

To view APN profile properties in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Profile > APN Profiles.**

Prime Network Vision displays the list of APN profiles configured under the container. You can view the individual APN profile details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Profile > APN Profiles >** *APN Profile*.

Table 26-27 describes the details available for each APN remap.

If additional properties are configured for the APN profile, you can click the respective tabs on the content pane to view the details:

- Gateway Entries
- RANAP ARP Entries
- QoS Class Entries
- Uplink Traffic Policing Entries/Downlink Traffic Policing Entries

Table 26-27 APN Profile Properties in Logical Inventory

Field	Description
Name	Name of the APN profile.
Description	Description of the APN profile.
QoS Service Capping Prefer Type	Operational preferences for QoS parameters, specifically QoS bit rates. Value could be one of the following: • both-hlr-and-local—Instructs the SGSN to use the locally configured QoS or HLR subscription. • hlr-subscription—Instructs the SGSN to use QoS bit rate from HLR configuration and use the same for session establishment. • local—Instructs the SGSN to use the locally configured QoS bit rate and use the same for session establishment.
Address Resolution Mode	Address resolution mode of the APN profile, which could be one of the following: • fallback-for-dns—Uses DNS query for address resolution. • local—Uses locally configured address.
CC Preferred Source	Charging characteristic settings to be used for S-CDRs, which could be one of the following: • hlr-value-for-scdrs—Instructs the system to use charging characteristic settings received from the HLR for S-CDRs. • local-value-for-scdrs—Instructs the profile preference to use only locally configured/stored charging characteristic settings for S-CDRs.
CC Local SCDR Behavior Bit	Value of the behavior bit for the charging characteristics for S-CDRs.
CC Local SCDR Behavior Profile Index	Value of the profile index for the charging characteristics for S-CDRs.
GGSN Algorithm Applicable	Selection algorithm for GGSNs. This parameter allows the operator to configure multiple GGSN pools by assigning the GGSN to a secondary pool of GGSNs.

Table 26-27 APN Profile Properties in Logical Inventory (continued)

Field	Description
IP Source Validation	Configures settings related to IP source violation detection with one of the following criteria: • deactivate—Deactivates the PDP context with one of the following conditions: – Deactivates all PDP contexts of the MS/UE. Default is to deactivate errant PDP contexts. – Excludes packets having an invalid source IP address from the statistics used in the accounting records. – Deactivates all assosiated PDP contexts (primary/secondary). Default is to deactivate errant PDP contexts. – Configures maximum number of allowed IP source violations before the session is deactivated. • discard—Discards errant packets and excludes packets having an invalid source IP address from the statistics used in the accounting records. • ignore—Ignores checking of packets for MS/UE IP source violation.
IP Source Validation Tolerance Limit	Maximum number of allowed IP source violations before the session is deactivated.
Direct Tunnel	Permission for direct tunnel establishment by GGSNs, which could be not-permitted-by-ggsn or remove.
Private Extension LORC IE to GGSN	Indicates whether GTPC private extension is enabled or not for the over charging protection feature of the GGSN.
Private Extension LORC IE to SGSN	Indicates whether GTPC private extension is enabled or not for the over charging protection feature of the SGSN.
Idle Mode Access Control List IPV4	Group of IPv4 Access Control Lists (ACLs) that define rules to apply to downlink data destined for UEs in an idle mode.
Idle Mode Access Control List IPV6	Group of IPv6 ACLs that define rules to apply to downlink data destined for UEs in an idle mode.
DNS Query with MSISDN Start Offset Position	The position of the first digit in the MSISDN to start an offset and create a new APN DNS query string that is intended to assist roaming subscribers to use the local GGSN.
DNS Query with MSISDN End Offset Position	The position of the last digit in the MSISDN to be part of the offset.
DNS Query with LAC or RAC	Indicates whether geographical information must be appended to the APN string that is sent to the DNS query or not. This information is used during the DNS query process to select the geographically closest GGSN.
DNS Query with RNC ID	Indicates whether the SGSN must include the ID of the calling RNC in the APN DNS query string or not.
DNS Query with Charging Characteristics	Indicates whether charging characteristic configuration is enabled for the APN profile or not.

Table 26-27 APN Profile Properties in Logical Inventory (continued)

Field	Description
DNS Query Charging Characteristics ID Format	Format of the charging characteristic information to be included.
Gateway Entries	
Gateway Entry	Gateway entry configured for the APN profile.
IP Address	IPv4 or IPv6 addresses of the gateway configured.
Priority	Priority of the gateway to consider during address selection.
Weight	Weightage or importance assigned to the gateway for load balancing.
Pool	Gateway pool assigned.
Gateway Type	Type of gateway configured, which could be GGSN or P-GW.
RANAP ARP Entries	
Traffic Class	Traffic class of the Radio Access Network Application Part (RANAP) configuration.
Subscription Priority	Subscription priority of the traffic class; the lowest number denoting the highest priority.
Priority Level	Priority level for the subscription priority.
Preemption Capability	Preemption capability value of the traffic class.
Preemption Vulnerability	Preemption vulnerability value of the traffic class.
Queuing Allowed	Indicates whether queuing is allowed for the traffic class or not.
QoS Class Entries	
Class Name	Traffing class of the QoS configuration.
Service Delivery Unit Delivery Order	Indicates whether bearer should provide in-sequence delivery of service data units (SDUs) or not.
Delivery of Erroneous Service Delivery Units	Indicates whether SDUs detected as erroneous should be delivered or discarded.
Max Bit Rate Uplink	Maximum bit rate, in kbps, allowed for uplink between MS and the core network.
Max Bit Rate Downlink	Maximum bit rate, in kbps, allowed for downlink between MS and the core network.
Allocation Retention Priority	Relative importance compared to other Radio Access Bearers (RABs) for allocation and retention of the RAB.
Traffic Handling Priority	Relative importance for traffic handling when compared to other RABs.
SDU Max Size	Maximum allowed SDU size, in bytes.
SDU Error Ratio	Fraction of SDUs lost or detected as erroneous.
Guaranteed Bit Rate Uplink	Uplink bit rate, in kbps, that is assured for a given RAB between MS and the core network.
Guaranteed Bit Rate Downlink	Downlink bit rate, in kbps, that is assured for a given RAB between MS and the core network.

