Diameter and Diameter Applications

In This Section

This section provides information pertaining to the Diameter authentication, authorization, and accounting protocol, and Diameter applications:

Restrictions

Diameter-Based Restrictions:

- Accounting (RFC 6733, *Diameter Base Protocol*) via Diameter is not supported in this release.
- Accounting-Request (ACR), Accounting-Answer (ACA), Session-Termination-Requests (STR) and Session-Termination-Answer (STA) messages are not supported.
- SCTP and IPSec as transport protocols are not supported. TCP is supported.

Gx-Based Restrictions:

- Static hosts and LAC/LNS (L2TP) hosts are not supported in Gx.
- Bridged Homes and AA subscribers — Since there is no notion of a subscriber-host in AA, the last AA policy submitted via Gx for any ESM subscriber-host within the home will be applied to the AA subscriber as a whole and overwrite any previously active AA policy.
- The <SAP,MAC> combination must be unique for each host (single stack or dual-stack).
- The Charging-Rule-Name within the Charging-Rule-Definition cannot contain double colon (::) set of characters in the name string. The use of double colon in the name string itself is reserved for future use.
- Reporting about successful rule activation in 7x50 (3GPP 29.212, §4.5.2) is not supported. The rule report is sent only if the rule instantiation fails.
- Time-based Usage-Monitoring is not supported.
- Gx persistency is not supported. However, upon node reboot with ESM persistency enabled, 7750 will re-initiate Gx sessions (new CCR-I will be generated for each Gx enabled host).
- Gy and Usage-Monitoring cannot be enabled for the same host and the same category-map at the same time. Gy is pre-configured at the time of the host instantiation. If a Usage-Monitoring request is received while Gy is enabled, the 7x50 will ignore the Usage-Monitoring request.
- Each ESM host can have up to three Usage-Monitoring entities enabled simultaneously. For example, two categories and a session. If three categories are enabled for Usage-Monitoring, then Usage-Monitoring cannot be enabled per session (host) since this would exceed the limit of three Usage-Monitoring entities per host.
- Per-session Usage-Monitoring is not supported for subscriber hosts (or IP-CAN sessions) that share the same sla-profile instance.

Terminology

Gx Interface (or simply Gx) term is used to refer to the implementation of Gx reference point in 7x50. Gx reference points are defined in 3GPP 29.212 document.

Enhanced Subscriber Management (ESM) subscriber is a host or a collection of hosts instantiated in 7x50 SR Broadband Network Gateway (7x50). The ESM subscriber represents a household or a business entity for which various services with committed Service Level Agreements (SLA) can be delivered.

AA Subscriber is a representation of ESM subscriber in MS-ISA for the purpose of managing its traffic based on applications (Layer 7 awareness). An AA subscriber has no concepts of ESM hosts.

7x50 BNG refers to the ALU network element on which a Gx interface is implemented and policy rules are enforced (PCEF). This term can be interchangeably used with the 7x50 term.

Flow – A flow in Gx context represents traffic matching criteria (traffic classification or traffic identification) based on any combination of the following fields:

- source IP address
- destination IP address
- source port or port ranges
- destination port or port ranges
- protocol field
- DSCP bits.

A Gx flow is defined in the Flow-Information AVP:

```
Flow-Information ::= < AVP Header: 1058 > 3GPP 29.212 §5.3.53
         [ Flow-Description ]        3GPP 29.214 §5.3.8
         [ ToS-Traffic-Class ]       3GPP 29.212 §5.3.15
         [ Flow-Direction ]               3GPP 29.212 §5.3.65
         *[ AVP ]
```

Gx flows are similar to dynamically created filter/ip-criteria (QoS) entries and are inserted within the entry range configured for the base filter/qos-policy.

IP-criterion – These fields are used in IPv4/v6 packet header used as a match criterion. The supported fields are DSCP bits and 5 tuple. This is part of traffic classification (or traffic identification) within the PCC rule or within the static qos-policy/filter entry.

Gx Policy Rule – There are three types of Gx policy rules supported within 7x50:

- Gx based overrides — Subscriber related overrides (sub/sla/aa-profile, subscriber-id, QoS, filter, category-map, etc.).
- NAS filter entry inserts via Gx — Basic permit/deny entries, similar to ACL filter entries.
- PCC rules or IP-criterion based rules which are fully constructed Policy and Charging Control (PCC) rules with multiple QoS/filter actions per rule and its own traffic classification.

PCC rule represents a single or a set of IP based classifiers (DSCP bits or 5 tuple) associated with a single or multiple actions.

For example:

Each PCC rule can be removed via Gx from 7x50 by referencing its name (Charging-Rule-Name AVP).

PCC rule can contain a combination of QoS and IPv4/v6 filter actions as they pertain to 7x50.

PCC Rule Classifier — A flow-based (5 tuple) or a DSCP classifier defined in Flow-Information AVP within the PCC Rule. There can be a single or multiple classifiers (Flow-Information AVPs) within a single PCC rule. In 7x50 terms, a PCC classifier (Flow-Information AVP) correspond to an entry (match criteria) within the filter/ip-criteria definition.

CAM entry – A single entry in the CAM that counts toward the CAM scaling limit. For example a match condition within ip-criteria in a filter or qos-policy can evaluate into a single CAM entry or into multiple entries (in the case where port-ranges are configured in the classifier, or where matching against UDP and TCP protocols are enabled simultaneously).

Subscriber Host Policy – A collection of PCC rules (classifiers and actions), Gx overrides, NAS filter inserts and statically configured rules (CLI defined QoS or filter) that are together applied to the subscriber host.

3GPP-Based Diameter Credit Control Application (DCCA) - Online Charging

The 3GPP-based Diameter Credit Control On-line charging applications allow the control of subscriber access to services based on a pre-paid credit. The volume and time accounting in the 7750 SR supports online charging using the Diameter Credit-Control Application (DCCA). The 7750 SR supports Session Charging with Unit Reservation (SCUR) allowing the 7750SR to reserve volume and time quota for rating-groups. Furthermore, the 7750 SR supports centralized unit determination and centralized rating: it requests quota and reports usage against the quota provided by the Online Charging Server (OCS). Credit control is always on a per rating group basis. A rating group maps to a category inside a category-map of the 7750SR volume and time based accounting function.

The following are the basic configuration steps:

1. Configure a diameter policy

   In the **config>aaa** CLI context, configure a diameter peer policy with one or multiple Diameter peers.

```
configure
    aaa
        diameter-peer-policy "diameter-peer-policy-1" create
            description "Diameter peer policy"
            applications gy
            connection-timer 5
            origin-host "bng.alcatel-lucent.com"
            origin-realm "alcatel-lucent.com"
            source-address 10.0.0.1
            peer "peer-1" create
                address 10.1.0.1
                destination-host "server.alcatel-lucent.com"
                destination-realm "alcatel-lucent.com"
                no shutdown
            exit
        exit
    exit
```

2. Configure a diameter application policy.

   In the **config>subscriber-mgmt** CLI context, configure a diameter application policy:

   – Set the application to Gy (Diameter Credit Control Application),

   – Specify the Diameter peer policy to use and optionally specific additional Gy application specific parameters (for example AVP format).

```
configure
    subscriber-mgmt
        diameter-application-policy "diameter-gy-policy-1" create
            description "Diameter Gy policy"
            application gy
            diameter-peer-policy "diameter-peer-policy-1"
            gy
                avp-subscription-id subscriber-id type e164
                include-avp
                    radius-user-name
                exit
            exit
        exit
    exit
```

3. Create a category-map in which you define:

   – The credit type (time or volume).

   – A category defining the queues to monitor for quota consumption and the rating-group this category maps to in DCCA.

```
configure
    subscriber-mgmt
        category-map "cat-map-1" create
            description "Category Map"
            credit-type time
            category "cat-1" create
                rating-group 1
                queue 1 ingress-egress
                exhausted-credit-service-level
                    pir 256
                exit
            exit
        exit
    exit
```

4. Create a credit control policy.

   Define the credit control servers to use by specifying the diameter application policy. Optionally, specify the default-category-map and an out-of-credit-action.

```
configure
    subscriber-mgmt
        credit-control-policy "cc-policy-1" create
            description "Credit Control Policy"
            credit-control-server diameter "diameter-gy-policy-1"
            default-category-map "cat-map-1"
            out-of-credit-action change-service-level
        exit
    exit
```

5. Configure the diameter credit-control-policy in the sla-profile of the subscriber host for which credit control should be activated.

```
configure
    subscriber-mgmt
        sla-profile "sla-profile-3" create
            description "SLA profile"
            credit-control-policy "cc-policy-1"
        exit
    exit
```

The following are examples of Diameter on-line charging flows:

Scenario 1 — Depicts a redirect use-case:

When the quota is depleted, the subscriber is redirected to a web portal. When the credit is refilled, the OCS server will notify the BNG and provide new quota. Note that 7750SR will install the configured out-of-credit-action when receiving a Final Unit Indication with action different from Terminate.

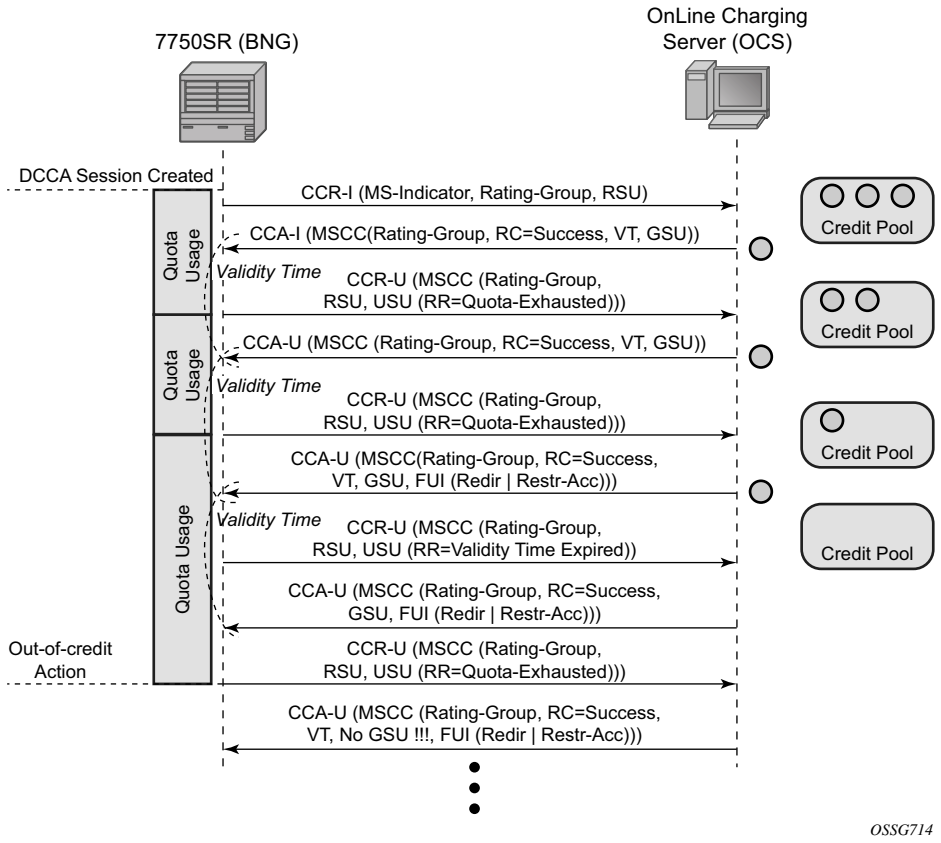

Figure 163: On-Line Charging Scenario 1 - Redirect (1/2)

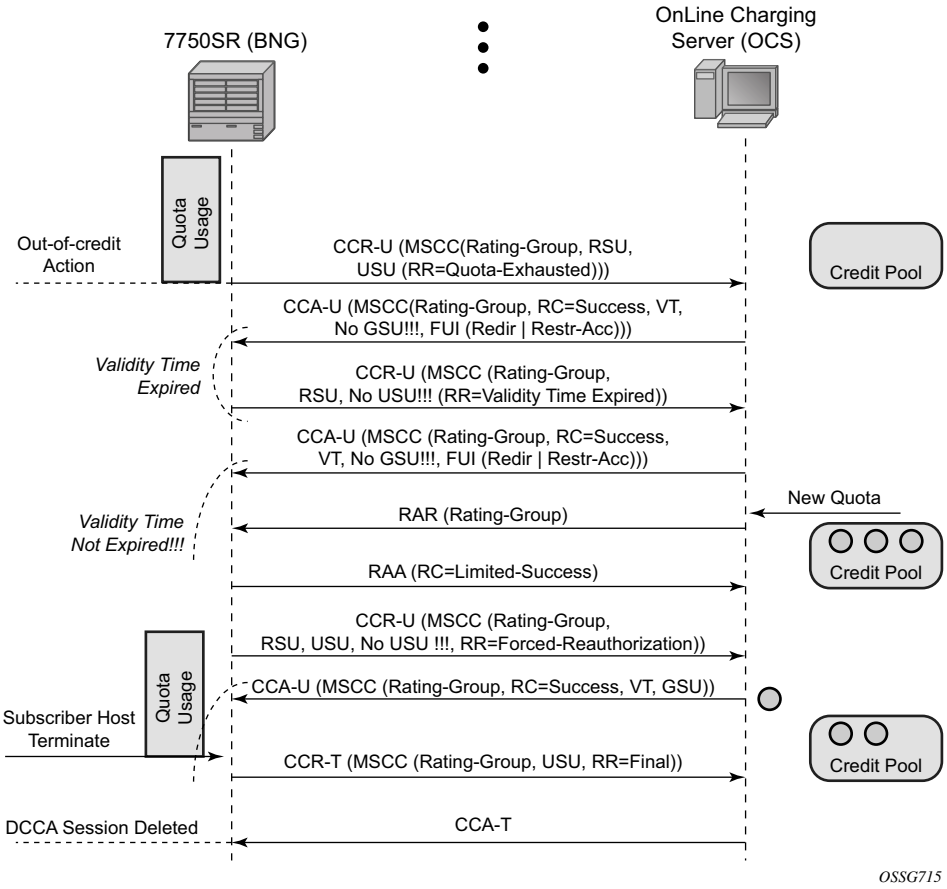

Figure 164: On-Line Charging Scenario 1 - Redirect (2/2)

Scenario 2 — Depicts a terminate use case:

When the quota is depleted after reception of a Final Unit Indication with action set to Terminate, the subscriber host is disconnected. The configured out-of-credit-action is ignored in this case.

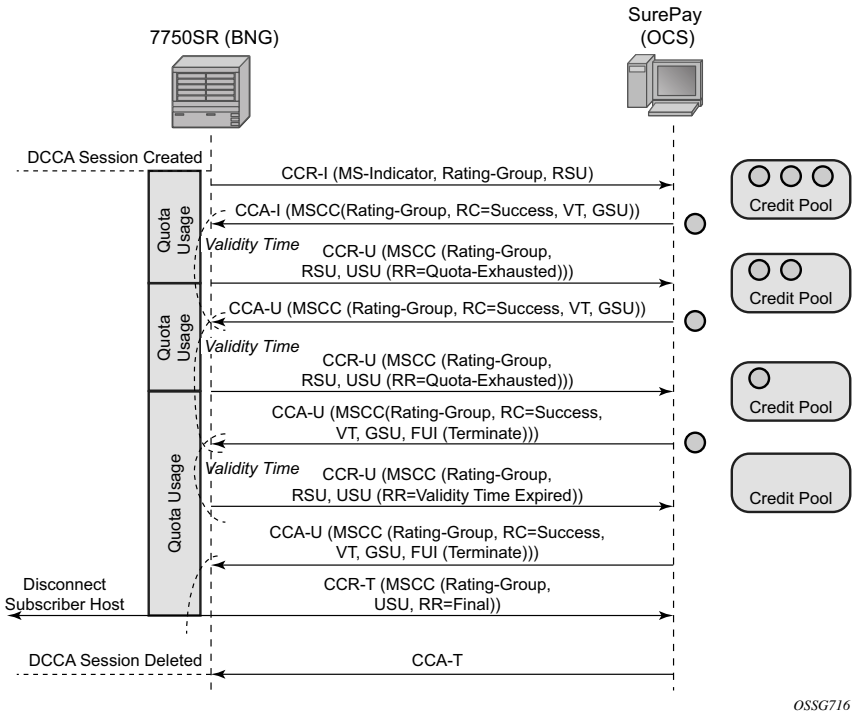

Figure 165: On-Line Charging Scenario 2 – Terminate

Abbreviations used in the previous drawings:

CCR	Credit Control Request (-Initial, -Update, -Terminate)
CCA	Credit Control Answer (-Initial, -Update, -Terminate)
RAR	Re-Authentication Request
RAA	Re-Authentication Answer
MSCC	Multiple Services Credit Control
GSU	Granted Service Unit
RSU	Requested Service Unit
USU	Used Service Unit
RC	Result Code
RR	Reporting Reason
VT	Validity Time

Policy Management via Gx Interface

Gx is a reference point in the network architecture model describing mobile service delivery. The network elements are described in various technical documents under the umbrella of 3GPP and are used to deliver, manage, report on and charge end-user traffic for mobile users. Gx reference point is used for policy control and charging control. As shown in Figure 166, it is placed between a policy server (PCRF - Policy and Rule Charging Function) and a traffic forwarding node (7x50 – Policy and Charging Enforcement Function) that enforces rules set by the policy server.

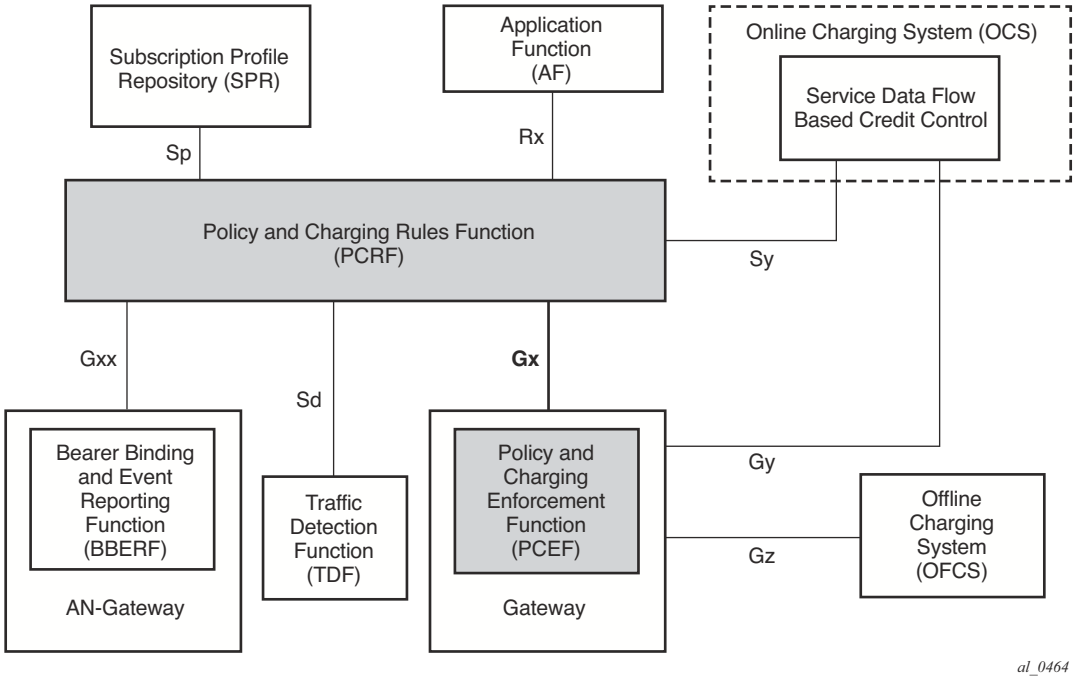

Figure 166: Gx Reference Point

The Gx reference point is defined in the Policy and Charging Control (PCC) architecture within 3GPP standardization body. The PCC architecture is defined in the document 23.203 while the Gx functionality is defined in the document 29.212. Gx is an application of the Diameter protocol (RFC 3588/6733).

Although Gx reference point is defined within 3GPP standardization body (spurred by mobile/ wireless industry) its applicability has spread to wire-line operation as well. For example, mobile operators that also have fixed line customers (residential + business) would like to streamline policy management in their mobile and non-mobile domains with a single and already existing Gx based policy management infrastructure. In other words they want to integrate policy management of nodes serving fixed line subscribers into the system that is currently managing mobile subscriber base.

In such mixed environments, the 7x50 node plays a role of a PCEF with an integrated TDF (Traffic Detection Function, or Application Awareness [AA] in ALU terminology) where policies and charging rules can be managed via PCRF.

With WiFi Offload as a new emerging application, supporting Gx reference point on 7x50 nodes is becoming even more important.

Gx Interface in 7x50 encompasses the following functionality:

- Per subscriber host policy management
- Usage-Monitoring

Gx will be applicable to Enhanced Subscriber Management (ESM) as well as to AA.

Gx Protocol

The Gx application is defined as a vendor specific Diameter application, where the vendor is 3GPP and the Application-ID for Gx application is 16777238. The vendor identifier assigned to 3GPP by IANA is 10415.

With regards to the Diameter protocol defined over the Gx interface, the 7x50 (PCEF) acts as a Diameter Client and the PCRF acts as a Diameter Server. The Gx Diameter Application uses existing Diameter Command Codes from the Diameter Base Protocol (RFC 6733) and Diameter Credit Control Application (RFC 4006), both of which are already implemented in 7x50.

Gx is using Attribute-Value Pairs (AVPs) for data representation within its messaging structures (command codes). AVPs in Gx come from various sources:

- Gx specific AVPs defined in 3GPP Gx specification TS 29.212.
- Re-used AVPs from other existing Diameter applications (RFC 4006, RFC 4005, etc), other 3GPP specs, ETSI, etc.
- RADIUS re-used attributes (AVP codes 0-255 are reserved for RADIUS re-used attributes)
- Vendor specific AVPs

The initialization and maintenance of the connection between the 7x50 (PCEF) and the PCRF is defined by the underlying Diameter protocol as defined in RFC 3588/6733.

Policy Assignment Models

Subscriber and AA policies in 7x50 (PCEF with integrated TDF) will be assigned via Gx protocol from the policy server (PCRF).

There are two modes of operation:

- Pull mode — The policy creation/modification is solicited by the 7x50 node.
- Push mode — The policy change is unsolicited by the 7x50 node.

In the pull mode, during the host creation process, a user is authenticated by the AAA server. This process is independent from PCRF. Once the user is authenticated and the IP address is allocated to it, the 7x50 sends a request for policies to the PCRF via CCR-i messages (initialization request message). This communication occurs via Gx interface. The subscriber-host must be uniquely identified in this request towards the PCRF. This sub identification over Gx interface could be by the means of IP address, username, SAP-id, etc.

Based on the user identification, PCRF will submit policies to the 7x50. Those policies can range from subscriber strings (sub/sla-profiles/AA-profiles) to qos and filter related parameters.

In the push mode, the PCRF initiates the mid-session policy change through the Re-Authentication Request (RAR) message.

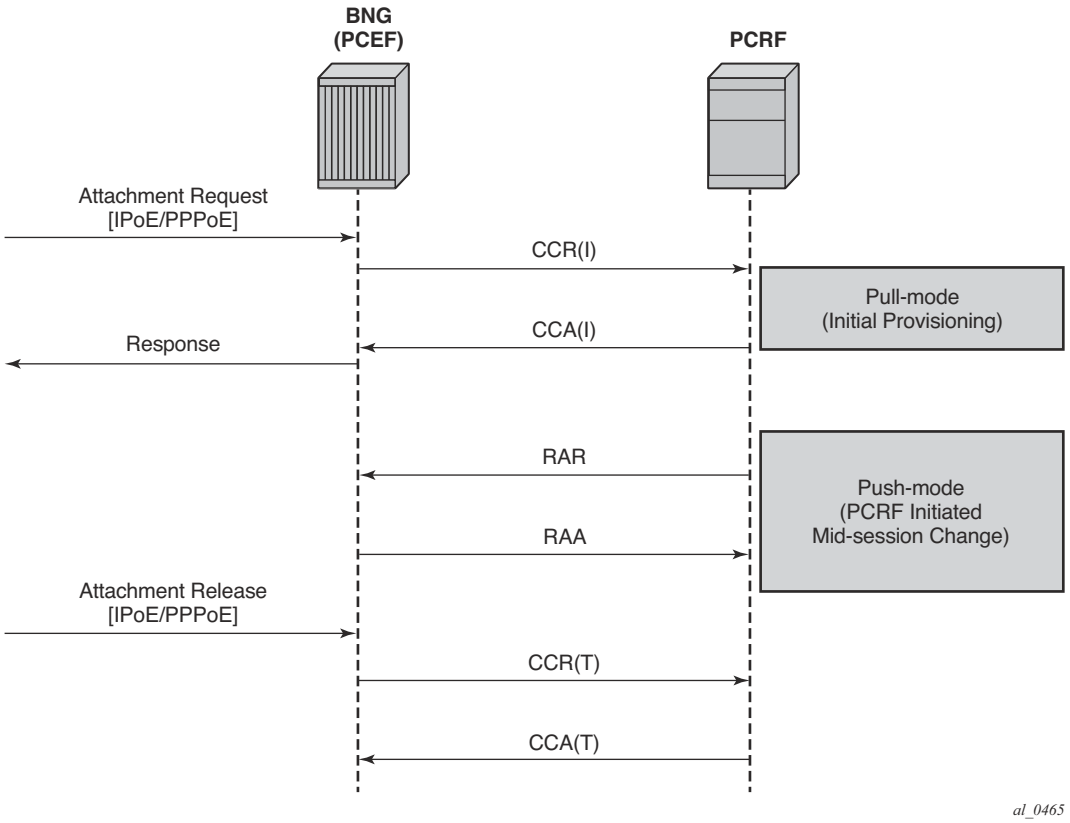

Figure 167: Policy Assignment Models

In case that Usage-Monitoring is requested, the PCRF submitted policy changes are triggered by the Credit Control Request (Update) messages. This is based on ESM or AA Usage-Monitoring. Once the specified usage threshold is reached on the session-level, credit-category level, pcc rule level or application level on the 7x50, the Usage-Monitoring is reported from the 7x50 to the PCRF in the CCR-u message. Refer to the SR OS Multi-Service Integrated Services Adapter Guide for details on AA based Usage-Monitoring.

Alternatively, PCRF can request usage reporting on-demand via RAR command.

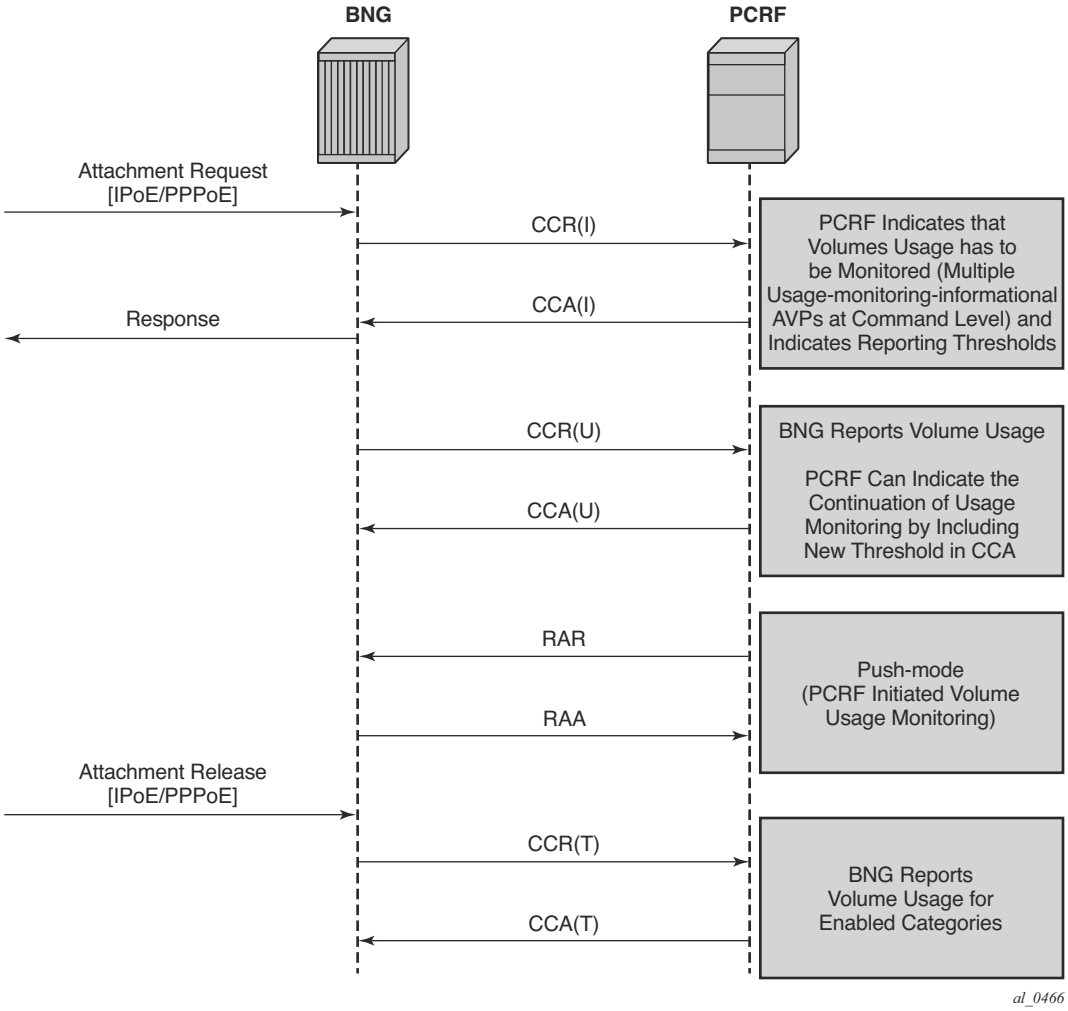

Figure 168: On-Demand Usage Reporting

IP-CAN Session – Gx Session Identification

IP Connectivity Access Network (IP-CAN) session is a concept that has roots in mobile applications. A policy rule via Gx interface can be applied/modified to an entity that is identified as IP-CAN session (in addition to individual bearers within the IP-CAN session, the bearer concept is currently not applicable to 7x50 BNG). For example, an UE (user interface or simply a mobile phone) can hosts several services, each of which appears as a separate IP-CAN session associated with the same IP address. For example in mobile world, an IP-CAN session can be defined as <IP_address, APN, IMSI>, where:

- APN (Access Point Name) is the service identifier
- IMSI (International Mobile Subscriber Identification) is the UE identifier (SIM Card)

In wireline environment (ESM deployments), an IP-CAN session will identify an entity to which the policy can be applied/modified, and currently, this is a subscriber-host instantiated in the 7x50.

