Gx Diameter Monitoring and Reporting

This module describes how to configure an Internet Service Provider to monitor the data utilized by subscribers and enforce restrictions on the amount of data utilized and bandwidth consumed. This feature runs on a repeated authorization model and helps enforce quota restrictions on the volume of traffic flows in the iEdge architecture framework. Monitoring and reporting can be requested by the PCRF (Policy Control Rules Function) with a CCA (Credit Control Answer) or RAR (Re-Authorization Request) message for an individual PCC (Policy Control and Charging) rule or for all rules activated during a subscriber session

Prerequisites for Gx Diameter Monitoring and Reporting

- Rule based monitoring must be installed at the time of rule installation
- The user must have knowledge of configuring Diameter applications

Restrictions for Gx Diameter Monitoring and Reporting

- GX Interface is supported only for IPoE Sessions
- Cisco IOS XR Everest 16.6.1 release supports monitoring of traffic flows based on the volume of data consumed. Monitoring of traffic flows based on the time utilized for a session is not supported in this release.
- This features works by reporting accumulated usage based on last reported data using a CCR message. If PCRF updates the quota before actual exhaustion of quota, ISG triggers a CCR-U (Credit Control Request- Update) immediately if the newly downloaded slice of quota has already exceeded the limit.

- It is not possible to use the same Monitoring-Key charging rule definition for session-level and rule-level configuration.
- Modification of session-level monitoring key is possible only after disabling the existing monitoring instance

Information About Gx Diameter Monitoring and Reporting

Overview of Usage and Report Monitoring

This module describes how to configure an Internet Service Provider to monitor the data traffic utilized by subscribers and enforce restrictions on the amount of data utilized and bandwidth consumed. This feature runs on a repeated authorization model and helps enforce quota restrictions on the volume of traffic flows in the iEdge architecture framework. Monitoring and reporting can be requested by the PCRF (Policy Control Rules Function) with a CCA (Credit Control Answer) or RAR (Re-Authorization Request) message for an individual PCC (Policy Control and Charging) rule or all rules activated during a session.

The counters (octets/bytes) consumed by a subscriber in Subscriber Gateway (ISG) are monitored and reported back to the Diameter server. The monitoring criteria is defined and controlled by the Diameter server. You can use Monitoring-Key and Granted-Service-Unit AVP (Attribute Value Pair) to monitor all the sessions for a subscriber or monitor specific traffic flows in a subscriber session. By monitoring specific traffic flows, you can either exclude traffic for a specific session or monitor a combination of one or more traffic flows for a session

The ISG triggers monitoring of usage in the following scenarios:

- The downloaded prepaid quota is exhausted
- A RAR message is sent by PCRF
- All the services associated with the Monitoring-Key charging rule definition are removed
- When the subscriber session is terminated
- Monitoring is specifically disabled by PCRF by setting Usage-Monitoring-Support AVP to USAGE_MONITORING_DISABLED

The ISG keeps track of the volume usage from the moment monitoring is enabled and resets the counters after reporting the existing usage. For example, if the user is allocated 500 MB, 200 MB is downloaded at start of the session. After reporting that 200 MB is consumed, the counter is reset to zero.

Benefits

- Provides the flexibility to monitor prepaid or postpaid traffic flows. This flexibility of configuration allows you to cover monitoring and reporting for varied customer needs
- Configure rules to monitor all the traffic of a subscriber session or monitor specific traffic flows in a subscriber session. You can also configure a combination of rules that will help you monitor varied usage patterns of the subscribe
- Utilize predefined ISG redirection policies to redirect the user to a portal where the user can replenish the quota without being disconnected from the service.

Types of Reporting and Monitoring

The Monitoring and Reporting feature is supported in two models:

- **Prepaid** - In this scenario, information about quota allocated is sent to ISG. Monitoring and reporting is based on this quota. Monitoring of prepaid quota can be performed in the following scenarios:
  - Prepaid at Session Level - Quota is allocated for an entire subscriber session.
  - Prepaid at Flow Level - Quota is allocated for only a specific traffic flow in a subscriber session.
  - Prepaid at Session Level excluding some flows - Quota is allocated for an entire subscriber session except for a specific traffic flow in a session.
  - Prepaid at Flow Level with multiple flows - Quota is allocated for multiple traffic flows in a subscriber session.

  In all prepaid scenarios, the information in Granted-Service-Unit AVP is included in the Usage-Monitoring-Information AVP. Monitoring and reporting of prepaid quota automatically occur on the following triggers:
  - The subscriber session ends.
  - All the rules associated with the Monitoring-Key charging rule definition are removed.
  - A RAR message is sent to PCRF
  - The accumulated counters exceed the prepaid quota allocated

  Monitoring by PCRF can be disabled by setting Usage-Monitoring-Support AVP to USAGE_MONITORING_DISABLED.