Table 26-27 APN Profile Properties in Logical Inventory (continued)

Field	Description
Minimum Transfer Delay	Minimum transfer delay, in milliseconds.
Residual BER	Undetected bit error ratio (BER) in the delivered SDUs.
MBR Map Down	Attribute that maps or converts the received HLR maximum bit rate (MBR) (from value) to a locally configured downlink MBR value (to value).
MBR Map Up	Attribute that maps or converts the received HLR MBR (from value) to a locally configured uplink MBR value (to value).
Uplink Traffic Policing Entries/Downlink Traffic Policing Entries	
Traffic Class	Traffic class of the QoS configuration.
Burst Size Auto Readjust	Indicates whether the auto readjustment of burst size is enabled or disabled. This parameter is used in dynamic burst size calculation, for traffic policing, at the time of PDP activation or modification.
Burst Size Auto Readjust Duration	The burst size readjustment duration in seconds. This parameter indicates the number of seconds that the dynamic burst size calculation will last for. This allows the traffic to be throttled at the negotiated rates.
Peak Burst Size (bytes)	The peak burst size allowed, in bytes, for the uplink/downlink direction and QoS class.
Guaranteed Burst Size (bytes)	The guaranteed burst size allowed, in bytes, for the uplink/downlink direction and QoS class.
Exceed Action	The action to be taken on packets that exceed the committed data rate, but do not violate the peak data rate. The action could be one of the following: • Drop • Lower IP Precedence • Transmit
Violate Action	The action to be taken on packets that exceed both committed and peak data rates. The action could be one of the following: • Drop • Lower IP Precedence • Shape • Transmit

Viewing Additional Characteristics of an APN Profile

To view additional characteristics of an APN profile:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Profile > APN Profiles >** *APN Profile*.

Step 3 Expand the *APN Profile* node. The following list of characteristics configured for the APN profile are displayed:

- PDP Inactivity Actions—Attributes related to PDP data inactivity. Once a data communication is in progress there are cases where this data communication can be inactive after some time, for example, when the user has locked the phone after browsing the internet or when the battery suddenly drains out. In such a case, the SGSN can take a configured action based on this inactivity. The inactivity timeout and the actions that can be taken based on certain conditions are modeled in this configuration.
- QoS to DSCP Mapping (Downlink) / Qos to DSCP Mapping (Uplink)—Mapping of QoS parameters to DSCP. Configuration of the local values for the traffic class (TC) parameters for QoS configured for the APN.
- PDP Restrictions (UMTS) / PDP Restrictions (GPRS)—Activation restrictions on PDP.

Step 4 Click each of one of these characteristics to view its properties on the right pane. See Table 26-28 for more details on the properties of each characteristics configured for the APN profile.

Table 26-28 APN Profile Additional Characteristics

Field	Description
PDP Inactivity Actions	
PDP Inactivity Idle Timeout	Timeout duration for PDP inactivity. PDP context is deactivated, if it is inactive for the given duration.
PDP Inactivity Idle Timeout Action	Action to be taken when the PDP data communication is inactive for the timeout duration.
PDP Inactivity Idle Timeout Action Condition	Condition when the GPRS detach procedure should be executed on the PDP context, when the timeout is reached or exceeded.
PDP IPV4 IPV6 Override	PDP type to use, per APN, if dual PDP type addressing is not supported by the network.
QoS to DSCP Mapping (Downlink) / Qos to DSCP Mapping (Uplink)	
Conversational	Real time conversational traffic class of service, which is reserved for voice traffic.
Streaming	Streaming traffic class of service, which handes one-way, real-time data transmission, such as streaming video or audio.
Interactive Threshold Priority 1/2/3	Interactive traffic class of service with threshold priorities 1, 2, and 3.
Background	Background traffic class of service. This best-effort class manages traffic that is handled as a background function, such as e-mail, where time to delivery is not a key factor.
Interactive TP1 Alloc P1/P2/P3	Interactive traffic class of service, with threshold priority 1 and allocation priorities 1, 2, and 3.
Interactive TP2 Alloc P1/P2/P3	Interactive traffic class of service, with threshold priority 2 and allocation priorities 1, 2, and 3.
Interactive TP3 Alloc P1/P2/P3	Interactive traffic class of service, with threshold priority 3 and allocation priorities 1, 2, and 3.

Table 26-28 APN Profile Additional Characteristics (continued)

Field	Description
PDP Restrictions (UMTS) / PDP Restrictions (GPRS)	
QoS Class Background	Indicates whether background traffic class of service is enabled or not.
QoS Class Interactive	Indicates whether interactive traffic class of service is enabled or not.
QoS Class Streaming	Indicates whether streaming traffic class of service is enabled or not.
QoS Class Conversational	Indicates whether conversational traffic class of service is enabled or not.

Working with Active Charging Service

Enhanced Charging Service (ECS), also known as Active Charging Service (ACS), is an in-line service, which is integrated within the platform and provides mobile operators the ability to offer tiered, detailed, and itemized billing to subscribers. Data packets flow through the ECS subsystem and relevant actions are performed based on the configured rules. Charging records (xCDRs) will be generated and forwarded to ESS or billing systems for prepaid and post paid billing.

The major components and functions of an ECS solution are given below.

Content Service Steering

Content Service Steering (CSS) enables directing selective subscriber traffic into the ECS subsystem. CSS uses Access Control Lists (ACLs) to redirect selective subscriber traffic flows. ACLs control the flow of packets into and out of the system. ACLs consist of rules (ACL rules) or filters that control the action taken on packets matching the filter criteria.

ACLs are configurable on a per-context basis and apply to a subscriber through either a subscriber profile (for PDSN) or an APN profile (for GGSN) in the destination context.

Protocol Analyzer

Protocol analyzer stack is responsible for analyzing the individual protocol fields during packet inspection. The analyzer supports the following types of packet inspection:

- Shallow Packet Inspection—Inspection of the Layer 3 (IP header) and Layer 4 (for example, UDP or TCP header) information.
- Deep Packet Inspection—Inspection of Layer 7 and above information. This functionality includes:
  - Detection of Uniform Resource Identifier (URI) information at level 7 (example, HTTP)
  - Identification of true destination in the case of terminating proxies, where shallow packet inspection only reveals the destination IP address/port number of a terminating proxy

Rule Definitions

Rule definitions (ruledefs) are user-defined expressions, based on protocol fields and protocol states, which define what actions to take when specific field values are true.

Most important rule definitions are related to Routing and Charging as explained below:

- Routing Ruledefs—Routing ruledefs are used to route packets to content analyzers. Routing ruledefs determine which content analyzer to route the packet to, when the protocol fields and/or protocol states in ruledef expression are true.
- Charging Ruledefs—Charging ruledefs are used to specify what action to take based on the analysis done by the content analyzers. Actions can include redirection, charge value, and billing record emission.