For the purpose of identifying the host in 7x50 in all Gx related transactions, the 7x50 will generate a unique, per host (single or dual-stack) session-id AVP (RFC 6733, §8.8). The Gx session-id will in essence represent the IP-CAN session from the standpoint of 7x50. Note that the Gx session-id AVP is not the same as the acct-session-id attribute used in RADIUS accounting.

User Identification in PCRF

The following identification related AVPs will be sent to the PCRF via Gx messages to aid in IP-CAN session identification:

- **subscription-id** AVP (RFC 4006, §8,46) — This can be used to identify the subscribers on the PCRF. For the supported fields within the subscription-id AVP, refer to the 7750 SR OS Gx AVPs Reference Guide.
- **NAS-Port-Id** AVP (RFC 2869 / §5.17; RFC 4005 / §4.3)
- **AN-GW-Address** AVP (3GPP 29.212 / § 5.3.49)
- **Calling-Station-ID** AVP (RFC 4005 / §4.6)
- **user-equipment-info** AVP (RFC 4006, §8.49)
- **logical-access-id** AVP (ETSI TS 283 034) — This will contain circuit-id from DHCPv4 Option (82,1) or interface-id from DHCPv6 option 18. The vendor-id will be set to ETSI (13019).
- **physical-access-id** AVP (ETSI TS 283 034) — This will contain remote-id from DHCPv4 option (82,2) or DHCPv6 option 37. The vendor-id will be set to ETSI (13019).

Physical and logical access IDs are also defined in BBF TR-134 (§7.1.4.1).

Table 25: PDP to PEP Direction Parameters

Parameter	Category	Type	Description
Logical access ID	User identification	Octet String	The identity of the logical access to which the user device is connected. It is stored temporarily in the AAA function connected to PDP. This corresponds to the Agent ID in case of IPv4 and to THR Interface Id of DHCP option 82 for IPv6
Physical Access ID	User identification	UTF8String	The identity of the physical access to which the user device is connected. It is stored temporarily in the AAA function connected to the PDP. This corresponds to the Agent Remote ID

A Subscription-id AVP is most commonly used to identify the subscriber but any combination of the above listed parameters can be used to uniquely identify the IP-CAN session on PCRF and consequently identify the subscriber.

In addition, NAS-Port, NAS-Port-Type, and Called-Station-ID AVPs from RFC 4005 (§4.2, §4.4, §4.5) can be passed to the PCRF.

NAS-Port-Id as Subscription-Id

7x50 allows the NAS-Port-Id to be carried within Subscription-Id AVP. Since the NAS-Port-Id may not be unique network-wide (two independent 7750s may use the same NAS-Port-Id), there is a need for another identifier in conjunction with NAS-Port-Id to make the Subscription-Id unique across network. This additional identifier is a custom string that can be appended to the NAS-Port-Id. It is defined when the NAS-Port-Id is configured for inclusion in Gx messages. Refer to the 7750 SR RADIUS Attribute Reference Guide to learn how to format NAS-Port-Id AVP in the SR 7x50.

The string can be used to identify the location of the node. For example:

```
@ALU-MOV-SITE-1
```

An example of the augmented NAS-Port-Id would look like:

```
NAS-Port-Id = lag-1.1/1/2:23.2000@ALU-MOV-SITE-1
```

where: 'lag-1.1/1/2:23.2000' is the part referencing the SAP in 7x50 (port + vlan tags) and the '*@ALU-MOV-SITE-1*' is the node itself.

Such NAS-Port-Id can be then inserted in the Subscription-Id AVP.

Gx Interface and ESM Subscriber Instantiation

Policy management via Gx enables operators to consolidate policy management systems used in wireline (mostly based on RADIUS/CoA) and wireless environment (PCRF/Gx) into a single system (PCRF/Gx).

The model for policy instantiation/modification via Gx is similar to the one using RADIUS CoA. The authentication and IP address assignment is provided outside of Gx while the policy management function is provided via Gx.

Some PCRFs may require that the IP address information is passed from the 7x50 in CCR-i. This assumes that the IP address assignment phase (via LUDB, RADIUS or DHCP Server) is completed before the PCRF is contacted via CCR-i. Message flow for various protocols (DHCP, AAA, Gx) related to IPv4 subscriber-host instantiation phase is shown in Figure 169

CCR-i message is sent to the PCRF once DHCP Ack is received from the DHCP server. Relaying DHCP Ack to the client in the final phase of the host instantiation process will depend on the answer from the PCRF and the configuration settings of the fallback function in case that the answer is not received.

This model allows the IP address of the host to be sent in the CCR-i message, even though the subscriber-host is not fully instantiated at the time when the CCR-i message is generated.

AAA/LUDB must still be used for authentication and assignment of parameters necessary to place the subscriber host in the proper routing context (service-id, grp-id, msap-policy).

Start of the accounting process nicely fits into this model since the host is not instantiated until the policy information from all sources (Gx, AAA, defaults) is known. Once the final sub-profile (containing the acct-policy) is known, the host will be instantiated and accounting can consequently be activated.

The IP address itself cannot be assigned via Gx, and this functionality is outside of the Gx scope (3GPP TS 23.203 Rel12, Annex S, IP-CAN Session Establishment section).

The purpose of the CCR-i message is the following:

- To notify the PCRF that the sub-host was about to be instantiated in 7x50. Consequently, the PCRF will create a Gx session for the subscriber host in case that the CCR-i is successfully processed by PCRF.
- To identify the subscriber host in the PCRF. The PCRF will use the subscriber host identification information to identify the policy (for the subscriber host) that needs to be submitted to 7x50. The policy rules can be sent via CCA-i immediately following the initial CCR-i or they can be modified at any time during the subscriber-host lifetime via RAR messages.

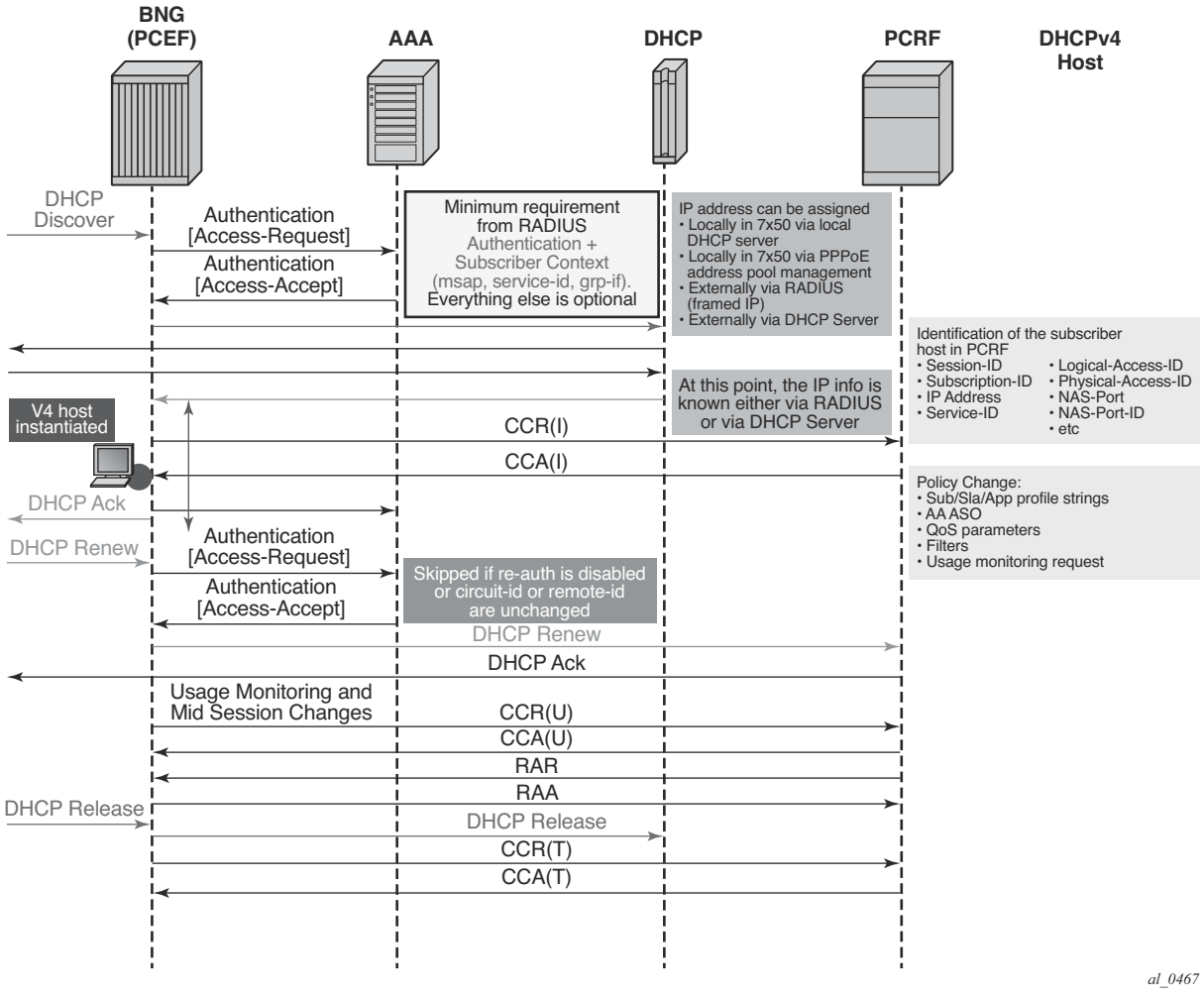

Figure 169: Messages Flow During DHCPv4 Host Instantiation Phase

Message flow for PPPoEv4 host is similar. The host will be instantiated once the answer from PCRF is received.

However, IPCP negotiation and Gx negotiation (CCR/CCA) are performed in parallel, independently of each other and therefore 7x50 will not wait for the Gx session to be established before the last IPCP ConfAck is sent (like it is the case for DHCP ACK).

Once the host is instantiated in the 7x50 (after the CCA-i is received or as defined by the fallback action in case that the PCRF is not available), the Accounting-Start message will be sent by the 7x50 (assuming that accounting is enabled).

The message flow is shown in Figure 170.

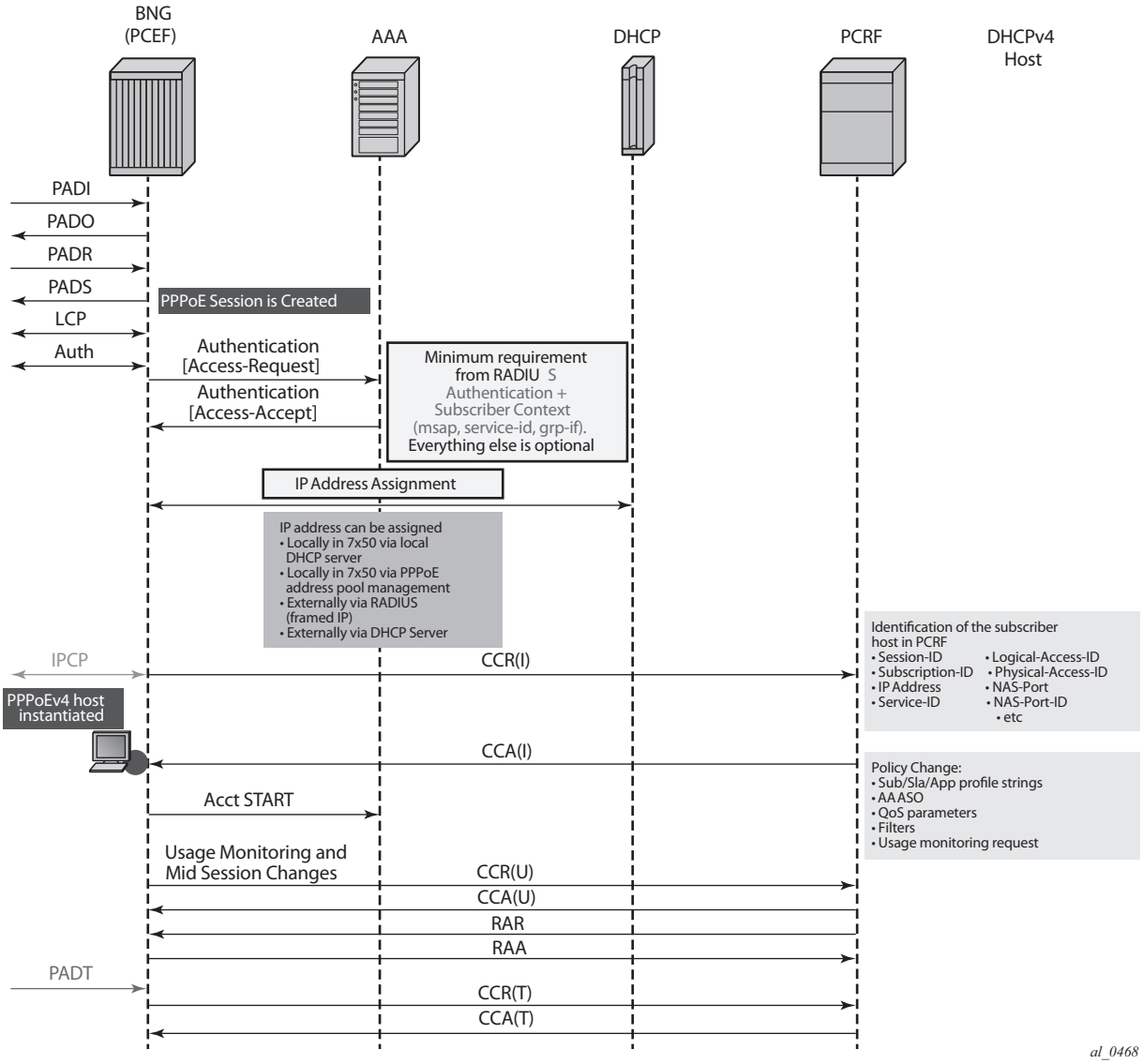

Figure 170: Message Flow During PPPoEv4 Host Instantiation Phase

The host is created when the Gx session is established and therefore the subscriber host will transition into the traffic forwarding state once the Gx processing is completed. In case that the PCRF is unavailable or unresponsive, the host creation/termination will be driven by the fallback configuration

Gx and Dual-Stack Hosts

Dual-stack (DS) hosts are treated as a single session from the Gx perspective. The PCRF submits the policy rule that will be applied to DS host as a whole, regardless of the IP address (IPv4 or IPv6) that triggered the CCR-i message. DHCPv4 and DHCPv6 requests for DS host are linked by the same <SAP,MAC> combination which must be unique per system, while in PPPoE case the existing concept of the PPPoE session provides the v4/v6 linking natively.

The CCR-i will contain the IP address that was allocated first (the one that triggered the session creation). The request for the second IP address family will trigger (if enabled by configuration) an additional CCR-u that will carry the IP address allocation update to the PCRF along with the UE_IP_ADDRESS_ALLOCATE (18) event. Apart from that, the CCR-u content will mirror the content of the CCR-i with exception of already allocated IP address(es). There is a single Gx message (CCR-i or CCR-u) carrying the update for DHCPv6 IA-NA+IA-PD and DHCPv6/PPPoE NA+PD address/prefix, assuming that NA+PD is requested in a single DHCP message.

Similarly for the Gx session teardown, CCR-u messages will be sent carrying the UE_IP_ADDRESS_RELEASE event, followed by the CCR-t message.

The message flow is depicted in Figure 171.

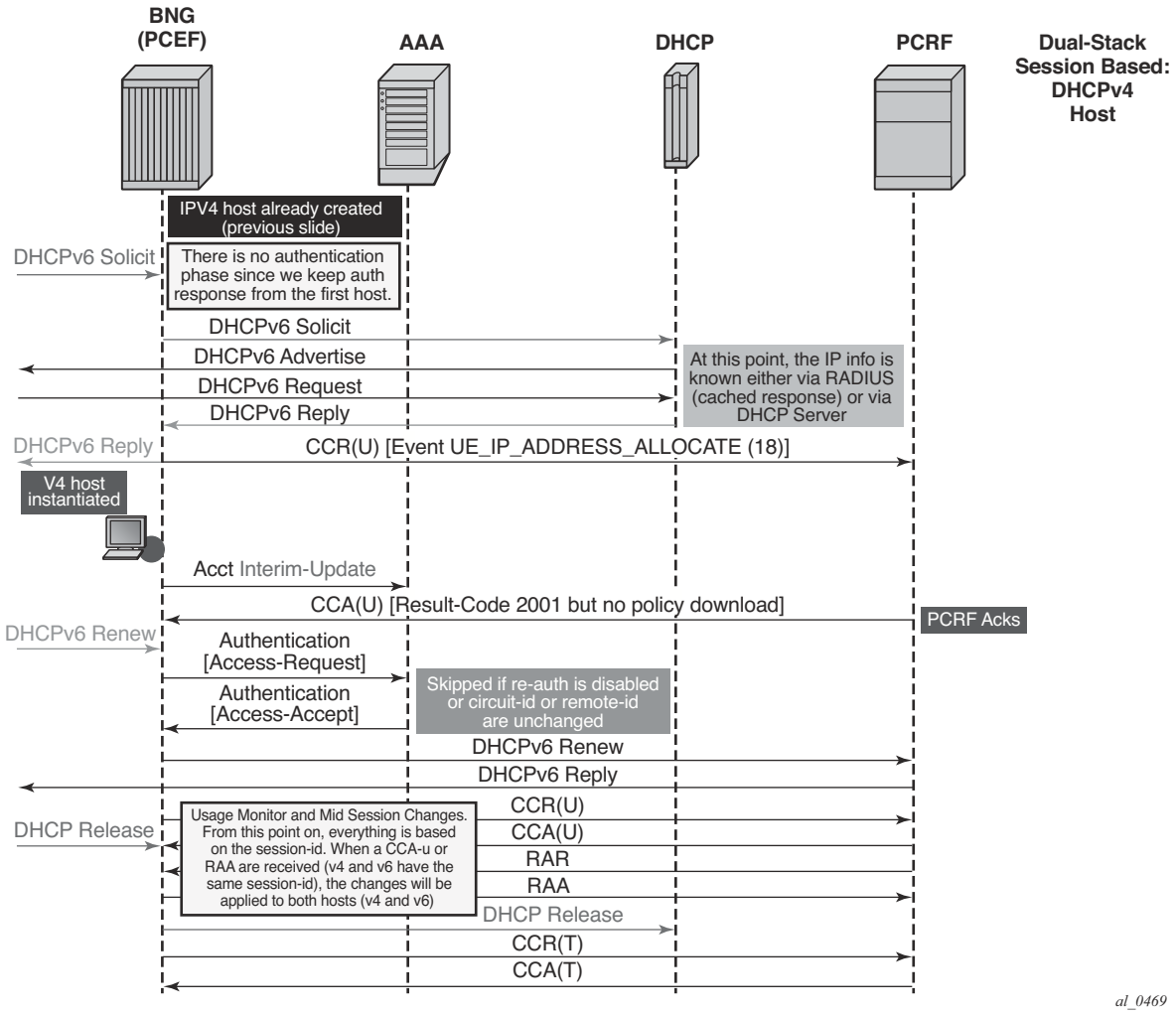

Figure 171: Gx and Dual Stack Session Instantiation

For Dual-Stack PPPoE host, the CCR-i is sent when the first IP address is assigned to the host. In the example in Figure 171, processing of the DHCPv6 Replay and CCR-u messages is performed in parallel. In other words, sending the DHCPv6 Reply message to the client will not be delayed until the response from the PCRF is received. The reason being is that the Gx session is already established (triggered by the IPv4 host in our example) and all parameters for IPv4 and IPv6 are already known as received in CCA-i. In this case, the CCR-u message is simply a notification message, informing the PCRF about the new IPv6 address/prefix being assigned to an existing client.

Gx and PPPoEv6-DHCP

For PPPoE v6 hosts, the IPv6 address is not obtained during IPCP phase (only interface-id is negotiated). In this case, the 7x50 will wait until the IPv6 address/prefix is allocated to the IPv6 hosts before it sends the CCR-I message. Otherwise the IP address would not be available in CCR-i.

This is shown in Figure 172.

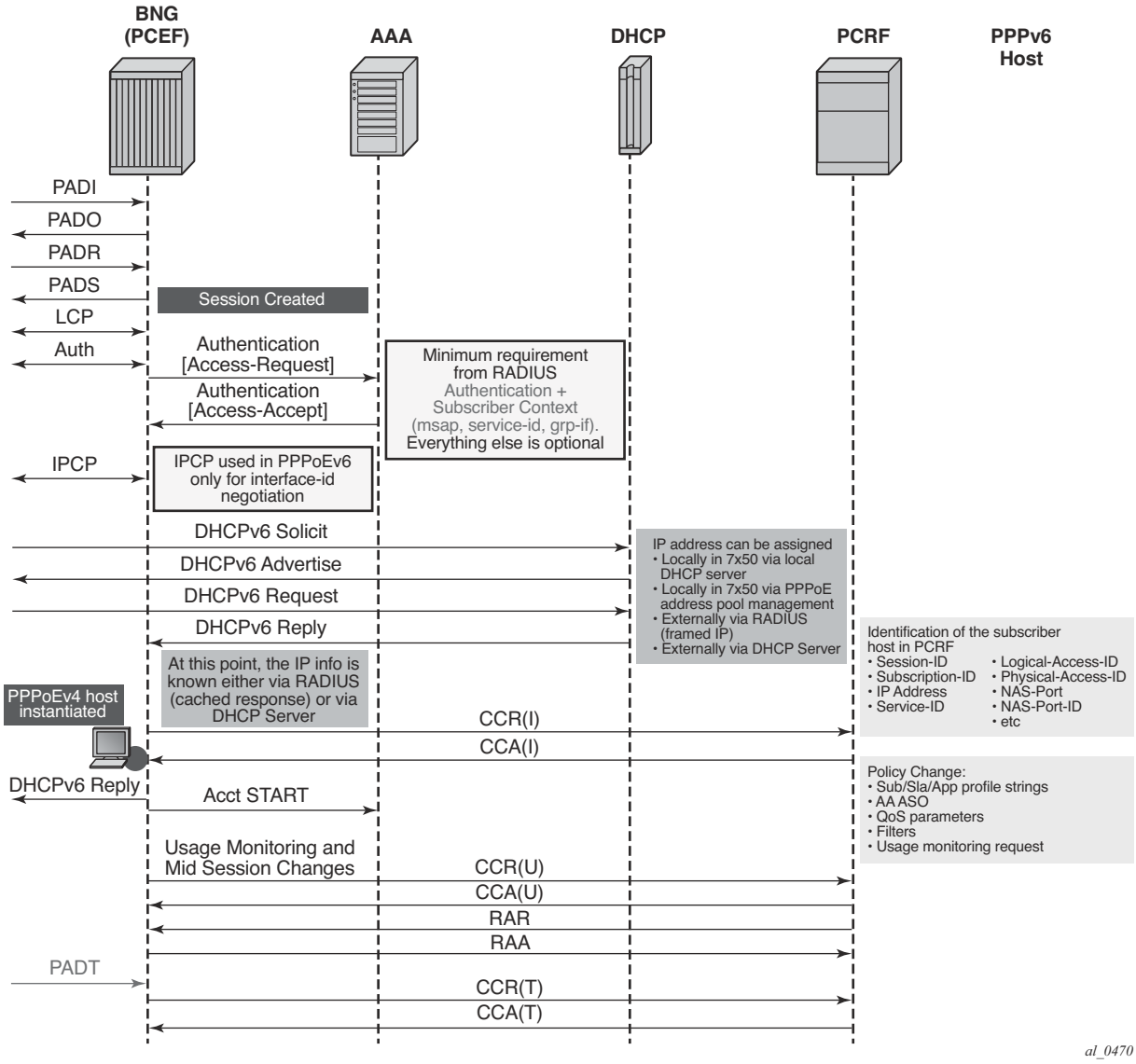

Figure 172: Gx and PPPoEv6 Host Instantiation

Gx Fallback Function

The Gx fallback functionality refers to the behavior related to the subscriber host instantiation in situations where the PCRF is unresponsive while peering connection(s) are up or the PCRF is unavailable with all peering connections down. This functionality affects only Gx session processing related to CCR-i messages in 7x50 and has no effect on already established Gx sessions.

The fallback behavior can be controlled via local configuration in 7x50 or can be controlled via certain AVPs provided by PCRF.

PCRF provided AVPs that control fallback behavior are:

- CC-Session-Failover AVP with the following values:
  - FAILOVER_NOT_SUPPORTED
  - FAILOVER_SUPPORTED
- Credit-Control-Failure-Handling AVP with the following values:
  - TERMINATE
  - CONTINUE
  - RETRY_AND_TERMINATE

In case the fallback-related AVPs are not provided via PCRF, the 7750 SR can provide local configuration option to define the fallback behavior. In case that the response from the PCRF cannot be obtained, the local configuration can allow the subscriber host to be instantiated with default parameters, or alternatively the local configuration can deny subscriber host instantiation.

PCRF provided AVPs will overrule local configuration.

The local configuration that defines Gx fallback behavior can be found under the following CLI hierarchy:

```
config
    subscr-mgmt
      diam-appl-plcy
        on-failure
          failover {enabled|disabled}
            handling {continue|retry-and-terminate|terminate}
```

The **failover** configuration option (equivalent to CC-Session-Failover AVP) controls whether the secondary peer will be used in case that the primary peer is unresponsive. The unresponsiveness is determined by the timeout of the previously sent message.

The **handling** configuration option (equivalent to Credit-Control-Failure-Handling AVP) controls whether the subscriber will be terminated or instantiated with default parameters in case that the

PCRF is unresponsive.

	Handling: CONTINUE	Handling: RETRY-AND-TERMINATE	Handling: TERMINATE
Failover: ENABLED Once the message sent to the primary peer times out, the secondary peer (and consecutive peers after that) will be attempted. Once the message times out after it has been sent to all available peers, the HANDLING action will be examined in order to determine whether to terminate the host instantiation attempt or whether to use default parameters to instantiate the host.	Once the message times out after it has been sent to all available peers, the subscriber host will be instantiated with default parameters (if they are configured)	Once the message times out after it has been sent to all available peers, the subscriber host instantiation will be terminated.	Once the message sent to the primary peer times out, the subscriber host instantiation will be terminated.
Failover: DISABLED Once the message sent to the primary peer times out, the HANDLING action will be examined in order to determine whether to terminate the host instantiation attempt or whether to use default parameters to instantiate the host.	Once the message sent to the primary server times out, the subscriber host will be instantiated with default parameters (if they are configured)	Once the message sent to the primary peer times out, the subscriber host will be terminated.	Once the message sent to the primary peer times out, the subscriber host will be terminated.

The CCR retransmissions are controlled by the **tx-timer** command under the **diameter-application-policy**. Refer to the SR OS CLI reference for the description of **retransmission** handling.

