Application Assurance — Usage Monitoring and Policy Control via Diameter Gx Protocol

In This Chapter

This section provides information about the diameter (Gx) control feature.

Topics in this section include:

Applicability

This configuration note is applicable to all 7750 SR/SR-c and 7450 ESS chassis supporting Application Assurance (AA).

The configuration was tested on release 12.0.R3.

Overview

The Gx reference point is defined in the Policy and Charging Control (PCC) architecture within the 3rd Generation Partnership Project (3GPP) standardization body. The Gx reference point is used for policy and charging control. The PCC architecture is defined in the 23.203 3GPP technical specification, while the Gx functionality is defined in the 29.212 3GPP technical specification. The SR OS implementation of Gx is based on Release 11 of the specification. Gx is an application of the Diameter protocol (RFC 6733). The Diameter protocol in SR OS is based on RFC 3588, *Diameter Base* Protocol.

As shown in Figure 188, Gx is placed between a policy server Policy and Charging Rule Function (PCRF) and a traffic forwarding node Policy and Charging Enforcement Function (PCEF) that enforces rules set by the policy server.

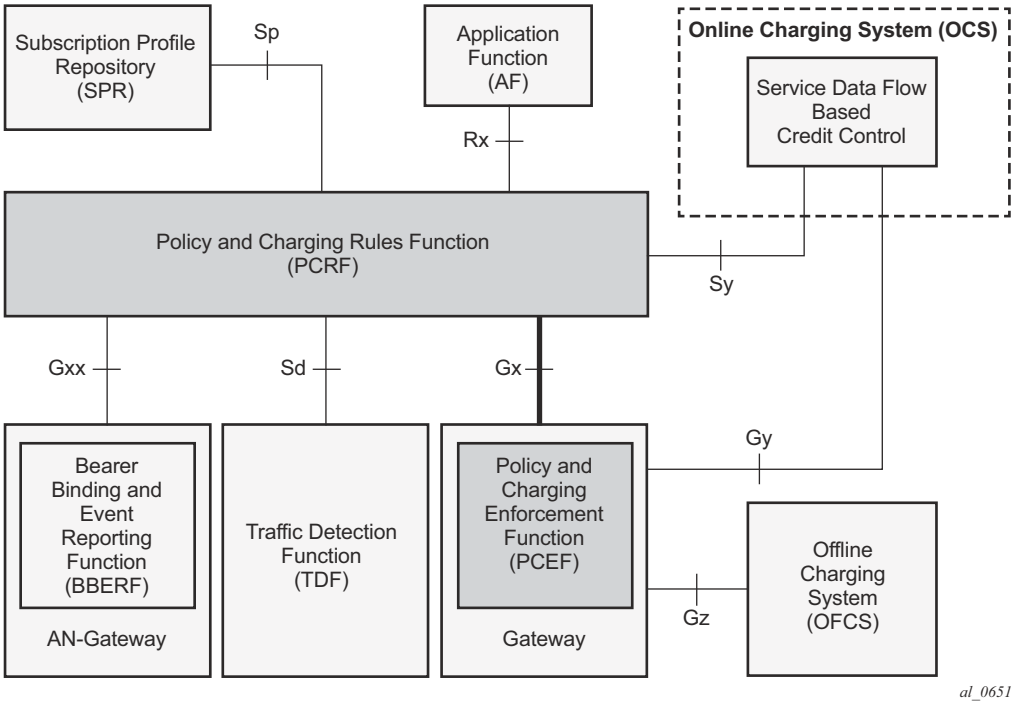

Figure 188: Gx Reference Point

Although the Gx reference point is defined within the 3GPP standardization body, its applicability has also spread to wire-line operations to achieve mobile–fixed convergence gains by streamlining policy management functions into a single Gx based infrastructure, see Figure 189.

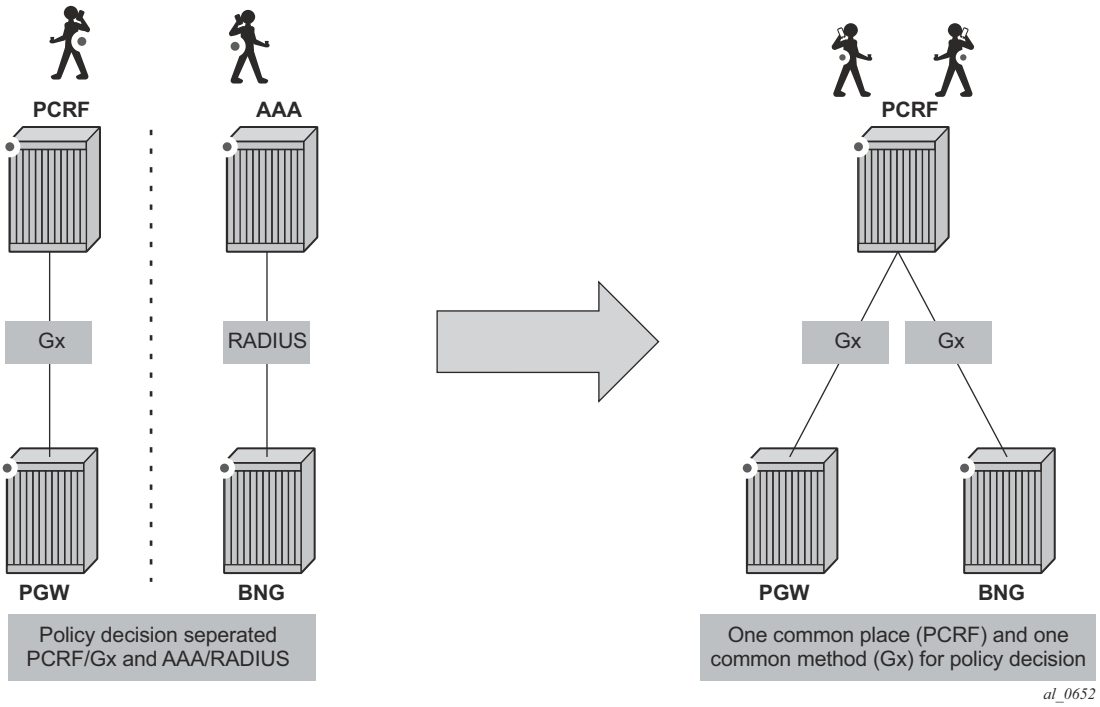

Figure 189: Convergence

Gx support on SR OS is applicable to Enhanced Subscriber Management (ESM) functions, including the Application Assurance (AA) functions. The focus of this example is on the AA aspects of Gx.