Rule Base

A rule base is a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. Rule bases can also be used to apply the same rule definitions for several subscribers, which eliminate the need to have unique rule definition for each subscriber. We can set priority, default bandwidth policy, type of billing for subscriber sessions, for a rule definition or group of rule definitions in the rule base.

Content Filtering

ACS also offers a content filtering mechanism. Content filtering is an in-line service available for 3GPP and 3GPP2 networks to filter HTTP and WAP requests from mobile subscribers, based on the URLs in the requests. Content filtering uses the DPI feature of ECS to discern HTTP and WAP requests. This enables operators to filter and control the content that an individual subscriber can access, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

The content filtering service offers the following solutions:

- URL Blacklisting—With this solution, all HTTP/WAP URLs in subscriber requests are matched against a database of blacklisted URLs. If there is a match, the flow is discarded, redirected, or terminated as configured. If there is no match, subscribers view the content as they would normally.
- Category-based Content Filtering
  - Category-based Static Content Filtering—In this method, all HTTP/WAP URLs in subscriber requests are matched against a static URL categorization database. Action is taken based on a URL's category, and the action configured for that category in the subscriber's content filtering policy. Possible actions include permitting, blocking, redirecting, and inserting content.
  - Category-based Static-and-Dynamic Content Filtering—In this method, each URL first undergoes static rating. If the URL cannot be rated by the static database or if the URL static rating categorizes a URL as either Dynamic or Unknown, the requested content is sent for dynamic rating; wherein the requested content is analyzed and categorized. Action is taken based on the category determined by dynamic rating, and the action configured for that category in the subscriber's content filtering policy. Possible actions include permitting, blocking, redirecting, and inserting content.

Note ACS is applicable only for the 'local' context in the logical inventory.

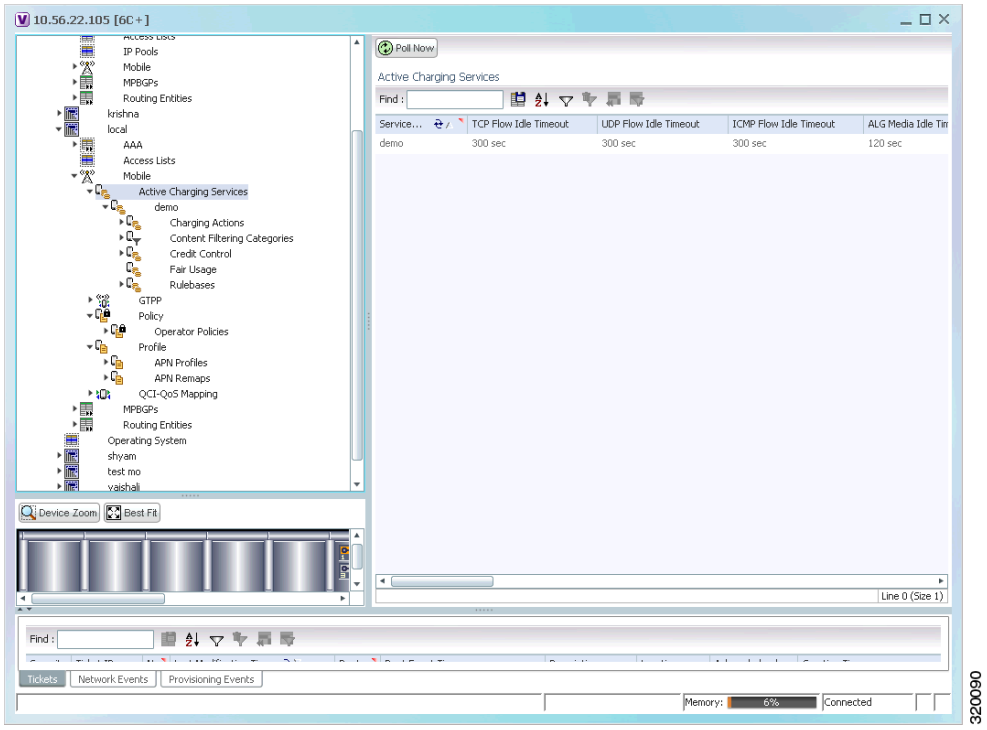
The following topics explain how to work with ACS in Prime Network Vision:

- Viewing Active Charging Services, page 26-54
- ACS Commands, page 26-67

Viewing Active Charging Services

You can view the active charging services in logical inventory as shown in Figure 26-4.

Figure 26-4 Mobile Technology Setup Nodes



Additionally, you can also perform the following for each ACS:

- Viewing Content Filtering Categories, page 26-56
- Viewing Credit Control Properties, page 26-56
- Viewing Charging Action Properties
- Viewing Rule Definitions
- Viewing Rule Base for the Charging Action
- Viewing Bandwidth Policies
- Viewing Fair Usage Properties

To view ACS details in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services**.

Prime Network Vision displays the list of active charging services configured under the container. You can view the individual ACS details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS*.

Table 26-29 describes the details available for each ACS.

Table 26-29 Active Charging Services in Logical Inventory

Field	Description
Service Name	Name of the active charging service.
TCP Flow Idle Timeout	Maximum duration, in seconds, a TCP flow can remain idle.
UDP Flow Idle Timeout	Maximum duration, in seconds, a UDP flow can remain idle.
ICMP Flow Idle Timeout	Maximum duration, in seconds, an Internet Control Message Protocol (ICMP) flow can remain idle.
ALG Media Idle Timeout	Maximum duration, in seconds, an application level gateway (ALG) media flow can remain idle.
TCP Flow Mapping Idle Timeout	The time for which the TCP flow mapping timer holds the resources.
UDP Flow Mapping Idle Timeout	The time for which the UDP flow mapping timer holds the resources.
Deep Packet Inspection	Indicates whether configuration of DPI is enabled or disabled in the mobile video gateway.
Passive Mode	Indicates whether the ACS is in or out of passive mode operation.
CDR Flow Control	Indicates whether flow control is enabled or disabled between the ACS Manager (ACSMGR) and Charging Data Record Module (CDRMOD).
CDR Flow Control Unsent Queue Size	Flow control unsent queue size at ACSMGR level.
Unsent Queue High Watermark	Highest flow control unsent queue size at ACSMGR level.
Unsent Queue Low Watermark	Lowest flow control unsent queue size at ACSMGR level.
Content Filtering	Indicates whether content filtering is enabled or disabled for the ACS.
Dynamic Content Filtering	Indicates whether dynamic content filtering is enabled or disabled for the ACS.
URL Blacklisting	Indicates whether URL blacklisting is enabled or disabled for the ACS.
URL Blacklisting Match Method	Method to look up the URLs in the URL blacklisting database.
Content Filtering Match Method	Method to look up the URLs in the category-based content filtering database.
Interpretation of Charging Rulebase Name	Charging rulebase configured for the ACS.
Selected Charging Rulebase Name for AVP	Charging rulebase name for attribute value pair (AVP) configured for the ACS.

