ISG Prepaid

Overview

ISG Prepaid, a feature of the Cisco Intelligent Services Gateway (ISG), allows for the ISG to check the subscriber's available credit to determine whether to activate a specified service and how long the session can last. The subscriber's credit is administered by the CPS MsBM as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). Allocating quotas in fragments rather than providing all the credit at once enables ISG to support the use of credit for multiple simultaneous prepaid sessions.

The ISG uses the RADIUS protocol to facilitate interaction with CPS acting as the authentication, authorization, and accounting (AAA) server.

To obtain the first quota for a session, ISG submits an authorization request to the CPS, and CPS coordinates with the MsBM acting as the prepaid billing server, which forwards the quota values to ISG. ISG then monitors the session to track the quota usage. When the quota runs out or a specified limit is reached, ISG performs re-authorization. During re-authorization, the prepaid billing server may provide ISG with an additional quota if there is available credit. If no further quota is provided, ISG will log the user off from the service or perform some other specified action.

When a service is deactivated, the cumulative usage is provided to the prepaid billing server in an Accounting-Stop message.

Refer to the Cisco “Intelligent Services Gateway Configuration Guide” for further information on configuring ISG Prepaid on the ISG.

Plug-in Configuration

In order to install the plug-in, the following lines must be added to the following `/etc/broadhop/xx/features` files on the cluster manager:

```
iomanager0x/features file:
com.broadhop.isgprepaid.service.feature
pb/features file:
com.broadhop.client.feature.isg.prepaid
pcrf/features file
com.broadhop.isgprepaid.interface.feature
```

After modifying the features files, run **build_all.sh** and **reinit.sh** on the cluster manager to update the system.

Set the Accounting and Authorization ports to match the ports configured on the ISG. The standard ports are 1815 for Accounting and 1814 for Authorization. Check the **Enabled** boxes in order to enable the ISG Prepaid service.

Configuration Overview

The following Prepaid configuration assumes familiarity with the basic ISG service configuration. The ISG Prepaid configuration is similar to the standard ISG configuration, with the addition of an MsBM Account Balance to set the quota and the setup of parameters needed by the ISG (for example, the name of the ISG Prepaid configuration that is configured on the ISG).

Following is an example of the ISG Prepaid configuration on the ISG:

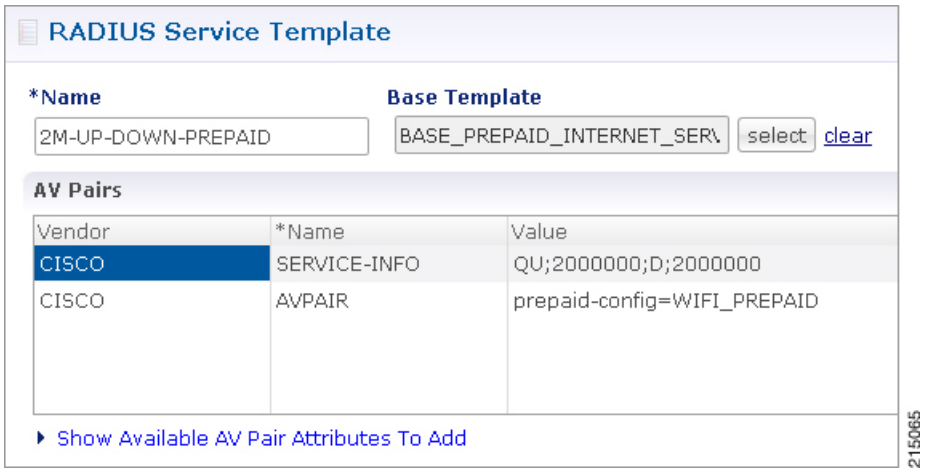
```
subscriber feature prepaid WIFI_PREPAID
threshold time 60 seconds
threshold volume 1000000 bytes
interim-interval 1 minutes
method-list author PREPAID_AUTHOR_LIST
method-list accounting PREPAID_ACCT_LIST
password cisco
```

Example - RADIUS Service Templates Configuration

The following RADIUS Service Templates must be configured as part of an ISG Prepaid Service. Just as in a standard ISG Service, the ISG Prepaid service templates below will be added to the final ISG Service to be used by the subscriber.