The SR OS based Gx interface offers the following functionalities:

- ESM subscriber based policy decision providing
  - QoS attributes
  - charging attributes
  - subscriber identification
- Usage management
  - usage reporting from PCEF to PCRF

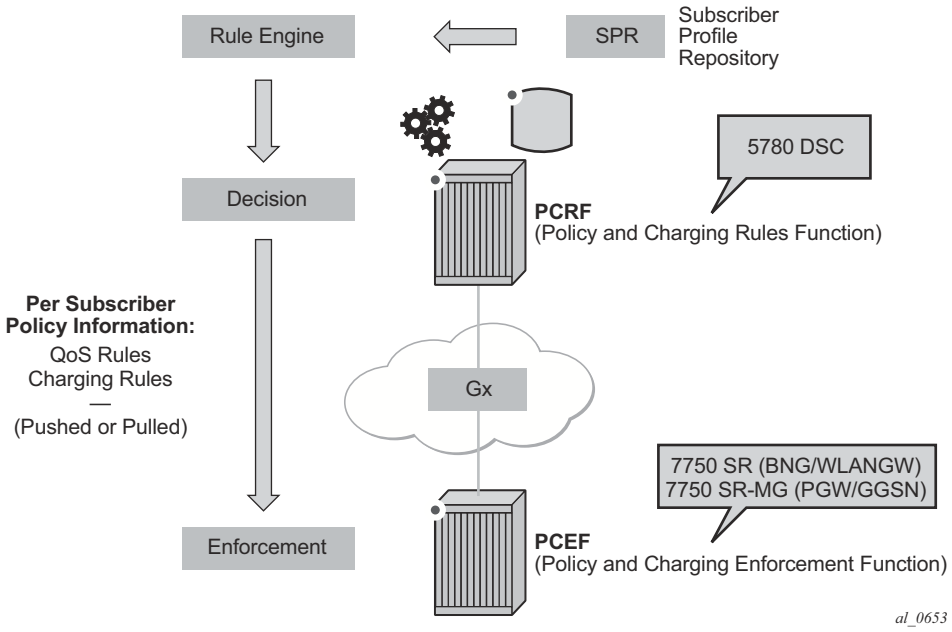

Figure 190: Gx Reference Point

Note that Gx does not provide subscriber authentication or subscriber IP address assignment.

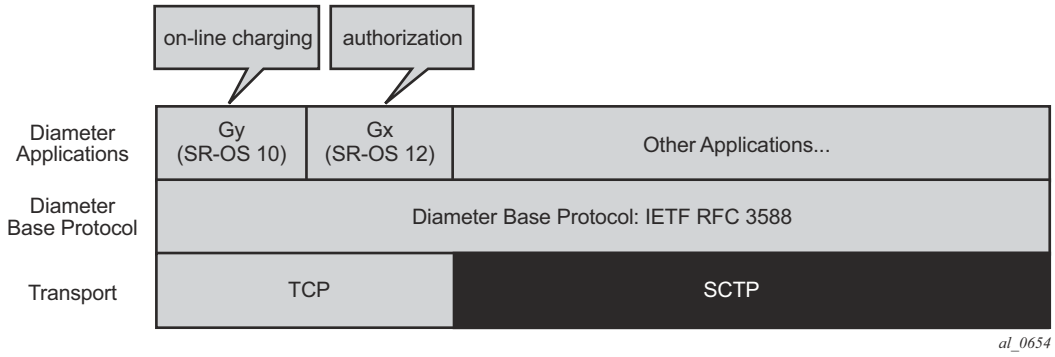

Figure 191: Diameter Protocol Stack

Policy Assignment Use Case

The SR OS accepts the following policy information from PCRF using Gx:

- Subscriber Profile strings and SLA Profile strings.
- Subscriber-QoS-Overrides.
- Application Profile strings.
- Application Subscriber Options (ASOs) related to AA.

Gx operates at subscriber host level and creates an “IP-CAN Session” (IP Connectivity Access Network) for every subscriber host. However, as AA operates at the subscriber level, AA related policies apply to all of the hosts belonging to that subscriber.

The scope of this example covers AA related functionalities, namely: application profile and ASO assignments and override. These functionalities are defined in what 3GPP calls Application Detection and Control (ADC) rules.

- **Application Profile** Alc-AA-Profile-Name Attribute-Value-Pair (AVP)
  - Radius equivalent is Alc-App-Prof-Str Vendor-Specific-Attribute (VSA)
- **ASO overrides** Alc-AA-Service-Options AVP
  - RADIUS equivalent is Alc-AA-App-Service-Options VSA

Details of the ADC rules and related ALU defined AVPs defined for use by AA are shown in Figure 192.