Viewing Content Filtering Categories

To view content filtering categories in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS*** >Content Filtering Categories**.

Prime Network Vision displays the list of content filtering categories configured under the container. You can view the individual content filtering category details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **>Content Filtering Categories** > *Content Filtering Category*.

Table 26-30 describes the details available for each content filtering category.

Table 26-30 Content Filtering Categories in Logical Inventory

Field	Description
Policy ID	ID of the content filtering policy.
Failure Action	Action to take for the content filtering analysis result.
EDR File	The EDR file name.
Content Category	Name of the content filtering category.
Content Insert	Content string to insert in place of the message returned from prohibited or restricted site or content server.
Content Priority	Precedence of the category in the content filtering policy.
Content Failure Action	Action to take for the indicated result of the content filtering analysis, which could be one of the following: • allow • content-insert • discard • redirect URL • terminate flow • www-reply-code-and-terminate-flow
Content Redirect	Content string to redirect the subscriber to a specified URL.
Content Reply Code	Reply code to terminate flow.
EDR File Format	Predefined EDR file format.

Viewing Credit Control Properties

In a prepaid environment, the subscribers pay for a service prior to using it. While the subscriber is using the service, credit is deducted from subscriber's account until it is exhausted or the call ends. In prepaid charging, ECS performs the metering function. Credits are deducted in real time from an account balance or quota. A fixed quota is reserved from the account balance and given to the system by a prepaid rating and charging server, which interfaces with an external billing system platform. The system deducts

volume from the quota according to the traffic analysis rules. When the subscriber's quota gets to the threshold level specified by the prepaid rating and charging server, system sends a new access request message to the server and server updates the subscriber's quota. The charging server is also updated at the end of the call.

ECS supports the following credit control applications for prepaid charging:

- RADIUS Credit Control Application—RADIUS is used as the interface between ECS and the prepaid charging server.
- Diameter Credit Control Application—The Diameter Credit Control Application (DCCA) is used to implement real-time credit control for a variety of services, such as networks access, messaging services, and download services.

To view credit control properties in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS* **> Credit Control**.

Prime Network Vision displays the list of credit control groups configured under the container. You can view the individual credit control group details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Credit Control** > *Credit Control Group*.

You can also view the following details by clicking the respective node under the credit control group:

- Diameter
- Failure Handling
- Pending Traffic Treatment
- Quota
- Server Unreachable Failure Handling

Table 26-31 describes the details available for each credit control group.

Table 26-31 Credit Control Properties in Logical Inventory

Field	Description
Group	Name of the credit control group for the subscriber.
Mode	Prepaid charging application mode, which could be Diameter or Radius.
APN Name to be Included	Type of APN name sent in the credit control application (CCA) message.
Trigger Type	Condition based on which credit reauthorization is triggered from the server.
Diameter MSCC Final Unit Action Terminate	Indicates whether to terminate a PDP session immediately when the Final-Unit-Action (FUA) in a particular multi service credit control (MSCC) is set as Terminate and the quota is exhausted for that service, or to terminate the session after all MSCCs (categories) have used their available quota.
Diameter Peer Select table	
Peer	Primary hostname.
Realm	Realm for the primary host.
Secondary Peer	Secondary hostname.

Table 26-31 Credit Control Properties in Logical Inventory (continued)

Field	Description
Secondary Realm	Realm for the secondary host.
IMSI Range Mode	Mode of peer selection based on IMSI prefix or suffix.
IMSI Start Value	Starting value of the IMSI range for peer selection.
IMSI End Value	Ending value of the IMSI range for peer selection.
Diameter	
End Point Name	Name of the diameter endpoint.
End Point Realm	Realm of the diameter endpoint.
Pending Timeout	Maximum time to wait for response from a diameter peer.
Session Failover	Indicates whether diameter session failover is enabled or not.
Dictionary	Diameter credit control dictionary for the ACS.
Failure Handling	
Initial Request	Failure handling behavior, if failure takes place during initial session establishment. Value could be continue, retry-and-terminate, and terminate.
Update Request	Failure handling behavior, if failure takes place during update request. Value could be continue, retry-and-terminate, and terminate.
Terminate Request	Failure handling behavior, if failure takes place during terminate request. Value could be continue, retry-and-terminate, and terminate.
Pending Traffic Treatment	
Trigger	Indicates whether to allow or drop a trigger while waiting for the credit information from the server. Value could be pass or drop.
Forced Reauth	Indicates whether to allow or drop reauthorization while waiting for the credit information from the server. Value could be pass or drop.
NoQuota	Indicates whether to allow or drop traffic, if there is no quota present. Value could be pass, drop, or buffer.
Quota Exhausted	Indicates whether to allow or drop traffic, if quota is exhausted. Value could be pass, drop, or buffer.
Validity Expired	Indicates whether to allow or drop traffic, if quota validity is expired. Value could be pass or drop.
Quota	
Request Trigger	Action taken on the packet that triggers the credit control application to request quota. Value could be exclude-packet-causing-trigger or include-packet-causing-trigger.
Holding Time	Duration for which ECS can hold the quota before returning to the credit control server.
Validity Time	Lifetime for which subscriber quota retrieved from the billing server is valid.
Time Threshold	Time threshold limit for subscriber quota in the prepaid credit control service.
Units Threshold	Unit threshold limit for subscriber quota in the prepaid credit control service.
Volume Threshold	Volume threshold limit for subscriber quota in the prepaid credit control service.

Table 26-31 Credit Control Properties in Logical Inventory (continued)

Field	Description
Server Unreachable Failure Handling	
Initial Request	Failure handling behavior if server is unreachable during initial session establishment. Value could be continue or terminate.
Update Request	Failure handling behavior if server is unreachable during update request. Value could be continue or terminate.

Viewing Charging Action Properties

Charging Action is an action taken on the incoming data packets once the data packets are treated by the routing and charging rule components. User can configure independent actions such as allow, forward, and block traffic, and bind these actions with other routing and charging rule components.

To view charging action properties in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS*** > Charging Action**.

Prime Network Vision displays the list of charging actions configured under the container as shown. You can view the individual charging action details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Charging Action** > *Charging Action.*

You can also view the following details by clicking the respective node under the Charging Action node:

- Allocation Retention Priority
- Bandwidth
- Flow Action
- QoS
- Video
- Billing Action

Table 26-32 describes the details available for each charging action record.