- **Postpaid** - In this scenario no quota is provided, but data usage is monitored and reported to PCRF, when queried. Monitoring of postpaid can be performed in the following scenarios:
  - Postpaid at Session Level - Monitoring is done for a subscriber session.
  - Post-Paid at Flow Level - Monitoring is done for a specific traffic flow in a subscriber session.
  - Post-Paid at Session Level excluding some flows - Monitoring is done for a subscriber session excluding specific traffic flows.
  - Post-Paid at Flow Level with Multiple flows - Monitoring is done for one or more traffic flows in a subscriber session

  In all Post-Paid scenarios the information on Granted-Service-Unit AVP is not included in Usage-Monitoring-Information AVP. Monitoring and reporting of postpaid session occurs on the following triggers.
  - The subscriber session ends.
  - All the rules associated with the Monitoring-Key charging rule definition are removed.
  - A RAR message is sent to PCRF.
  - Monitoring is disabled by PCRF.

Quota and Threshold

The Granted-Service-Unit AVP contains the following parameters:

- CC-Total-Octets --- Total volume
- CC-Input-Octets --- Uplink volume
- CC-Output-Octets --- Downlink volume
- CC-Input-Octets and CC-Output-Octets --- Uplink and Downlink Volume

Any of the above parameters retrieved from Granted-Service-Unit AVP is termed as Quota.

Levels of Monitoring

Monitoring and reporting of subscriber session usage can be performed at the following levels:

- **Session Level**
  - All traffic flows for a subscriber session
  - All traffic flows for a subscriber session excluding specific traffic flows
- **PCC Rule Level**
  - All traffic flows are monitored for a single PCC Rule
  - All traffic flows are monitored for multiple PCC Rules

Session Level Monitoring or Rule Level Monitoring

Monitoring of a session based on a specific traffic flow can be configured using rules. To enable monitoring of traffic flows using rules, set Usage-Monitoring-Level AVP with RULE_LEVEL (1). You can associate one or more rules with the M onitoring- Key parameter .

To enable session level monitoring, set Usage-Monitoring-Level AVP to value SESSION_LEVEL (0). Monitoring of traffic flows in a session can be activated either when the session loads or when the session is in progress.

Note Monitoring at a RULE level can be enabled only at the time when the rule is installed. It is not possible to enable a rule after the rule installation is done.

Supported AVP for Gx Diameter on ISG

Figure 1: Supported AVP Pair

AVP ID	Name	Type	CCR I	CCR U	CCR T	CCA I	CCA U	CCA T	RAR	RAA
1001	Charging-Rule-Install	Grouped	0	0	0	0-n	0-n	0	0-n	0
2828	-Monitoring-Flags	Unsigned32	0	0	0	0-1	0-1	0	0-1	0
1067	Usage-Monitoring-Information	Grouped	0	0-n	0-n	0-n	0-n	0	0-n	0
1066	• Monitoring-Key	OctetString	-	1	1	1	1	0	1	0
431	• Granted-Service-Unit	Grouped	-	-	-	0-1	0-1	0	0-1	0
421	- CC-Total-Octets	Unsigned64	-	-	-	0-1	0-1	0	0-1	0
412	- CC-Input-Octets	Unsigned64	-	-	-	0-1	0-1	0	0-1	0
414	- CC-Output-Octets	Unsigned64	-	-	-	0-1	0-1	0	0-1	0
446	• Used-Service-Unit	Grouped	0	0-1	0-1	-	-	-	-	0
421	- CC-Total-Octets	Unsigned64	0	0-1	0-1	-	-	-	-	0
412	- CC-Input-Octets	Unsigned64	0	0-1	0-1	-	-	-	-	0
414	- CC-Output-Octets	Unsigned64	0	0-1	0-1	-	-	-	-	0
1068	• Usage-Monitoring-Level	Enumerated	-	-	-	0-1	0-1	0	0-1	0
1069	• Usage-Monitoring-Report	Enumerated	-	-	-	0-1	0-1	0	0-1	0
1070	• Usage-Monitoring-Support	Enumerated	-	-	-	0-1	0-1	0	0-1	0

366725

How to Configure Gx Diameter Monitoring and Reporting

Enable Diameter Configuration

Configure Diameter base configuration with peer details like PCRF IP address and port

To enable diameter configuration:

```
aaa new-model
!
diameter timer watchdog 300
diameter redundancy
diameter origin realm cisco.com
diameter origin host isg-pcef1
diameter source interface GigabitEthernet0/0/0
diameter gx retransmit 3
diameter gx tx-timer 15
!
diameter peer PCRF
 address ipv4 209.165.200.225
 transport tcp port 3868
 source interface GigabitEthernet0/0/0
 timer connection 20
 timer watchdog 100
 timer transaction 20
```