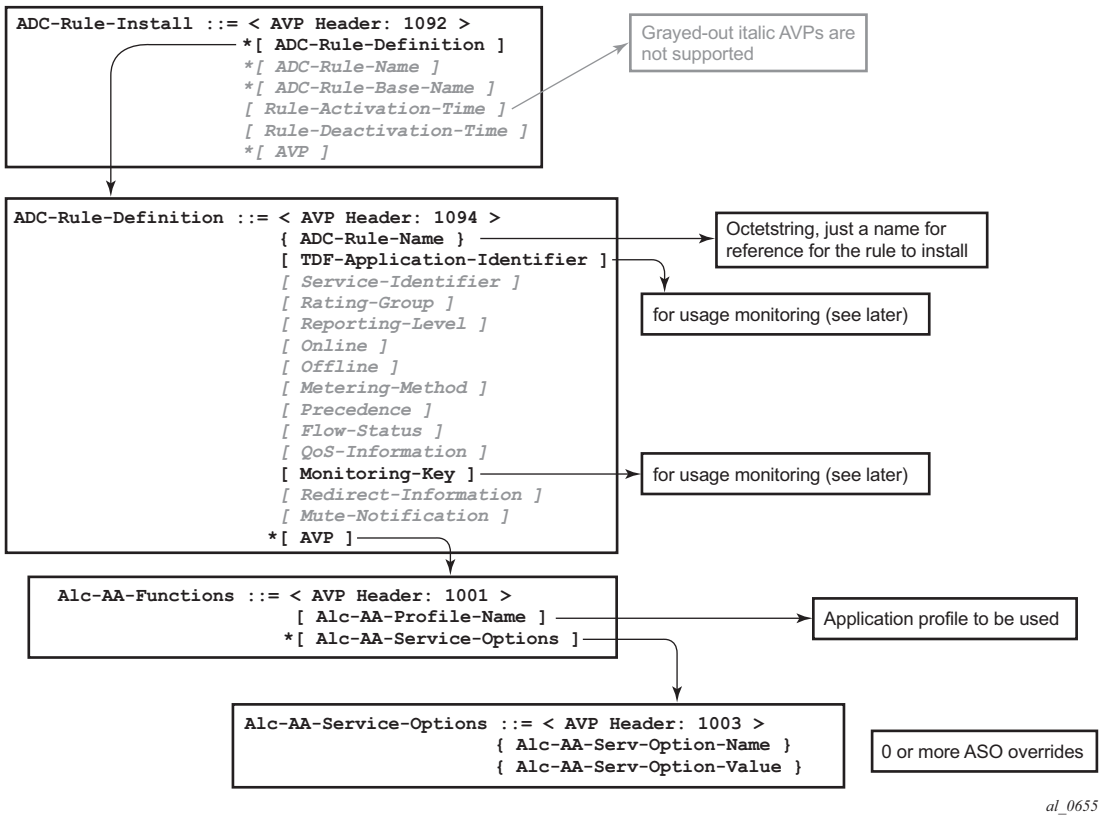

Figure 192: ADC Rules and Related ALU Defined AVPs Defined for Use by AA

The ADC-Rule-Install is at the root level of the GX message.

An example of the AVPs to install the “gold_level” application profile is shown in Figure 193.

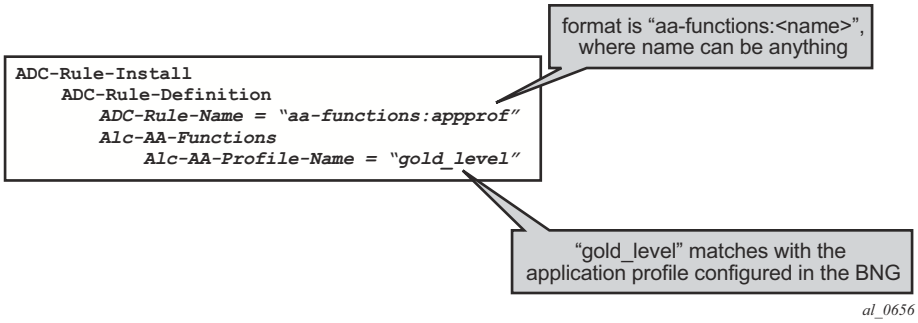

Figure 193: Example of AVPs to Install the “gold_level” Application Profile

NOTE: An ADC-Rule-Name has to start with "**aa-functions**" when it contains an Alc-AA-Functions AVP**.**

The assignment of the "gold_level" appProfile is shown in another format in Figure 194.

```
adc-rule-install (1092) V------- [184]
      vendor-id TGPP
      data [172] (Grouped)
        adc-rule-definition (1094) V------ [172]
          vendor-id TGPP
          data [160] (Grouped)
            adc-rule-name (1096) V------ [32]
              vendore-id TGPP
              data [20] (UTF8String) : aa-functions:appprof
            AA-Functions (1001) V------ [128]
              vendor-id ALU
              data [116] (Grouped)
                AA-Profile-Name (1002) V------ [17]
                vendor-id ALU
                data [5] (UTF8String) : gold level
                AA-App-Service-Options (1003) V------ [48]
                  vendor-id ALU
                  data [36] (Grouped)
                    AA-App-Service-Options-Name (1004) V------ [17]
                      vendor-id ALU
                      data [5] (UTF8String) : level
                    AA-App-Serv-Options-Value (1005) V------ [16]
                      vendor-id ALU
                      data [4] (UTF8String) : high
                AA-App-Service-Options (1003) V------ [48]
                  vendor-id ALU
                  data [36] (Grouped)
                    AA-App-Serv-Options-Name (1004) V------ [18]
                      vendor-id ALU
                      data [6] (UTF8String) : p2p
                    AA-App-Serv-Options-Value (1005) V------ [14]
                      vendor-id ALU
                      data [2] (UTF8String) : unlimited
```

al_0657

Figure 194: Capture of the Assignment of the "gold_level" appProfile

Application profiles and ASO overrides can be changed on-the-fly with a Re-Authentication-Request (RAR) message according to these rules:

- If an Application profile is present in the Gx message it is applied first. Then ASO AVPs are applied when present (in the Gx message) In other words:
  - If an RAR message only contains the same application profile and no ASO overrides, then all previous ASO overrides are removed.
  - When an RAR message contains the same application profile and new ASO overrides, then the new ASO overrides are applied, and the previous ASO overrides are removed.
  - When an RAR message contains a new application profile, all previous ASO overrides are removed and replaced with the ASOs in the RAR if present.

- When an RAR message does not contain an application profile but only ASO overrides, then the new ASO overrides are added to the existing ASO overrides.

Note that a single Gx ADC rule cannot contain both AA subscriber policies (appProfile/ASO) and AA Usage monitoring (as outlined later). These have to be in separate ADC rules.

Usage Management/Monitoring Use-Case

The AA-ISA can monitor application usage at the subscriber level and report back to the PCRF whenever the usage exceeds the threshold(s) set by the PCRF when receiving requests from the PCRF over the Gx interface.

Usage monitoring can be used by operators to report to PCRF when:

- The AA-ISA detects the start of a subscriber application by setting the usage threshold to a very low value.
- A pre-set usage volume per subscriber application is exceeded.

AA can monitor subscriber's traffic for any defined:

- Application,
- Application group, and/or
- Charging group.

The AA-ISA reports the accumulated usage when:

- A usage threshold is reached.
- The PCRF explicitly disables the usage monitoring.
- The PCRF requests a report.
- The ADC rule associated with the monitoring instance is removed or deactivated.
- A session is terminated.

An AA defined application, application group and/or charging group is automatically allowed to be referenced by an ADC rule for the purpose of usage monitoring only if:

{It is already selected for either XML or RADIUS per subscriber accounting
OR
It is explicitly enabled by the operator for per subscriber statistics collection}

AND

Usage monitoring is enabled for the given AA group:partition

Figure 195 illustrates the different messaging/call flows involved in application level usage monitoring. Details of the different supported AVPs used in these messages are illustrated later.