In the case that all peers are down (no connections are open), the **handling** action will determine the behavior. If the action is set to **continue**, the subscriber-host will be immediately instantiated with the default-settings (provided that the defaults are available). In all other action cases, the host instantiation will be immediately terminated.

Gx CCR-I Replays

As described in the previous section, the subscriber host can be optionally (configuration controlled) established with default settings (sla-profile, sub-profile, app-profile) in the case where PCRF is not available to answer CCR-i. This results in a subscriber-host state mismatch between the 7750 SR and PCRF, where the subscriber-host is established in the 7750 SR but there is no corresponding Gx session established in PCRF.

In order to resolve this situation, ESM periodically sends CCR-i for the Gx *orphaned subscriber-host* until the response from PCRF is received. The CCR-i is periodically retransmitted every 60 seconds.

Gx CCR-t Replays

Termination of the subscriber-host in 7x50 without termination of the corresponding Gx session in PCRF will result in state mismatch between 7x50 and the PCRF whereby the host Gx session is present in the PCRF while it is removed from 7x50.

Some PCRFs can cope with such out-of-sync condition by periodically auditing all existing Gx sessions. For example, a **probing** RAR can be sent periodically for each active Gx session. The sole purpose of this probing RAR is to solicit a response from the PCEF (7x50) and provide indication on whether the corresponding Gx session is alive in 7x50 or is vanished. The 'probing' RAR can contain an Event-Trigger that is already applied in 7x50, or if none is applied, then the Event-Trigger can contain NO_EVENT_TRIGGER. In either case the 'probing' RAR will not cause any specific action to be taken in 7x50 and it is used only to solicit reply from PCRF.

To minimize the impact on performance, **probing** RARs are sent infrequently and thus it may take days to discover stale Gx session on PCRF. 7x50 offers a mechanism that can clear the stale session in PCRF sooner. It does this by re-playing CCR-t messages until the proper response from PCRF is received (CCA-t). The CCR-t messages will be re-played up to 24 hours. This period of 24 hours is not configurable. In case that 24hour period expires before the proper answer is received, the CCR-t is deleted and a log is generated. The log contains Gx session-id.

The T-bit (retransmission bit) is set in all re-played CCR-t messages.

The following command will clear all orphaned sessions in 7x50 for a given diameter application policy:

```
clear subscriber-mgmt diameter-session CCR-t-replay diameter-application-policy <gx-pol-
icy-name>.
```

RAR and CCR-t Replay

Certain scenarios will make possible that PCRF sends a RAR message to an orphaned Gx session running CCR-t replays in 7x50. The ESM host associated with such orphaned Gx session does not exist and therefore RAR cannot be applied.

In this scenario, 7x50 will reply with RAA carrying Result-Code= DIAMETER_UNKNOWN_SESSION_ID (5002).

CCR-t Replay And Multi-Chassis Redundancy

The first CCR-t reply for each Gx session will be synchronized, but the consecutive CCR-t replays for the same Gx sessions will not be synchronized. Once the answer (CCA-t) is received, the CCR-t replay will be terminated and this event (deletion of CCR-t replay) will be synchronized to the other node.

CCR-t replays are sent from the node that was in SRRP active state at the time when the CCR-t was initiated. They will continue to be sent from the same node even if the SRRP is switched over in the meantime.

This entire process can be thought of as if the CCR-t initiating node (active SRRP) armed its MCS peer with CCR-t replay for a given Gx session. This occurs at the very beginning, when a CCR-t replay is first initiated for a given Gx session. The armed node will stay silent until the MCS peer that is actively sending CCR-t replays for a given Gx session, reboots. Only when the MCS peer reboots, the armed node will start sending CCR-t replays for a given Gx session in the following fashion: first message is sent with cleared T-bit, followed by replays at the configured replay interval and a fresh 24 hour lifetime.

CCR-t Replay And High Availability

On CPM switchover, the newly active CPM will immediately trigger a new CCR-t replay with T-bit set. From then onwards, CCR-t replays will be sent according to the configured replay interval. In other words, the replay interval will be reset on the CPM switchover. However, the lifetime is not reset when CPM switchover occurs, and is synchronized between CPMs.

Automatic Updates for IP Address Allocation/De-allocation

During the subscriber-host setup phase, the first allocated IP address is sent in the CCR-i message from the 7x50 to the PCRF.

Each subsequent IP address allocation/de-allocation for the same host can optionally trigger a CCR-u, notifying the PCRF of the IP address allocation/de-allocation event.

This behavior can be enabled via the following CLI command:

```
configure
    subscriber-mgmt
      diameter-application-policy <pol-name>
        gx
          [no] report-ip-addr-event
```

The IP address allocation/dea-llocation event driven CCR-u message will carry the respective event code [UE_IP_ADDRESS_ALLOCATE(18) or UE_IP_ADDRESS_RELEASE(19)] along with the corresponding IP address.

The IP address allocation/de-allocation events are applicable to the following addresses:

- Framed-IP-Address (AVP Code 8) IPv4
- Framed-IPv6-Prefix (AVP Code 97) SLAAC
- Delegated-IPv6Prefix (AVP Code 123) IA-PD
- Alc-IPv6-Address (AVP Code 1023) IA-NA

These event-codes will only be sent in CCR-u messages and not in CCR-i and CCR-t messages (when the host is instantiated and terminated).

Examples:

- IPv6 attachment request arrives with two IP addresses: IA-NA and IA-PD. This is a new host. CCR-i will be generated with two IP addresses included (IA-NA and IA-PD, assuming that request for their allocation is carried in the same DHCPv6 message).
- Some time later, the attachment request for an IPv4 address arrives on the same host. CCR-u will be generated with the event UI_IP_ADDRESS_ALLOCATE and corresponding AVP (framed-address) will be sent to the PCRF. No IP address other than this new IPv4 address will be sent.
- RAR is received for the (any) policy change. 7x50 will reply with RAA and it will contain all three IP addresses (AVPs) that have been allocated to the host.

If the IP address notification event is enabled, 7x50 originated Gx message will carry all known IP addresses/prefixes associated with the subscriber-host (Gx session), unless those messages contain one of the two event codes:

UE_IP_ADDRESS_ALLOCATE(18) or UE_IP_ADDRESS_RELEASE(19). In the case that one of those two events is present in the Gx message, the IP address/prefix carried in that message will be only relevant to the event contained in the message (address/prefix allocated or released).

If the IP address notification event is disabled, 7x50 will only send the IP address from the first host. This IP address will be included in all messages related to the Gx session. If this IP address is removed (de-allocated) mid-session from the dual-stack host, 7x50 will stop advertising it, or any other address, from Gx messages for that particular session.

DHCPv4/v6 Re-Authentication and RADIUS CoA Interactions With Gx

In case that re-authentication for DHCPv4/v6 hosts is enabled, any policy changes that may be submitted during re-authentication (for example sla-profile update via Access-Accept) will overwrite the one previously applied, regardless of the source of the policy update. For example, in case that the Gx policy is applied to a subscriber host via RAR (mid-session policy update) and then some time later an overlapping policy with different values is submitted via RADIUS or LUDB during the re-authentication phase, the RADIUS/LUDB submitted policy will overwrite the one applied via Gx. In other words, the origin of the current policy in effect is not maintained internally in the system and therefore the overlapping policy update cannot be prioritized according to the source of the policy.

The following guidelines should be followed in case where the policy is provided via Gx:

In case that LUDB access is enabled, there should be no overlap between the LUDB provided parameters and Gx provided parameters. LUDB is accessed during every DHCP lease renew process and consequently parameters configured via LUDB would overwrite parameters provided by Gx.

- In case that LUDB access is enabled, there should be no overlap between the LUDB provided parameters and Gx provided parameters. LUDB is accessed during every DHCP lease renew process and consequently parameters configured via LUDB would overwrite parameters provided by Gx.

In case that re-authentication is enabled, there should be no overlap between the RADIUS provided parameters and Gx provided parameters. With re-authentication enabled, RADIUS is contacted during every DHCP lease renew process and consequently parameters configured via RADIUS would overwrite parameters provided by Gx.

These guidelines are not applicable for PPPoE subscriber-hosts since re-authentication cannot be enabled for PPPoE hosts. Consequently, LUDB or RADIUS parameters cannot override Gx provided parameters.

Coexistence of RADIUS CoA and Gx for the same host is allowed. The two policy change

mechanisms are independent of each other and as such they can override each other. For example, if the RADIUS CoA for policy change for the host is received, the policy will be updated but the PCRF (Gx) will not be notified of the change. If both policy management mechanisms are deployed simultaneously, then it is the operator's responsibility to synchronize the actions between the two.

Gx, ESM and AA

Although the ESM subscriber and the AA subscriber are two separate instantiations within the 7x50, their policy management and Usage-Monitoring are handled uniformly through a single Gx session.

ESM Subscriber-host vs AA Subscriber

Since ESM and AA modules are part of integrated service offering (ESM with residential AA on the same node), they share the same subscriber-id string. However, Gx interface in ESM is primarily applicable to hosts (basic entity to which policy is applied) while AA has no awareness of hosts. AA is only aware of subscribers (which is, in broader terms, a collection of hosts within a residence). Refer to the SR OS Multi-Service Integrated Services Adapter Guide for details on Application Assurance concepts.

AA Subscriber State

AA subscriber state must exist for App-profiles and ASO overrides to be applied.

The app-profile for the aa-sub is applied explicitly by a CCR-i or RAR message with an AVP AA-App-Profile-Name.

App-profiles interact with ASO characteristics in this way:

- The AA-App-Service-Options AVP within the app-profile assignment is optional at subscriber instantiation time and may be used later to modify the policy.
- The newly submitted AA-App-Profile-Name AVP will overwrite the one that is already applied. Any ASO AVPs that is received within the Gx message will be applied.

  Note: If an app-prof AVP is present, even if it is the same app-profile as currently applied, all previous ASO override policies are removed for the sub.

The state of the subscriber policy attributes is modified by ASO AVPs in this way:

- The app profile can define one or more ASO characteristics attributed to a subscriber

- If there are multiple ASO AVPs for the same characteristic in the message, the first one will take effect.
- There is no explicit delete of ASO overrides (PCRF can always resend or change the app-profile in order to delete all overrides).

Policy Management via Gx

Policy change can be implicitly requested by 7x50 at IP-Can session establishment time via CCR-i command. 7x50 will supply user identification attributes to the PCRF so that the PCRF can identify rules to be applied. However, 7x50 will not explicitly request specific policy update, for example via Event-Trigger = RESOURCE_MODIFICATION_REQUEST.

Another way to request policy update in 7x50 is via RAR command in a PUSH model.

Gx policies in 7x50 can be enforced via these three mechanisms:

- Gx-based overrides — this refers to subscriber related overrides (sub/sla/aa-profile, subscriber-id, QoS, filter, category-map, etc.).
- PCC rules or IP-criterion based rules which are fully constructed Policy and Charging Control (PCC) rules with multiple qos/filter actions per rule and its own traffic classification.
- NAS filter entry inserts via Gx — basic permit/deny entries, akin to ACL filter entries.

Gx-Based Overrides

Gx-based overrides refer to activation or modification of the existing subscriber-host related objects in 7x50.

Subscriber-host related objects are shown in Figure 173. A subscriber represents a residence or home and it is identified by Subscriber-Id string in 7x50. Subscriber in 7x50 can be comprised of multiple hosts in bridged home environment or a single host in routed home environment.

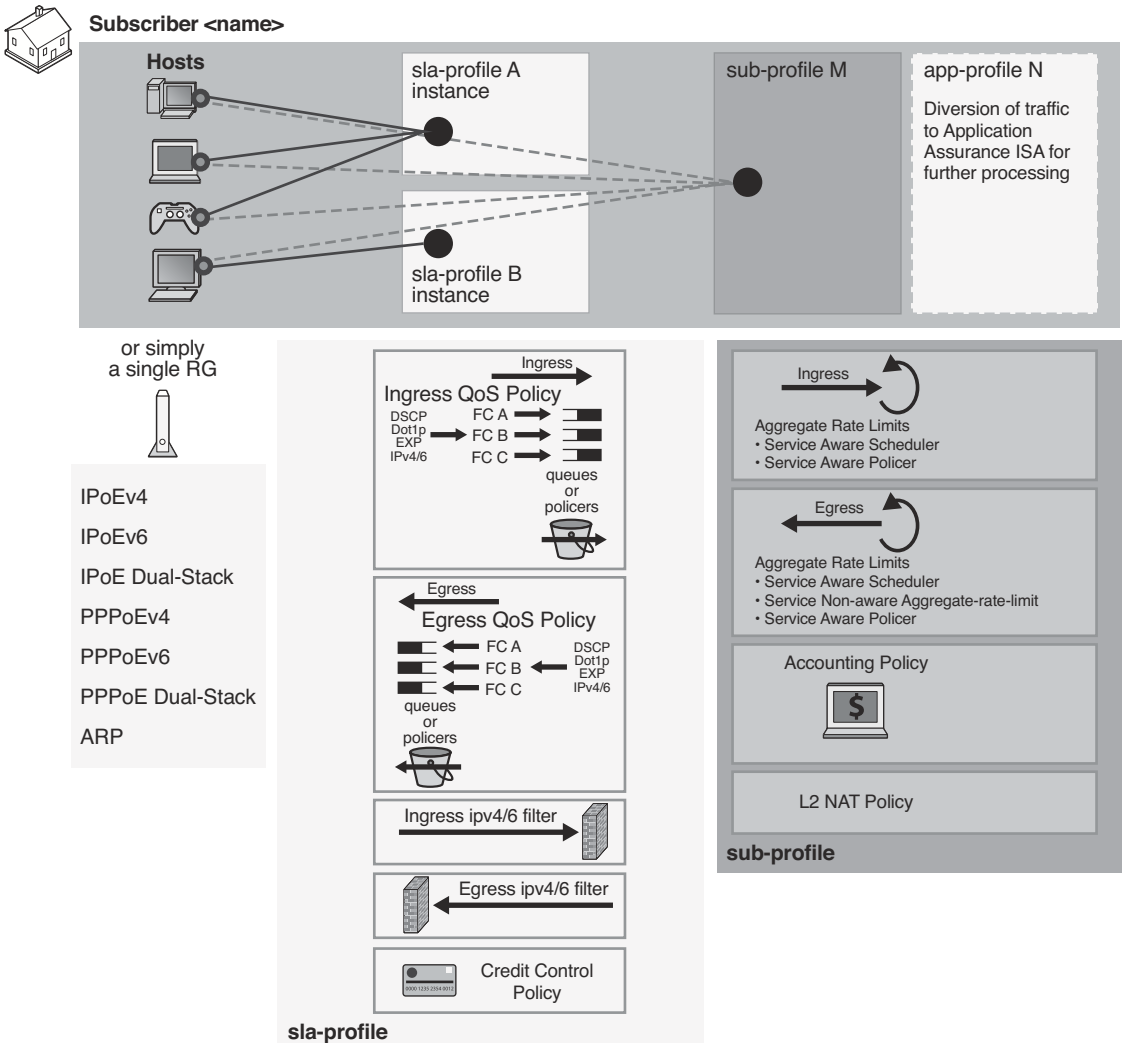

Figure 173: ESM Objects Managed via Various Policies and Profiles

The two basic concepts in ESM context are sla-profile with its associated objects and sub-profile with its associated objects.

- Sla-profile defines a service level (rates, queues, filters) for a group of hosts sharing the same sla-profile instance within the subscriber. There can be multiple sla-profile instances per subscriber.
- Sub-profile defines aggregate rate of the subscriber along with accounting policy. There is only one sub-profile per subscriber.

Instantiation of Gx Overrides

For a list of Gx related AVPs supported in 7x50, refer to the 7750 SR OS Gx AVPs Reference Guide.

Gx overrides are installed via Charging-Rule-Install AVP (for ESM or AA) or ADC-Rule-Install AVP (for AA only – 3GPP Release 11) sent from the PCRF towards 7x50.

AVP Format:

```
Charging-Rule-Install ::= < AVP Header: 1001 >
                                *[ Charging-Rule-Definition ]
                                *[ Charging-Rule-Name ]
                                *[ AVP ]

ADC-Rule-Install ::= < AVP Header: 1092 >
                                *[ ADC-Rule-Definition ]
                                *[ ADC-Rule-Name ]
                                *[ AVP ]
```

Every Gx override must have a Charging-Rule-Name (ESM) or ADC-Rule-Name (AA - 3GPP Release 11 and Release 12) associated with it. This is important in order to return the override status from 7x50 to the PCRF upon the override instantiation.

The objects (subscriber-hosts) to which the new overrides are applied must exists in 7x50 otherwise the override installation will fail.

Removal of overrides is not supported. The parameters defining a new override will simply replace the existing parameters that are already applied to the subscriber-host, without the need to remove the previously installed parameters.

There are four types of overrides that are currently supported via Gx:

- ESM string overrides (sla/sub/app-profiles, subscriber-id, etc.)
- Update of subscriber host QoS information (queue rate change, etc.)
- Filter override for the subscriber host (including one-time http redirect)
- Category-map installation/override

Charging-Rule-Name AVP within the Charging-Rule-Install grouped AVP points to the preconfigured filter in the system, the preconfigured subscriber profiles or it simply represents the ESM string (such as inter-destination-string used to associate the subscriber host with a vPort construct). The existing objects applied to the subscriber-host will be replaced with the referenced one.

It is important to distinguish two locations for invoking Charging-Rule-Name AVP for overrides:

1. Directly under the Charging-Rule-Install AVP – in this case the Charging-Rule-Name will reference the predefined structures (profiles, filter-ids, cat-maps, etc) within 7x50. The type of the structure is contained within the Charging-Rule-Name AVP in the form of a reserved keyword that has to be prepended (in bold below) to the identifier of structure:

   Filter installation/overrides:

   - Charging-Rule-Name = Ingr-v4:<id>
   - Charging-Rule-Name = Ingr-v6:<id>
   - Charging-Rule-Name = Egr-v4:<id>
   - Charging-Rule-Name = Egr-v6:<id>
   - Charging-Rule-Name = In-Othr-v4:<id> (othr - one-time-http-redirect)
   - Charging-Rule-Name = In-Othr-v6:<id> (othr - one-time-http-redirect)

   Subscriber-Id override:

   - Charging-Rule-Name = Sub-Id:sub-id-string

   Profile installation/overrides:

   - Charging-Rule-Name = Sla-Profile:sla-profile-name
   - Charging-Rule-Name = Sub-Profile:sub-profile-name

   Inter-destination string override:

   - Charging-Rule-Name = Inter-Dest:inter-dest-string

   Usage-Monitoring:

   - Charging-Rule-Name = Cat-Map:category-map-name

   AA:

   - Charging-Rule-Name = AA-UM:<string-name>
   - Charging-Rule-Name=AA-Functions:<string-name>

In summary, the reserved prefixes “ingr-v4:”, “ingr-v6:”, “egr-v4:”, “egr-v6:”, “in-othr-v4:”, “in-othr-v6:”, “sub-id:”, “sla-profile:”, “sub-profile:”, “inter-dest:”, “cat-map:”, “aa-um:” and “aa-functions:” have special meaning within the Charging-Rule-Name AVP in 7750.

2. Under the Charging-Rule-Install — Charging-Rule-Definition AVP. In this case the override itself is not pre-provisioned in 7x50 but instead directly defined in the Charging-Rule-Definition. Part of the override definition is the name assignment via Charging-Rule-Name AVP. The Charging-Rule-Name AVP is used to report on the override status.

   For example, the Charging-Rule-Name AVP for QoS overrides is an arbitrary name. This AVP is part of Charging-Rule-Definition AVP in which QoS-Information is provided. Such Charging-Rule-Name is used to report errors related to instantiation of the override.

   ADC-Rule-Name AVP within the ADC-Rule-Install grouped AVP handles application policy related processing (AA). This AVP is applicable under the ADC-Rule-Install—ADC-Rule-Definition AVP. In this case the ADC rule itself is not pre-provisioned in 7x50 but instead directly defined in the ADC-Rule-Definition. In AA, such rule definition can define AA overrides that will be applied to the subscriber. In other words, the existing objects for the subscriber will be replaced with the ones referenced in the rule. Part of the ADC rule definition is the ADC rule name assignment via ADC-Rule-Name AVP. The ADC-Rule-Name defined in such manner is used to report on the rule status.

   “AA-Functions:" prefix in the ADC rule name is reserved for ADC rule definitions applicable to “AA-functions” (namely: app-profile and ASOs):

   ADC-Rule-Name = AA-Functions:aa-rule-name

   In this case, the aa-rule-name is an arbitrary name that will be used in rule status reporting.

   In case that ADC-Rule-Name is used in AA Usage-Monitoring, the “AA-Functions:” prefix must not be present (Usage-Monitoring in AA is covered in details in the SR OS Multi-Service Integrated Services Adapter Guide). Note however, that AA-Function AVP and AA-Usage-Monitoring cannot co-exist in the same ADC rule.

   Charging-Rule-Definition AVP (AVP code 1003, 3GPP 29.212 §5.3.4) is of type Grouped, and it defines the override sent by the PCRF to the 7x50.

   The Charging-Rule-Name in this AVP can be arbitrarily set and it is used to uniquely identify the overrride in error reporting.

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
                                { Charging-Rule-Name }
                                [ QoS-Information ]
                                [ Nas-Filter-Rule]
                                [ Alc-NAS-Filter-Rule-Shared]
                                *[ AVP ]
```

ADC-Rule-Definition AVP (AVP code 1094, 3GPP 29.212 §5.3.87) is of type Grouped, and it defines the ADC override sent by the PCRF to the 7x50. The ADC-Rule-Name AVP within the ADC-Rule-Definition AVP uniquely identifies the ADC policy rule and it is used to reference to a policy rule in communication between the 7x50 and the PCRF within one IP CAN session.

```
ADC-Rule-Definition ::= < AVP Header: 1094 >
```

```
{ ADC-Rule-Name }
[AA-Functions]
*[ AVP ]
```

In summary:

- Central AVP for Gx overrides in 7x50 is Charging-Rule-Install AVP. Multiple overrides can be submitted to 7x50 via a single Charging-Rule-Install AVP or each Gx override can be submitted via its own Charging-Rule-Install AVP.
- Gx override is identified by Charging-Rule-Name AVP. This AVP is also used to report on the status of Gx override. The Charging-Rule-Name can reference a pre-configured construct within 7x50 (profiles, cat-maps, filters) or it can be assigned by PCRF to identify the PCRF defined override (QoS policy modifications, AA ASO modifications, etc.).
- Aforementioned overrides cannot be removed by Charging-Rule-Remove AVP. They can only be overridden. Charging-Rule-Remove AVP is ignored for Gx overrides. However, it is not ignored for PCC rules.

Examples of Gx Overrides

There are two ways of enforcing a Gx override in 7x50:

1. Multiple Gx overrides in single Charging-Rue-Install AVP
2. Single Gx override per Charging-Rule-Install AVP.

The following AVPs will identify Gx overrides that will be applied to a subscriber host. These AVPs can be included in CCA-i, CCA-u or RAR message sent from the PCRF. Note that in the first approach, all Gx overrides are submitted under a single Charging-Rule-Install AVP:

```
Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "sub-id:residence-1"
     Charging-Rule-Name <AVP Header: 1005> = "ingr-v4:7"
     Charging-Rule-Name <AVP Header: 1005> = "eggr-v6:5"
     Charging-Rule-Name <AVP Header: 1005> = "Sub-Profile:prem"
     Charging-Rule-Name <AVP Header: 1005> = "Sla-Profile:voip+data"
     Charging-Rule-Name <AVP Header: 1005> = "Inter-Dest:vport-AN-1"

     Charging-Rule-Definition <AVP Header: 1003>
          Charging-Rule-Name <AVP Header: 1005> = "premium-service"
          QoS-Information <AVP Header: 1016>
               Alc-Queue <AVP Header; vnd ALU; 1016>
                                                  Alc-Queue-id <AVP Header; vnd ALU; 1007> =
5
                                                  Max-Requested-Bandwidth-UL <AVP Header:
516> = 10000
                    Max-Requested-Bandwidth-DL <AVP Header: 515> = 100000
                    Guaranteed-Bitrate-UL <AVP Header: 1026> = 5000
               Guaranteed-Bitrate-DL <AVP Header: 1027> = 50000
                                                  Alc-Committed-Burst-Size-UL <AVP Header;
vnd ALU; 1008> = 1000
                                  Alc-Maximum-Burst-Size-UL <AVP Header; vnd ALU; 1009> =
2000
                                  Alc-Committed-Burst-Size-DL <AVP Header; vnd ALU; 1010> =
1000
                                  Alc-Maximum-Burst-Size-DL <AVP Header; vnd ALU; 1011> =
2000

                                  Alc-Queue <AVP Header; vnd ALU; 1006>
                                           Alc-Queue-id <AVP Header; vnd ALU; 1007> = 7
                                           Max-Requested-Bandwidth-UL <AVP Header: 516> =
10000
               Max-Requested-Bandwidth-DL <AVP Header: 515> = 100000
               Guaranteed-Bitrate-UL <AVP Header: 1026> = 5000
               Guaranteed-Bitrate-DL <AVP Header: 1027> = 50000
                                           Alc-Committed-Burst-Size-UL <AVP Header; vnd
ALU; 1008> = 1000
                            Alc-Maximum-Burst-Size-UL <AVP Header; vnd ALU; 1009> = 2000
                            Alc-Committed-Burst-Size-DL <AVP Header; vnd ALU; 1010> = 1000
                            Alc-Maximum-Burst-Size-DL <AVP Header; vnd ALU; 1011> = 2000

                                  Alc-Sub-Egress-Rate-Limit <AVP Header; vnd ALU; 1016> =
10000
```

```
ADC-Rule-Install ::= <AVP Header: 1092>
         ADC-Rule-Definition <AVP Header: 1094>
              ADC-Rule-Name <AVP Header: 1096> = "AA-Functions:apps"
              AA-Functions
                   AA-App-Profile-Name = "apps-prof"
                   AA-App-Service-Options
                        AA-App-Serv-Options-Name = "bitttorent"
                        AA-App-Serv-Options-Value = "low-prio-1mbps"
                   AA-App-Service-Options
                        AA-App-Service-Options-Name =  "ftp"
                        AA-App-Service-Options-Value = "hi-prio"
```

In this example various subscriber profiles (sub/sla) will be applied to the subscriber host and at the same time a new ingress v4 and egress v6 filter will be installed. The subscriber-id will be overridden with the new name 'residence-1'. Characteristics for queue 5 and 7 will be overridden.

Also the egress rate limit for the subscriber will be overridden and the subscriber host will be associated with the vPort named vport-AN-1.

All x overrides are aggregated under the same Charging/ADC-Rule-Install AVP.

```
In the following example all Gx overrides are submitted via a separate Charging-Rule-
Install AVP:
Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "sub-id:residence-1"

Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "ingr-v4:7"

Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "eggr-v6:5"

Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "Sub-Profile:prem"

Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "Sla-Profile:voip+data"

Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "Inter-Dest:Gx-inserted-string"

Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Definition <AVP Header: 1003>
          Charging-Rule-Name <AVP Header: 1005> = "premium-service"
          QoS-Information <AVP Header: 1016>
               Alc-Queue <AVP Header; vnd ALU; 1016>
                    Alc-Queue-id <AVP Header; vnd ALU; 1007> = 5
                         Max-Requested-Bandwidth-UL <AVP Header: 516> = 10000
               Max-Requested-Bandwidth-DL <AVP Header: 515> = 100000
       Guaranteed-Bitrate-UL <AVP Header: 1026> = 5000
       Guaranteed-Bitrate-DL <AVP Header: 1027> = 50000
                         Alc-Committed-Burst-Size-UL <AVP Header; vnd ALU; 1008> = 1000
```

```
                Alc-Maximum-Burst-Size-UL <AVP Header; vnd ALU; 1009> = 2000
                Alc-Committed-Burst-Size-DL <AVP Header; vnd ALU; 1010> = 1000
           Alc-Maximum-Burst-Size-DL <AVP Header; vnd ALU; 1011> = 2000

                Alc-Queue <AVP Header; vnd ALU; 1006>
                          Alc-Queue-id <AVP Header; vnd ALU; 1007> = 7
                          Max-Requested-Bandwidth-UL <AVP Header: 516> = 10000
      Max-Requested-Bandwidth-DL <AVP Header: 515> = 100000
      Guaranteed-Bitrate-UL <AVP Header: 1026> = 5000
      Guaranteed-Bitrate-DL <AVP Header: 1027> = 50000
                          Alc-Committed-Burst-Size-UL <AVP Header; vnd ALU; 1008> = 1000
           Alc-Maximum-Burst-Size-UL <AVP Header; vnd ALU; 1009> = 2000
           Alc-Committed-Burst-Size-DL <AVP Header; vnd ALU; 1010> = 1000
           Alc-Maximum-Burst-Size-DL <AVP Header; vnd ALU; 1011> = 2000

                Alc-Sub-Egress-Rate-Limit <AVP Header; vnd ALU; 1016> = 10000



ADC-Rule-Install ::= <AVP Header: 1092>
     ADC-Rule-Definition <AVP Header: 1094>
          ADC-Rule-Name <AVP Header: 1096> = "AA-Functions:apps"
          AA-Functions
               AA-App-Profile-Name = "apps-prof"
               AA-App-Service-Options
                    AA-App-Service-Options-Name = "bitttorent"
                    AA-App-Service-Options-Value = "low-prio-1mbps"
               AA-App-Service-Options
                    AA-App-Service-Options-Name =  "ftp"
                    AA-App-Service-Options-Value = "hi-prio"
```

Gx overrides (qos rates, sub/sla-profiles, filters, etc.) can be examined individually via subscriber specific operational commands. In the example below, fields in bold can be overridden.