Table 26-32 Charging Action Properties in Logical Inventory

Field	Description
Name	Name of the charging action.
Content ID	Content ID to use in the generated billing records as well the AVP used by the credit control application.
Service ID	Configured service ID used to associate the charging action in rule definitions configuration.
Charging EDR Name	Name of the EDR format for the billing action in the ACS.

Table 26-32 Charging Action Properties in Logical Inventory (continued)

Field	Description
EGCDRs	Indicates whether eG-CDRs must be generated when the subscriber session ends or an interim trigger condition occurs.
Rf	Indicates whether Rf accounting is enabled or not.
UDRs	Indicates whether UDRs must be generated based on the UDR format declared in the rule base.
Flow Idle Timeout	Maximum duration a flow can remain idle after which the system automatically terminates the flow.
Limit for Flow Type State	Indicates whether the limit for flow type is configured or not.
Limit for Flow Type Value	Maximum number of flows of a particular type.
Limit for Flow Type Action	Action to be taken, if the number of flows exceeds the maximum limit.
IP Type of Service	IP Type of Service (ToS) octets used in the charging action.
Retransmission Count	Indicates whether to count the number of packet retransmissions when the charging action is applied on the incoming data packets.
Content Filtering	Indicates whether content filtering must be applied on the incoming packets or not.
Credit Control	Indicates whether to apply credit control or not.
Credit Rating Group	Coupon ID used in prepaid charging as rating group.
Charge Volume	Method used for charge volume calculation based on the protocol and packet.
Next Hop Forwarding Address	Next hop forwarding address for a charging action.
VLAN ID	VLAN ID configured for the subscriber
Flow Mapping Idle Timeout	Maximum duration, in seconds, a flow can remain idle after which the system automatically terminates the flow.
Allocation Retention Priority	
Priority Level	Priority value that indicates whether to accept or reject a request for establishment or modification of a bearer in a limited resource condition.
Priority Vulnerability Indicator	Defines whether an active bearer can be preempted by a preemption-capable high priority bearer.
Priority Capability Indicator	Defines whether the bearer request can preempt the resources from the Low Priority Pre-empatable Active Bearers.
Bandwidth	
Bandwidth ID	The bandwidth policy ID for the ACS.
Uplink	Indicates whether uplink flow limit is configured for the subscriber or not.
Downlink	Indicates whether downlink flow limit is configured for the subscriber or not.
Charging Action Bandwidth Direction	
Direction	Direction of the packet flow: Uplink or Downlink

Table 26-32 Charging Action Properties in Logical Inventory (continued)

Field	Description
Peak Data Rate	Peak data rate configured for the uplink or downlink packet flow.
Peak Burst Size	Peak burst size allowed for the uplink or downlink packets.
Committed Data Rate	Committed data rate for the uplink or downlink packet flow.
Committed Burst Size	Committed burst size allowed for the uplink or downlink packets.
Exceed Action	Action to take on packets that exceed committed data rate but do not violate the peak data rate.
Violate Action	Action to take on packets that exceed both committed and peak data rates.
Bandwidth Limiting ID	Identifier for bandwidth limiting.
Flow Action	
Redirect URL	Indicates whether packets matched to the rule definition must be redirected to a specified URL or not.
Clear Quota Retry Timer	Indicates whether to reset the CCA quota retry timer for a specific subscriber upon redirection of data packets.
Conditional Redirect	Indicates whether packets matching to a configured user agent must be conditionally redirected to a specified URL.
Discard	Discards packets associated with the charging action.
Random Drop	Indicates whether to degrade voice quality and specify the time interval in seconds at which the voice packets will be dropped.
Readdress	Redirects unknown gateway traffic based on the destination IP address of the packets to known or trusted gateways.
Terminate Flow	Indicates whether to terminate the flow by terminating the TCP connection gracefully between the subscriber and external server.
Terminate Session	Indicates whether to terminate the session.
QoS	
Traffic Class	QoS traffic class for the charging action, which could be background, conversational, interactive, or streaming.
Class Identifier	The QCI value.
Video	
Bit Rate	Bits per second, at which the TCP video flow must be paced during video pacing.
CAE Readdressing	Indicates whether Content Adaptation Engine (CAE) readdressing is enabled, allowing video traffic to be fetched from the CAEs in the CAE group.
Transrating	Indicates whether transrating is enabled or not. Transrating is a mobile video feature that reduces the encoded bit rates by adjusting video encoding.
Target Rate Reduction	Percentage of the input bit rate of a video flow.
Billing Action	
EDR	Name of the EDR format for the billing action in the ACS.
EGCDR	Indicates whether eG-CDRs must be generated when the subscriber session ends or an interim trigger condition occurs.

Table 26-32 Charging Action Properties in Logical Inventory (continued)

Field	Description
Rf	Indicates whether Rf accounting is enabled or not.
UDRs	Indicates whether UDRs must be generated based on the UDR format declared in the rule base.
Radius Accounting Record	Indicates whether radius accounting is enabled or not.

Viewing Rule Definitions

Rule definitions are user-defined expressions, based on protocol fields and protocol states, which define what actions to take when specific field values are true. Each rule definition configuration consists of multiple expressions applicable to any of the fields or states supported by the respective analyzers.

Rule definitions areof the following types:

- Routing—Used to route packets to content analyzers. Routing rule definitions determine which content analyzer to route the packet to when the protocol fields and/or protocol states in the rule definition expression are true. Up to 256 rule definitions can be configured for routing.
- CharginG—Used to specify what action to take based on the analysis done by the content analyzers. Actions can include redirection, charge value, and billing record emission. Up to 2048 charging rule definitions can be configured in the system.
- Post-processing—Used for post-processing purposes. Enables processing of packets even if the rule matching for them has been disabled.
- TPO—Used for Traffic Performance Optimization (TPO) in-line service match-rule and match advertisement features.

To view rule definitions in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Rule Definitions**.

Prime Network Vision displays the list of rule definitions configured under the container. You can view the individual rule definition details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS* **> Rule Definitions** > *Rule Definition.*

Table 26-33 describes the details available for each rule definition.