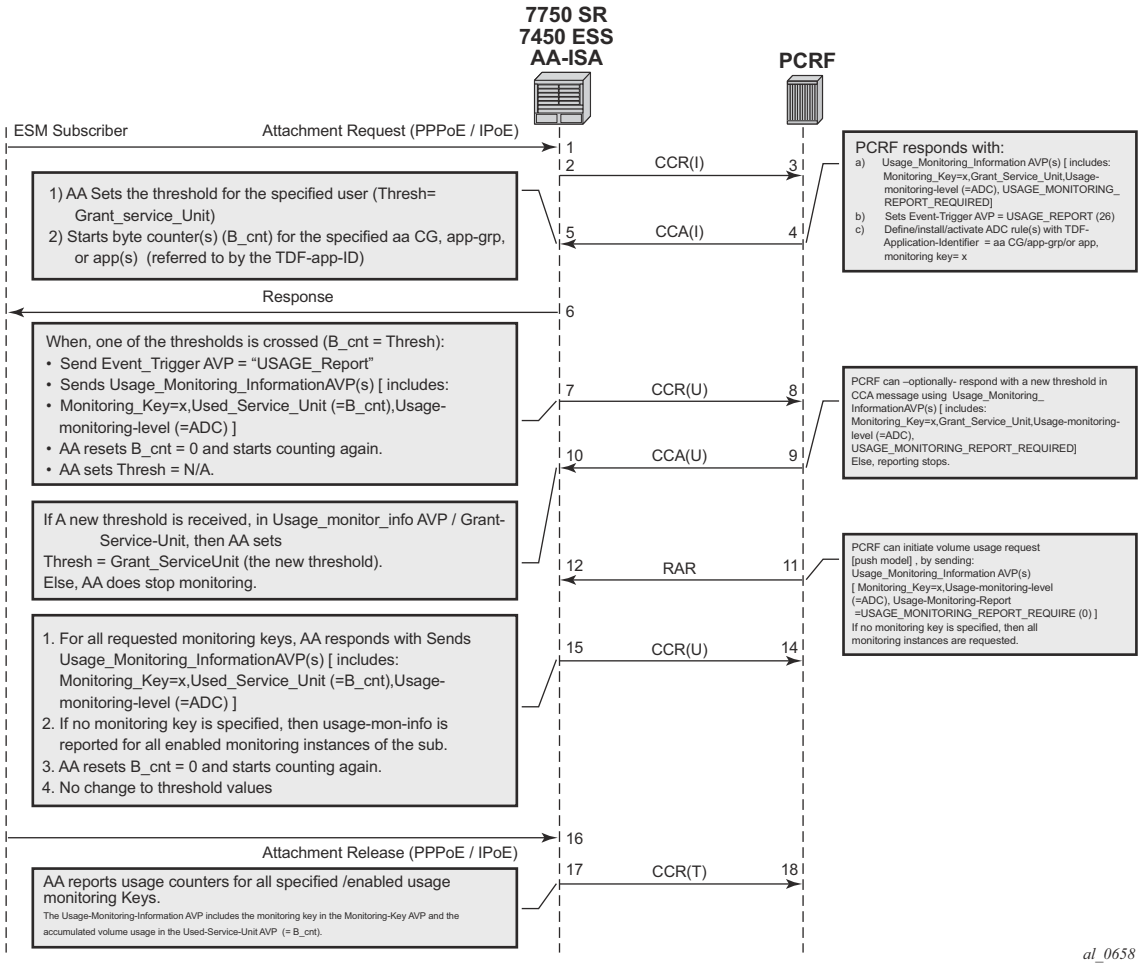

Figure 195: Call Flow Diagram

The AA-ISA/PCEF supports Usage-Thresholds AVPs that refer to the thresholds (in bytes) at which point an event needs to be sent back to the PCRF, (see Figure 195).

Time based thresholds are not supported.

AA supports the "grant-service-unit" AVP using the following possible values (AVP):

- CC-Input-Octets AVP (code 412) : From Subscriber total byte count threshold.
- CC-Output-Octet AVP (code 414): To subscriber total byte count threshold.
- CC-Total-octets AVP (code 421): Threshold of aggregate traffic (Input and Output byte counters).

As shown in Figure 195, (T=7), AA sends a Credit Control Request (CCR_ message) with a "USAGE_REPORT" Event-Trigger AVP to the PCRF when the usage counter reaches the configured usage monitoring threshold for a given subscriber (and given application group). AA counters are reset (to zero) when the monitoring threshold is reached (and an event is sent back to the PCRF). The counter(s) however does not stop counting newly arriving traffic. AA counters only include “admitted” packets. Any packets that were discarded by AA due to, for example, policing actions are not counted for usage-monitoring purposes.

The TDF-Application-Identifier AVP (within the ADC rule) refers to an AA Charging group, an AA application group or to an AA application. TDF-Application-Identifiers (for example, charging-groups) have to be manually entered at the PCRF to match the AA charging groups defined in the AA. If the TDF-Application-Identifier refers to a name that is used for both a charging group and an application (or an application group), AA monitors the charging group. In other words, the AA charging group has a higher precedence than the AA application group.

Gx Usage Monitoring AVP Summary

The Vendor-Specific-Application-Id AVPs shown below indicates the manufacturer (ALU=6527) of the Diameter node as per RFC 3588.

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

ADC-Rule-Definition ::= < AVP Header: 1094 >
    { ADC-Rule-Name }
    [ TDF-Application-Identifier ]; AA app/app-grp/chrg-grp
    [ Monitoring-Key ] ];

    *[ AVP ]
    [AA-specific_attributes; vnd=ALU]  Vendor-specific AVP of type 'group'
        [AA-profile-name; vnd=ALU]//application assurance profile
        [AA-Characteristic; vnd=ALU] ;  < type group - optional >
            [Name; vnd=ALU]  ; type string
            [Value; vnd=ALU] ; type string


Usage-Monitoring-Information::= < AVP Header: 1067 >
    [ Monitoring-Key ]
    0,2[ Granted-Service-Unit ]
         Granted-Service-Unit ::= < AVP Header: 431 >
              [ CC-Total-Octets ]
              [ CC-Input-Octets ]
              [ CC-Output-Octets ]
    0,2[ Used-Service-Unit ]
         Used-Service-Unit ::= < AVP Header: 446 >
              [ CC-Total-Octets ] ;
              [ CC-Input-Octets ]
              [ CC-Output-Octets ]

    [ Usage-Monitoring-Level ]
       ; ADC_RULE_LEVEL (2)

    [ Usage-Monitoring-Report ]
       ; immediate report -- USAGE_MONITORING_REPORT_REQUIRED (0)