Verifying Diameter Configuration

Use **show diameter peer**command to check for Diameter server connection status. If diameter connection is up and running, the **Peer connection status** field will have value Open. The status Closed indicates that the Diameter server is not functional.

```
Device# show diameter peer PCRF

Peer information for pcrf2
------------------------------
Peer name : PCRF
Peer type : undefined
Peer IP address : 209.165.200.225
Peer transport protocol : TCP
Peer listening port : 3868
Peer security protocol : IPSEC
Peer connection timer value : 10 seconds
Peer watchdog timer value : 300 seconds
Peer transaction timer value : 10 seconds
Peer VRF name :
Peer connected interface : GigabitEthernet0/0/0
Peer destination realm :
Peer destination host name :
Peer connection status : Open


       Peer Statistics
---------------------------------
            IN     /    OUT
---------------------------------
ASR          0             0
ASA          0             0
ACR          0             0
ACA          0             0
CER          0             9
CEA          9             0
DWR          0          5968
DWA       5966             0
DPR          0             2
DPA          2             0
RAR          0             0
RAA          0             0
STR          0             0
STA          0             0

Prot. Errs Sent  :        0     Prot. Errs Rcvd  :           0
Trans. Errs Sent :        0     Trans. Errs Rcvd :           0
Perm. Errs Sent  :        0     Perm. Errs Rcvd  :           0
Conn. Down Errs  :
```

Enable AAA Configuration

Configure AAA authorization method-lists. Authorization method-list is configured with details of the Diameter server

```
aaa new-model
!
aaa authorization policy-if AUTH group SERVER_GROUP1
aaa authorization subscriber-service default local
!
```

```
aaa group server diameter SERVER_GROUP1
    server name PCRF
```

Verifying AAA Configuration

Use show running-config aaa command to display the aaa and diameter configurations.

```
Device##show running-config aaa
aaa authorization subscriber-service default local
aaa authorization policy-if AUTH group SERVER_GROUP1
!
diameter redundancy
diameter origin realm cisco.com
diameter origin host isg-pcef1
diameter source interface GigabitEthernet0/0/0
diameter timer watchdog 300
diameter gx retransmit 3
diameter gx tx-timer 15
!
diameter peer PCRF
 address ipv4 209.165.200.225
 timer connection 20
 timer watchdog 100
 timer transaction 20
 source interface GigabitEthernet0/0/0
!
aaa group server diameter SERVER_GROUP1
server name PCRF

Conn. Down Errs  :
```

Enable ISG Services

Configure the ISG Service with details of network type and initiator

```
ip access-list extended drl_in
 permit ip any any
!
ip access-list extended drl_out
 permit ip any any
!
   class-map type traffic match-any DRL
    match access-group output name drl_out
    match access-group input name drl_in
!
   policy-map type service DRL_TC
    100 class type traffic DRL
    gx-monitoring-key MK1
    police input 20000 50000 70000
    police output 8000 1000 1000
```

Create ISG Control Policy and Associate Policy to Access Interface

Configure the ISG control policy using the following configuration:

```
policy-map type control GX_TEST
 class type control always event session-start
  10 collect identifier source-ip-address
  20 authorize aaa list AUTH identifier <mac-address/source-ip-address/nas-identifier>
```

Associate ISG control policy to access interface

```
interface GigabitEthernet0/1
 ip address 10.0.0.1 255.255.255.0
 service-policy type control GX_TEST
 ip subscriber l2-connected
  initiator unclassified mac
  initiator dhcp
```

Configuration Examples on Using Usage-Monitoring-Information AVP

Sample Usage-Monitoring-Information AVP Configuration for Session -Level Traffic Flow

Example: Configuration for Session Level Traffic Flow

```
Usage-Monitoring-Information {
  Monitoring-Key = “Post-Session”
  Usage-Monitoring-Level = “Session-Level”
}
```

Sample Usage-Monitoring-Information AVP Configuration for Monitoring Rule-Level Traffic Flow

Example: Configuration for Monitoring Rule Level Traffic Flow

```
Usage-Monitoring-Information {
  Monitoring-Key = “Post-Rule”
  Usage-Monitoring-Level = “Rule-Level”
}
Charging-Rule-Definition {
  Charging-Rule-Name = “Rule1”
  Monitoring-Key = “Post-Rule”
}
```

Sample Usage-Monitoring-Information AVP Configuration for Monitoring Multiple Traffic Flows