Table 26-33 Rule Definition Group Properties in Logical Inventory

Field	Description
Name	Name of the rule definition group.
Application Type	Purpose of the rule definition, which could be charging, routing, post-processing, or Traffic Performance Optimization (TPO).
Copy Packet To Log	Indicates whether to copy every packet that matches the rule to a log file.
Tethered Flow Check	Indicates whether tethered flow check if enabled or not. Tethering detection flow check feature enables detection of subscriber data traffic flow originating from PC devices tethered to mobile smart phones, and also provides effective reporting to enable service providers take business decisions on how to manage such usage and to bill subscribers accordingly.
Multiline OR	Indicates whether to apply the OR operator to all lines in a rule definition. This allows a single rule definition to specify multiple URL expressions.
Protocol Configuration	
Protocol	The protocol that this rule definition is applied on.
Fields	Particular protocol field, which is applied on the data packets for inspection. Value could be, host, payload, or domain.
Operator	Logical operator that indicates how to logically match the value in the field analyzed based on the data type.
Value	Value of a particular protocol in a rule definition which has to be applied on the incoming data packets for inspection.

Viewing Rule Definition Groups

A rule definition group enables grouping the rule definitions into categories. A rule definition group may contain optimizable rule definitions. Whether a group is optimized or not is decided on whether all the rule definitions in the group can be optimized. When a new rule definition is added, it is checked if it is included in any rule definition group and whether it needs to be optimized or not.

To view rule definition groups in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Group of Rule Definitions**.

Prime Network Vision displays the list of rule definition groups configured under the container. You can view the individual rule definition group details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS* **> Group of Rule Definitions** > *Rule Definition Group.*

Table 26-33 describes the details available for each rule definition group.

Table 26-34 Rule Definition Group Properties in Logical Inventory

Field	Description
Name	Name of the rule definition group.
Application Type	Purpose of the rule definition group, which could be charging, routing, content filtering, post-processing, or Traffic Performance Optimization (TPO).
Dynamic Command Content Filtering Policy ID	Content filtering policy ID to add or remove dynamic commands from the rule definition group.

Rule Definition Group Commands

The following commands can be launched from the inventory by right-clicking a rule definition group and choosing **Commands > Configuration** or **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-35 Rule Definition Group Commands

Command Type	Command	Inputs Required and Notes
Configuration	**Delete Group of RuleDefs**	Click **Execute Now** to delete the rule definition group.
Show	**Show Group of RuleDefs**	Click **Execute Now** to display the group of rule definitions.

Viewing Rule Base for the Charging Action

A rule base is a collection of rule definitions and their associated billing policy. The rule base determines the action to be taken when a rule is matched. A maximum of 512 rule bases can be specified in the ECS service. It is possible to define a rule definition with different actions.

Rule bases can also be used to apply the same rule definitions for several subscribers, which eliminate the need to have unique rule definition for each subscriber. We can set priority, default bandwidth policy, type of billing for subscriber sessions, for a rule definition/ group of rule definitions in the rule base. Additionally we can configure content based billing and firewall/NAT constituent to rule base.

To view a rule base in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Rulebase Container**.

Prime Network Vision displays the list of rule bases configured under the container. You can view the individual rule base details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >***ACS* **> Rulebase Container** > *Rule Base.*

Table 26-36 describes the details available for each rule base record.

Table 26-36 Rule Base Properties in Logical Inventory

Field	Description
Rulebase Name	Name of the rule base.
Flow Any Error Charging Action	Charging action to be used for packets dropped due to any error conditions after data session is created.
Limit for Total Flows	Maximum number of simultaneous uplink and downlink packet flows.
Limit for TCP Flows	Maximum number simultaneous TCP packet flows per subscriber or APN allowed for a rulebase.
Limit for Non TCP Flows	Maximum number simultaneous non-TCP packet flows per subscriber or APN allowed for a rulebase.
Charging Rule Optimization	Internal optimization level to use, for improved performance, when evaluating each instance of the action.
QoS Renegotiation Timeout	Timeout value after which QoS renegotiation is performed.
RTP Dynamic Routing	Indicates whether the Real Time Streaming Protocol (RTSP) and SDP analyzers are enabled to detect the start/stop of RTP (a Transport Protocol for Real-Time Applications) and RTP Control Protocol (RCP) flows.
Ignore Port Number In Application Header	Indicates whether to consider or ignore the port number embedded in the application.
Delayed Charging	Indicates how to charge for the control traffic associated with an application.
XHeader Certificate Name	Name of the encryption certificate to be used for x-header encryption.
XHeader Reencryption Period	Indicates how often to regenerate the encryption key for x-header encryption.
Default Bandwidth Policy	Name of the default bandwidth policy per subscriber.
P2P Dynamic Routing	Indicates whether P2P analyzer is enabled to detect the P2P applications flow configured in ACS.
Fair Usage Waiver Percentage	Waiver percent on top of the average available memory credits per session for the Fair Usage feature of active charging.
URL Blacklisting Action	Configured URL blacklisting action to take when the URL matches ones of the blacklisted URLs.
URL Blacklisting Content ID	Specific content ID for which URL blacklisting is enabled in the rulebase.
Charging Action Priorities tab	Charging rule definitions and their priorities in the rulebase.

Table 26-36 Rule Base Properties in Logical Inventory (continued)

Field	Description
Routing Action Priorities tab	Routing actions and their priorities in the rulebase.
Post Processing Action Priorities	Post-processing actions and their priorities in the rulebase.

Viewing Bandwidth Policies

Bandwidth policies are helpful in applying rate limit to potentially bandwidth intensive and service disruptive applications. Using this policy, the operator can police and prioritize subscribers' traffic to ensure that no single or group of subscribers' traffic negatively impacts another subscribers' traffic. Each policy will be identified by a unique ID, which will be associated to a particular group. Bandwidth policies are used to control the direction (uplink/downlink) of bandwidth, peak data rate, and peak burst size, and the actions that need to be taken on violation, if the bandwidth exceeds the burst size and data rate.

To view bandwidth policy in logical inventory:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Bandwidth Policy Container**.

Prime Network Vision displays the list of bandwidth policies configured under the container. You can view the individual bandwidth policy details from the table on the right pane or by choosing **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Bandwidth Policy Container** > *Bandwidth Policy*.

Table 26-37 describes the details available for each bandwidth policy.

Table 26-37 Bandwidth Policy Properties in Logical Inventory

Field	Description
Name	Name of the bandwidth policy configured.
Total Bandwidth ID Configured	Total number of bandwidth IDs configured.
Total Group Limit Configured	Total number of bandwidth group limits configured.
Flow Limit for Bandwidth ID and Group ID Associations and Group ID tables	Holds all bandwidth IDs and group IDs of the bandwidth policy.

Viewing Fair Usage Properties

To view fair usage properties configured for the ACS:

Step 1 Right-click the required device in Prime Network Vision and choose **Inventory**.