    [ Usage-Monitoring-Support ]
       ; to disable :  USAGE_MONITORING_DISABLED (0)
```

Configuration

This configuration example highlights the commands illustrating how Gx can be used to:

- Override AppProfile and ASO characteristics.
- Set and retrieve AA level usage monitoring metrics.

While the configuration associated with setting up the Gx interface towards the PCRF is shown for the sake of completeness, that aspect of the configuration is not explored in detail. Similarly, the Gx policies and usage monitoring associated with ESM host policies (non-AA aspects) are out of the scope of this example.

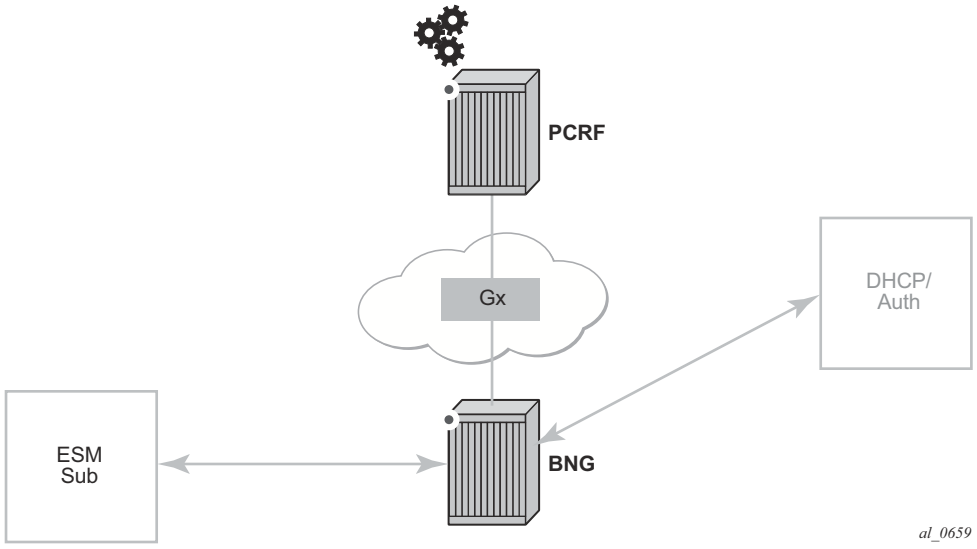

Figure 196: Example Configuration Setup

The BNG is set up with at least one IOM and one MS-ISA mda configured as ISA-AA.

```
configure
    card 1
        card-type iom3-xp
        mda 1
            mda-type m20-1gb-xp-sfp
            no shutdown
        exit
        mda 2
            mda-type isa-aa
            no shutdown
        exit
        no shutdown
    exit
```

```
card 3
    card-type iom3-xp
    mda 1
        mda-type isa-aa
        no shutdown
    exit
    mda 2
        mda-type isa-aa
        no shutdown
    exit
    no shutdown
exit
```

The configurations in this example are broken down into 4 main steps:

Step 1. Configuring the Gx interface (high-level)

Step 2. Configuring AA application profiles and ASOs (high-level)

Step 3. Configuring AA applications filters (high-level)

Step 4. Configuring AA usage-monitoring

The focus of this configuration example is on Step 4 and the updated show routines related to AA ESM subscriber state are shown at the end of Step 2.

Step 1. Configuring the Gx interface (high-level)

These commands bring up the Gx diameter controller channel between the Gx Controller(/Server), also known as PCRF, and the PCEF(/BNG).

```
configure
 aaa
    diameter-peer-policy "ppol" create
       applications gx
        connection-timer 5
        origin-host "router.workstation"
        origin-realm "alcatel-lucent.com"
        transaction-timer 5
        watchdog-timer 10
        peer "ppeer0" create
            address 10.1.0.10
            destination-host "primary-pcrf.alcatel-lucent.com"
            destination-realm "alcatel-lucent.com"
            no shutdown
        exit
    exit
exit
```

The diameter peer policy "**ppol**" is then referenced under subscriber management.

```
configure
  subscriber-mgmt
    diameter-application-policy "diamAppPlcy" create
        application gx
        diameter-peer-policy "ppol"
    exit
```

Then the created subscriber management policy "**diamAppPlcy**" is applied to the subscriber interface.

```
configure
    service
        customer 1 create
            description "Default customer"
        exit
        ies 1 customer 1 vpn 1 create
            description "Default Ies description for service id 1"
            subscriber-interface "ies-1-172.16.0.0" create
                address 172.16.0.0/12
                group-interface "grp-1-35782656-1" create
                    dhcp
                        server 172.16.200.200
                        trusted
                        lease-populate 2000
                        gi-address 172.16.0.0
                        no shutdown
                    exit
                    diameter-application-policy "diamAppPlcy"
                    sap 1/1/4:1 create
```

```
                    description "sap-grp-1"
                    sub-sla-mgmt
                        def-sub-profile "sub_prof"
                        def-sla-profile "sla_prof"
                        def-app-profile "app_prof_1"
                        sub-ident-policy "sub_ident_A_1"
                        multi-sub-sap 2
                        no shutdown
                    exit
                exit
            exit
        exit
        service-name "ACG Ies 1"
        no shutdown
    exit
```

Now verify the configuration and connectivity towards the PCRF by running the following command:

```
*A:BNG-1# show aaa diameter-peer-policy "ppol"
===============================================================================
Diameter Peer Policy : ppol
===============================================================================
Last Mgmt Change      : 05/30/2014 18:53:38
-------------------------------------------------------------------------------
Diameter Config Values
-------------------------------------------------------------------------------
Origin Host           : router.workstation.be
Origin Realm          : lucent.com
Connection Timer      : 5                  Source Address     : 0.0.0.0
Transaction Timer     : 5                  Router             : Base
Watchdog Timer        : 10
Vendor Support        : 3GPP (default)
Python Policy         : N/A
-------------------------------------------------------------------------------
Peer Name            Oper  PSM State     Susp  Cooldown  Pref  Order  Pri/Sec
-------------------------------------------------------------------------------
ppeer0               Yes   I-Open        No    -         50    1      Primary
===============================================================================
*A:BNG-1#
```

The Peer-State-Machine State (PSM), as per RFC 3588, has the value I-OPEN indicating that the peer is operational. The “I-” stands for **I**nitiator state, in this case the BNG is the initiator.

A detailed look into the traffic statistics between the PCEF and the PCRF (Gx controller) can be viewed using a show statistics command (see below). These statistics provide a breakdown of the messages exchanged:

```
*A:BNG-1# show aaa diameter-peer-policy "ppol" peer "ppeer0" statistics
===============================================================================
Diameter Peer Policy : ppol (statistics)
===============================================================================
Diameter Peer             : ppeer0
time statistics cleared   : 05/30/2014 18:53:38
-------------------------------------------------------------------------------
```