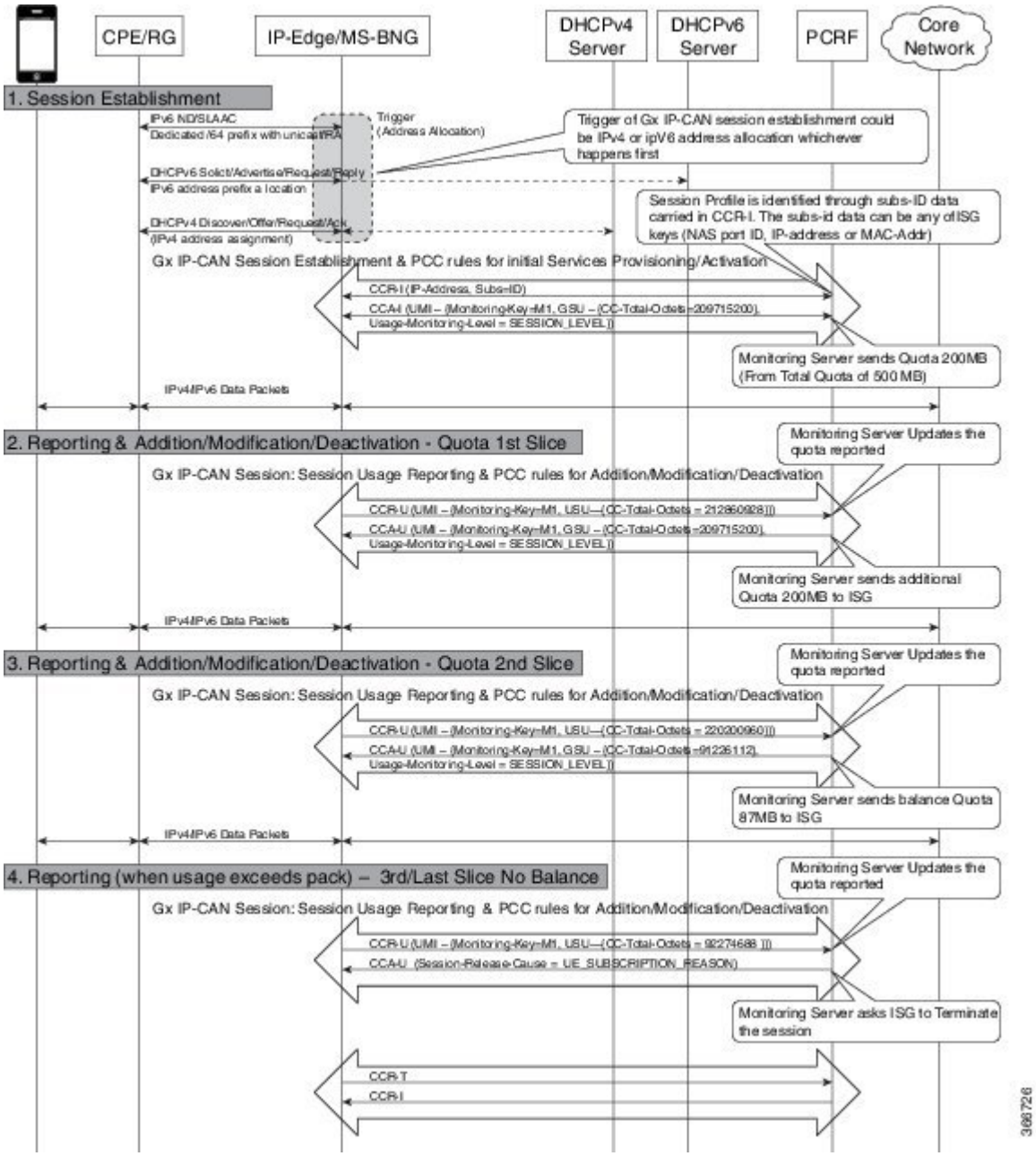
Example: Configuration for Monitoring Multiple Traffic Flows

```
Usage-Monitoring-Information {
```