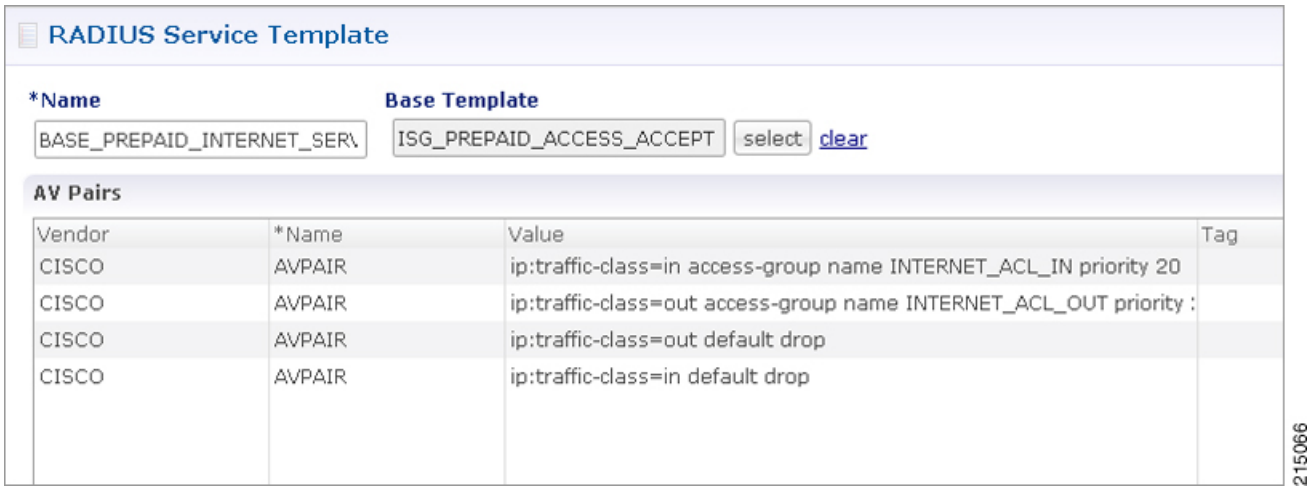
The below example 2M-UP-DOWN-PREPAID uses the BASE_PREPAID_INTERNET_SERVICE template, and is instructing the ISG to use a prepaid configuration called WIFI_PREPAID which must be defined on the ISG. Change the values to match your particular setup.

Figure 1: RADIUS Service Template



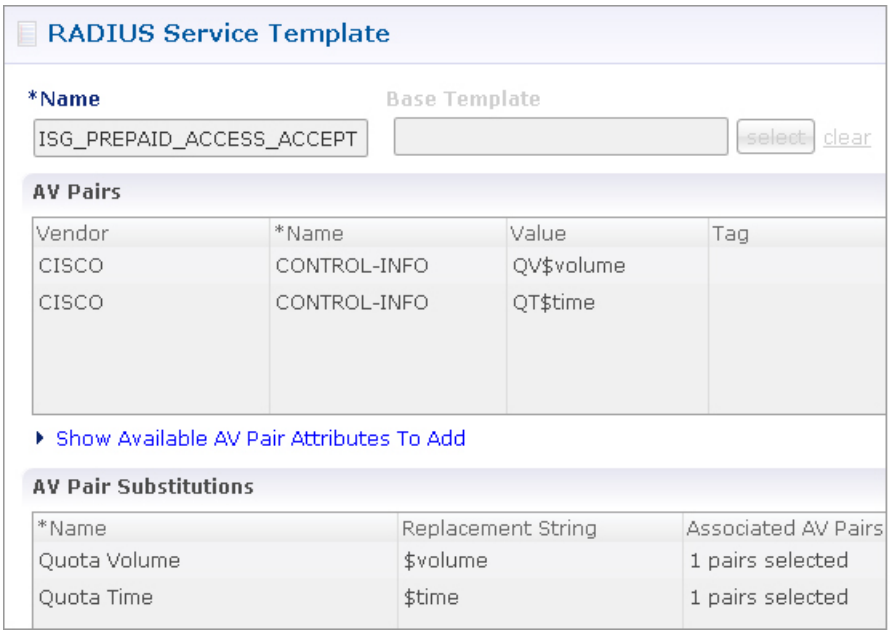
The BASE_PREPAID_INTERNET_SERVICE template below is based on the ISG_PREPAID_ACCESS_ACCEPT which is a read-only template provided with the system. The values should match what is configured on your ISG.

Figure 2: BASE_PREPAID_INTERNET_SERVICE



The ISG_PREPAID_ACCESS_ACCEPT passes CONTROL-INFO parameters to the ISG. If you are only passing time or volume, you can select a different template to use to only pass the values needed by the ISG.

Figure 3: ISG_PREPAID_ACCESS_ACCEPT



Use Case Configuration

Step 1 Open the Policy Builder GUI.