```
Client initiated tx/rx                  Server initiated tx/rx
-------------------------------------------------------------------------------
TCP Send Failed           : 0           TCP Send Failed           : 0
Diam Rx Drop Count (Resps): 0           Diam Rx Drop Count (Reqs) : 0
Diam Tx Requests          : 313         Diam Rx Requests          : 204
Diam Rx Responses         : 313         Diam Tx Responses         : 204
Pending Messages          : 0
Request Timeouts          : 0
-------------------------------------------------------------------------------
Diameter message breakdown
-------------------------------------------------------------------------------
CCR initial Tx            : 111         CCA initial Rx            : 111
CCR update Tx             : 88          CCA update Rx             : 88
CCR terminate Tx          : 11          CCA terminate Rx          : 11
CER Tx                    : 1           CEA Rx                    : 1
DWR Tx                    : 102         DWA Rx                    : 102
DWR Rx                    : 0           DWA Tx                    : 0
ASR Rx                    : 0           ASA Tx                    : 0
RAR Rx                    : 204         RAA Tx                    : 204
DPR Tx                    : 0           DPA Rx                    : 0
DPR Rx                    : 0           DPA Tx                    : 0
===============================================================================
*A:BNG-1#
```

Step 2. Configuring AA application profiles and ASOs (high-level)

To illustrate the use of application profiles and ASO overrides using Gx RAR messages, four ASOs and 2 appProfiles are defined, see below.

“app_prof_1“ is the default app-profile used when a subscriber is created on AA.

```
configure
   application-assurance
       group 129:34883 create
           policy
               begin
               app-service-options
                   characteristic "permitDNS" persist-id 1 create
                       value "no"
                       value "yes"
                       default-value "yes"
                   exit
                   characteristic "permitRDP" persist-id 2 create
                       value "no"
                       value "yes"
                       default-value "yes"
                   exit
                   characteristic "permitHTTP" persist-id 3 create
                       value "no"
                       value "yes"
                       default-value "yes"
                   exit
               exit
               app-profile "app_prof_1" create
                   description "Application Profile Id app_prof_1"
                   divert
               exit
               app-profile "app_prof_2" create
                   description "Application Profile Id app_prof_2"
                   divert
               exit
```

Step 3. Configuring AA applications filters (high-level)

First create the application group, as follows.

```
 configure isa
        application-assurance-group 129 create
            primary 3/2
            backup 1/2
            partitions
            divert-fc be
            no shutdown
        exit
```

Then create the partition and associated charging groups, application groups, applications, etc.

```
configure
    application-assurance
        group 129:34883 create
            policy
                begin
                charging-group "0_rated" create
                    export-id 1
                exit
                charging-group "default_charge_group" create
                    export-id 255
                exit
                default-charging-group "default_charge_group"
                app-group "Other" create
                    export-id 8
                exit
                app-group "Peer to Peer" create
                    export-id 3
                exit
                app-group "Remote Connectivity" create
                    export-id 4
                exit
                app-group "Unknown"
                    charging-group "0_rated"
                    export-id 1
                exit
                app-group "Web" create
                    export-id 10
                exit
                application "DNS" create
                    description "default-description for application DNS"
                    app-group "Other"
                    export-id 12
                exit
                application "BitTorrent" create
                    app-group "Peer to Peer"
                    export-id 3
                exit
                application "HTTP" create
                    description "default-description for application HTTP"
                    app-group "Web"
```

```
                export-id 26
            exit
            application "RDP" create
                description "default-description for application RDP"
                app-group "Remote Connectivity"
                export-id 61
            exit
            application "Unknown"
                charging-group "0_rated"
                export-id 1
            exit
        exit
        commit
    exit
exit
```

Example app-filter definitions defining HTTP, DNS, Bittorrent and RDP applications are show below.

```
configure
    application-assurance
        group 129:34883
            policy
                begin
                app-filter
                    entry 6 create
                        description "default-description for AppFilter entry 6"
                        protocol eq "rdp"
                        ip-protocol-num eq tcp
                        application "RDP"
                        no shutdown
                    exit
                    entry 9 create
                        description "default-description for AppFilter entry 9"
                        protocol eq "dns"
                        ip-protocol-num eq udp
                        server-port eq range 53 55
                        application "DNS"
                        no shutdown
                    exit
                    entry 20 create
                        description "default-description for AppFilter entry 20"
                        protocol eq "bittorrent"
                        ip-protocol-num eq tcp
                        application "BitTorrent"
                        no shutdown
                    exit
                    entry 38 create
                        description "default-description for AppFilter entry 38"
                        protocol eq "http"
                        ip-protocol-num eq tcp
                        server-port gt 8738
                        application "HTTP"
                        no shutdown
                    exit
                exit
```

```
                commit
            exit
        exit
    exit
```

Note: The focus of this example is on the definition of app-filters and/or AQPs. These are listed above (and below) for illustration purposes. The “sample” AQP configurations and app-filters shown here should not be used in a real-life configuration. Their configuration should follow the information in Application Assurance — Application Identification and User-Defined Applications on page 1375.

Example AQP configurations for blocking DNS, RDP and HTTP traffic are listed below.

```
configure
    application-assurance
        group 129:34883
            policy
                begin
                app-qos-policy
                    entry 2 create
                        match
                            application eq "DNS"
                            characteristic "permitDNS" eq "no"
                        exit
                        action
                            drop
                        exit
                        no shutdown
                    exit
                    entry 3 create
                        match
                            application eq "HTTP"
                            characteristic "permitHTTP" eq "no"
                            ip-protocol-num neq 0
                        exit
                        action
                            drop
                        exit
                        no shutdown
                    exit
                    entry 4 create
                        match
                            application eq "RDP"
                            app-group eq "Remote Connectivity"
                            characteristic "permitRDP" eq "no"
                            ip-protocol-num neq udp
                        exit
                        action
                            drop
                        exit
                        no shutdown
                    exit
                exit
                commit
            exit
        exit
```

```
    exit
```

When an ESM subscriber is created, it is associated with the default AA app-profile, as seen using the show command below.