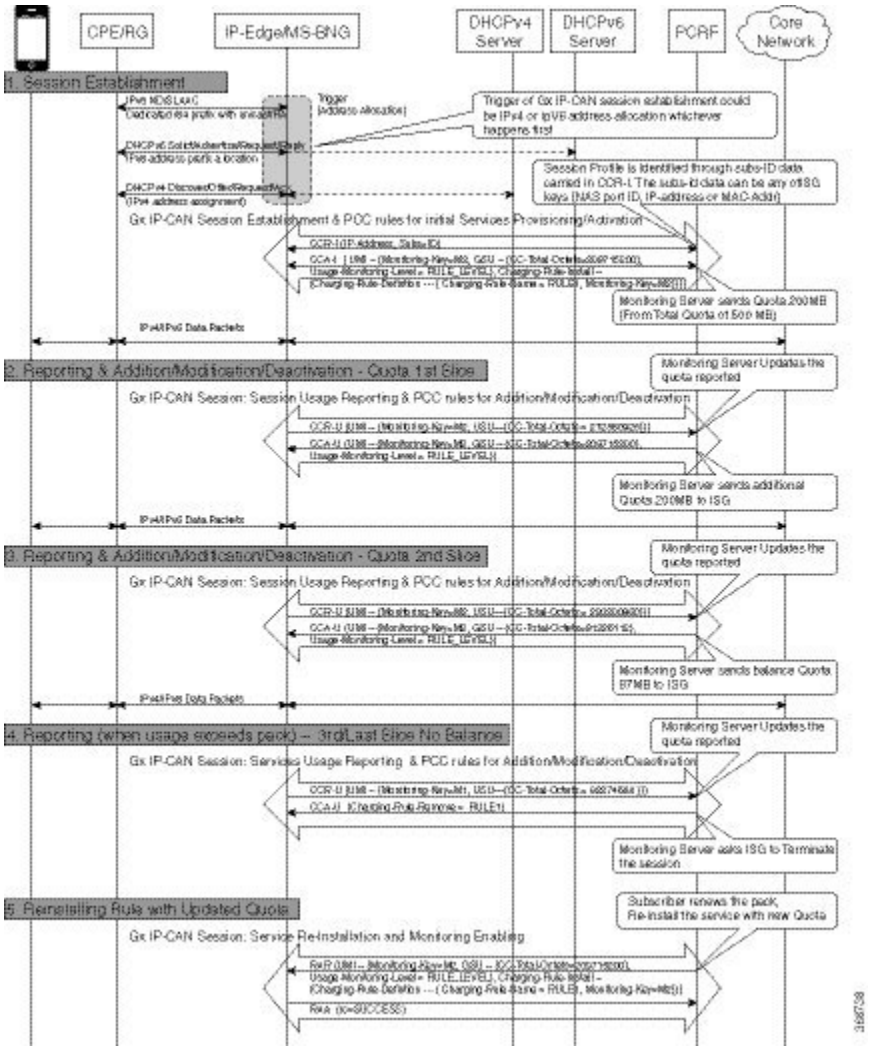
```
  Monitoring-Key = "Post-Session"
  Usage-Monitoring-Level = "Session-Level"
}
Charging-Rule-Install {
  Charging-Rule-Name = "Rule1"
  Charging-Rule-Name = "Rule2"}
```

Monitoring and Reporting Call Flows

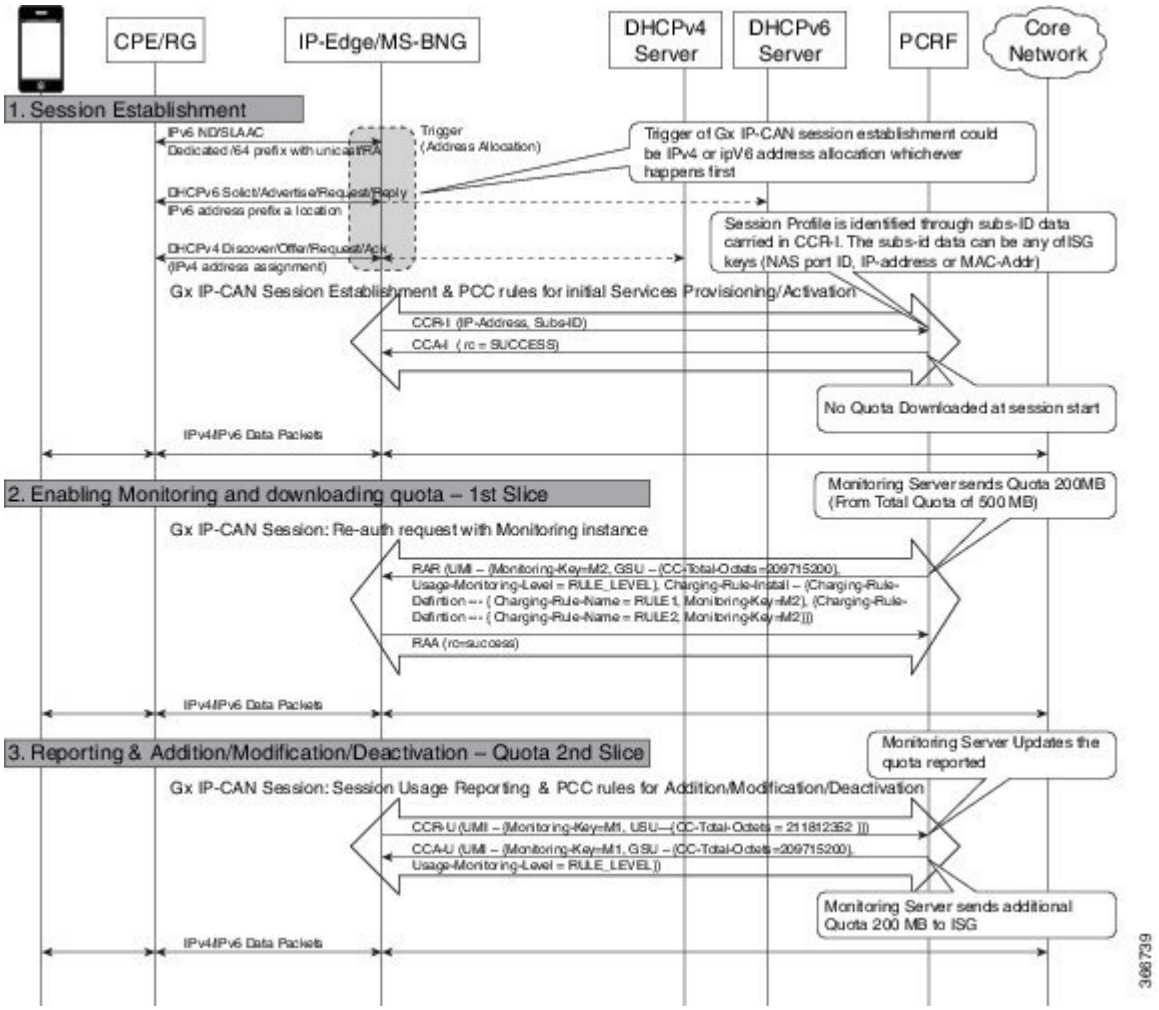
Monitoring Using CCR-When a Session is Loaded