```
show service  active-subscribers detail
===============================================================================
Active Subscribers
===============================================================================
-------------------------------------------------------------------------------
Subscriber residence-1 (prem)
-------------------------------------------------------------------------------
I. Sched. Policy : basic_policy
E. Sched. Policy : N/A               E. Agg Rate Limit: 10000
I. Policer Ctrl. : N/A
E. Policer Ctrl. : N/A
Q Frame-Based Ac*: Disabled
Acct. Policy     : N/A               Collect Stats    : Disabled
Rad. Acct. Pol.  : N/A
Dupl. Acct. Pol. : N/A
ANCP Pol.        : N/A
HostTrk Pol.     : N/A
IGMP Policy      : N/A
MLD Policy       : N/A
Sub. MCAC Policy : N/A
NAT Policy       : N/A
Def. Encap Offset: none             Encap Offset Mode: none
Avg Frame Size   : N/A
```

```
Vol stats type   : full
Preference       : 5
Sub. ANCP-String : "iope-left-dupl"
Sub. Int Dest Id : "Gx-inserted-string"
Igmp Rate Adj    : N/A
RADIUS Rate-Limit: N/A
Oper-Rate-Limit  : 10000


show service id 10 subscriber-hosts detail
===============================================================
Subscriber Host table
===============================================================
Sap                    Subscriber
  IP Address
    MAC Address          PPPoE-SID Origin       Fwding State
---------------------------------------------------------------
[1/1/5:6.2]            iope-sub
  192.168.0.11
    00:00:65:06:02:01    N/A       DHCP         Fwding
---------------------------------------------------------------
Subscriber-interface  : int1
Group-interface       : g1
Sub Profile           : prem
SLA Profile           : voip+data
App Profile           : apps-prof
Egress Q-Group        : N/A
Egress Vport          : N/A
Acct-Session-Id       : D896FF0000001852EDFF46
Acct-Q-Inst-Session-Id: D896FF0000001952EDFF51
Address Origin        : DHCP
OT HTTP Rdr IP-FltrId : N/A
OT HTTP Rdr Status    : N/A
OT HTTP Rdr Fltr Src  : N/A
HTTP Rdr URL Override : N/A
GTP local break-out   : No
```

PCC Rules

A generic use case for flow based dynamic policy is related to customized network level treatment of on-demand services. Such services can represent wide range of applications, such as video-on-demand or an access to a specific application in the network. The service can be identified by traffic destination parameters or DSCP bits. Once the service is identified within 7x50, a set of actions can be applied to the service (rate change, forwarding-class change, Usage-Monitoring, etc.).

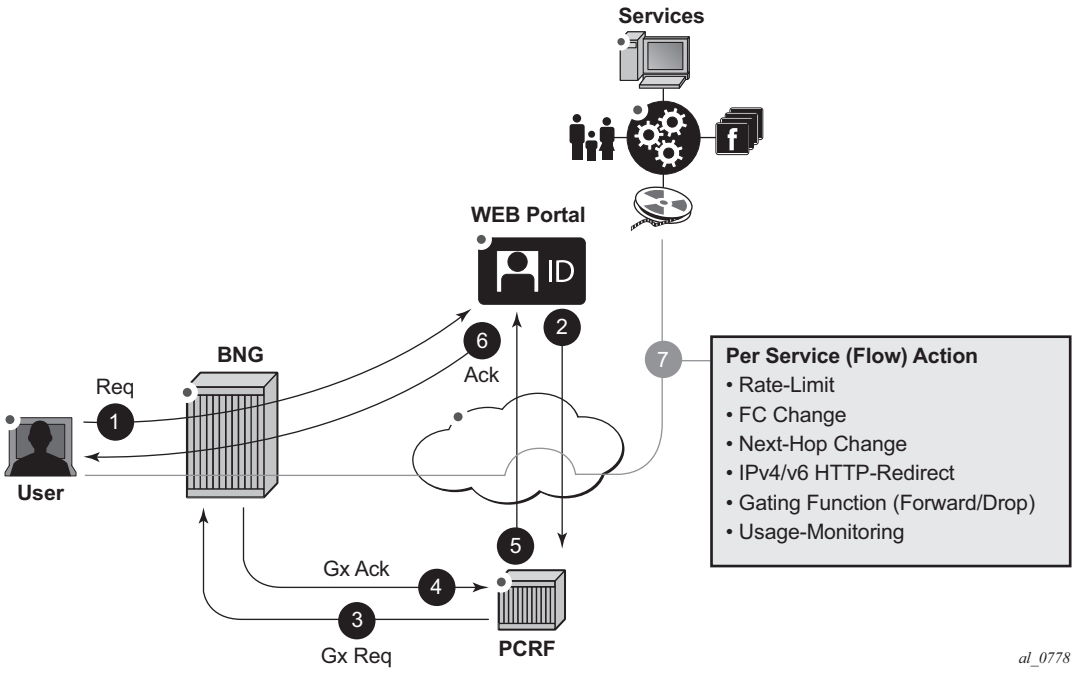

Figure 174: Generic Use Case For IP-Criterion Based Policy Change via Gx

Typical flow of events for service activation is shown in Figure 174:

1. An established user subscribes to a service in the network via a Web portal at any given time.
2. Once the authentication/payment is accepted, the back end (the Web portal integrated in OSS for example) identifies the service and submits the parameters defining the network delivery of the offered service to the PCRF.
3. The PCRF converts those parameters into rules and submits those rules to the subscriber-host in 7x50-BNG via Gx. The rules identify the service on the network level (destination IP@ and port) along with the desired action.

4. [and 5) and 6)] Before the service can be started, the action of individual policy management elements must be acknowledged to ensure that the resources for the service delivery are available and instantiated before the service is delivered to the subscriber.
7. The service traffic can be started from the subscriber side. Network requirements for the successful service delivery will be enforced on a per flow/DSCP basis as defined by the PCC rule.

PCC Rule Concept

A PCC rule consists of traffic classifiers (Flow-Information AVPs) required for traffic identification, and one or more actions associated with such classified traffic. PCC rules are unidirectional, which means that each rule is applied on ingress or egress. They are provisioned from PCRF via Gx interface.

Traffic classification is based on:

- 5 Tuple (IPv4 and IPv6)
- DSCP bits. In cases where the content hosting device cannot be identified by the IP addres, port and protocol, the DSCP marking can be used instead. In that case, the DSCP marking will be set by the client application and the markings should be preserved throughout the network until they reach BNG.

Supported actions are:

- Rate-limiting (in | out)
- Forwarding-Class (FC) change (in | out)
- Next-hop Redirect (in)
- Service-Id Redirect (in)
- HTTP Redirect (in)
- Gate Function (in | out)
- Usage-Monitoring (in | out)

PCC Rule Instantiation

A PCC rule that is submitted to 7x50 via PCRF is internally instantiated using two basic policy constructs within 7x50, qos-policy and filter (ACL). Behavior-wise, this internal division is transparent to the operator at the time of the rule provisioning. The operator perceives Gx as a unified method for provisioning policy rules in 7x50, regardless of whether the rule is QoS related of filter (ACL) related.

The type of action within the PCC rule will determine whether the PCC rule is split within 7x50 between the qos-policy and the filter.

Rules with actions:

- rate-limit
- forwarding-class change

- usage-monitoring

will be converted into a qos-policy within 7x50, while the rules with actions:

- next-hop redirect
- service-id redirect
- HTTP Redirect
- enable/drop (gating function)

will be converted into filter rules.

The operator should be aware of this division for the dimensioning (scaling) purposes. Operational commands can be utilized to reveal resource consumption within 7x50.

A PCC rule is addressed to a subscriber-host (single stack or dual-stack) via the Diameter session-id. However, qos-policy-related entries are applied per sla-profile instance since the qos resources are allocated per sla-instance[1]. This means that all hosts sharing the same sla-profile instance will inherit the change.

Filter-related entries are applied per each subscriber-host, irrespective of whether the hosts are sharing an sla-profile instance or not.

The concept of splitting the rules in 7x50 is shown in Figure 175.

1. An sla-profile instance and sla-profile are two distinct concepts. An sla-profile instance is an instantiation of the sla-profile which is a configuration concept in which parameters are defined. An sla-profile is instantiated per a subscriber-host, or multiple subscriber-hosts can share an sla-profile instance as long as they belong to the same SAP and have the same subscriber-id.

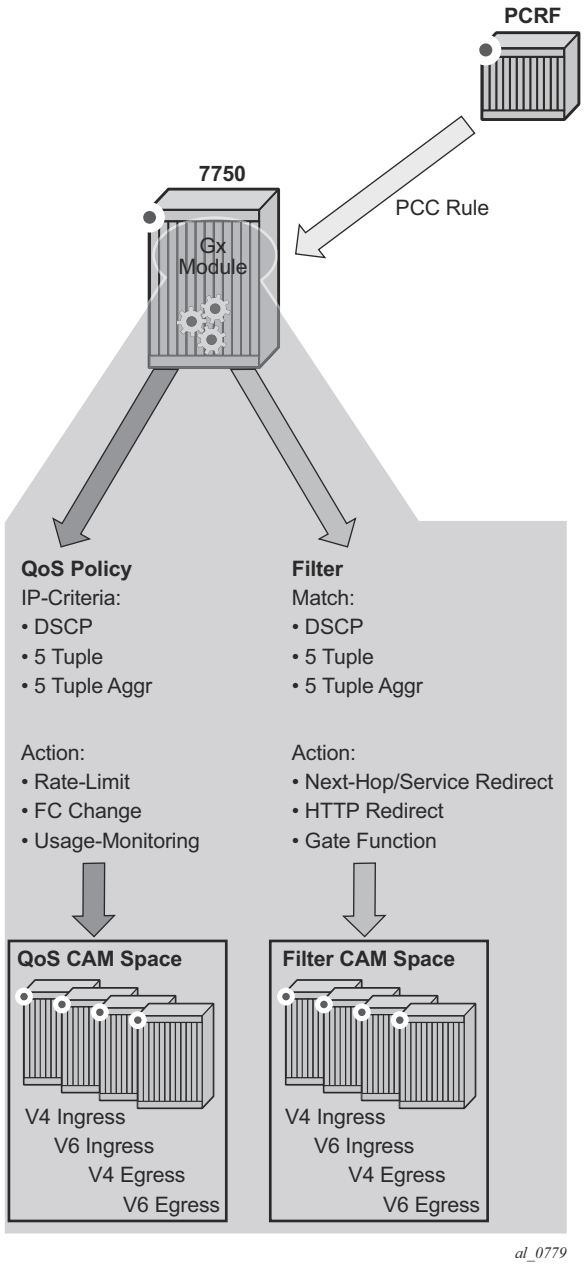

Figure 175: PCC Rule Conversion within 7x50

The PCC rule instantiation will fail in 7x50 in case that a PCC rule contains only actions, without any classification, or if it contains only classification without any actions.

Base QoS-Policy and Base Filter

Subscriber host must have an explicit static (or base) filter or qos-policy before any dynamic entries can be inserted via Gx. For example, a base filter/qos-policy can be referenced by a sla-profile when the subscriber is instantiated. However, the parameters in the base qos-policy and base filter cannot be modified via Gx.

In the absence of explicitly defined qos-policy for the subscriber host, the default **qos-policy 1** will be in effect. In this case, PCC rules with qos related action cannot be applied.

PCC rule entries can be inserted in specifically allocated range in the base filter or qos-policy. The insertion point is controlled by the operator. This is shown in Figure 176. The entries reserved for PCC rules start at the beginning of the range specified by the following CLI command:

```
sub-insert-shared-pccrule start-entry <entry-id> count <count>
```

under the following CLI hierarchy:

```
configure>filter>ip-filter>
configure>filter>ipv6-filter
configure>qos>sap-ingres>
configure>qos>sap-egress>
```

An entry corresponds to a Flow-Information AVP and is equivalent to a match condition defined as any combination of the following parameters under a filter or **qos-policy ip-criteria**:

- source IP address
- destination IP address
- source port or port range
- destination port or port range
- protocol
- DSCP

Such defined entry will map into a single CAM entry with exception of port range configured as match criteria whereby a single port range command can expand into multiple CAM entries.

Static entries in filter/qos-policy can be inserted before and after the range reserved for PCC rules.

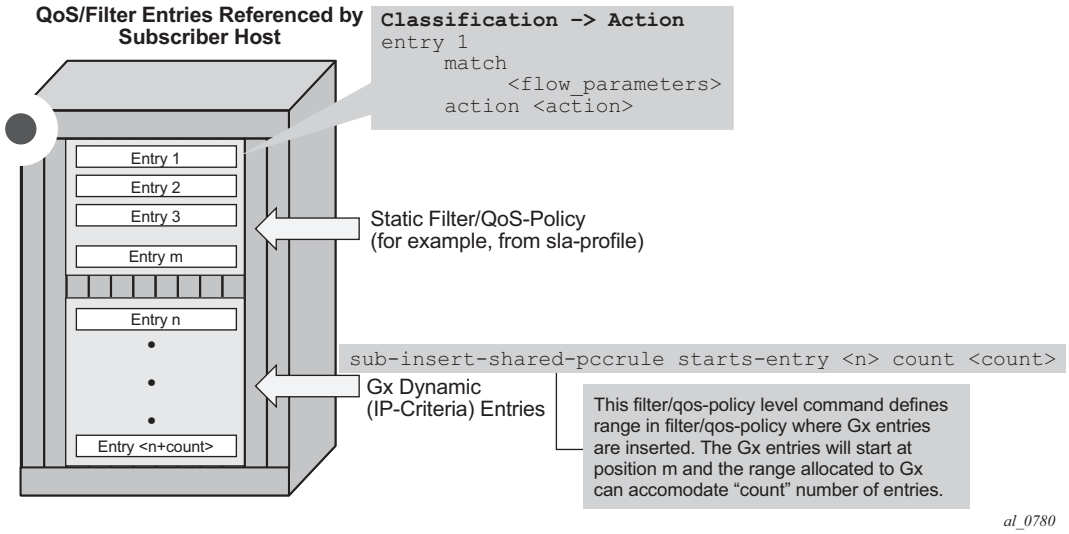

Figure 176: Static and Dynamic QoS-Policy/Filter Entries

Generic Policy Sharing and Rule Sharing

Policy[2] sharing between the subscriber hosts is depicted in Figure 177. In order to simplify CAM scaling explanations, the examples in this section assume that one rule within the policy occupies exactly one CAM entry. For simplicity, only PCC rules are shown but in reality a subscriber-host policy consist of PCC rules together with the base qos-policy/filter.

A policy, as a set of rules, can be shared amongst the subscriber-hosts. However, when a new rule is added to one of the subscriber-host, the newly created set of rules for this host becomes unique. Hence, a new policy for the subscriber-host will be instantiated. This new policy will consume additional resources for all the old rules (clone of the old policy) along with the new rule. Figure below shows that a new policy (3) is instantiated when rule D is added to User 1, even though the rules A, B and C remain the same for Users 1 and 2. Policy 3 is a newly cloned with the same rules as Policy 1, and then Rule D is added onto it. On the other hand, when the rule C is applied to User 3, the set of rules becomes identical to the set of rules for User 2. Thus the two can start sharing rules and therefore the resources are freed.

Figure 177: Policy Cloning

2. Policy is in this context defined as a collection of static and dynamic rules.

PCC Rule Name and PCC Rule Removal

Each PCC rule has a subscriber-host scope and it is referred to it by its name which is assigned by the operator on PCRF. The rules with exactly the same content but different rule names are evaluated into separate rules. To optimize performance and maximize scale, it is recommended that the rules sharing the same content have the same name (as provisioned in the PCRF).

PCC rules can be removed from 7x50 via a Gx directive by referencing the PCC rule name. The rule name is supplied via Charging-Rule-Name AVP at the time of the rule submission to the 7x50 by the PCRF. There is no Gx mechanism that would remove all PCC rules at once. Each PCC rule must be removed individually.

The AVP used to remove the rule from 7x50 is:

```
Charging-Rule-Remove ::= < AVP Header: 1002 >
                                *[ Charging-Rule-Name ]
```

An example of rule instantiation and rule removal is shown in Figure 178.

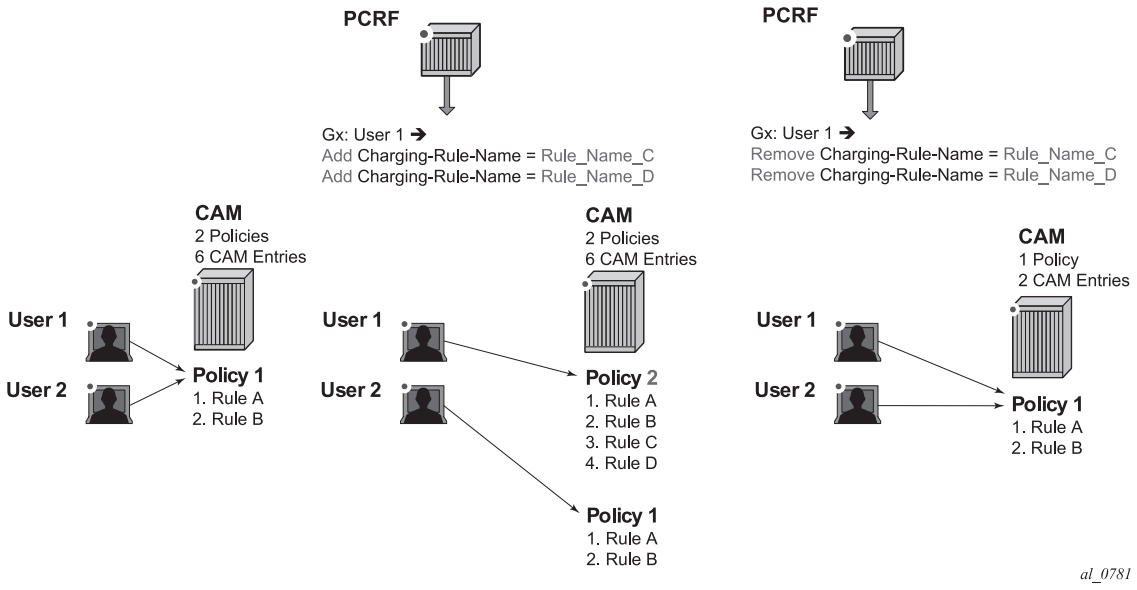

Figure 178: Policy Removal by Name

Gx Rule Ordering

Entries in IPv4/v6 filter and QoS policy created via CLI are ordered according to the numerical value associated with each entry command (which corresponds to the match condition) within the policy. CLI rules can be re-ordered with the **renum** command (in filters and QoS policies).

On the other hand, the PCC rules are ordered in one of the two ways[3]:

- PCC rules are prioritized according to the Precedence AVP within the Charging-Rule-Definition AVP. They are inserted within the subscriber-host policy, according to the Precedence AVP relative to the other PCC rules already applied to the subscriber-host. A PCC rule with a lower Precedence value will be applied before a rule with a higher Precedence value.

The ordering behavior according to the Precedence is shown in Figure 179.

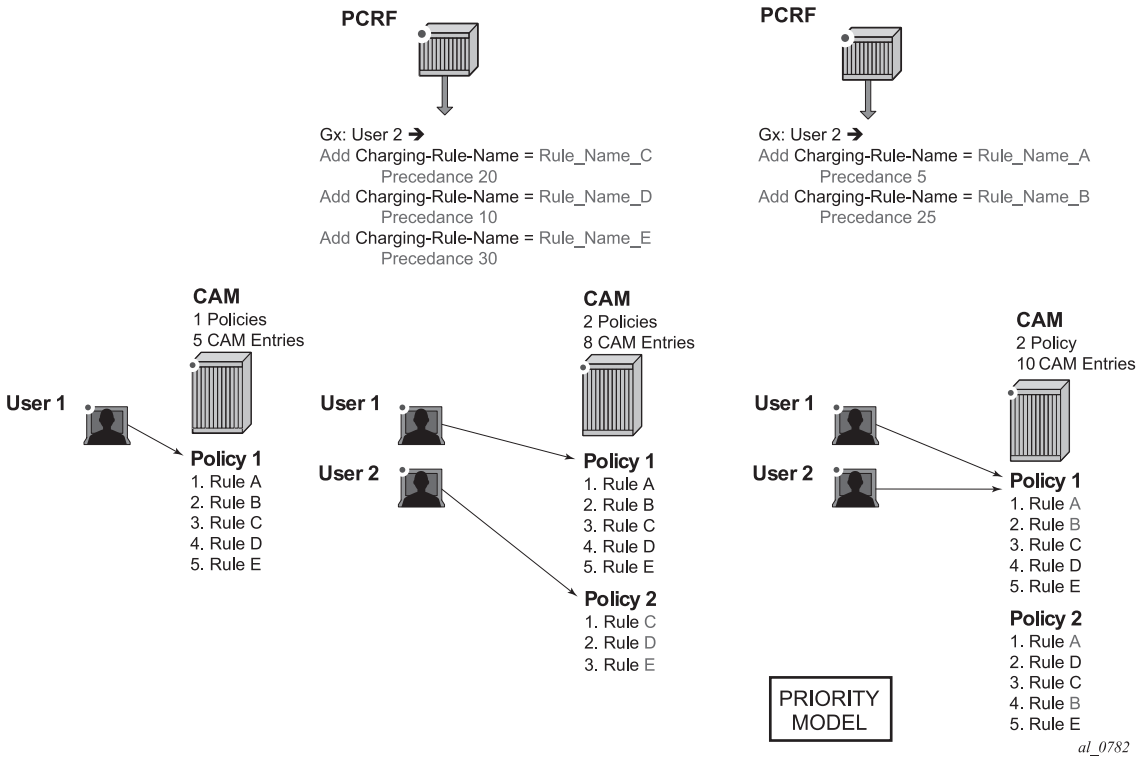

Figure 179: PCC Rule Ordering - Priority Model

3. Note the difference between ordering of the entries with the rules, and the ordering of the rules themselves.

- Automatic optimization of PCC rules. Automatic optimization is used in cases where the PCC rule order is not important for the operator. In this case, the 7x50 will optimize the rule ordering to achieve the best possible scale by means of maximizing the sharing of the rules. This optimization (or internal rule ordering) is performed for PCC rules without the Precedence AVP, or for PCC rules with the same Precedence value.

The premise of the automatic rule optimization is shown in Figure 179.

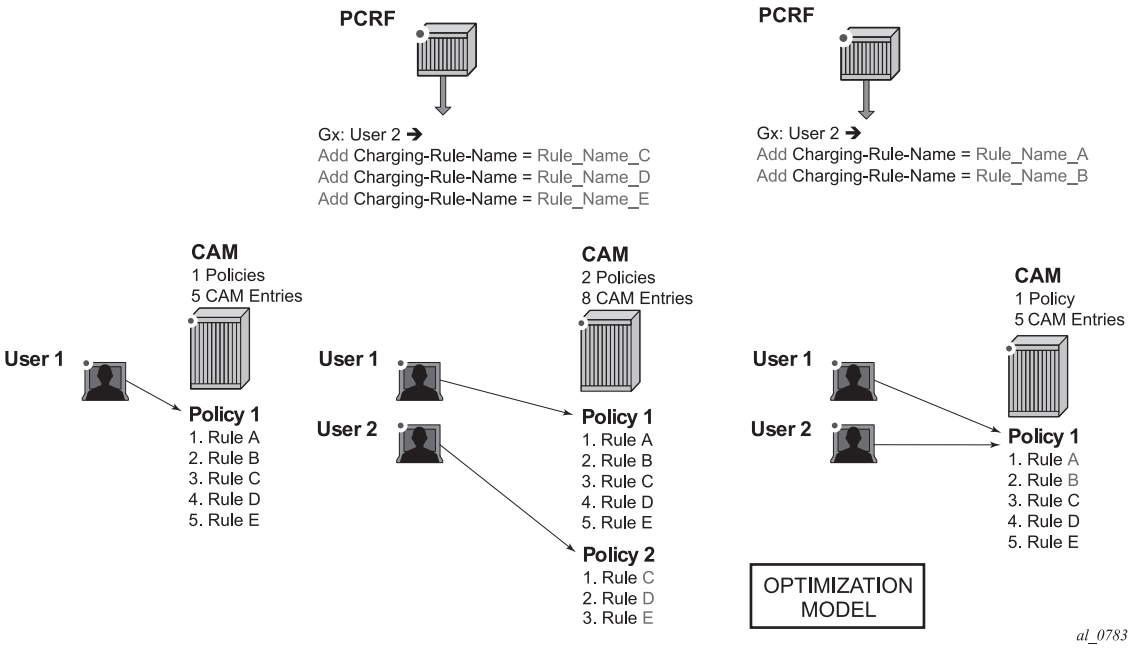

Figure 180: Rule Ordering - Optimization Model

The ordering of PCC rules has no effect on the ordering of the static entries in the base qos-policy or filter.

Mixing of the PCC rules with the Precedence AVP and without Precedence AVP is allowed for the same subscriber-host. PCC rules without the Precedence AVP will be inserted at the end of all PCC rules that do have the Precedence value set explicitly. In other words, the Precedence value for PCC rules without the explicitly configured Precedence AVP is assumed to be the highest. The PCC rules without the Precedence value are automatically inserted at the bottom of the PCC rule range.

A distinction should be made between the order of PCC rules in a PCC rule set and the order between the entries within each PCC rule. A PCC rule contains a group of classifiers that are all associated with the same actions. Therefore, the order of the entries (equivalent to match conditions) within any given PCC rule does not matter (all entries result in the same action). For this reason, PCC rules with identical name and identical entries but different order of the entries

are automatically ordered within 7x50 in a way that what would allow more optimal sharing of the rules between different subscribers

PCC Rule Override

A PCC rule applied to a subscriber-host in 7x50 can be overridden by re-submitting the PCC rule with the same name but different contents.

In case that at least 1 new flow is sent in the PCC rule update, then the existing flows are removed and replaced with the new flow. In case that no new flows are submitted, then the existing flows stay in place.

In case that there are conflicting parameters between the existing rule and the modified rule (for example the combination of the unsupported actions), the PCC rule override will fail.

Aggregation of IP-Criterion

An action with a PCC rule can be applied for a set of IP-criterion.

For example, a single policer can be instantiated for a set of flows for rate-limiting purposes.

A pseudo Gx directive would look like this:

```
Charging-Rule-Install — Directive to install the rule in 7x50
         Charging-Rule-Definition — PCC rule definition created on PCRF
              Charging-Rule-Name = Rule-1 — PCC rule name
                   Flow1      — match-criteria for flow 1
                   Flow2      — match-criteria for flow 2
                   Flow 2     — match-criteria for flow 3
                   Rate-limit – rate-limiting action applicable as an aggregate action for all 3 flows
```

All three flows will be fed into the same rate limiter (policer).

Gx Rules with Multiple Actions and Action Sharing

PCC rule can contain multiple actions.

The following table shows combinations of actions that are supported simultaneously within a given rule.

Legend:

- QoS:
  - rateLim: PIR/CIR upstream/downstream
  - fcChg: set/change forwarding class
- ACL:
  - rdNhR: redirect to next hop IP@ and/or router
  - rdrUrl: redirect to URL
  - gate-enable: default action that must be accompanied with one or more other qos or filter related actions within the same rule. If this is the only action in the rule, the entire rule will be rejected.
  - gate-disable: drop traffic.
  - UM: Usage-Monitoring

Ingress:

Table 26: Combinations of Allowed Actions on Ingress

	rateLim	fcChg	rdrNhR	rdrUrl	gate-enable	gate-disable	UM
rateLim	OK	OK	OK	-	OK	OK	OK
fcChg	OK	OK	OK	OK	OK	OK	OK
rdrNhR	OK	OK	OK	-	OK	OK	OK
rdrUrl	-	OK	-	OK	OK	OK	-
gate-enable	OK	OK	OK	OK	OK	-	OK
gate-disable	OK	OK	OK	OK	-	OK	OK
UM	OK	OK	OK	-	OK	OK	OK

Egress:

Table 27: Combinations of Allowed Actions on Egress

	rateLim	fcChg	gate-enable	gate-disable	UM
rateLim	OK	OK	OK	OK	OK
fcChg	OK	OK	OK	OK	OK
gate-enable	OK	OK	OK	-	OK
gate-disable	OK	OK	-	OK	OK
UM	OK	OK	OK	OK	OK

Combining IPv4 and IPv6 Entries within the Rule

IPv4 flow entries and IPv6 flows entries can be combined within the same PCC rule. The actions that carry the IP address are address-type specific (for example next-hop-redirect). All other non IP address aware actions (rate-limit, FC change, etc.) are universal and it will be applied to both flow types (IPv4 and IPv6). 7x50 will automatically sort out flow types (IPv4 and IPv6) within the rule and apply corresponding actions.

In case that the rule contains a mismatching flow type and actions (for example IPv4 flows and IPv6 specific action), the 7x50 will reject the rule. It is the operator's responsibility to ensure that the address type specific actions in the rule have corresponding flows to which they can be applied.

Alc-NAS-Filter-Rule-Shared AVP vs Flow-Information AVP

A Gx rule (as defined in a single Charging-Rule-Definition AVP) can contain either Flow-Information AVP or Alc-NAS-Filter-Rule-Shared AVP, but not both simultaneously.

Presence of either AVP within the Charging-Rule-Definition AVP determines the mode of operation for the rule:

- Alc-NAS-Filter-Rule-Shared AVP indicates the mode of operation in which the permit or deny action is part of the flow definition itself (Alc-NAS-Filter-Rule-Shared AVP). This mode of operation is referred as NAS filter inserts. The basic format of the AVP is the following (RFC 4849 and 4005; AVP Code 400):