Step 2 In the logical inventory window, choose **Logical Inventory > *local* > Mobile > Active Charging Services >** *ACS* **> Fair Usage**.

Prime Network Vision displays the details on the content pane.

Table 26-38 describes the fair usage properties.

Table 26-38 Fair Usage Properties in Logical Inventory

Field	Description
CPU Threshold Percent	Percentage of system CPU resources that the dynamic inline transrating feature is allowed to use.
Threshold Percent	Percentage of system resources that the dynamic inline transrating feature is allowed to use.
Deactivate Margin Percent	Fair usage deactivate margin, below which monitor action is disabled.

ACS Commands

The following commands can be launched from the inventory by right-clicking an ACS and choosing **Commands > Configuration** or **Commands > Show.** Before executing any commands, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-39 ACS Commands

Command Type	Command	Inputs Required and Notes
Configuration	**Create Group of Ruledefs**	Group of Ruledefs Name, Group of Ruledefs Configuration
	Create Rulebase	Rulebase Name, Rulebase Configuration
	Create Ruledef	Ruledef Name, Ruledef Configuration
	Delete Active Charging Service	Click **Execute Now** to delete the ACS.
	Modify Active Charging Service	Access Ruledef, Ruledef, Group of Ruledefs, Rulebase
	Create Access Ruledef (*ACS* **> Commands > Configuration > Access Ruledef**	Access Ruledef Name, Access Ruledef Configuration
	Delete Access Ruledef (*ACS* **> Commands > Configuration > Access Ruledef**	Access Ruledef Name
Show	**Show Access Ruledef**	Access Ruledef Name

Using Commands to Configure and View Mobile Technologies under a Context

The following commands can be used to configure and view mobile technologies under a particular context in the Prime Network Vision. These commands can be launched from the logical inventory by choosing the *Context* **> Commands > Configuration** or *Context* **> Commands > Show.** Before executing any command, you can preview them and view the results. If desired, you can also schedule the commands. To find out if a device supports these commands, see the *Cisco Prime Network 3.10 Supported Cisco VNEs*.

Note You might be prompted to enter your device access credentials while executing a command. Once you have entered them, these credentials will be used for every subsequent execution of a command in the same GUI client session. If you want to change the credentials, click **Edit Credentials**. Edit Credentials button will not be available for SNMP commands or if the command is scheduled for a later time.

Table 26-40 Configuration Commands

Command	Inputs Required and Notes
Configure BFD	• Protocol • Echo
Create AAA Group	Create Group Name tab: • Group Name
	Diameter Authentication/Diameter Accounting tab: • Dictionary • End Point • Max Retries • Request Timeout

Table 26-40 Configuration Commands (continued)

Command	Inputs Required and Notes
Create APN	General tab: • APN Name • Selection Mode • Accounting Mode • Authentication Type • Authentication Protocol Priority • Bearer Control Mode • Home-Agent IP Address (IPV4)
	PDP/Context tab: • Primary Contexts • Total Contexts • PDP Type • Destination Context Name
	Charging Characteristics tab: • CC SGSN Type • Home Behavior • Home Profile Bit • Roaming Behavior • Roaming Profile Bit • Visiting Behavior • Visiting Profile Bit
	Timeout tab: • TimeOut Type • Absolute Duration • Emergency Inactivity Duration • Idle Duration • Long Duration • Long Duration Inactivity Time • Long Duration Action Type • Long Duration Disconnection Type

Table 26-40 Configuration Commands (continued)

Command	Inputs Required and Notes
	IP tab: • IP Address Allocation Method • DHCP Proxy : Allow Deferred • DHCP Proxy : Allow User Specified • DHCP Proxy : Prefer DHCP Options • DHCP Relay : Allow User Specified • Local : Allow Deferred • Local : Allow User Specified • No Dynamic : Allow Deferred • No Dynamic : Allow User Specified • IP Pool Name
	IPV6 tab: • IPV6 Pool Name • IPV6 DNS Type • IPV6 DNS Address (IPV6) • IPV6 Advertisement Interval • IPV6 Number of Advertisement
	AAA/DNS tab: • AAA Type • AAA Group Name • AAA Secondary Group Name • DNS Type • DNS IP Address (IPV4)
	GTPP Group tab: • GTPP Group Name • Accounting Context Name
	Miscellaneous tab: • Source Violation Type • Drop Limit • Restriction Value
Create Active Charging Service	Active Charging Service Name

Table 26-40 Configuration Commands (continued)

Command	Inputs Required and Notes
Create EGTP	General tab: • Service Name • GTPU Service • Interface • Validation Mode
	GTPC Attributes tab: • Retransmission Timeout • Ech Retransmission Timeout • Maximum Retries • Echo Interval • Dynamic Echo Timer • Smooth Factor • IP Qos DSCP • Bind Address Type • Bind Address • Path Failure Detection Policy
Create GGSN	General tab: • Service Name • Accounting Context Name • CC Behavior ID • GTPU Service Name • P-GW Service Name • Port Number • PLMN Unlisted Value
	Timing Interval tab: • Retransmission Count • Echo Retransmission Count • Setup Timeout • Echo Interval • Dynamic • Smooth Factor • Guard Interval • Max Retransmission

Table 26-40 Configuration Commands (continued)

Command	Inputs Required and Notes
	Bind Address tab: • Bind Address (IPV4) • PPP PDP Context • Total PDP Context
Create GTPP	General tab: • Group Name • Dictionary • Transport Layer Protocols • Accounting Type • RAT Generation Type
	Charging Address/CDR tab: • Charging Agent Address (IPV4) • Charging Agent Port • Max CDRS Number • Max CDRS Wait Time (Sec)
Create GTPU	• GTPU Name • Retransmission Timeout • Echo Retransmission Timeout • Maximum Retransmission • Echo Interval
Create IP Pool	• Pool Name • IP Address (IPV4) • Network Bits • Subnet Mask (IPV4) • Pool Type • Pool Priority • Group Name • VRF Name

Table 26-40 Configuration Commands (continued)

Command	Inputs Required and Notes
Create P-GW	General tab: • P-GW Service Name • Associate Service Type • Associate Service Name • QCI-QoS Mapping Name • New Call Policy • Session Delete Delay • Session Delete Delay Timeout
	FQDN tab: • FQDN Host Name • Realm Name
Create QCI-QOS Mapping	Name
Create S-GW	• S-GW Service Name • Accounting Mode • Accounting Context Name • Accounting GTPP Group Name • QCI-QOS Mapping Name • Egress Protocol • Egress Context Name • EGTP Service Name • MAG Service Name • Ingress EGTP Service Name • Accounting Policy Name • IMS Authorization Service • New Call Policy
Create VRF	General tab: • VRF Name • Router BGP
	Route Distinguisher tab: • Route Distinguisher Type • IP (IPV4) • ASN • RT