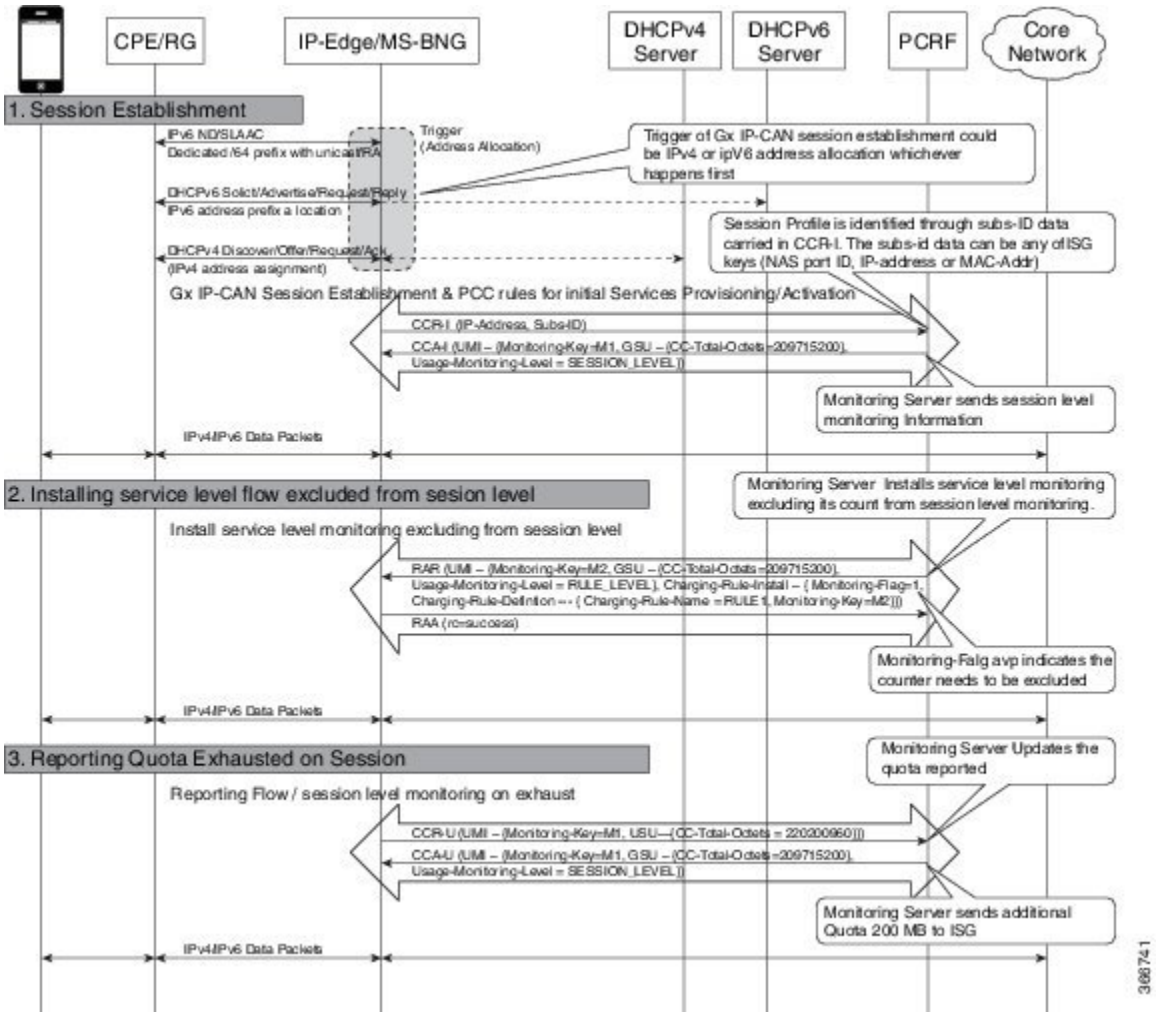
Enabling Service-Level Monitoring and Removing the Rule on Exhaust of Quota