```
<action> <direction> <protocol>  from <source> to <destination> <options>.
```

There can be multiple ip-criteria definitions within the rule per subscriber-host, and each ip-criteria carries its own permit/deny action. There can be only one such rule (Charging-Rule-Definition) per subscriber-host. The rule entries are installed within the filter range defined by the following command:

```
sub-insert-shared-radius start-entry <entry-id> count <count>
under the following CLI hierarchy:
configure>filter>ip-filter>
configure>filter>ipv6-filter
```

Such rule cannot be removed by the Charging-Rule-Remove directive referencing the rule name. Instead, each such Gx rule will overwrite the previous one.

- Flow-Information AVP indicates the mode of operation whereby all the flows in the rule share the same actions carried in separate AVPs. This mode of operation is referred to as PCC rule inserts. The rule entries are installed within the filter or qos-policy range defined by the following command:

```
sub-insert-shared-pccrule start-entry <entry-id> count <count>
under the following CLI hierarchy:
configure>filter>ip-filter>
configure>filter>ipv6-filter>
configure>qos>sap-ingress>
configure>qos>sap-egress>
```

There can be multiple flow based rules present in an orderly fashion and each rule can be individually removed by referencing its name.

Both modes of operation are supported simultaneously for the subscriber host.

RADIUS and Gx Interaction

Gx and RADIUS (CoA) policy management interfaces are simultaneously supported for the same subscriber-host.

RADIUS and Gx share the same entries for filter entry inserts (NAS-Filter-Rules and Alc-NAS-Filter-Rule-Shared) and therefore the most recent insert will override the previous one. Similar logic applies to subscriber-string overrides and QoS overrides, where the most recent source, overrides the previous one.

However, PCC rules (IP-criteria based Gx rules) are provisioned in a separate filter ‘entry’ space from RADIUS and Gx filter inserts and therefore the PCC rules and RADIUS/Gx based filter inserts can independently coexist.

Filter/QoS-policy entry order is shown in Figure 181. The order of configuration blocks (static, PCC rules or NAS filter inserts) is configurable. For example, an operator can specify that static filter entries are populated before PCC rules which are then populated before NAS filter inserts.

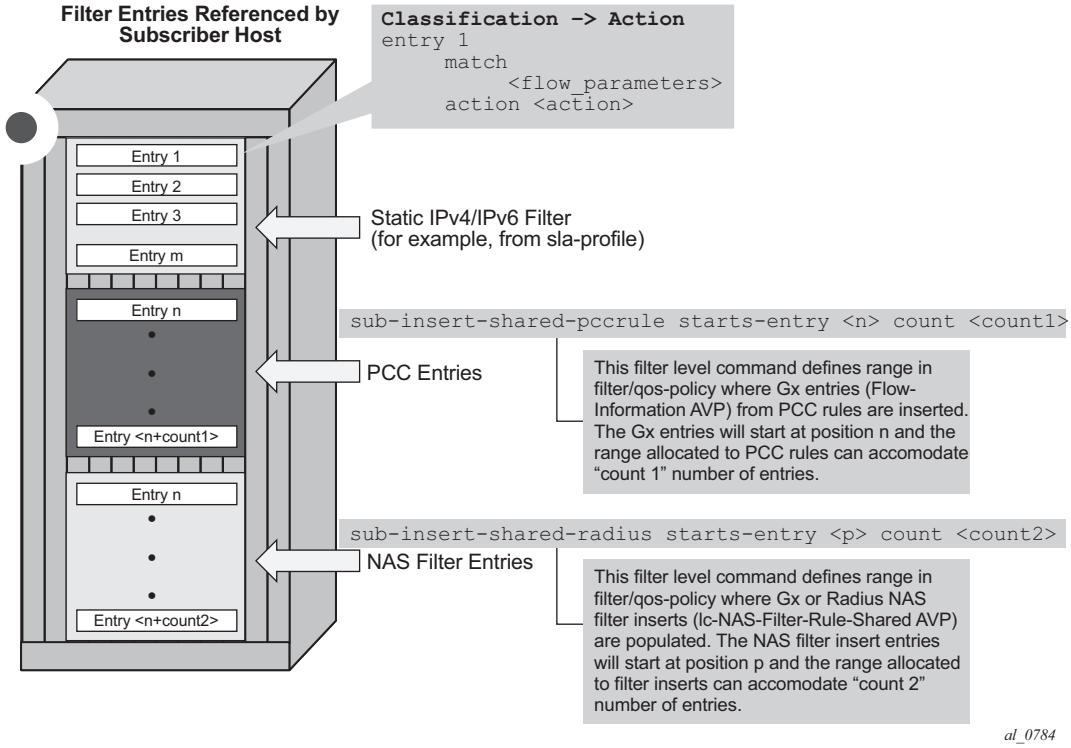

Figure 181: CAM Table Population

Bulk Changes via CLI while Gx Rules are Active

Once PCC rules are applied to a subscriber-host, the operator is allowed to modify via CLI some of the parameters in the base filter/qos-policy. For example, the operator is allowed to add/remove terms in the base ACL filter.

The list of the parameters in the QoS policy that can be changed is shown in Table 3. Adding/removing queue/policer, re-mapping of FC, modifying dscp-map or modifying static ip-criteria is not allowed.

Modified parameters in the base-policy/filter referenced in the sla-profile will affect all subscribers using this sla-profile. Replacing the base qos-policy/filter in sla-profile is not allowed for any subscriber-host in case that a clone of the base qos-policy/filter exist anywhere in the system.

However, replacing the base filter-id for a host via CoA or Gx override is allowed. In this case, only the targeted host will be affected and all existing PCC rules for this host will be merged with the new filter.

Table 28: CLI Modifiable Parameters in Base QoS-Policy that Contains Clones

CLI
config>qos>sap-ingress>queue
[no] cbs - Specify CBS
[no] high-prio-only - Specify high priority only burst size
[no] mbs - Specify MBS
[no] packet-byte-of* - Specify packet byte offset
[no] parent - Specify the scheduler to which this queue feeds
[no] percent-rate - Specify percent rates (CIR and PIR)
[no] rate - Specify rates (CIR and PIR)
config>qos>sap-egress>queue
[no] cbs - Specify CBS rate
[no] high-prio-only - Specify high priority only burst size
[no] mbs - Specify MBS rate
[no] parent - Specify the scheduler to which this queue feeds
[no] percent-rate - Specify percent rates (CIR and PIR)
[no] port-parent - Specify the port-scheduler to which this queue feeds
[no] rate - Specify rates (CIR and PIR)
config>qos>sap-egress>queue>xp-specific
[no] packet-byte-of* - Specify packet byte offset
config>qos>sap-ingress>policer
[no] cbs - Specify Cbs
[no] high-prio-only - Specify high priority only percent-of-mbs
[no] mbs - Specify Mbs
[no] packet-byte-of* - Specify packet byte offset
[no] parent - Specify the arbiter to which this policer feeds
[no] percent-rate - Specify percent rates (CIR and PIR)
[no] rate - Specify rates (CIR and PIR)
config>qos>sap-egress>policer
[no] cbs - Specify Cbs
[no] high-prio-only - Specify high priority only percent-of-mbs
[no] mbs - Specify Mbs

Table 28: CLI Modifiable Parameters in Base QoS-Policy that Contains Clones (Continued)

CLI
[no] packet-byte-of* - Specify packet byte offset
[no] parent - Specify the scheduler to which this policer feeds
[no] percent-rate - Specify percent rates (CIR and PIR)
[no] rate - Specify rates (CIR and PIR)

PCC Rule Direction

PCC rules are unidirectional. The PCC rule direction is determined based on the value of the Flow-Direction AVP within the Flow-Information AVP. In the absence of the Flow-Direction AVP, the PCC rule direction is determined based on the Flow-Description AVP (as part of IPFilterRule direction field). Both of these AVPs (Flow-Direction and Flow-Description) are part of the PCC rule definition.

In case that the action within the PCC rule is in conflict with the direction of the flow, the PCC rule instantiation will fail. For example, an error will be raised if the flow direction is UPSTREAM, while the action is 'Max-Requested-Bandwidth-DL' (downstream bandwidth limit).

Action

A PCC rule may contain multiple actions. Each action is carried in a separate, action specific AVP. The action specified in the **flow-description->ipfilterrule** data type is ignored. In case that the rule contains multiple instances of the same action, each with a different value, the last occurrence of the action value will be in effect.

Not all of the action types can be applied at the same time. The allowed combination of the actions per direction is given in Table 26 and Table 27.

Rate-Limiting Action (Ingress, Egress)

Rate-limiting action is implemented via policers. The policer is dynamically created at the PCC rule instantiation time. The rate can be enforced based on Layer 2 rates or Layer 3 rates.

Dynamically instantiated policers have their own policer id range to avoid the conflict with static policers.

The dynamically created policers will share common properties configured under the dynamic-policer CLI hierarchy:

```
configure
     qos
          sap-ingress/egress
               dynamic-policer
                    stat-mode no-stats|minimal|offered-profile-no-cir|
offered-profile-cir|offered-total-cir|
offered-limited-capped-cir|offered-profile-capped-cir
                    parent             <arbiter-name> [weight <weight-level>] [level
<level>
                    mbs                               <size> [bytes | kilobytes]
                    cbs                               <size> [bytes | kilobytes]
packet-byte-offset{add <add-bytes> | subtract <sub-bytes>}
range               start-entry <entry-id> count <count>
```

The policer rates are part of PCC rule itself and are not part of static configuration.

The generic Gx directive for rate-limiting action is:

```
Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Definition <AVP Header: 1003>
          Charging-Rule-Name <AVP Header: 1005>
          QoS-Information <AVP Header: 1016>
               Max-Requested-Bandwidth-UL <AVP Header: 516>[bps] 3GPP 29.214 §5.3.15
     Max-Requested-Bandwidth-DL <AVP Header: 515>[bps] 3GPP 29.214 §5.3.14
     Guaranteed-Bitrate-UL <AVP Header: 1026> [bps] 3GPP 29.214 §5.3.26
     Guaranteed-Bitrate-DL <AVP Header: 1027> [bps] 3GPP 29.214 §5.3.25
```

The above rate limits refer to PIR and CIR rates of the dynamic policer in the respective direction.

Dynamic Policers and Queue Mappings

Once traffic is processed by the dynamic policers on **ingress**, the traffic will flow through the policer-output-queues shared queues. Traffic through dynamic policers will always bypass subscriber queues or policers on **ingress** that are statically configured in the base qos-policy.

Similar behavior is exhibited when static policers are configured on **egress**. Traffic outputting dynamic policer is never mapped to another static policer. Instead, such traffic will be mapped to the corresponding shared queue in a queue-group. By default, this queue-group is the policer-output-queue group. However, the selection of the queue-group is configurable.

In contrast to the above, traffic processed by dynamic policers can be fed into statically configured **subscriber (local) queues on egress**. Dynamic policers and subscriber queues are tied through the forwarding-class.

The policer to local queue mapping and inheritance of the forwarding-class is shown in Figure 15. In this example, the mapping of traffic —> forwarding-class in rule 2 (flow 2) will depend on the DSCP bits in the traffic flow. If the DSCP value in this traffic flow are different from the explicitly configured DSCP values in the static (base) QoS policy, then traffic will be mapped to the default forwarding-class.

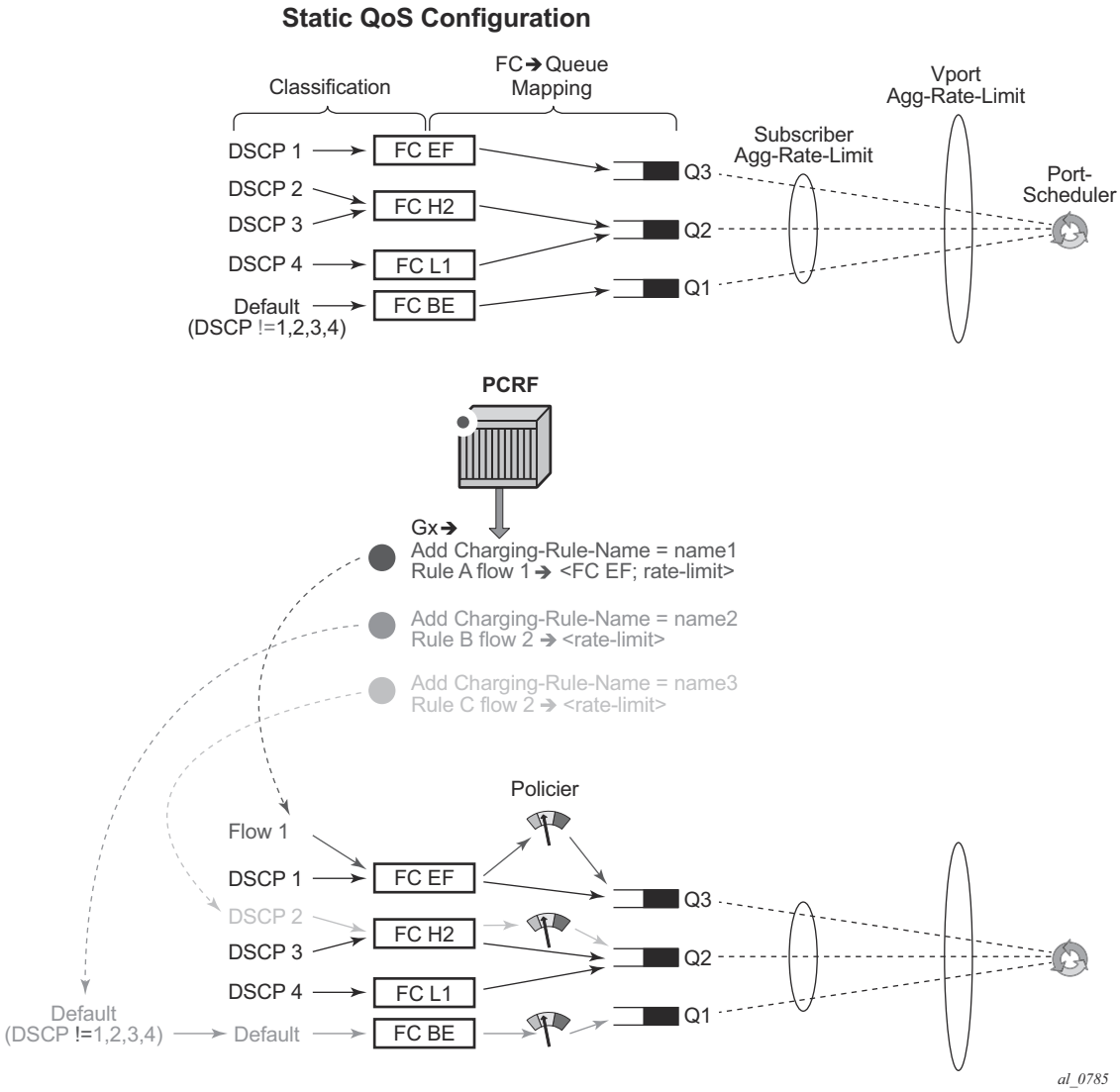

Figure 182: FC Inheritance for Dynamically Instantiated Policers on Egress

Dynamic Policer Rates and Accounting Statistics

By default, policer rates are configured based on Layer 2 frame length (for example, the Ethernet header plus the IP packet). This can be changed by the packet-byte-offset (PBO) command under the policer. In case that the policer is fed into a local queue, the PBO of the policer will not affect the PBO of the local queue it is feeding.

The rates for local subscriber queues can be independently measured based on Layer 2 or Layer 1 frame length and the queue statistics can be measured based on Layer 1, Layer 2 or Layer 3 (IP-only) frame length. The IP-only stats for queues can be configured in the **sub-profil>volume-stats-type {ip|default}.**

Dynamic policer[4] statistics are not reported in RADIUS-based accounting. On egress, this will have no effect on volume counters in RADIUS-based accounting, since the dynamic policers are normally fed into local queues whose statistics are reported in RADIUS-based accounting. However, on ingress, the dynamic policers are always fed into the queue-group queues which are excluded from RADIUS based accounting. The consequence is that the ingress RADIUS-based accounting will lack statistics for the traffic that is flowing via dynamic policers.

In case that the dynamic policer is feeding a local queue, the aggregate statistics in show commands for such queue are not reported in order to avoid double counting (since the traffic statistics in show commands are already reported for the dynamic policer). However, the per-queue statistics are reported in **show** commands, irrespective of whether the policer is mapped to the local queue or not.

To avoid losing aggregate SAP or subscriber stats in show commands, the recommendation is to have policers feed into local queues which are not already mapped to an FC.For example:

```
queue 4 create //Not counted since policer 2 is feeding it
exit
policer 2 create
exit
fc be create
     queue 4     //Not counted
exit
fc l1 create
     queue 4     //Not counted
exit
fc ef create
     policer 2 queue 4
exit
```

FC BE, FC2 L1 —> queue 4

FC EF —> policer 2, queue 4

4. Dynamic policers are instantiated due to rate-limiting or usage-monitoring action in PCC rules.

In this case, traffic from queue 4 will not be counted in aggregate stats at all and consequently the aggregate accounting information will be lost for FC BE and FC L1.

Forwarding-Class Change (Ingress, Egress)

Traffic can be re-prioritized via PCC rule by re-classification into a different forwarding class. The forwarding-class can be changed for the following cases:

- The original static mapping between traffic type, forwarding-class and the queue/policer in the base qos-policy is configured outside of ip-criteria CLI hierarchy.

  For example:

```
configure>qos>sap-egress#
 dscp af11 fc "af"
```

  Such mapping is configured outside of CAM and as such it has lower evaluation priority than the mapping configured via PCC rule which is installed in CAM.

- The original static mapping is provisioned in the base qos-policy via ip-criteria CLI hierarchy.

  For example:

```
config>qos>sap-egress>#
 ip-criteria
      entry 40000 create
           match
                  dscp af11
      exit
    action fc "af"
    exit
   exit
```

  In this case, the configured entry range for PCC rules **must** precede the static entry (match criteria) in which the original forwarding-class is configured. The insertion point (entry) is controlled via configuration: **sub-insert-shared-pccrule start-entry** <*entry-id*> **count** <*count*> command under the qos-policy.

  In both of the above cases, the following PCC rule would override forwarding-class for traffic with DSCP value of 10 (‘af11’ traffic class) from value ‘af’ to ‘h2’.

```
Charging-Rule-Install
Charging-Rule-Definition
 Charging-Rule-Name = fc-change
 Flow-Information
      ToS-Traffic-Class = 00101000 11111100
      Flow-Direction = 1
 QoS-Information
      QoS-Class-Identifier  = 2
```

The eight forwarding classes in 7x50 are mapped to QCIs (3GPP TS 23.203 §6.1.7.2) in the following manner:

BE — QCI 8

L2 — QCI 7

AF — QCI 6

L1 — QCI 4

H2 — QCI 2

EF — QCI 3

H1 — QCI 1

NC — QCI 5

The generic Gx directive for forwarding-class change:

```
Charging-Rule-Install ::= <AVP Header: 1001>
Charging-Rule-Definition <AVP Header: 1003>
 Charging-Rule-Name <AVP Header: 1005>
     QoS-Information <AVP Header: 1016>            3GPP 29.212 §5.3.16
          QoS-Class-Identifier <AVP Header: 1028>  3GPP 29.212 §5.3.17
```

Next-Hop Redirect (Ingress)

The next hop redirection will explicitly or implicitly change the next-hop for the traffic flow within the same service ID (routing context) or a different service ID (routing context).

In case that the next-hop is not explicitly provided, the next-hop will be selected automatically, according to the routing lookup in the referenced service ID.

The generic Gx directive:

```
Charging-Rule-Install <AVP Header: 1001>
     Charging-Rule-Definition <AVP Header: 1003>
          Charging-Rule-Name <AVP Header: 1005>
               Alc-Next-Hop :: <AVP Header: 1023>
                    Alc-Next-Hop-IP <AVP Header: 1024>
Alc-V4-Next-Hop-Service-id <AVP Header: 1025>
                    Alc-V6-Next-Hop-Service-id <AVP Header: 1026>
```

This action overwrites the routing table lookup based on the destination IP and sets the next hop to the:

- IPv4/6 address within the same service id
- IPv4/6 address within a different service id

The next-hop search is indirect, which means that if the explicitly provided next-hop in the PCC rule cannot be found in the routing table, then an additional routing table lookup will be performed to find the path (next-hop) to the indirect next hop from the PCC rule.

In case that only the service-id is specified in PCC rule (without the next-hop), then the next-hop will be selected from the specified service-id based on the destination IP address of the packet.

HTTP Redirect (Ingress)

HTTP redirect utilizes Redirect-Information AVP from 3GPP 29.212, §5.3.82.

The generic Gx directive:

```
Redirect-Information < AVP Header: 1085 >
     Redirect-Support < AVP Header: 1086 >
     Redirect-Address-Type < AVP Header: 433 >
     Redirect-Server-Address < AVP Header: 435 >
```

Gate Function

The gate function is analogous to the **forward | drop** action within IP filters in CLI.

The Flow-Status AVP <AVP Header: 511> (3GPP 29.214, §5.3.11.) defines the gating action. The two supported values are enable and disable.

The gating action **enabled (2)** is the default action and it must be accompanied by at least one other action. In other words, the gating action **enable** cannot be the only action in the PCC rule. Otherwise the PCC rule is treated as it would not have any action at all and as such it will be rejected.

In case that the gating action is set to **disable (3)**, all other actions within the same rule will lose their meaning since the packet will be dropped. In effect, the **disabled** directive will disable the flow of classified traffic through the system. Note that this is not the same as **disabling** the rule in a sense that the flow of packets would be permitted through the 7x50 although with no actions applied.

This AVP is carried inside of Charging-Rule-Definition (3GPP 29.212, §5.3.5):

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
                               { Charging-Rule-Name }
                              *[ Flow-Information ]
                               [ Flow-Status ]
                               [ QoS-Information ]
                               [ Precedence ]
                              *[ Flows ]
                               [ Monitoring-Key]
                               [ Redirect-Information ]
                              *[ AVP ]
```

PCC Rule Provisioning Example

An example for PCC rule provisioning in CCA-I message is given below:

```
<CC-Answer> ::=  < Diameter Header: 272, PXY >
     < Session-Id >
     { Auth-Application-Id }
     { Origin-Host }
     { Origin-Realm }
     [ Result-Code ]
     [ Experimental-Result ]
     { CC-Request-Type }
     { CC-Request-Number }
     *[ Supported-Features ]
     *[ Event-Trigger ]
     [ Origin-State-Id ]

     Charging-Rule-Install ::= <AVP Header: 1001>— host instantiation
          Charging-Rule-Name = "ingr-v4:7"
          Charging-Rule-Name = "eggr-v6:5"
          Charging-Rule-Name = "Sub-Profile:prem"
          Charging-Rule-Name = "Sla-Profile:voip+data"
          Charging-Rule-Name = "Inter-Dest:vport-AN-1"


     Charging-Rule-Install  — service instantiation
          Charging-Rule-Definition
               Charging-Rule-Name = "service-1"  — should be able to remove the rule by name later on
                    Flow-Information — traffic flow definition
                    Flow-Description = "permit in 6(TCP) from any to ip 10.10.10.10/32
40000-40010"
                    ToS-Traffic-Class = 00101000 11111100]  – DSCP definition (value mask). In case
of the DSCP, Flow-Direction (1080) AVP must be included.
                    Flow-Direction = UPSTREAM  — traffic flow direction
                    QoS-Information <AVP Header: 1016>
                         Max-Requested-Bandwidth-UL = 10000000  — UPSTREAM rate definition (not
downstream, since the traffic flow direction is IN)
                         QoS-Class-Identifier  = 3 — EF forwarding class; in general one of 8 forward-
ing-classes (FC) in 7x50 (be|l2|af|l1|h2|ef|h1|nc). This is used for re-prioritization of the traffic.
```

In this example the host is instantiated using the two Charging-Rule-Install AVPs. The first one is used to instantiate the host. The second one is used to instantiate the IP-criterion based service named service-1. Service-1 is defined as the upstream traffic flow with traffic class AF11, destined to the TCP port range 40000-40010 on the node with IP address 10.10.10.10/32.

The actions for this traffic flow are:

- Rate-limit of 10M
- Change forwarding-class to AF11.

Operational Aspects

The commands used to examine dynamic rules and NAS filter inserts associated with the subscriber hosts are shown in Figure 183.

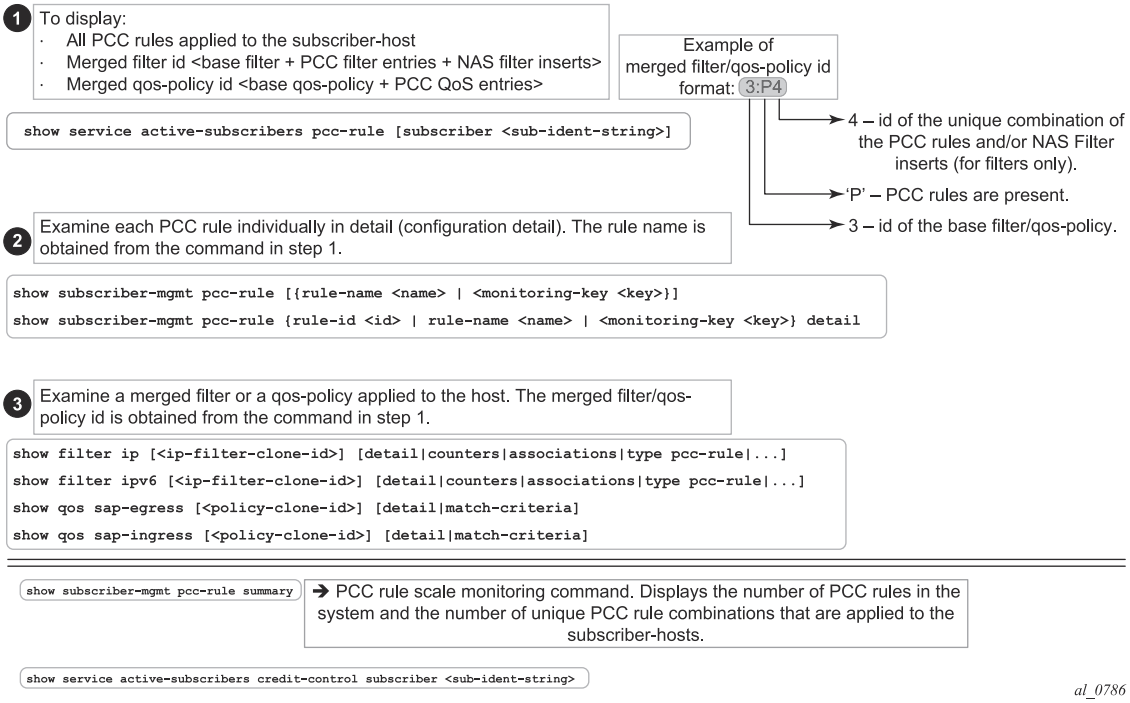

Figure 183: Overview of PCC Rule-Related Operational Commands

PCC Rules and Capacity Planning

One of the most important factors to be considered for capacity planning with PCC rules is the number of unique policies that are applied to subscribers.

A unique policy constitutes a set of base qos-policy or filter-id along with all PCC rules that are applied to a subscriber or a set of subscribers.