Step 2 Go to the **Services** tab.

Step 3 Under **Use Case Templates**, click **Summary** and then create a child use case template.

Step 4 Name the new template IsgPrepaid.

Step 5 In the newly created template, under the **Service Configurations** section, click **Add**. This lists all the service configuration objects available on the PCRF and then select the **IsgChargeConfiguration** object from the 'isgprepaid' section as shown below:

Figure 4: Select Service Configuration

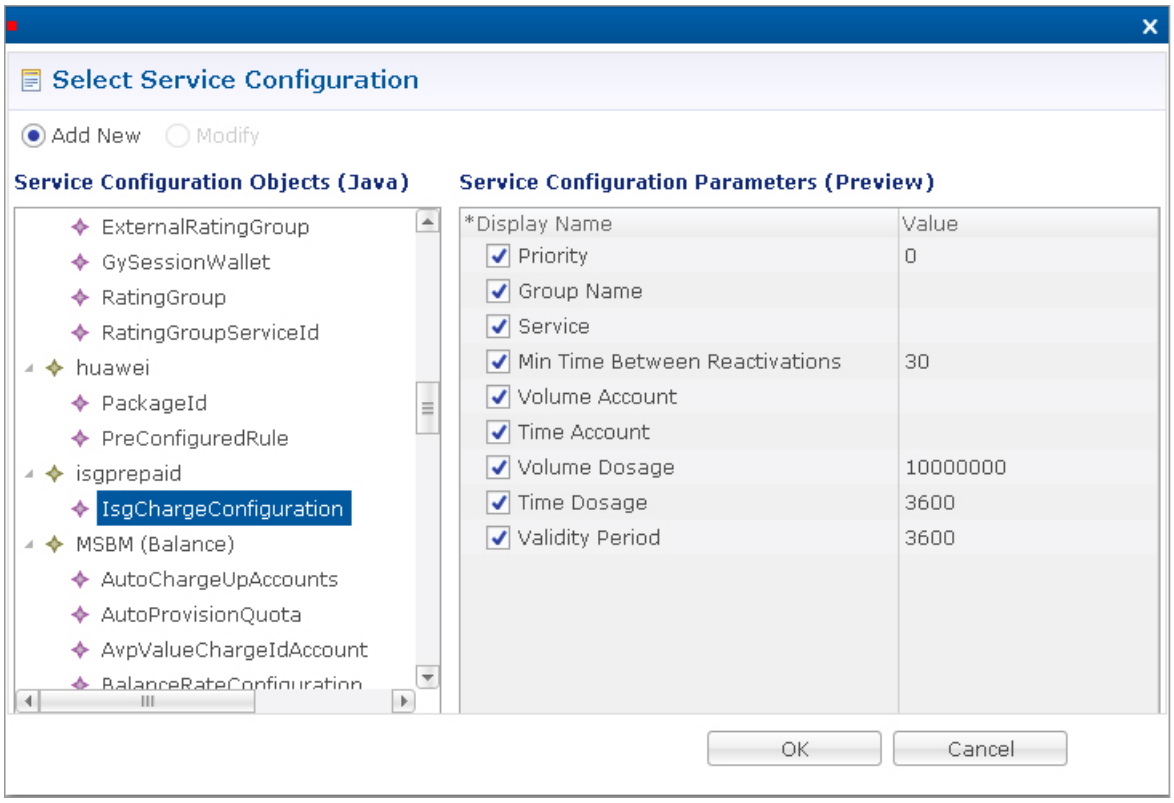
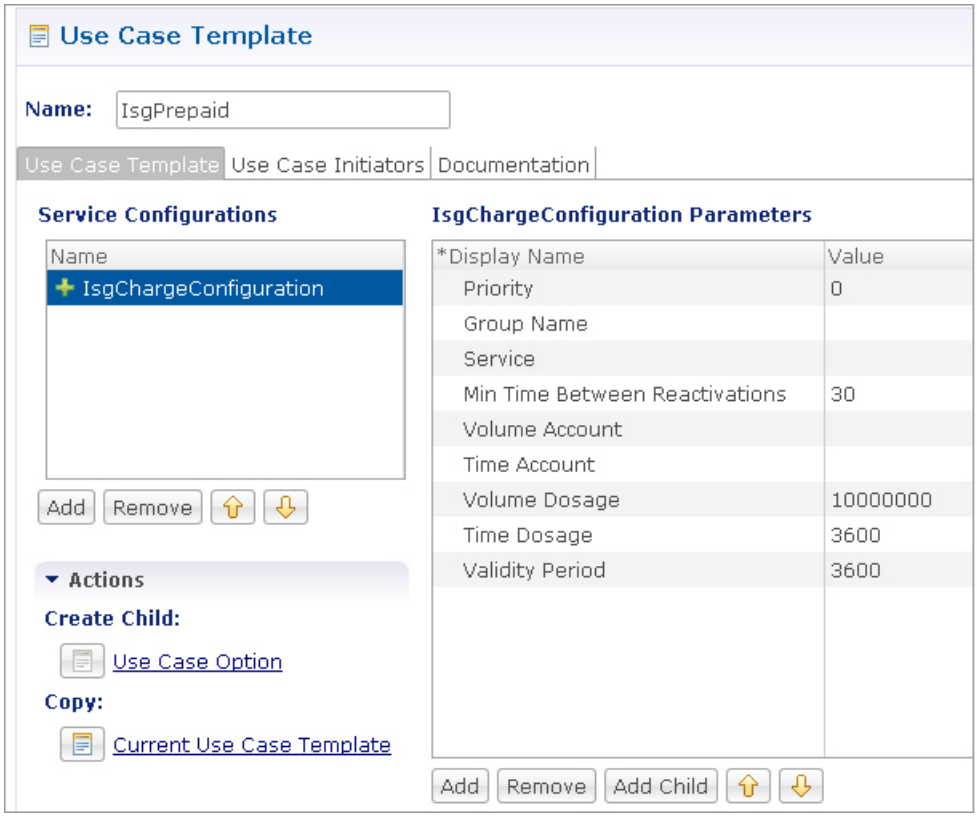