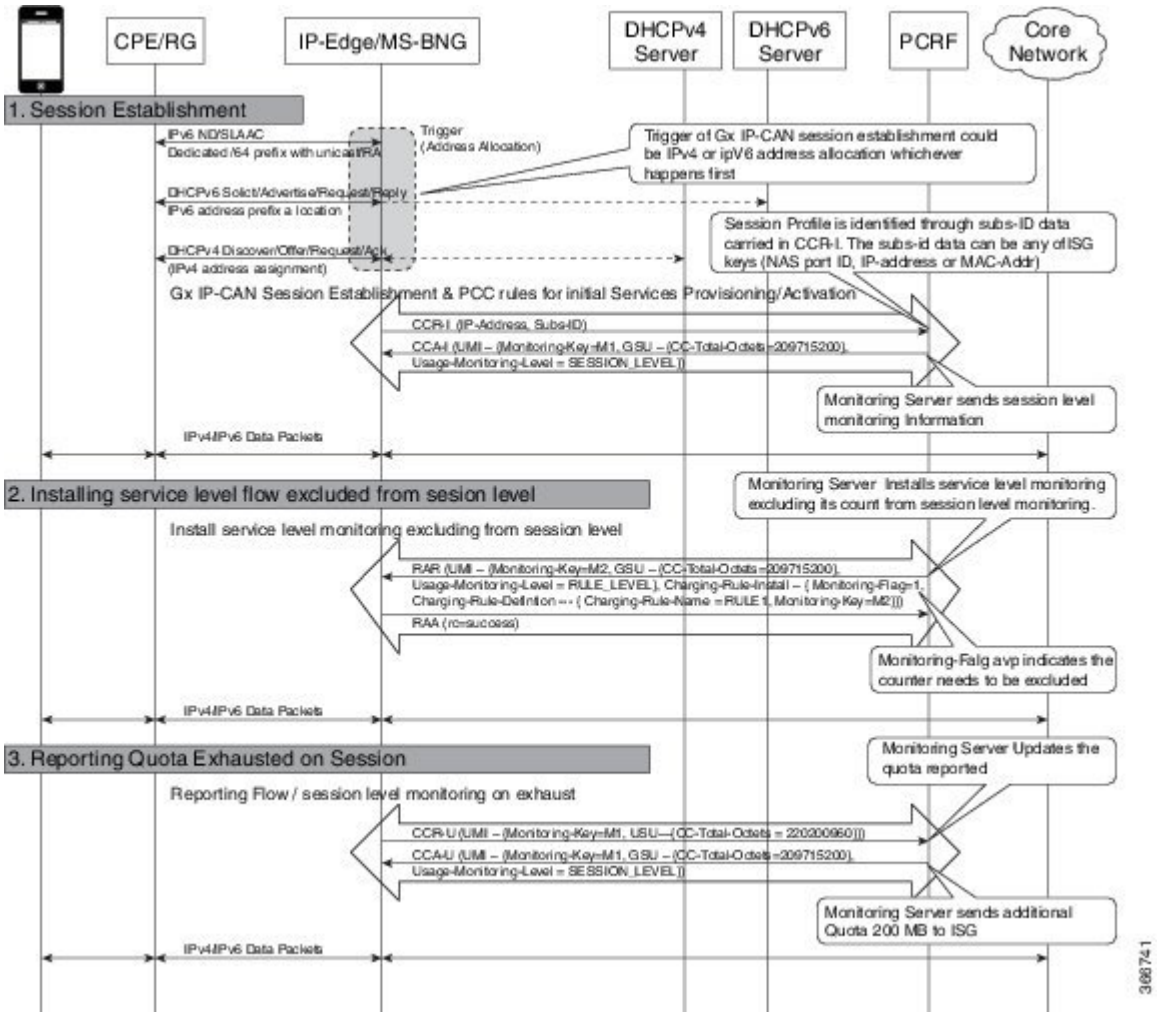
Enabling Monitoring for Multiple Services