```
*A:BNG-1>show>app-assure>group# aa-sub esm "sub_172.16.0.2" summary
===============================================================================
Application-Assurance Subscriber Summary (realtime)
===============================================================================
AA-Subscriber           : sub_172.16.0.2 (esm)
ISA assigned            : 3/2
App-Profile             : app_prof_1
App-Profile divert      : Yes
Capacity cost           : 1
Aarp Instance Id        : N/A
HTTP URL Parameters     : (Not Specified)
Last HTTP Notified Time : N/A
-------------------------------------------------------------------------------
Traffic                         Octets              Packets                Flows
-------------------------------------------------------------------------------
From subscriber:
  Admitted                           0                    0                    0
  Denied                             0                    0                    0
  Active flows                                                                 0
To subscriber:
  Admitted                           0                    0                    0
  Denied                             0                    0                    0
  Active flows                                                                 0
Flow counts:
  Terminated                                                                   0
  Short duration                                                               0
  Med duration                                                                 0
  Long duration                                                                0
Total flow duration :  0 seconds
-------------------------------------------------------------------------------
Top App-Groups                                  Octets        Packets        Flows
-------------------------------------------------------------------------------
None
-------------------------------------------------------------------------------
Application Service Options (ASO)
-------------------------------------------------------------------------------
Characteristic                  Value                             Derived from
-------------------------------------------------------------------------------
permitDNS                       yes                               default
permitRDP                       yes                               default
permitHTTP                      yes                               default
===============================================================================
*A:BNG-1>show>app-assure>group#
```

After the PCRF sends out AppProfile and ASO override AVPs in RAR messages (as shown below) it can be seen that the new parameters (new profile and new values for permitDNS and permitHTTP ASOs) are updated for that ESM subscriber.

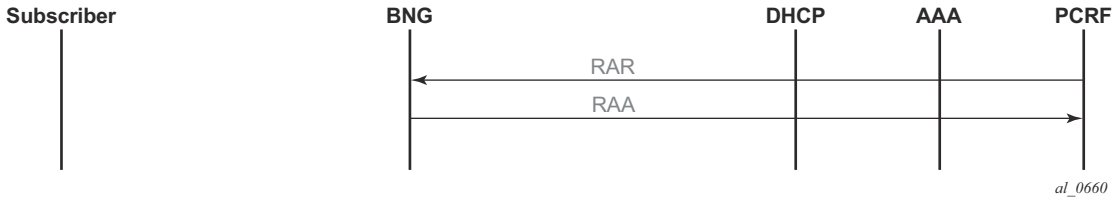

Figure 197: PCRF AVPs Override Call Flow Diagram

```
adc-rule-install (1092) V------- [184]
       vendor-id TGPP
       data [172] (Grouped)
          adc-rule-definition (1094) V------ [172]
             vendor-id TGPP
             data [160] (Grouped)
               adc-rule-name (1096) V------ [32]
                 vendore-id TGPP
                 data [20] (UTF8String) : aa-functions:appprof
               AA-Functions (1001) V------ [128]
                 vendor-id ALU
                 data [116] (Grouped)
                   AA-Profile-Name (1002) V------ [17]
                   vendor-id ALU
                   data [5] (UTF8String) : app_prof 2
                   AA-App-Service-Options (1003) V------ [48]
                     vendor-id ALU
                     data [36] (Grouped)
                       AA-App-Serv-Options-Name (1004) V------ [17]
                         vendor-id ALU
                         data [5] (UTF8String) : permitDNS
                       AA-App-Serv-Options-Value (1005) V------ [16]
                         vendor-id ALU
                         data [4] (UTF8String) : no
                   AA-App-Service-Options (1003) V------ [48]
                     vendor-id ALU
                     data [36] (Grouped)
                       AA-App-Serv-Options-Name (1004) V------ [18]
                         vendor-id ALU
                         data [6] (UTF8String) : permitHTTP
                       AA-App-Serv-Options-Value (1005) V------ [14]
                         vendor-id ALU
                         data [2] (UTF8String) : no
```

al_0661

Figure 198: RAR Containing ASOs and AppProfile Override AVPs Example

```
*A:BNG-1>show>app-assure>group# aa-sub esm "sub_172.16.0.2" summary
===============================================================================
Application-Assurance Subscriber Summary (realtime)
===============================================================================
AA-Subscriber           : sub_172.16.0.2 (esm)
ISA assigned            : 3/2
App-Profile             : app_prof_2
App-Profile divert      : Yes
Capacity cost           : 1
Aarp Instance Id        : N/A
HTTP URL Parameters     : (Not Specified)
```

```
Last HTTP Notified Time : N/A
-------------------------------------------------------------------------------
Traffic                         Octets              Packets                Flows
-------------------------------------------------------------------------------
From subscriber:
  Admitted                           0                    0                    0
  Denied                             0                    0                    0
  Active flows                                                                 0
To subscriber:
  Admitted                           0                    0                    0
  Denied                             0                    0                    0
  Active flows                                                                 0
Flow counts:
  Terminated                                                                   0
  Short duration                                                               0
  Med duration                                                                 0
  Long duration                                                                0
Total flow duration :  0 seconds

-------------------------------------------------------------------------------
Top App-Groups                                 Octets        Packets        Flows
-------------------------------------------------------------------------------
None

-------------------------------------------------------------------------------
Application Service Options (ASO)
-------------------------------------------------------------------------------
Characteristic                   Value                            Derived from
-------------------------------------------------------------------------------
permitDNS                        no                               dyn-override
permitRDP                        yes                              default
permitHTTP                       no                               dyn-override
===============================================================================
```

Step 4. Configuring AA Usage Monitoring

Once the applications, application groups and/or charging groups are defined and configured (see previous steps), the operator needs:

- to enable the collection of per-subscriber statistics so they can be used for Gx based usage-monitoring. This step is not needed for any app/appgrp or charging group that is already enabled for per-subscriber statistics. In other words, if XML or RADIUS accounting is enabled for a given app/appgrp or charging group, then Gx usage-monitoring is also automatically enabled.
- to enable usage-monitoring for the given AA group:partition.

```
config
    application-assurance
        group 129:34883
            statistics
                aa-sub
                    usage-monitoring
                    app-group "Unknown" export-using accounting-policy
                                                     radius-accounting-policy
                    charging-group "0_rated" export-using accounting-policy
                                                     radius-accounting-policy
                    charging-group "default_charge_group" export-using
                                                          accounting-policy
                    radius-accounting-policy
                    application "BitTorrent" no-export
                exit
```

In the example above:

- The usage-monitoring command is used to enable Gx usage monitoring for the specified AA partition.
- The aa-group and charging-group commands specify which charging groups and AA groups are selected for export. In this case *0-rated*, *Unknown*, and *default-charging-group* are selected for RADIUS accounting and they automatically qualify for Gx-usage monitoring.
- The BitTorrent application however needs to be explicitly configured as “no-export” as it needs to be enabled for Gx-usage monitoring.

The operator can display the number of usage monitoring rules for a given subscriber. This is shown below after the ESM subscriber is created but before any ADC rules are installed for usage-monitoring by PCRF, so AA reports that no rules apply (“0”).