Let's examine an example where there are 'n' PCC rules in the system ('n' qos rules and 'n' ACL filter rules). Those rules are applied to IPv4 traffic in ingress direction. Further, let's assume that the PCC rules do not have defined Precedence AVP, which means that the system can optimize their order for maximum sharing and maximized scale. In this case, 'n' PCC rules can be combined by various permutation into 2^n-1 unique combinations Next assumption is that there are five possible base qos-policies for IPv4 traffic in ingress direction and five possible base filters for IPv4 traffic in the ingress direction.

Given the above, the unique PCC rule combinations (2^n-1) together with five base qos-polices will produce 5*(2^n-1) unique qos-policies per ingress IPv4. Same logic can be applied for ingress IPv4 filters.

This exercise must be repeated for egress direction as well as for IPv6 type traffic, by taking into consideration the number of respective base qos-policies/filters and the number of PCC rules.

Once the number of unique policy combinations is determined and ensured that it is within the system limits, each policy must be further evaluated to determine the number of entries it will take in CAM.

PCC Rule Scaling Example

The Figure 184 depicts an example relevant to capacity planning, with focus on understanding the scaling limits when it comes to the number of PCC rules and their mutual combinations when they are applied to the subscriber hosts.

This example is focusing on an IPv4 filter applied in ingress direction but similar logic can be used in understanding other policy types (qos, egress, IPv6).

The system/line card limits in this example are set to the following values only for illustration purposes:

- Number of PCC rules per system: 1K
- Max number of rules per subscriber host: 64
- Max number of combinations of the PCC rules (or services) that are active (applied to the subscriber-hosts) per system: 4K

- Max ingress IPv4 filter CAM entries per FP2/FP3: 64k
- Max filters per system: 16k

Note that the actual CAM limits vary per policy type (filter/qos), direction and IP address type (v4 vs v6). The actual scaling limits can be found in SROS Scaling Guides for the relevant software release.

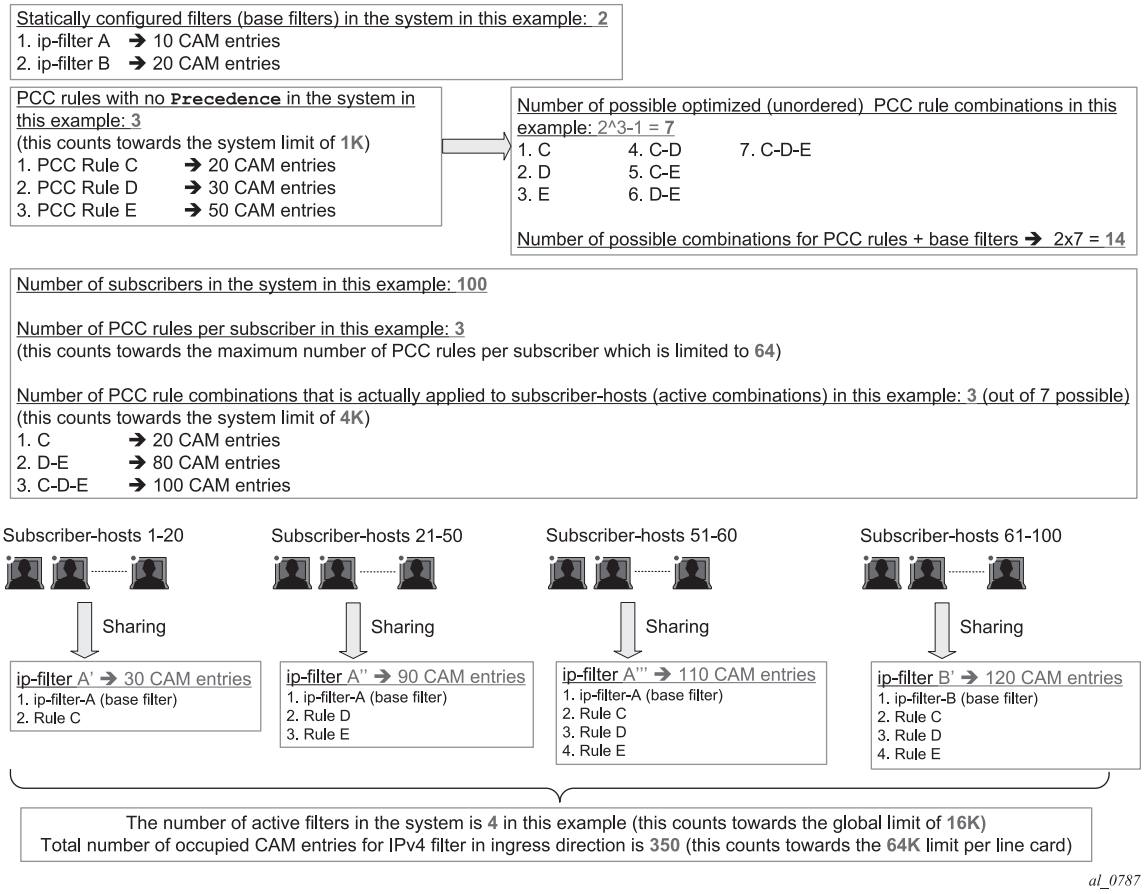

Figure 184: Example of the Scaling Limits for PCC Rules

NAS Filter Inserts

Gx filter entries inserted via NAS-Filter-Rule are subscriber-host specific entries. This means that in the upstream direction, the source IP address in the NAS-Filter-Rule will always be internally set by 7x50 to the IP address of the subscriber host itself. Similarly, in the downstream direction the destination IP address in the NAS-Filter-Rule will be set by 7x50 to be the IP address of the subscriber-host itself.

On the other hand, the entries in the Alc-NAS-Filter-Rule-**Shared** AVP are processed as received without any modifications. This means that such entries can be shared with all the hosts that have the same Alc-NAS-Filter-Rule-Shared applied.

Similarly to QoS overrides, NAS filter entries are not predefined in 7x50 but instead they are defined under the Charging-Rule-Install — Charging-Rule-Definition AVP.

The Charging-Rule-Name AVP for NAS filter inserts is an arbitrary name that is part of Charging-Rule-Definition AVP in which NAS-Filter-Rule AVP or Alc-NAS-Filter-Rule-Shared is provided. Such Charging-Rule-Name will be used to report errors related to instantiation of the inserts.

Examples of NAS Entry Inserts

The following AVPs will identify NAS filter inserts that will be applied to a subscriber host. Those AVPs can be included in CCA-i, CCA-u or RAR message sent from the PCRF.

```
Charging-Rule-Install ::= <AVP Header: 1001>
Charging-Rule-Definition <AVP Header: 1003>
              Charging-Rule-Name <AVP Header: 1005> = “allow-all”
              Alc-NAS-Filter-Rule-Shared <AVP Header: 158> = "permit in ip from any to any
"ASCII NUL" permit out ip from any to any"
```

In this example, the filter entry defined in Alc-NAS-Filter-Rule-Shared AVP will be inserted in the clone of the existing base filter for the subscriber(s).

Error Handing and Rule Failure Reporting in ESM

The Gx rule (overrides, PCC rules or NAS filter inserts) instantiation failure in 7x50 can occur on two levels:

- AVP Decoding level in the Diameter - the Gx message contains an unrecognized AVP with the M-bit set. In this case all Gx rules (ESM, UM and AA) in the message will be rejected and the CCR-u with the Charging-Rule-Report AVP (rule status) and Error-Massage AVP (failure description) or an RAA message with the appropriate Result-Code AVP (fail – 5xxx), Error-Message AVP (description) and the Failed-AVP AVP will be sent to the PCRF.

  Invalid content of a supported AVP will the M-bit set will also trigger the same response. Invalid content of an AVP refers to the malformed syntax of an AVP that carries the type of the AVP value implicitly embedded in the AVP value itself. Consider sla-profile:rule-name-1 string. In this case, the sla-profile: refers to the type of the value carried in the Charging-Rule-Name AVP. The value that Charging-Rule-Name carries is rule-name-1 and it this value represents the sla-profile name already configured within 7x50 (as opposed to filter, sub-profile, category-map, etc). In case that sla-profile: in our example is misspelled (type is unrecognized), the whole AVP will be un-decodable.
- Gx rule instantiation level in ESM, UM or AA – in this case each module (ESM, UM or AA) would fail all rules destined for it. The failure of a Gx rule within a module can be caused by referencing non-existing profile (for example sla-profile:unknown-name) or a lack of resources in 7x50. In this case CCR-u message from the respective module will be sent with the Rule-Report-Status AVP listing all the rules destined for this module and the corresponding Error-Message AVP describing the cause for the failure.

  Another example that can cause all rules with the ESM module to fail would be invalid combination of actions within the rule.

AVP Decoding Failure in Gx

Reporting an AVP decoding problem in Gx is described in the following example:

A Gx directive is received to install two overrides in 7x50. The two overrides are supposed to change the sla and sub profiles for the subscriber host. The AVP that is used to change the sla-profile is miss-formatted. The predefined sla-profile keyword in the Charging-Rule-Install AVP is misspelled as spa-profile instead of sla-profile.

```
Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "Sub-Profile:prem"
     Charging-Rule-Name <AVP Header: 1005> = "Spa-Profile:voip+data"
```

Since the *Charging-Rule-Name* AVP has the M-bit set, the whole message will fail and an error will be reported. No rules within this Gx message will be installed (not even the valid ones, in this

case this would be the *Charging-Rule-Name* = "**Sub-Profile**:prem"). Note that if the M-bit was clear in the *Charging-Rule-Name* AVP, the erroneous AVP would be simply ignored and we would proceed with installation of the remaining, 'correctly formatted' rules.

The nature of the error will depend on the original directive sent by the PCRF (RAR or CCA – push or pull model)

In case that the directive from the PCRF is passed via CCA command, the response will be CCR-u command with the following error related AVPs:

```
[ Error-Message ]  –     "Invalid value spa-profile:voip+data"

Charging-Rule-Report ::= < AVP Header: 1018 >
     *[ Charging-Rule-Name ] — Spa-Profile:voip+data
     [ PCC-Rule-Status ]     — INACTIVE (1)
     [ Rule-Failure-Code ]   — GW/PCEF_MALFUNCTION (4)


Charging-Rule-Report ::= < AVP Header: 1018 >
     *[ Charging-Rule-Name ]      —    Sub-Profile:prem
     [ PCC-Rule-Status ]          —    INACTIVE (1)
     [ Rule-Failure-Code ]        —    GW/PCEF_MALFUNCTION (4)

Failed-AVP ::= < AVP Header: 279 >
     Charging-Rule-Name = Spa-Profile:voip+data
```

- In case that the directive is passed to 7x50 via RAR, the 7x50 will respond with the following RAA message:

```
Failed-AVP ::= < AVP Header: 279 >
     Charging-Rule-Name = Spa-Profile:voip+data

Result-Code ::= < AVP Header: 268 > = DIAMETER_INVALID_AVP_VALUE (5004)
```

Similarly, if the number of filter entries for each entry type (NAS-Filter-Rule — host-specific or Alc-NAS-Filter-Rule-Shared — shared) exceeds the maximum supported number (see the 7750 SR OS Gx AVPs Reference Guide), the whole message will fail the decoding phase.

The reason that the Result-Code AVP is present in the RAA message and not in the CCR-u message is that this code is only allowed to be present in the answer messages, according to the standard.

ESM Rule-Installation Failure

This assumes that the rule installation directives are successfully passed from the Gx module to the ESM module and the failure to install rules occurs in the ESM module.

In the Gx override case below, the referenced sla-profile is unknown. In such case, all directives passed to the ESM module will fail and consequently no rules/overrides will be installed. The sub-profile change will fail as well although the prem sub-profile is known in the system.

```
Charging-Rule-Install ::= <AVP Header: 1001>
     Charging-Rule-Name <AVP Header: 1005> = "Sub-Profile:prem"
               Charging-Rule-Name <AVP Header: 1005> = "Sla-Profile:unknown"
```

The error reporting flow will be the following:

- In case that the directives are passed via CCA command, the response will be CCR-u command with the following error related AVPs:

```
[ Error-Message ]        — "sla-profile 'unknown' lookup failed"

Charging-Rule-Report ::= < AVP Header: 1018 >
     *[ Charging-Rule-Name ] —   Sla-Profile:unknown
     [ PCC-Rule-Status ]     —   INACTIVE (1)
     [ Rule-Failure-Code ]   —   GW/PCEF_MALFUNCTION (4)


Charging-Rule-Report ::= < AVP Header: 1018 >
     *[ Charging-Rule-Name ] — Sub-Profile:prem
     [ PCC-Rule-Status ]     —   INACTIVE (1)
     [ Rule-Failure-Code ]   —   GW/PCEF_MALFUNCTION (4)
```

- In case that the directive is passed to 7x50 via RAR, the 7x50 will respond with the following messages:

  RAA = OK since the Gx module successfully processed the AVP parsing.

  The RAA will be followed by CCR-u, triggered by the rule instantiation failure in ESM module. CCR-u will contain the following AVP related to the rule status:

```
[ Error-Message ]   –   "sla-profile 'unknown' lookup failed"

Charging-Rule-Report ::= < AVP Header: 1018 >
     *[ Charging-Rule-Name ]   — Sla-Profile:unknown
     [ PCC-Rule-Status ] — INACTIVE (1)
     [ Rule-Failure-Code ] — GW/PCEF_MALFUNCTION (4)


Charging-Rule-Report ::= < AVP Header: 1018 >
     *[ Charging-Rule-Name ]    — Sub-Profile:prem
     [ PCC-Rule-Status ] — INACTIVE (1)
     [ Rule-Failure-Code ] — GW/PCEF_MALFUNCTION (4)
```

Similar behavior would be exhibited if the directive is sent to the UM or AA modules. However, note that ESM, UM and AA are separate modules and failure to install rule in one module will not affect rule installation in another.

Failure Reporting in AA

Failure reporting in AA is performed in similar fashion as in ESM.

Instead of Charging-Rule-Report AVP, the ADC-Rule-Report will be used:

```
ADC-Rule-Report ::= < AVP Header: 1097 >
                            *[ ADC-Rule-Name ]
                             [ PCC-Rule-Status ]
                             [ Rule-Failure-Code ]
                            *[ AVP ]
```

Summary of Failure Reporting

Table 29 summarizes Gx failure reporting in 7750.

Table 29: Failure Reporting

Failure Event	Gx Message Received on 7x50 via CCA (Pull Model)	Gx Message Received on 7x50 via RAR (Push Model)
AVP decoding/interpreting failure; M-bit cleared	Ignore AVP	Ignore AVP
AVP decoding/interpreting failure; M-bit set	CCR-u will be sent by 7x50. CCR-u will contain: • Charging-Rule-Report AVP for all rules (all rules inactive) • First failed AVP in Failed-AVP AVP • Error-Message AVP at the top level describing the reason for the failure. No rules within the message will be instantiated in 7x50.	RAA will be sent by 7x50. RAA will contain: • Result-Code AVP [DIAMETER_INVALUID_AVP_VALUE (5004), DIAMETER_AVP_UNSUPPORTED (5001), DIAMETR_UNAMBLE_TO_COMPLY (5012) • First failed AVP in Failed-AVP AVP No rules within the message will be instantiated in 7x50.

Table 29: Failure Reporting (Continued)

Failure Event	Gx Message Received on 7x50 via CCA (Pull Model)	Gx Message Received on 7x50 via RAR (Push Model)
Rule failure in ESM	CCR-U will be sent by 7x50. CCR-u will contain: •Charging-Rule-Report AVP for all rules (all rules inactive) • Error-Message AVP at the top level describing the reason for the failure. No rules will be instantiated in the ESM module.	RAA with the Result-Code AVP 'success' (2001) will be sent by 7750, followed by a CCR-u. CCR-u will contain: •Charging-Rule-Report AVP for all rules (all rules inactive) • Error-Message AVP at the top level describing the reason for the failure. No rules will be instantiated in the ESM module.
Rule failure in Usage-Monitoring (UM)	CCR-U will be sent by 7x50. CCR-u will contain: •Charging-Rule-Report AVP for all rules (all rules inactive) •Error-Message AVP at the top level describing the reason for the failure. No rules will be instantiated in the UM module.	RAA with the Result-Code AVP 'success' (2001) will be sent by 7750, followed by a CCR-u. CCR-u will contain: • Charging-Rule-Report AVP for all rules (all rules inactive) • Error-Message AVP at the top level describing the reason for the failure. No rules will be instantiated in the UM module.
Rule failure in AA	CCR-U will be sent by 7750. CCR-u will contain: •ADC-Rule-Report AVP for all rules (all rules inactive) • Error-Message AVP at the top level describing the reason for the failure. No AA rules will be instantiated in the AA module.	RAA with the Result-Code AVP 'success' (2001) will be sent by 7750, followed by CCR-u. CCR-u will contain: •ADC-Rule-Report AVP for all rules (all rules inactive) • Error-Message AVP at the top level describing the reason for the failure. No rules will be instantiated in the AA module.

Usage-Monitoring and Reporting

Usage-Monitoring and reporting refers to the collection and reporting of octets (volume) that a service or application on the 7x50 has consumed during certain period. The usage on the 7x50 is reported via Gx interface to the PCRF. Based on this information, the PCRF can apply specific action (policy change) to the entity being monitored. For example, QoS can be modified, or the service can be blocked when specific thresholds are reached.

Usage-Monitoring and reporting is performed over a single Gx session for the ESM/AA subscriber. In other words, there is only a single session for an ESM subscriber(-host) and corresponding AA subscriber. Via this single Gx session, Usage-Monitoring can be requested simultaneously in ESM context (PCC rule level, credit-category and/or IP-CAN session) and AA context (application based Usage-Monitoring).

ESM Usage-Monitoring - What is Being Monitored

In the ESM context, volume consumption (octets - 3GPP 23.203 §4.4) can be monitored on three levels:

- per entire IP-CAN session
- per credit-category
- per PCC rule

Usage-Monitoring can be monitored simultaneously on all three levels.

An IP-CAN session in the 7x50 represents a subscriber-host whose service types are determined by the sla-profile instance. In per IP-CAN session volume monitoring, the aggregated queue/policer counters will be reported per direction (in | out). This includes dynamic policers that are instantiated as a result of a Gx action (for example rate-limiting).

In case that the sla-profile instance changes mid-session, the counters will be reset.

One obvious difference between regular RADIUS accounting and Gx Usage-Monitoring is that in RADIUS accounting the cumulative byte number for sla-profile instance is presented in each report (interim-updates or stop acct messages), while in Usage-Monitoring this count is reset between the two reports (when the quota is reached, the usage report is triggered).

Per credit-category monitoring refers to volume monitoring of a single queue/policer or a set of queues/policers within the sla-profile instance. Each such queue/policer (or set of queues/policers as a subset of sla-profile instance) represents a service for which the Usage-Monitoring is required. Those queues/policers (services) are organized within 7x50 in credit categories.

```
*A:7750>config>subscr-mgmt>cat-map# info
----------------------------------------------
            activity-threshold 1
            credit-exhaust-threshold 50
            category "queue1" create
                queue 1 ingress-egress
            exit
            category "queue3-5" create
                queue 3 ingress-egress
                queue 5 ingress-egress
            exit
            category "rest-queues" create
                queue 2 egress-only
                queue 4 egress-only
                queue 6 egress-only
                queue 7 egress-only
                queue 8 egress-only
            exit
----------------------------------------------
```

Each service category has a name that is used to reference the category in Usage-Monitoring and reporting.

The category-map (predefined in 7750) that is used in Usage-Monitoring can be associated with the subscriber-host through the following methods (in the order of priority):

- PCRF - Charging-Rule-Install AVP that references the category map in Charging-Rule-Name = cat-map:<cat-map-name>
- LUDB
- RADIUS
- Python script

PCC rule Usage-Monitoring reports volume usage per flow or set of flows. PCC rule Usage-Monitoring is described in a separate section below.

Usage-Monitoring for the subscriber host can be configured on the 7x50 but it will not be active until it is turned on by the PCRF either via CCA-i, CCA-u or RAR.

Usage-monitoring can be enabled per ingress and/or egress direction or as total count. However monitoring the total count is mutually exclusive with per direction count. For example, total Usage-Monitoring cannot be enabled simultaneously with ingress (or egress) Usage-Monitoring for the same monitoring entity (session or category).

AA Usage-Monitoring – What is Being Monitored

In AA, charging groups (CG), application groups (AG) and applications are monitored. Refer to the SR OS Multi-Service Integrated Services Adapter Guide for details.

Requesting Usage-Monitoring in ESM

Gx Usage-Monitoring is activated explicitly from the PCRF via CCA-I, CCA-U or RAR. It is triggered via the Usage-Monitoring-Information AVP along with the event-trigger = usage-report (33). The Usage-Monitoring Information AVP contains the following AVPs:

```
Usage-Monitoring-Information::= < AVP Header: 1067 >
                                  [ Monitoring-Key ]
                            0,2   [ Granted-Service-Unit ]
                            0,2   [ Used-Service-Unit ]
                                  [ Usage-Monitoring-Level ]
                                  [ Usage-Monitoring-Report ]
                                  [ Usage-Monitoring-Support ]
```

There could be multiple instances of Usage-Monitoring-Information AVP present in a single CCA or RAR messages. For example, simultaneous Usage-Monitoring for IP-CAN session level, credit-category level or pcc rule level can be requested.

Usage-Monitoring-Level for IP-CAN session is set to SESSION_LEVEL (0).

Usage-Monitoring-Level for category-map is set to PCC_RULE_LEVEL (1)

Usage-Monitoring-Level for PCC rules is set to PCC_RULE_LEVEL (1)

Reporting Accumulated Usage

The 7x50 reports usage information to the PCRF under the following conditions:

- When a usage threshold is reached
- When all pcc rules associated with the monitoring are removed or deactivated
- When Usage-Monitoring is explicitly disabled by PCRF
- When a session is terminated
- When requested by PCRF (on demand)

To report accumulated usage for a specific monitoring-key the 7x50 sends a CCR with the Usage-Monitoring-Information AVP containing the accumulated usage information since the last report. For each of the enabled monitoring-key, the Usage-Monitoring-Information AVP will include the

Monitoring-Key AVP and the accumulated volume usage in the Used-Service-Unit AVP.

Usage report on the 7x50 can be triggered by reaching the usage threshold communicated to the 7x50 by PCRF in CCR-u message carrying accumulated usage for that monitoring entity along with the Event-Trigger AVP set to USAGE_REPORT.

PCRF will in response to CCR-u message communicate to the 7x50 via CCA-u message whether the Usage-Monitoring should continue:

- If the new thresholds for the currently monitored entity/levels are provided in Granted-Service-Units AVP, the Usage-Monitoring will continue
- If the thresholds are not included in Granted-Service-Units AVP, the Usage-Monitoring will stop.

Threshold are incremental. For example if the quota of 100MB is submitted to the 7x50, the usage should be reported when that quota is reached. At that point the user can be granted another 100MB. The new usage report on the 7x50 will be triggered when another 100MB are accumulated. Absence of the threshold for a given entity in CCA-u message is an indication that the Usage-Monitoring should stop.

When the PCRF informs the 7x50 that Usage-Monitoring should stop (by not including thresholds in CCA-u), the 7x50 will not report usage which has accumulated between sending the CCR and receiving the CCA.

Another possibility of usage reporting is on-demand. In such scenario, usage for one or more monitoring keys will be reported regardless of whether the usage threshold has been reached. This is achieved by sending to the 7x50 Usage-Monitoring-Report AVP (within the Usage-Monitoring-Information AVP) set to USAGE-MONITORING_REPORT_REQUIRED. If the Monitoring-Key AVP is omitted in such a request, Usage-Monitoring for all enabled entities will be reported to the PCRF.

In case that the credit-category is removed from the subscriber host (the sla-profile instance referencing the category-map is changed for the subscriber host), the 7x50 will report the outstanding usage in CCR-u command with the Event-Trigger set to USAGE_REPORT.

Disabling Usage-Monitoring

When the PCRF explicitly disables Usage-Monitoring on the 7x50, the 7x50 will report the accumulated usage which has occurred while Usage-Monitoring was enabled.

To disable Usage-Monitoring for an entity, the PCRF sends the Usage-Monitoring-Information AVP referencing only the applicable monitoring entity with the Monitoring-Key AVP and the Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED.

When the PCRF disables Usage-Monitoring in a RAR or CCA command, the 7x50 sends new

CCR-U and the Event-Trigger AVP set to "USAGE_REPORT" to report accumulated usage for the disabled Usage-Monitoring entities.

Usage-Monitoring for PCC Rules

Each PCC rule for which Usage-Monitoring is required, contains Monitoring-Key AVP.

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
                                { Charging-Rule-Name }
                               *[ Flow-Information ]
                                [ Flow-Status ]
                                [ QoS-Information ]
                                [ Precedence ]
                                [ Monitoring-Key]
                               *[ AVP ]
```

Usage-Monitoring for PCC rules is implemented through a dynamic policer. The policer is instantiated at the time when the PCC rule with Monitoring-Key AVP is installed.

The same monitoring-key can be used in multiple PCC rules assuming that these rules are for the same direction. In other words, the charging rule will be rejected if the same monitoring-key is used for ingress and egress.

Session Termination

At IP-CAN session termination the 7x50 sends the accumulated usage information for all entities for which Usage-Monitoring is enabled in the CCR-t.

Usage-Monitoring Examples

For the description of the specific AVP, refer to the 7750 SR OS Gx AVPs Reference Guide.

IP-CAN session Usage-Monitoring

PCRF in RAR sends the following AVPs (among all the other mandatory ones: session-id, etc.)

```
Usage-Monitoring-Information
         Monitoring-Key = "any-string"
         Granted-Service-Unit
              CC-Input-Octets = 1000000
              CC-Output-Octets = 1000000
         Usage-Monitoring-Level = session_level(0)

Event-Trigger = USAGE_REPORT
```

The 7x50 reports usage when the thresholds are reached some time later in CCR-U. The usage is monitored inetrnally on the 7x50 based on the current sla-profile instance.

```
Usage-Monitoring-Information
         Monitoring-Key = "any-string"
         Used-Service-Unit
         CC-Input-Octets = 1000000
                  CC-Output-Octets = 1000000
```

PCRF instructs 7x50 to continue Usage-Monitoring with the new thresholds in CCA-U:

```
Usage-Monitoring-Information
         Monitoring-Key = "any-string"
         Granted-Service-Unit
              CC-Input-Octets = 1000000
              CC-Output-Octets = 1000000
         Usage-Monitoring-Level = session_level(0)
```

Category Usage-Monitoring

Assume that the following category-map is associated with the subscriber host:

```
*A:7750>config>subscr-mgmt>cat-map# info
----------------------------------------------
            activity-threshold 1
            credit-exhaust-threshold 50
            category "queue1" create
                queue 1 ingress-egress
            exit
            category "queue3-5" create
                queue 3 ingress-egress
                queue 5 ingress-egress
            exit
            category "rest-queues" create
                queue 2 egress-only
                queue 4 egress-only
                queue 6 egress-only
                queue 7 egress-only
                queue 8 egress-only
            exit
```

The PCRF will send the following AVPs in the RAR message (among all the other mandatory ones: session-id, etc.)