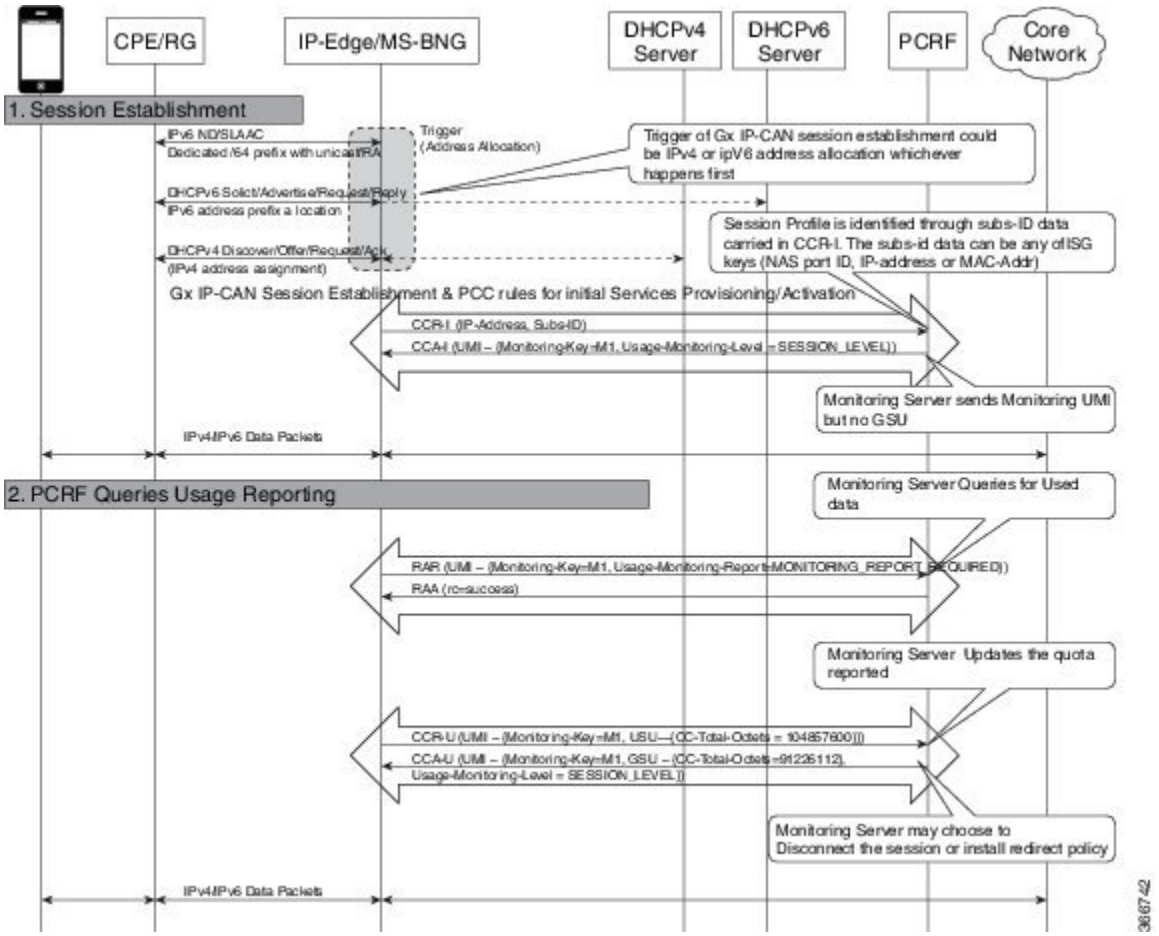
Enabling Session-Level and Service-Level Monitoring



Excluding Session-Level Monitoring from Session Counters



Monitoring Postpaid Services



Additional References for Gx Diameter Monitoring and Reporting

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards and RFCs

Standard/RFC	Title
Standard	*Title*

MIBs

MIB	MIBs Link
• CISCO-GGSN-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Gx Diameter Monitoring and Reporting

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Gx Diameter Monitoring and Reporting

Feature Name	Releases	Feature Information
Gx Diameter Monitoring and Reporting	Cisco IOS XE Everest 16.6.1	The Gx Diameter Monitoring and Reporting The following commands were introduced by this feature: **h225**.