```
*A:BNG-1>show>app-assure>group# aa-sub esm "alcatel_A_1" usage-monitor status
===============================================================================
Application-Assurance Subscriber "alcatel_A_1" (esm)
Usage Monitor Status
===============================================================================
Type             Name                              Oper Status
```

```
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
No. of rules: 0
===============================================================================
*A:BNG-1>show>app-assure>group#
```

The PCRF then sends a RAR message with a usage monitoring ADC rule for the BitTorrent application to set the usage thresholds for BitTorrent for the ESM subscriber “alcatel_A_1” to (in bytes):

Input (from sub)	1378168
Output (to sub)	1381148
Total traffic (up and down)	18446744073709551614

```
adc-rule-install (1092) V------- [96]
      vendor-id TGPP
      data [84] (Grouped)
         adc-rule-definition (1094) V------ [84]
           vendor-id TGPP
           data [72] (Grouped)
             adc-rule-name (1096) V------ [20]
               vendore-id TGPP
               data [8] (UTF8String) whatever
             tdf-application-id (1088) V------[22]
               vendor-id ALU
               data [10] (UTF8String) : BitTorrent
             monitoring-key (1066) V------ [25]
               vendor-id TGPP
               data [13] (UTF8String) : torrentmonkey
```

```
usage-monitoring-information (1067) V------- [80]
      vendor-id TGPP
      data [68] (Grouped)
        monitoring-key (1066) V------ [25]
          vendor-id TGPP
          data [13] (UTF8String) : torrentmonkey
        granted-service-units (431) ------- [24]
          data [16] (Grouped)
            cc-input-octets (412) ------ [16]
              data [8] (Unsigned64) : 1378168
            cc-output-octets (414) ------ [16]
              data [8] (Unsigned64) : 1378168
            cc-total-octets (421) ------ [16]
              data [8] (Unsigned64) : 18446744073709551614
        monitoring-key (1068) V------ [16]
          vendor-id TGPP
          data [4] (Enumerated) : 2 : ADC RULE LEVEL
```

al_0662

Figure 199: RAR Containing Usage Monitoring ADC Rules Example

This is then reflected on the AA-ISA:

```
*A:BNG-1>show>app-assure>group# aa-sub esm "alcatel_A_1" usage-monitor status
===============================================================================
Application-Assurance Subscriber "alcatel_A_1" (esm)
Usage Monitor Status
===============================================================================
Type             Name                            Oper Status
-------------------------------------------------------------------------------
application      BitTorrent                      active
-------------------------------------------------------------------------------
No. of rules: 1
===============================================================================
*A:BNG-1>show>app-assure>group#
```

Note the “active” oper status is set since there is at least one usage monitoring threshold associated with this application.

Given that there is no traffic flowing yet to or from the subscriber the counters currently are “0”:

```
*A:BNG-1>show>app-assure>group# aa-sub esm "alcatel_A_1" usage-monitor count
===============================================================================
Application-Assurance Subscriber "alcatel_A_1" (esm)
Usage Monitor Credit Statistics
===============================================================================
Application: "BitTorrent"
Direction     Status                    Granted                 Used     % Used
-------------------------------------------------------------------------------
to sub        valid                     1378168                    0         0%
from sub      valid                     1381148                    0         0%
both          valid        18446744073709551614                    0         0%
===============================================================================
*A:BNG-1>show>app-assure>group#
```

The status is set to “valid” since a threshold (or Grant) is received.

When, at a later stage, traffic starts flowing again usage-monitor subscriber statistics are updated as shown below.

```
*A:BNG-1>show>app-assure>group# aa-sub esm "alcatel_A_1" usage-monitor count
===============================================================================
Application-Assurance Subscriber "alcatel_A_1" (esm)
Usage Monitor Credit Statistics
===============================================================================
Application: "BitTorrent"
Direction     Status                    Granted                  Used     % Used
-------------------------------------------------------------------------------
to sub        valid                     1378168     137816         10%
from sub      valid                     1381148                 13781         1%
both          valid        18446744073709551614                151597         5%
===============================================================================
*A:BNG-1>show>app-assure>group#
```

The PCRF can also at the same time set ADC rules for other applications (such as the *0_rated* and the default_charging_group charging groups).

In the following case, the PCRF installs an ADC usage monitoring rule for:

- Charging group: “0-rated”, but without usage thresholds
- Charging group: “default_charge_group”, and sets only a threshold for “to sub” traffic.

This results in having a usage policy for the “0-rated” charging group installed but this is not active since there are no grants associated with it:

```
*A:BNG-1>show>app-assure>group# aa-sub esm "alcatel_A_1" usage-monitor status
===============================================================================
Application-Assurance Subscriber "alcatel_A_1" (esm)
Usage Monitor Status
===============================================================================
Type             Name                              Oper Status
-------------------------------------------------------------------------------
application      BitTorrent                        active
charging-group   0_rated                           inactive
charging-group   default_charge_group              active
-------------------------------------------------------------------------------
No. of rules: 3
===============================================================================
*A:BNG-1>show>app-assure>group#
```

Note that the “inactive” status for the “0-rated” charging group is due to no grants being received.

Moreover, detailed counters show:

```
*A:BNG-1>show>app-assure>group# aa-sub esm "alcatel_A_1" usage-monitor count
===============================================================================
Application-Assurance Subscriber "alcatel_A_1" (esm)
Usage Monitor Credit Statistics
===============================================================================
Application: "BitTorrent"
Direction     Status                    Granted                 Used     % Used
-------------------------------------------------------------------------------
to sub        valid                     1378168     137816        10%
from sub      valid                     1381148                 13781         1%
both          valid        18446744073709551614                151597         5%
-------------------------------------------------------------------------------
Charging-Group: "0_rated"
Direction     Status                    Granted                 Used     % Used
-------------------------------------------------------------------------------
to sub        invalid                       n/a                    0        n/a
from sub      invalid                       n/a                    0        n/a
both          invalid                       n/a                    0        n/a
-------------------------------------------------------------------------------
Charging-Group: "default_charge_group"
Direction     Status                    Granted                 Used     % Used
-------------------------------------------------------------------------------
to sub        valid                     1000000              1378084       100%
from sub      invalid                       n/a                 1574        n/a
```

```
both          invalid                       n/a              1379658        n/a
===============================================================================
*A:BNG-1>show>app-assure>group#
```

Again, the “invalid” status above reflects the fact that no grants have been received.

Conclusion

The introduction of the diameter (/Gx) control feature on the 7x50 BNG enables operators to consolidate policy management systems used in wire-line and wireless environments into a single system. This provides an increase in operational efficiency as mobile and fixed networks convergence gains more traction.

This example illustrates how policy control and usage monitoring of the 7x50 BNG Application Assurance services can be achieved over standard 3GPP Diameter Gx protocol.