```
Charging-Rule-Install
         Charging-Rule-Name = Cat-Map:cat1 – cat-map rule install

Usage-Monitoring-Information
         Monitoring-Key = "queue-1"
         Granted-Service-Unit
              CC-Input-Octets = 1000000
              CC-Output-Octets = 1000000
```

```
              Usage-Monitoring-Level = PCC_RULE_LEVEL (1)
Usage-Monitoring-Information
          Monitoring-Key = "queue-3-5"
          Granted-Service-Unit
               CC-Input-Octets = 2000000
               CC-Output-Octets = 2000000
               Usage-Monitoring-Level = PCC_RULE_LEVEL (1)
Event-Trigger = USAGE_REPORT
```

The 7x50 reports usage when the thresholds are reached some time later in CCR-U:

```
Usage-Monitoring-Information
          Monitoring-Key = "queue-1"
          Used-Service-Unit
          CC-Input-Octets = 1000000
                    CC-Output-Octets = 1000000
Usage-Monitoring-Information
          Monitoring-Key = "queue-3-5"
          Used-Service-Unit
          CC-Input-Octets = 2000000
                    CC-Output-Octets = 2000000
```

The PCRF instructs the 7x50 to continue Usage-Monitoring with the new thresholds in CCA-U:

```
Usage-Monitoring-Information
          Monitoring-Key = "queue-1"
          Granted-Service-Unit
               CC-Input-Octets = 1000000
               CC-Output-Octets = 1000000
               Usage-Monitoring-Level = PCC_RULE_LEVEL (1)
Usage-Monitoring-Information
          Monitoring-Key = "queue-3-5"
          Granted-Service-Unit
               CC-Input-Octets = 2000000
               CC-Output-Octets = 2000000
               Usage-Monitoring-Level = PCC_RULE_LEVEL (1)
```

Event Triggers

PCRF may subscribe to an event trigger in the 7x50. The PCRF subscribes to new event triggers or remove armed event triggers unsolicited at any time. When an event matching the event trigger occurs, the 7x50 reports the occurred event to the PCRF. The event triggers that are required in procedures will be unconditionally reported (for example IP address allocation/de-allocation) from the 7x50, while the PCRF may subscribe to the remaining events (for example Usage-Monitoring).

When sent from the PCRF to the 7x50, the Event Trigger AVP indicates an Event that will trigger an action in 7x50. When sent from the 7x50 to the PCRF, the Event Trigger AVP indicates that the corresponding event has occurred. If no Event Trigger AVP is included in a CCA or RAR operation, any previously provisioned event trigger will be still applicable.

The PCRF may remove all previously provided event triggers by providing the Event-Trigger AVP set to the value NO_EVENT_TRIGGERS. When an Event-Trigger AVP is provided with this value, no other Event-Trigger AVP will be provided in the CCA or RAR command. Upon reception of an Event-Trigger AVP with this value, the 7x50 will not inform PCRF of any event except for those events that are always reported and do not require provisioning from the PCRF.

When the PCRF subscribes to one or more event triggers by using the RAR command, 7x50 will send the corresponding currently applicable values to the PCRF in the RAA if available, and in this case, the Event-Trigger AVPs will NOT be included.

For a list of the supported events in the 7x50, refer to the 7750 SR OS Gx AVPs Reference Guide.

Subscriber Verification

At any time, the PCRF can query 7x50 for the presence of the subscriber-host via a RAR message.

The 7x50 will respond with the following result-codes in RAA:

- DIAMETER_SUCCES (2001) — subscriber active
- DIAMETER_UNKNOWN_SESSION_ID (5002) — subscriber does not exist

Subscriber Termination

The PCRF can request IP-CAN session termination in the 7x50 via two messages:

- a RAR directive with the Session-Release-Cause AVP to the 7x50.
- ASR

Upon the arrival of either of those messages, the 7x50 will start the IP-CAN session termination procedure (CCR-t with corresponding Termination-Cause AVP will be sent to the PCRF). This is described in the 3GPP 29.212 document, §4.5.9.

For a list of the supported Termination-Cause AVP values in the 7x50, refer to the 7750 SR OS Gx AVPs Reference Guide.

Mobility Support in WiFi

When a WiFi subscriber moves between the access points (APs), a CCR-u message is triggered on the 7x50, carrying the Called-Station-Id AVP. The Called-Station-Id AVP carries the MAC IP address of the new AP. This functionality allows the PCRF to make location based policy decision.

This functionality is enabled via event trigger USER_LOCATION_CHANGE (13) [3GPP 29.212, §5.3.7] sent to 7x50 by PCRF in CCA or RAR message.

The same event will be reported back from 7x50 to the PCRF in CCR-u message when the user location changes.

Redundancy

Redundancy in Gx relies on the Diameter redundancy mechanisms described in the Diameter Redundancy on page 2169.

Persistency and Origin-State-ID AVP (RFC 6733, §8.6 and §8.16).

Persistency (saving the state of IPoE hosts on the compact flash) for Gx sessions is not supported. This means that upon the reboot, the 7750 will restore the subscriber-hosts from the persistency but the Gx session awareness for the recovered hosts is lost. Any previously applied qos or filter overrides will be lost. However, subscriber-strings (subscriber-id, sub-profile, sla-profile, aa-profile) can be made persistent and can be preserved across reboots.

The Origin-State-Id (OSI) AVP is NOT stored in persistency. In case that the 7x50 reboots, the Origin-State-ID AVP is set to boot time (UTC).

The Origin-State-Id AVP is contained in the CER messages and application messages that are sent from 7x50 to the PCRF/DRA. In the other direction, (sent by PCRF to 7x50) the OSI is ignored.

To restore lost session after the reboot, 7x50 will initiate CCR-i message for every host that is recovered from persistency. The CCR-i will contain the new session-id and origin-state-id. Based on this CCR-i, it is expected that the PCRF returns the most current policy for the host.

Overload Protection

7x50 has a receiving queue per Gx application (ESM, UM, AA). Each queue can hold 10K messages. While the queue is in the overloaded state, 7x50 replies to every new RAR message with the RAA message that contains the Result-Code AVP set to DIAMETER_TOO_BUSY (3004) value. This can be considered as explicit signaling towards the PCRF notifying it of the condition on the 7x50.

In case that the messages in the overwhelmed 7x50 queue do not require sending an answer (in case that the overwhelmed queue contains CCA-i/u messages), the TCP window will fill up, TCP ACKs will not be sent and consequently this will be an implicit notification to the PCRF to slow down.

If 7x50 receives a response from an overloaded PCRF (Result-Code = DIAMETER_TOO_ BUSY), the 7x50 will timeout (tx-timer) the originally sent message. Once the message is timed out, the configuration settings (on-failure) will determine whether to trigger the peer-failover procedure or not (Peer-failover based on DIAMETER_TOO_BUSY Result-Code is recommended in RFC6733, §7.1.3.

Diameter NASREQ Application

The Diameter NASREQ application is used for Authentication, Authorization, and Accounting services in the Network Access Server (NAS) environment. SR OS supports a stateless operation of NASREQ authentication and authorization, interacting with a NASREQ server that does not maintain session state.

Subscriber host or session authentication results in an AA-Request (AAR) message being sent to the Diameter NASREQ server. An Auth-Session-State AVP with value equal to 1 (No State Maintained) is included in the AAR to inform the server of the stateless mode. The server responds with an AA-Answer (AAA) message and must include the Auth-Session-State AVP with value equal to 1 (No State Maintained), together with the authorization AVPs.

Diameter NASREQ accounting is not supported.

Table 30 lists the supported Diameter NASREQ messages. Vendor-specific AVP's are shown as: v-<vendor-id>-<AVP id>.

Table 30: Supported Diameter NASREQ Messages

Diameter Message		Code
AAR	AA-Request	265
AAA	AA-Answer	265

Diameter NASREQ authentication is supported for IPoE hosts and sessions, PPPoE PTA PAP/CHAP authentication. Diameter NASREQ authentication is not supported for L2TP LAC/LNS.

NASREQ and RADIUS authentication cannot be configured simultaneously on a capture-sap, local-user-database, or group-interface. They have the same priority in the hierarchy of different sources (such as local user database, Gx, defaults, etc.) for obtaining the subscriber host or session authorization parameters.

Multi-chassis redundancy is supported via separate Diameter NASREQ peers on each redundant node. Each node of the multi-chassis redundancy pair has its own Diameter Identity (origin host/realm). The subscriber host or session is authenticated on the BNG where it is initially connected. Due to the stateless operation, there is no need to synchronize NASREQ session state. Alternatively, the Diameter proxy can be used if it is required to have a single Diameter Identity (origin host/realm) per pair of multi-chassis redundant nodes.

There is no NASREQ re-authentication for active subscriber hosts or sessions, except for a forced re-authentication when the circuit ID/interface ID or remote ID of a DHCP host is changed.

Stateless NASREQ authentication can be complemented with Diameter Gx policy management for policy control and mid-session changes. Diameter NASREQ and Gx applications are supported simultaneously on a single Diameter peer.

Figure 185 shows a sample call flow for a subscriber using Diameter NASREQ for authentication and Diameter Gx for policy management.

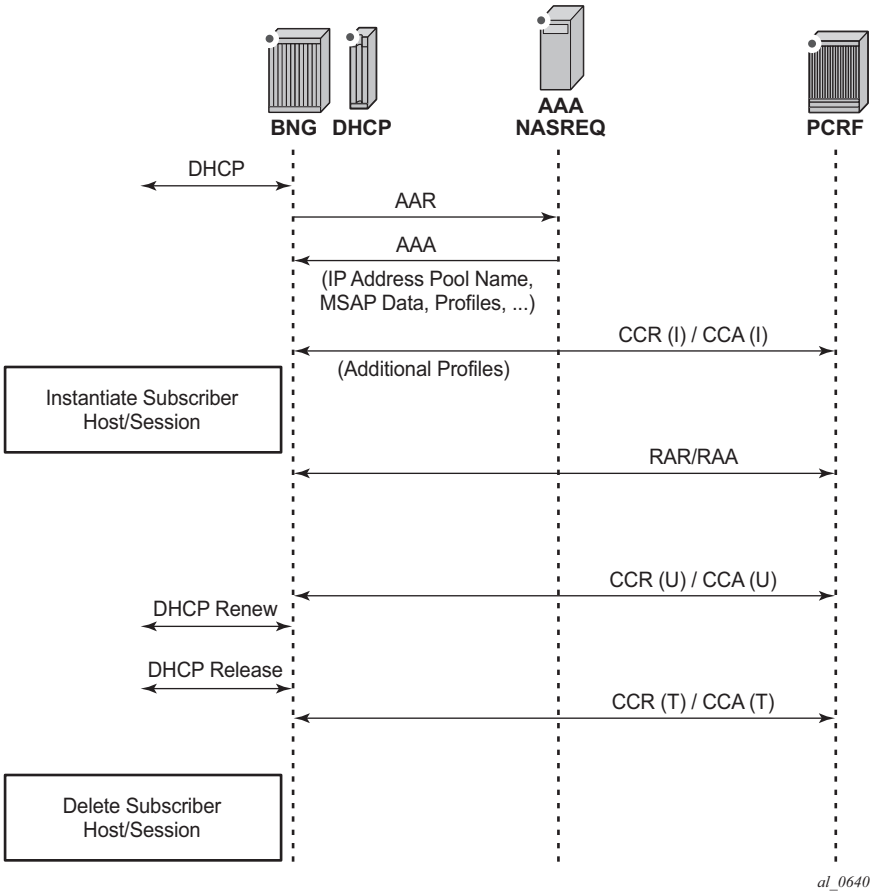

Figure 185: Sample Diameter NASREQ Call Flow

Table 31 lists the authorization AVPs that are accepted in a Diameter NASREQ AA-Answer message. Vendor-specific AVPs are shown in the table as: v-<vendor-id>-<AVP-id>.

Table 31: AA-Answer Message — Accepted Authorization AVPs

AVP ID	AVP Name	Description
1	User-Name	Overrides the “Radius User-Name”.
8	Framed-IP-Address	The IPv4 address of the subscriber host.
9	Framed-IP-Netmask	The IPv4 netmask of the subscriber host.

Table 31: AA-Answer Message — Accepted Authorization AVPs (Continued)

AVP ID	AVP Name	Description
22	Framed-Route	IPv4 managed route to be configured on the NAS for a routed subscriber host.
25	Class	Opaque value; echoed in RADIUS accounting.
88	Framed-Pool	The name of an IPv4 address pool.
97	Framed-IPv6-Prefix	SLAAC IPv6 prefix (wan-host).
99	Framed-IPv6-Route	IPv6 managed route to be configured on the NAS for a v6 routed subscriber host..
100	Framed-IPv6-Pool	The name of an IPv6 IA-NA address pool (wan-host).
123	Delegated-IPv6-Prefix	DHCPv6 IA-PD IPv6 prefix (pd-host).
v-6527-9	Alc-Primary-Dns	The IPv4 address of the primary DNS server.
v-6527-10	Alc-Secondary-Dns	The IPv4 address of the secondary DNS server.
v-6527-11	Alc-Subsc-ID-Str	Unique subscriber ID string.
v-6527-12	Alc-Subsc-Prof-Str	Subscriber profile string.
v-6527-13	Alc-SLA-Prof-Str	SLA profile string.
v-6527-16	Alc-ANCP-Str	ACNP string.
v-6527-17	Alc-Retail-Serv-Id	The service-id of the retailer to which this subscriber host belongs.
v-6527-18	Alc-Default-Router	The default gateway for the user (DHCP option [3] default-router for a DHCPv4 proxy)
v-6527-28	Alc-Inc-Dest-Id-Str	Intermediate destination ID string.
v-6527-29	Alc-Primary-Nbns	The IPv4 address of the primary NetBios Name Server (NBNS).
v-6527-30	Alc-Secondary-Nbns	The IPv4 address of the secondary NetBios Name Server (NBNS).
v-6527-31	Alc-MSAP-Serv-Id	Service ID where the managed SAP is to be created.
v-6527-32	Alc-MSAP-Policy	Managed SAP policy used to create the MSAP.
v-6527-33	Alc-MSAP-Interface	Group-interface name where the managed SAP is to be created.

Table 31: AA-Answer Message — Accepted Authorization AVPs (Continued)

AVP ID	AVP Name	Description
v-6527-45	Alc-App-Prof-Str	Application profile string.
v-6527-99	Alc-Ipv6-Address	DHCPv6 IA-NA IPv6 address (wan-host).
v-6527-105	Alc-Ipv6-Primary-Dns	The IPv6 address of the primary DNSv6 server.
v-6527-106	Alc-Ipv6-Secondary-Dns	The IPv6 address of the secondary DNSv6 server.
v-6527-131	Alc-Delegated-Ipv6-Pool	The name of an IPv6 IA-PD prefix pool (pd-host).
v-6527-161	Alc-Delegated-Ipv6-Prefix-Length	DHCPv6 IA-PD prefix length (pd-host).
v-6527-174	Alc-Lease-Time	The lease-time for proxy, in seconds.
v-6527-181	Alc-SLAAC-IPv6-Pool	The name of an IPv6 SLAAC prefix pool (wan-host).

Sample Configuration Steps

To specify the peers to reach the Diameter NASREQ server in a diameter peer policy:

```
configure
    aaa
        diameter-peer-policy "diameter-peer-policy-1" create
            description "Diameter NASREQ peer policy"
            applications nasreq
            origin-host "bng@alcatel-lucent.com"
            origin-realm "alcatel-lucent.com"
            peer "peer-1" create
                address 172.16.3.1
                destination-realm "myDSCRealm.com"
                no shutdown
            exit
        exit
```

To specify the Diameter NASREQ application specific parameters, such as AVP format and values, in a Diameter application policy:

```
configure
    subscriber-mgmt
        diameter-application-policy "diameter-nasreq-policy-1" create
            description "Diameter NASREQ application policy"
            application nasreq
            diameter-peer-policy "diameter-peer-policy-1"
            nasreq
                user-name-format mac
                include-avp
                    circuit-id
                    nas-port-id
                    nas-port-type
                    remote-id
                exit
            exit
        exit
```

To apply the Diameter NASREQ application policy as Diameter authentication policy at a VPLS capture SAP, at an IES/VPRN group-interface and/or at a local user database:

(**Note:** A Diameter authentication policy cannot be configured simultaneously with a RADIUS authentication policy on the same group-interface or capture SAP, nor for the same host in a local user database.)

```
configure
    service
        vpls 10 customer 1 create
            sap 1/1/4:*.* capture-sap create
                ---snip---
                diameter-auth-policy "diameter-nasreq-policy-1"
        ies 1000 customer 1 create
```

```
            subscriber-interface "sub-int-1" create
                ---snip---
                group-interface "group-int-1-1" create
                ---snip---
                    diameter-auth-policy "diameter-nasreq-policy-1"
        vprn 2000 customer 1 create
            subscriber-interface "sub-int-1" create
                ---snip---
                group-interface "group-int-1-1" create
                ---snip---
                    diameter-auth-policy "diameter-nasreq-policy-1"

configure
    subscriber-mgmt
        local-user-db "ludb-1" create
            ipoe
                host "ipoe-host-1" create
                    ---snip---
                    diameter-auth-policy "diameter-nasreq-policy-1"
            ppp
                host "ppp-host-1" create
                    diameter-auth-policy "diameter-nasreq-policy-1"
```

If no AA-Answer message is received from the primary or secondary Diameter peer, then the host or session can be instantiated with the configured defaults. This is achieved by the following NASREQ application policy configuration:

```
configure
    subscriber-mgmt
        diameter-application-policy "diameter-nasreq-policy-1" create
            on-failure failover enabled handling continue
```

To enable flexible integration with different NASREQ servers, a Python policy can be configured on the Diameter peer policy. The Python script can interact on the AVPs present in the AA-Request and AA-Answer messages.