Table 26-40 Configuration Commands (continued)

Command	Inputs Required and Notes
	Route Target tab: • IP Import (IPV4) • ASN Import • RT Import • IP Export (IPV4) • ASN Export • RT Export • IP Both (IPV4) • ASN Both • RT Both
Delete Context	NA
Modify License	License Key

The following commands can be launched from the logical inventory by choosing *Context* **> Commands > Configuration > DHCP.**

Command	Inputs Required and Notes
Create DHCP	General tab: • Service Name • Bind Address (IPV4) • Nexthop IP (IPV4/IPV6) • Server Address (IPV4) • Server Algorithm
	Timing Interval tab: • Retransmission Timeout • Max Retransmission • Lease Min Value • Lease Max Value • DeadTime
Delete DHCP	Service Name

Command	Inputs Required and Notes
Modify DHCP	General tab: • Service Name • Bind Address (IPV4) • Nexthop IP (IPV4/IPV6) • Server Address (IPV4) • Server Algorithm
	Timing Interval tab: • Retransmission Timeout • Max Retransmission • Lease Min Value • Lease Max Value • DeadTime

The following commands can be launched from the logical inventory by choosing *Context* **> Commands > Configuration > HA SPI List.**

Command	Inputs Required and Notes
Create HA SPI List	• HP SPI List Name • Remote Address (IPV4 and IVP6). • Remote Address Prefix • SPI Number • Encrypted • Secret Value • Hash Algorithm • Description
Delete HA SPI List	HA SPI List Name
Modify HA SPI List	• HA SPI List Name • Delete SPI Entry • Remote Address (IPV4/IPV6) • Remote Address Prefix • SPI Number • Encrypted • Secret Value • Hash Algorithm • Description

The following commands can be launched from the logical inventory by choosing *Context* **> Commands > Configuration > HA Service.**

Command	Inputs Required and Notes
Create HA Service	• Service Name • Local Port • Authentication • Fa-Ha-SPI Configuration • Mn-Ha-SPI Configuration • Lifetime • Binding • Bind Address (IPV4) • Max-Subscribers
Delete HA Service	Service Name
Modify HA Service	• Service Name • Local Port • Authentication • Fa-Ha-SPI Configuration • Mn-Ha-SPI Configuration • Delete Lifetime • Lifetime • Binding • Delete Bind Address • Bind Address (IPV4) • Max-Subscribers

The following commands can be launched from the logical inventory by choosing Context **> Commands > Configuration** > **PDP Context.**

Command	Inputs Required and Notes
Create Network Requested PDP Context	• IP Address (IPV4/IPV6) • GSN Map IpAddress (IPV4/IPV6) • Destination Context • APN Name • IMS Identifier
Delete Network Requested PDP Context	• IP Address (IPV4/IPV6) • Destination Context

The following commands can be launched from the logical inventory by choosing Context **> Commands > Configuration** > **Proxy DNS.**

Command	Inputs Required and Notes
Create Proxy DNS	• Proxy DNS Intercept List Name • Pass Through (IPV4/IPV6) • Pass Through Prefix • Redirect (IPV4/IPV6) • Redirect Prefix • Primary DNS (IPV4) • Secondary DNS (IPV4)
Delete Proxy DNS	Proxy DNS Intercept List Name
Modify Proxy DNS	• Proxy DNS Intercept List Name • Delete Pass Through • Pass Through (IPV4/IPV6) • Pass Through Prefix • Delete Redirect • Redirect (IPV4/IPV6) • Redirect Prefix • Primary DNS (IPV4) • Secondary DNS (IPV4)

The following commands can be launched from the logical inventory by choosing Context **> Commands > Configuration > Route Map and Route Access List.**

Command	Inputs Required and Notes
Create Route Access List	• Route Access List Type • Route Access List Identifier • Operation Type • Network Parameter • Network Address (IPV4) • Network Mask (IPV4) • Host Network Address (IPV4) • Mask Parameter • Mask (IPV4) • Wildcard Mask (IPV4) • Host Mask (IPV4) • Exact Match
Create Route Map	• Route Map Name • Operation • Sequence Number • Route Map Configuration
Delete Route Access List	• Route Access List Type • Route Access List Identifier • Operation Type • Network Parameter • Network Address (IPV4) • Network Mask (IPV4) • Host Network Address (IPV4) • Mask Parameter • Mask (IPV4) • Wildcard Mask (IPV4) • Host Mask (IPV4) • Exact Match
Delete Route Map	Route Map Name

Command	Inputs Required and Notes
Modify Route Access List	• Route Access List Type • Route Access List Identifier • Operation Type • Network Parameter • Network Address (IPV4) • Network Mask (IPV4) • Host Network Address (IPV4) • Mask Parameter • Mask (IPV4) • Wildcard Mask (IPV4) • Host Mask (IPV4) • Exact Match
Modify Route Map	• Route Map Name • Operation • Sequence Number • Route Map Configuration

The following commands can be launched from the logical inventory by choosing Context **> Commands > Configuration > Subscriber.**

Command	Inputs Required and Notes
Create Subscriber	Create Subscriber tab: • Subscriber Name • Accounting Mode • IP Context Name • Hide Service Address • IP Address (IPV4) • Allocation Method • IP Address Pool Name • Proxy DNS Intercept List Name • Proxy DNS Subscriber Address As Source
	Subscriber Configuration tab: • Subscriber Configuration
Delete Subscriber	Subscriber Name

Command	Inputs Required and Notes
Modify Subscriber	Modify Subscriber tab: • Subscriber Name • Accounting Mode • Delete IP Context • IP Context Name • Hide Service Address • Delete IP Address • IP Address (IPV4) • Allocation Method • Delete IP Address Pool • IP Address Pool Name • Delete Proxy DNS • Proxy DNS Intercept List Name • Proxy DNS Subscriber Address As Source
	Subscriber Configuration tab: • Subscriber Configuration

The following commands can be launched from the logical inventory by choosing the *Context* **> Commands > Show.**

Table 26-41 Show Commands

Command	Inputs Required and Notes
Show APN	APN Name
Show DHCP	DHCP Name
Show EGTP	Service Name
Show HA SPI List	HA SPI List Name
Show HA Service	Service Name
Show IP Pool	Pool Name
Show License	Show License
Show Route Access List	Route Access List Identifier
Show Route Map	Route Map Name
Show Subscriber	Subscriber Name