```
configure
    python
        python-policy "py-policy-nasreq-1" create
            diameter aar direction egress script "NasreqAar"
            diameter aaa direction ingress script "NasreqAaa"
configure
    aaa
        diameter-peer-policy "diameter-peer-policy-1" create
            ---snip---
            python-policy "py-policy-nasreq-1"
```

Diameter Redundancy

Diameter redundancy is supported on multiple levels:

- **Diameter Peer Level Redundancy:** A Diameter client in 7x50 supports up to five open peers, two of which (primary and secondary) can actively participate in Diameter transactions. The purpose of the secondary peer is to protect the primary peer, should the primary peer experience problems.
- **Diameter Multi-Chassis Redundancy**: Diameter sessions are synchronized on the application level (via ESM in case of Gx and NASREQ) between two redundant 7x50 nodes. Only one of the 7750 SRs opens up a peering connection on behalf of the redundant 7750 SR pair towards DRA/PCRF.
- **High Availability (HA)**: This refers to control plane redundancy with dual Control Plane Modules (CPMs) in a single chassis configuration. Diameter transactions are fully synchronized between CPMs and the peering connection towards DRA/PCRF remains uninterrupted in case that one of the control plane modules fails.

Diameter Peer Level Redundancy

Once the peer in the Diameter policy (maximum five peers per policy) is administratively enabled (**no-shutdown**), the 7x50 starts connecting to it. If the establishment of the TCP connection fails, the 7x50 periodically retries to connect.

If creation of the TCP connection succeeds, the peer is placed in the **peer table**, and in that table the “preference” defines the **current usability** of the peers. All administratively enabled peers that are in the open state have keepalives (DWR/DWA) enabled to check the liveliness of the connection, but only the two open peers with the highest preference are considered as primary and secondary. In this fashion, the application messages (for example, DCCA or Gx) are sent only to the primary and/or the secondary peer.

Initially all messages are sent to the primary peer. If a session-failover occurs (timeout or primary peer closes), the messages are sent to the secondary peer (which could have become primary by that time). Once an (application) session has switched, the consecutive messages are sent to the peer where it had its last success request/answer (it sticks to the peer).

The status of primary and secondary peer is constantly re-evaluated, in case an error condition occurs at the primary or secondary peer.

The following example shows how DCCA messages are treated:

1. There are ten sessions that have been created; the primary peer at that moment is peer-a, secondary peer is peer-b, and peer-c, peer-d and peer-e are in state open (being kept alive

with diameter watchdog request/watchdog-answer messages). Consequently, all CCR-i messages are sent to peer-a since this is the **preferred** peer at the time of handling CCA-i.

2. All ten sessions start requesting credit updates (CCR-u), but only six of them are successfully completed (CCR-u/CCA-u) by the peer-a. Their **preferred** peer will remain peer-a. Then, the connection to the peer-a fails (connection is closed). Peer-b becomes the primary, peer-c becomes the secondary. The remaining four CCR-u sessions that were pending will now be redirected to the peer-b with the retransmission bit (T) set in the diameter header. When these four outstanding transactions successfully complete (CCA-u received), they will have the peer-b as the **preferred** peer.
3. In the meantime, peer-a recovers, and the cooldown sequence is deactivated (by three successful DWR/DWAs). Peer-a becomes primary again and peer-b becomes secondary.
4. Now, the sessions need a new credit. Six of them will ask peer-a and four will ask peer-b.

   In case that peer-a did not become alive in time, peer-c would be used for re-transmissions. At some point later, when peer-a and peer-b become the primary and the secondary peers again, those sessions with the **preferred** peer-c will be redirected back to peer-a (as we only use peer-a and peer-b to send application messages).

   So in essence, a **revertive** mode is used for the peer recovery, where the sessions are reverted back to the peer on which the session was originally setup, as long as this peer is one of the two active peers (primary and secondary).

Diameter Multi-Chassis Redundancy

The Diameter Multi-Chassis Redundancy solution in the 7750 SR is based on the model where communication with the PCRF/DRA occurs over a single Diameter peering connection for the redundant pair of 7750 SR nodes; that is, an active Diameter proxy module running on the 7750 SR is front-ending the communication with the PCRF/DRA, and is relaying messages between the Diameter clients (in redundant 7750 SRs) and the DRA/PCRF. Both 7750 SR nodes run Diameter proxy module, but only the active one opens the TCP peering connection towards the DRA/PCRF.

The benefits of the Diameter proxy model are:

- The redundant pair of 7750 SR nodes appear as a single node to the PCRF/DRA.
- Diameter Identity is uniform across the pair of redundant 7750 SR nodes; that is, both 7750 SR nodes share the same origin-host/realm, a property that carries operational benefits.
- There is a robust and predictable failover of a single connection, as opposed to having separate diameter peering sessions per node.

The goal of this redundancy model is to provide a predictable and quick recovery after a 7750 SR nodal failure, PCRF failure, or relevant components within those two entities (such as line cards,

MDAs, and physical ports).

Figure 186 illustrates the basic concept for Diameter Multi-Chassis Redundancy for a Gx application. The model shows two 7750 SRs (BNGs). Each BNG contains an ESM module and a Gx/Diameter module which have a peering connection to the active Diameter proxy module. The peering connections are IP connections. Both nodes communicate with the PCRF/DRA through the active Diameter proxy which maintains a peering connection with the PCRF/DRA.

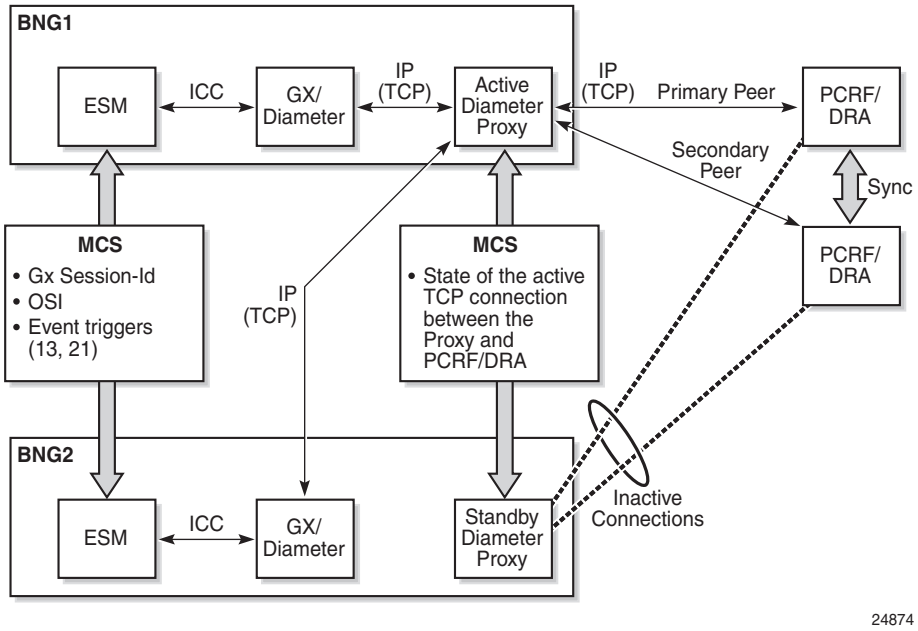

Figure 186: Proxy Gx Model

Diameter Proxy Model General Operational Principles

The fundamental principles of the Diameter proxy-based redundant solution are described below (also refer to Figure 186):

1. There can be only one active Diameter proxy per redundant pair of 7750 SRs. This active Diameter proxy maintains peering connections (primary/secondary) towards the PCRF/DRA at any given time. There are no peering connections open on the standby Diameter proxy. The active Diameter proxy accepts the connections from the client side, while the standby does not. The standby Diameter proxy ignores, without any reply, requests from the clients to open peering connections.
2. The activity selection is based on the system MAC address of each node and the current state of the Diameter proxy (Init, Active, Standby, Active-Wait, Standby-Wait and the Proxy-Switchover-Reg) in each node. This information is exchanged between the 7750 SR

nodes via MCS. The system MAC address is unique per 7750 SR node. The activity selection is automatic and cannot be influenced via CLI, other than shutting down peers on the currently active Diameter proxy.

Application level information (Gx session, NASREQ session, etc.) is not synchronized between Diameter proxies. Instead, synchronization of session level information is performed on the application level; for example, Gx session information is performed through subscriber management (ESM) synchronization.

3. Preemption is not supported in the case where a node coming up from a boot-up sequence would cause the MCS peer to transition from active to standby state. Only in the case where the two nodes are booting simultaneously, or are recovering from the MCS synchronization loss (both nodes are joining MCS while in the active state), would the node with a higher system MAC address transition into the active state (during the simultaneous node boot-up) or remain in the active state (after isolation re-synchronization).
4. When the Diameter proxy transitions from an active to standby state, the newly-transitioned standby Diameter proxy closes the TCP connections towards the Diameter clients. The clients then initiate a new connection towards the secondary peer, but only after the current connection-timer expires (30 s by default). For example, assume that the connection timer is set for 30 s. If the TCP RST is received when the running connection-timer is at 15th s, then the secondary peer is not initiated for another 15 s.
5. In the case where the active Diameter proxy receives messages from the client while it does not have any peers on the server side open, the Diameter proxy sends a DIAMETER_UNABLE_TO_DELIVER (3002) message to the client. The client then retransmits the message to the same peer since it has only one peer that is in the UP state. Upon receipt of the DIAMETER_UNABLE_TO_DELIVER (3002) message, the client leaves the original message to time out, and then retransmits it (that is, the message is NOT retransmitted from the client side immediately upon the arrival of the DIAMETER_UNABLE_TO_DELIVER (3002) message).

6. The TCP protocol handles retransmissions on the transport layer to the same peer. This is valid on the Diameter client side and on the Diameter proxy side. A TCP retransmission normally occurs at the intervals driven by an exponential back-off. The initial timeout depends on the implementation, but for the most common case, it can be assumed to be 1.5 s, followed by an exponential back-off capped at 64 s (1.5 s, 3 s, 6 s, 12 s, 24 s, 48 s, 64 s).
7. The Diameter client handles retransmissions on the Diameter level. The Diameter client will be able to retransmit on the same socket since it only has a single socket (to the active Diameter proxy). The T-bit in the Diameter header will be set for every retransmitted message. The watchdog interval should be set to 1 s, so that the dead TCP connection (dead proxy) can be quickly identified.

   The Diameter client will retransmit when:

   - The original request times out.
   - It receives a reply with the E-bit set. Such retransmissions will not be triggered immediately upon the arrival of the response with E-bit set. Instead, the original messages that need to be retransmitted will be left in the pending queue to time out and will be retransmitted after the timeout period, which is controlled by the tx-timer command.
   - The primary peer is closed and the secondary peer is available.
8. The Diameter proxy never retransmits a message on the Diameter level since it does not perform any buffering (Tx/Pending queue). However, it does retransmit on the TCP level (hop-by-hop).
9. The Diameter proxy only relays messages between the client (application) and the server side (DRA/PCRF). The two bits in the Diameter header that the proxy is reacting on are the T-bit and the E-bit.

   If the T-bit is set in the message coming from the client side, the Diameter proxy sends the message to the secondary peer (invokes the peer failover procedure). That is, the application level retransmissions is performed by the Diameter client (which is peering with the Diameter proxy). The client sets the T-bit (retransmission bit) in the Diameter header and this signals to the Diameter proxy that it needs to failover the message to the alternate peer. This operation is performed on a per message basis and not on a per session basis.

   The Diameter proxy initiates a failover procedure to the secondary peer when the primary peer on Diameter proxy is closed, or the watchdog timer on the primary peer expires.

   All messages in the DRA/PCRF-to client direction with the E-bit set (the E-bit can be present only in answer messages) are dropped in the proxy. Consequently, the client retransmits the request, upon timeout.

   The messages with the E-bit set that are traveling in the opposite direction are not dropped; they are transparently passed to the DRA/PCRF.
10. On an SRRP Switchover, the AN-GW-IP of the newly-transitioned Master can be reported in CCR-u as an indication of the switchover. This functionality is enabled by arming the 7750 SR with the event-trigger id 13 (USER_LOCATION_CHANGE) from PCRF.

11. On a Diameter proxy switchover, a SNMP Log/Trap is generated.
12. The standby client (SRRP standby) discards all messages received by the Diameter proxy.

Diameter Proxy Activity Selection

The Diameter proxy with the highest system MAC address assumes the controller role. The controller node decides which proxy becomes ACTIVE or STANDBY. Activity election information is processed by the controller node and then the controller node delegates the actual ACTIVE/STANDBY roles to Diameter proxies. The ACTIVE proxy may not necessarily be the same node as the controller node.

The activity selection (by the controller node) in the Diameter proxy is based on the current states of both Diameter Proxies (local and remote) and the system MAC.

Preemption is not supported, which means that newly brought up Diameter proxy does not overtake the activity state from the existing active Diameter proxy, regardless of the system MAC addresses.

Once the node becomes active, it advertises the new state to the MCS Diameter proxy peer and tries to open a DRA/PCRF peering connections and at the same time accept the client connections. The active Diameter proxy replies to the client with a DIAMETER_UNABLE_TO_DELIVER error-code in cases where server side peers cannot be opened.

Synchronization and MCS

All application level (Gx or NASREQ) sessions related parameters are synchronized on the ESM level via MCS.

The parameters synchronized on the ESM level are:

- Session-Id
- Event-Triggers
- CC-Request-Number

The Diameter proxy module is synchronized via MCS; the information passed between the two nodes is:

- System MAC address: this address plays a role in the Diameter proxy state selection
- Controller MAC address: the System MAC address of the node that is performing the Diameter proxy state selection. The node with the highest system MAC address assumes the controller role. Once the controller makes the state selection for both nodes, it

delegates those states to Diameter proxies. The controller role is collocated with one of the Diameter proxy nodes.

- Origin-State-Id (OSI)
- Diameter proxy States

The above information is used to determine the activity of the Diameter proxy at each node.

In the case where an MCS link fails, the nodes become isolated. Each node acts independently and tries to become active. This scenario is described in Isolated Chassis on page 2185.

Retransmissions

The handling of Diameter retransmissions is crucial for the Diameter Multi-Chassis Redundancy operation. Retransmissions provide the means to recover a Diameter session that was left in an unacknowledged state due to failure of the path between the 7750 SR and the DRA/PCRF.

Retransmissions of Diameter messages are handled on two levels by a pair of redundant 7750 SR nodes:

1. At the TCP level: request and answer messages are retransmitted by TCP. These types of retransmissions are only significant between two directly connected peers, hop-by-hop retransmissions. For example, if the failure occurs beyond two directly connected peers, these type of retransmissions will not help.
2. At the application (Gx, Gy, NASREQ) level: only request messages are retransmitted. These types of retransmissions extend beyond two directly connected peers and can cover end-to-end failure cases.

A more detailed explanation of the processing that occurs on each level for a Gx application is given below.

1. The first level of retransmissions occurs at the TCP level. The Gx message is handed over to the TCP socket Base Diameter module. TCP tries to deliver this message in a connection-oriented (reliable) fashion. If a TCP ACK for the transmitted message is not received, the message, in the most common case, is retransmitted in intervals of 1.5 s, 3 s, 6 s, up to 64 s. After 10 s of trying to retransmit the message to the same peer at the TCP level, the Base Diameter tries to retransmit (configuration dependent) the message to the next TCP socket (secondary peer). The assumption is that the primary peer is unavailable (busy, failed, or the network path to it is broken) after 10 s of trying. The TCP retransmissions are peer oriented and very localized (to the particular TCP connection on the particular BNG node). In the case of a network failure, TCP retransmissions cannot re-route the traffic to an alternate destination. As such, they cannot protect against the peer (PCRF) failure or the BNG node failure. They can, however, indirectly provide a clue that something is happening at the peer level, so that the upper layers can take adequate actions. Note that watchdogs are

also used to detect peer failure and they can provide faster detection of the peer failure (after 2 s).

2. Re-routing of the traffic occurs at the Application/Diameter level. Once the peer is considered unavailable, or the original requests message times out, the Diameter has the ability to re-route the retransmitted message to an alternate (secondary) peer. The Diameter level retransmissions can protect against a PCRF/DRA failure. Traffic can be switched to the secondary peer (this functionality must be enabled via configuration).

   Since the Diameter proxy only relays the messages between the client and the DRA/PCRF, it never buffers and retransmits the Diameter message. Retransmissions are the responsibility of the Diameter peer (Diameter client) that sits behind the Diameter proxy. Retransmitting Diameter client sets the T-bit in the Diameter header of the retransmitted message (CC-req-num is kept the same in the original and retransmitted message). The T-bit in the message triggers the Diameter proxy to re-route the messages to the secondary peer while the primary peer is still active. This means that the Gx client has already retransmitted the message, and the Diameter proxy re-route its.

   In case of a single peer, the Diameter **client** retransmits the message to the same peer and it sets the T-bit in the Diameter header.

   In case of a single peer, the Diameter **proxy** sends the message with the T-bit set to the same peer.

   The Gx client typically re-routes the message to the secondary peer in the following cases:

   - The primary peer is closed and the secondary peer is available.
   - The Diameter message times out due to no response.
   - The Diameter message times out due to a received answer with E-bit set in the Diameter header (E-bit can be only set in the answer messages and it indicates *protocol errors* with Result-Code from the 3xxx range). Once the reply with E-bit set is received, the corresponding request message is left on the pending queue where it times out after the interval controlled by the tx-timer statement in the diameter-application-policy. Upon message timeout, the 7750 SR retransmits the message to the secondary peer if the secondary peer is available. If not, the message will is retransmitted to the same (primary) peer.

In summary:

- TCP handles retransmissions towards the peer (hop-by-hop retransmissions).
- Diameter and Diameter applications (Gx, Gy, NASREQ) retransmit to the secondary peer in cases where the application level message times out, a protocol error is received (Result-Code 3xxx) in the answer from the DRA/PCRF, or the primary peer is 'closed'. In case that there is only one peer available (primary), the Diameter application retransmits to that peer. The T-bit in retransmitted messages is always set. Diameter level retransmissions cover failure cases that extend beyond two directly connected hops.

- The Diameter proxy never retransmits (retransmissions are handled by the Diameter client that sits behind the proxy). However, the Diameter proxy sends messages with the T-bit set to the secondary peer.

These scenarios are shown in Figure 187, Figure 188, and Figure 189.

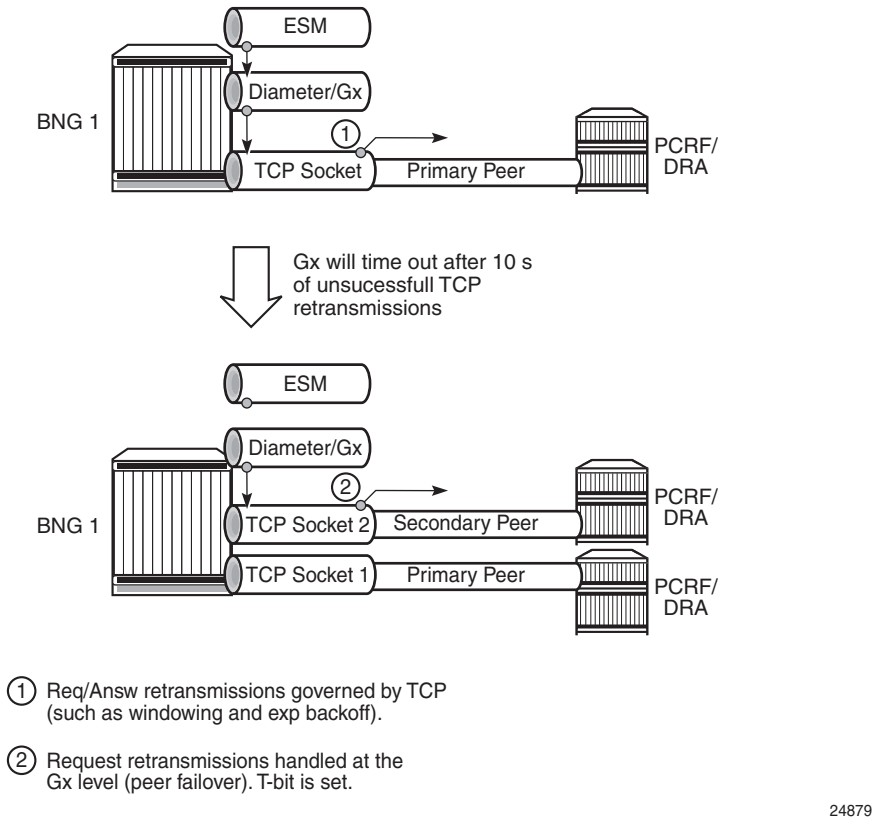

Figure 187: Retransmissions with Two Peers and no Diameter Proxy

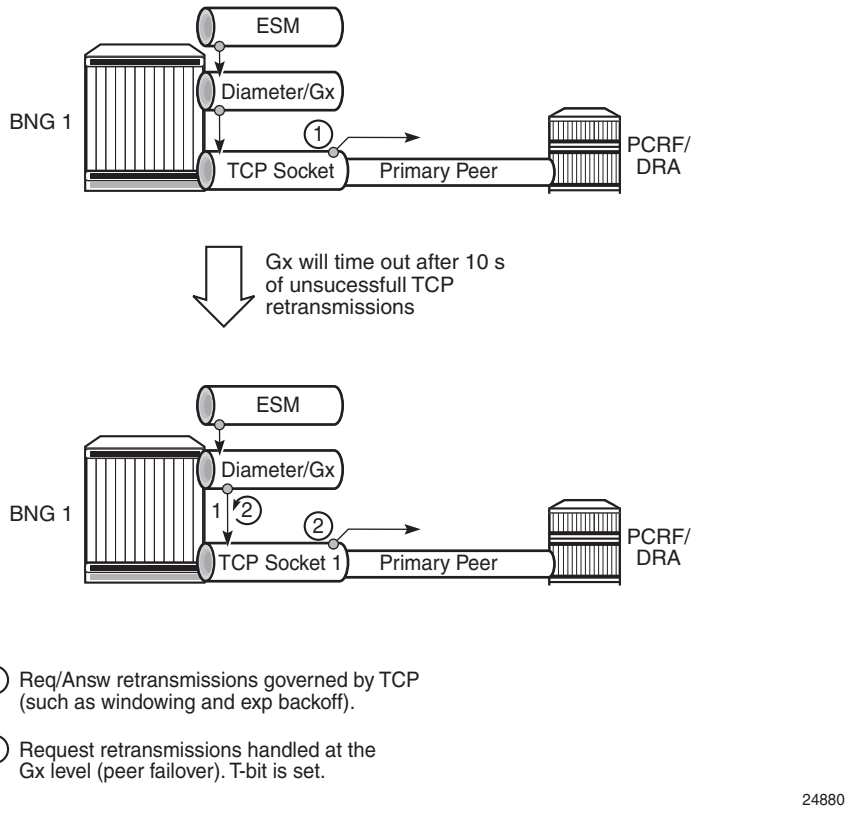

Figure 188: Retransmissions with a Single Peer and no Diameter Proxy

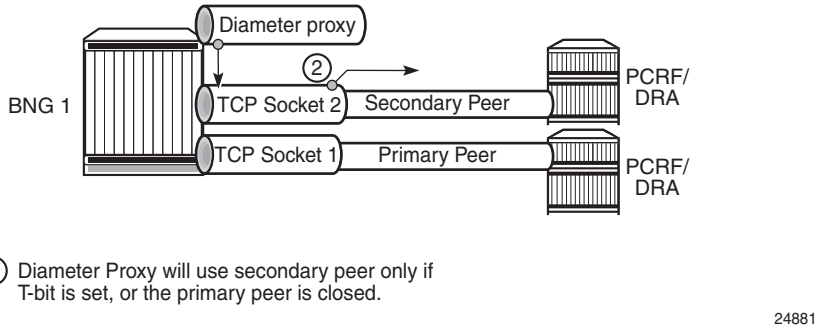

Figure 189: Redirection with Diameter Proxy (T-bit set)

Retransmissions and the T-bit

Multi-chassis redundancy is less concerned with the retransmissions of the answer messages (RAA) since, if the answer is not received, the PCRF retransmits the request (RAR). Retransmission of the **answer** messages is performed only on the TCP level within a single 7750 SR node. It is not performed on the Diameter level.

When the **request** message is retransmitted by the Diameter application (due to the Tx timer timeout, primary peer failure - DWR timeout, or receipt of the answer message with E-bit set), the content of the message stays the same, including the CC-Request numbers but the T-bit in the Diameter header is set. The T-bit indicates to the PCRF that the message is retransmitted (mostly used for accounting purposes so that the counting records are not duplicated). It also signals to the Diameter proxy that the message rerouting to the secondary peer should be performed.

Diameter Proxy Role

The Diameter proxy is applied to an IPv4 address within a routing-context on a 7750 SR. This IPv4 address is a Diameter proxy listening IPv4 address that is associated with an interface on a 7750 SR, including the system interface (system IPv4 address), or loopback interface (loopback IPv4 address).

The number of Diameter Proxies per listening IPv4 address is limited to one. That is, each proxy diameter-peer-policy requires a unique combination of source-ipv4 (listening IPv4 address) and the routing-context (router).

The number of Diameter-peer-policies on a 7750 SR is limited to 32. This means that the combined number of Diameter clients and Proxies on a 7750 SR cannot exceed 32.

The Diameter Proxy has the following role on a 7750 SR:

1. The active Diameter proxy relays messages between the application (Gx and NASREQ) module on a 7750 SR and the PCRF/DRA.
2. Only the active Diameter proxy allows peering connection with the client (the Diameter on a 7750 SR). The standby Diameter proxy refuses the client connection.
3. The Diameter proxy with open peering connections is referred to as the active Diameter proxy (ADP). Its counterpart is called the standby Diameter proxy.
4. The Diameter proxy retransmits the message on the TCP level towards the same peer.

5. However, the Diameter proxy does not perform application level message retransmission and the peer failover procedure due to the timeout of the application level message. Instead, the application level retransmission is performed by the Diameter client (which is peering with the Diameter proxy). The client sets the T-bit (retransmission bit) in the Diameter header of the retransmitted message (same CC-Req_Number) and this signals to the Diameter proxy that it needs to failover the message to the alternate peer. Note that this re-routing operation in the proxy is performed per message and not per sessions, as it is the case for a Diameter client.
6. When the primary peer is closed, or the watchdog timer on the primary peer expires, the Diameter proxy initiates failover procedure to the secondary peer.
7. The standby client (SRRP standby) discards received RAR messages.
8. The active Diameter proxy replies to the client with the error message UNABLE_TO_DELIVER in case that the peering connection towards the server cannot be open. The client retransmits the messages (since it has only one connection) after the timeout interval.

   Table 32 summarizes the differences between the regular Diameter client and the Diameter proxy.

Table 32: Summary of Differences Between the Regular Diameter Client and the Diameter Proxy

Regular Diameter Client	Diameter Proxy
Initiates messages.	Transparently passes all messages between the client and the server. Never initiates the messages.
Buffering is implemented, thus retransmissions are supported.	Buffering is not implemented (pending queue), thus messages are never retransmitted.
When retransmitting, it sets the T-bit in the Diameter Header.	Never retransmits the messages.
Failover to the secondary peer is triggered by: • Message timeout • Primary peer is down; immediate failover. • All messages with an E-bit set triggers failover after the message times out on the pending queue.	Failover to the secondary peer is triggered by: • Messages with T-bit set; immediate failover per message. • Primary peer shutdown
Diameter client performs peer failover per session.	Diameter proxy performs peer failover per message (with the T-bit set).

Diameter Proxy and CC-Request-Number AVP

CC-Request-Number AVP (RFC 4006, 8.2) are typically used to match requests with answers. Session-id and CC-Req-Num are a unique per-message pair. CC Request Numbers along with the session-id uniquely identify a transaction (matching requests and answer messages) on a global level.

The Diameter proxy does not re-write the CC-Request-Number in the messages received by the client.

CC-Req-numbers are synchronized at the ESM level. This is needed so that operation with proper CC-Req-Num can resume after the switchover.

For example, the following CC-Req-Num sequence for the session is preserved across SRRP switch-overs:

- 1st host (e.g. IPv4) of a dual-stack host is setup
- CCR-I with CC-Req-Num = 1 is sent
- 2nd host (for example,. IPv6 IA-NA) of the same dual-stack host is set up
- CCR-U with CC-Req-Num=2 is sent
- SRRP switchover occurs
- 2nd host in the dual-host is removed (DHPCv6 release)
- CCR-U with CC-Req-Num=3 is sent from the new SRRP Master

Stateless Diameter Proxy

The Diameter proxy does not maintain any session state. Forwarding is based on transactions which are short lived. Transactions are based on a pairing request/answer messages matched by the same hop-by-hop identifier and the peer from which the request was received. In this fashion, answer messages coming from the DRA/PCRF can be unambiguously forwarded to the proper Diameter client (from which the request was received).

Since the session state is not kept in Diameter proxy, RAR request are be flooded to both Diameter clients. The Diameter client on the standby SRRP node will silently drop such RAR requests and only the master SRRP will r

Switchover Scenarios

The following are four types of switchovers that are most likely to occur:

1. Switchover to a new DRA/PCRF peer at a Diameter proxy
2. Diameter proxy switchover due to failed peers on the server side
3. Diameter proxy switchover due to Diameter proxy node failure

4. SRRP switchover

Each switchover type for a Gx application is discussed in more detail below:

1. Switchover to a new PCRF/DRA peer is handled at the Diameter proxy level. This scenario is shown in Figure 190.

   The Diameter proxy switches over to the new peer in the event of two cases:

   - It receives a Diameter message with the T-bit set (retransmission bit in the Diameter header) from the Diameter client.

     Retransmission due to the message timeout is performed at the Diameter **client** level, and setting the T-bit signals to the Diameter proxy that peer failover is needed for this particular message.

   - The TCP connection to the primary peer is explicitly closed (for example, due to TCP RST or watchdog timeouts). In this case, the Diameter proxy performs a fail-over of all sessions to the secondary peer immediately.

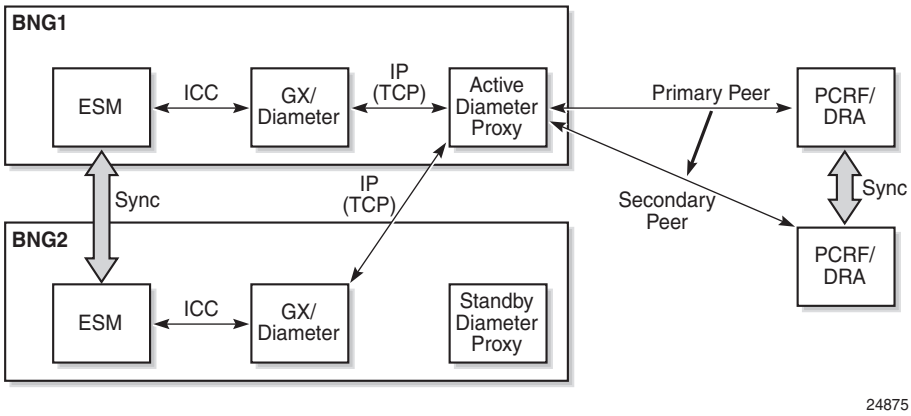

Figure 190: PCRF/DRA Peer Switchover

2. Activity switchover between the Diameter proxies occurs when the active Diameter proxy loses all peering connections to the PCRFs/DRAs while both 7750 SR nodes (including MCS) are operational.

   This type of switchover (without the node failure) is unlikely to occur. For example, a Diameter proxy switchover (without the node failure) would mean that all PCRFs/DRAs have failed, since normally the same pair of PCRF/DRA peers are configured in both Diameter proxy nodes. This would mean that all DRA/PCRFs are unavailable, which indicates a problem on the network side (either network paths to DRA/PCRFs are broken or all DRA/PCRFs have crashed).

   Another example where this scenario could occur is poor redundancy design practices. For example, the active Diameter proxy has a single peering connection to one PCRF (no

secondary peer), while the standby Diameter proxy is configured with a separate PCRF peer (the two PCRFs are still synch'd). This scenario is shown in Figure 191.

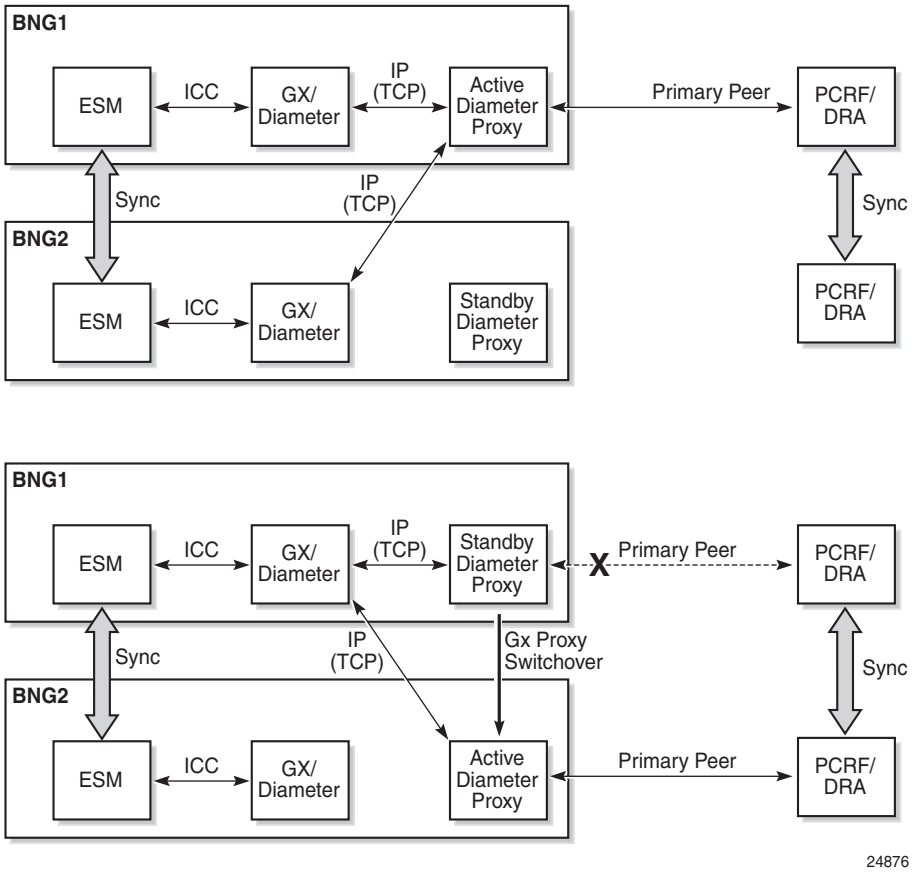

Figure 191: Diameter Proxy Switchover

As always, only the active Diameter proxy maintains an open TCP peering connection towards the PCRF/DRA. If this connection fails, the active proxy sends a TCP RST towards the client and transitions into standby state. The client then, upon expiry of connection-timer, open a new TCP connection towards the newly active Diameter proxy.

3. In this scenario, the entire proxy node fails, as shown in Figure 192. The surviving node resumes operation.

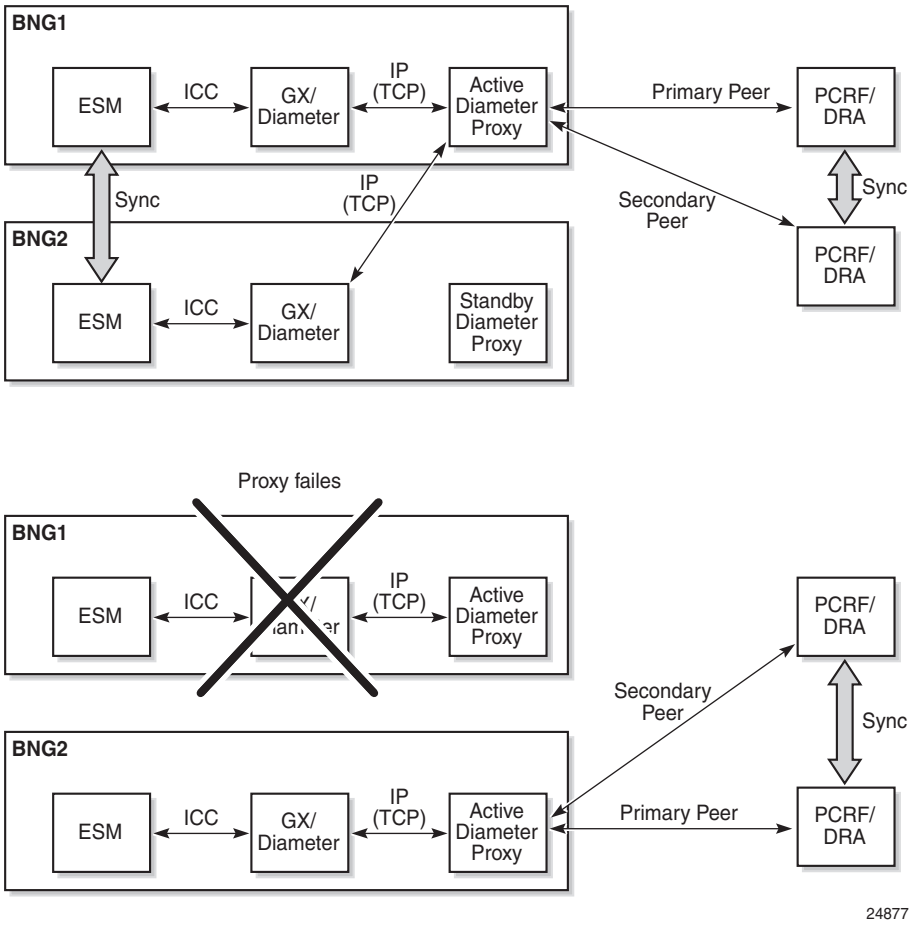

Figure 192: Node Failure

4. The last scenario is where the switchover occurs in the access and the SRRP switches activity. The new SRRP master resumes uninterrupted operation.

Log/Trap Generation Caused by Diameter Proxy State Change

In cases where the Diameter proxy changes its states (INIT, ACTIVE, STANDBY), a log/trap is generated. This log is enabled by default in log-event control. The notification name is `tmnxDiamProxyStateChange`.

Switchover Update Event (CCR-u)

The AN-GW-Address carried in the CCR-I message for the Diameter application session (for

example, Gx) is the IP address of the node on which the underlying SRRP instance (for this Gx session) is in the SRRP master state.

When the SRRP switches over due to the failure in the access part of the network (including the ports on a 7750 SR), a CCR-U can be optionally (configuration dependent) sent with the AN-GW-Address AVP of the node on which an SRRP instance transitioned into the master state.

This behavior is controlled via the event trigger id 13 (USER_LOCATION_CHANGE).

Isolated Chassis

In cases where the MCS connection is broken, the Diameter proxy on both 7750 SR nodes try to become active since they each consider that they are the only functional node. From the local point of view, the MCS peer is dead.

While in isolation scenario, both nodes are most likely able to open the TCP peering session with the PCRF/DRA (see Figure 193).

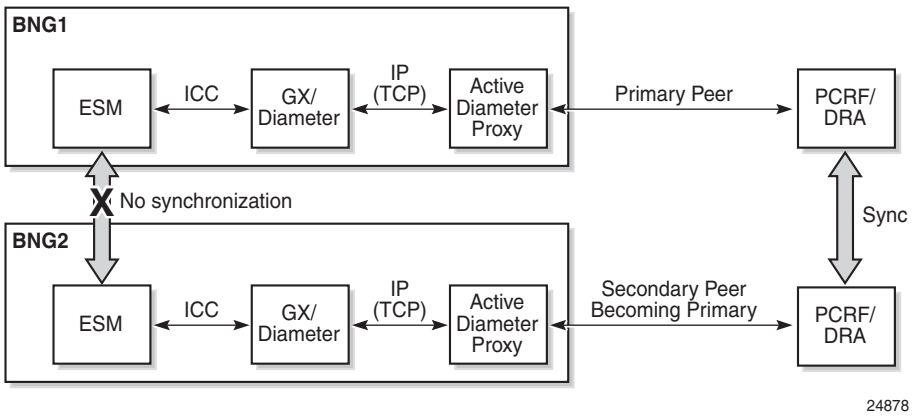

Figure 193: Isolated Nodes

Once the MCS is recovered, the states are re-synchronized.

Diameter Identities

Diameter identities (origin-host/realm) can be configured to be the same on both 7750 SR nodes. This ensures that the redundant pair of 7750 SRs appears as a single node at the Diameter level (Diameter Identities).

High Availability

A CPM switchover on the active Diameter proxy causes the peering connections between the client and the proxy to be lost. Consequently, the clients have to re-establish their peering connections. Peering connections on the active Diameter proxy towards the server remain uninterrupted.

Gx Specific Behavior

Gx specific behavior in a multi-chassis configuration is as follows:

1. A Gx client at a 7750 SR attempts to open a TCP connections to both Diameter proxies, but only the active Diameter proxy accepts accept the TCP request (see Diameter Multi-Chassis Redundancy on page 2170).
2. The standby Diameter proxy ignores the connection request and does not respond in any way (not even TCP RST).
3. The Gx client normally tries to reopen the configured connections (peers) every connection-timer interval (30 s by default).
4. Since the Gx client has only one peering connection open, retransmissions due to the application level message timeout occurs on that same peer. The T-bit is set and signals to the Diameter proxy that it needs to perform a peer failover procedure.
5. The Gx client discards/ignores all messages received on the standby node (standby SRRP).