Figure 5: Use Case Template

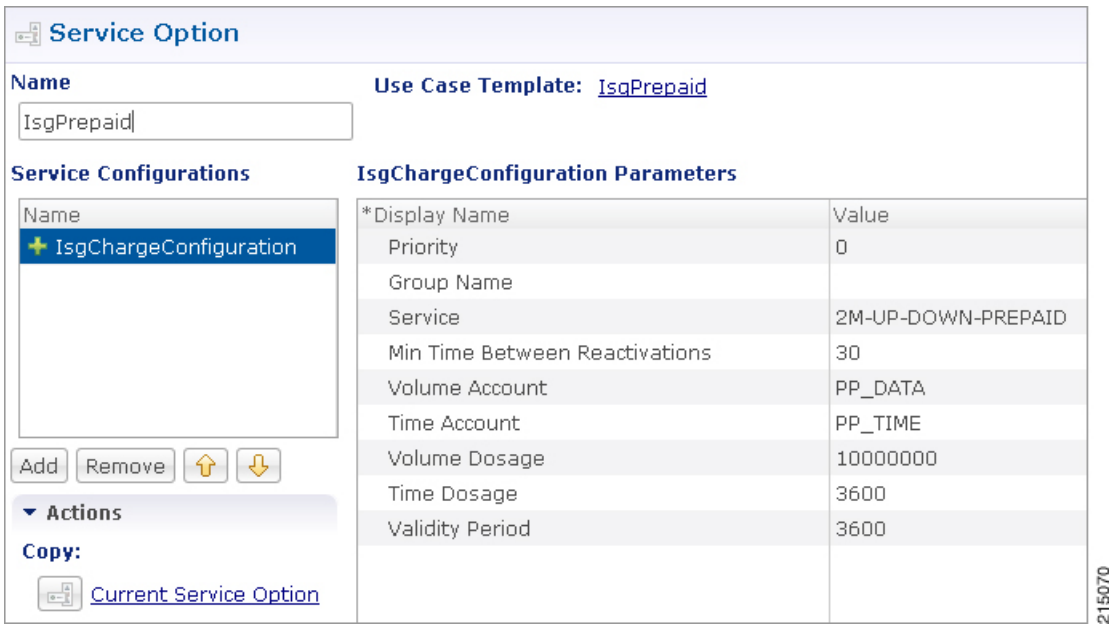


Step 6 Whenever a new Use Case Template is created, a corresponding empty Service Option container is created as well. Go to the **Services** section and then under **Service Options** find the **IsgPrepaid** folder, which represents the new ISG Prepaid Use Case Template created above. Create a child **Service Option** and name it IsgPrepaid.

Step 7 Below are the parameters that can be configured as part of the ISG Service Option. The actual values will vary depending on your particular setup.

Note Refer to Account Balance Templates for details on setting up an account balance.

Figure 6: Service Option

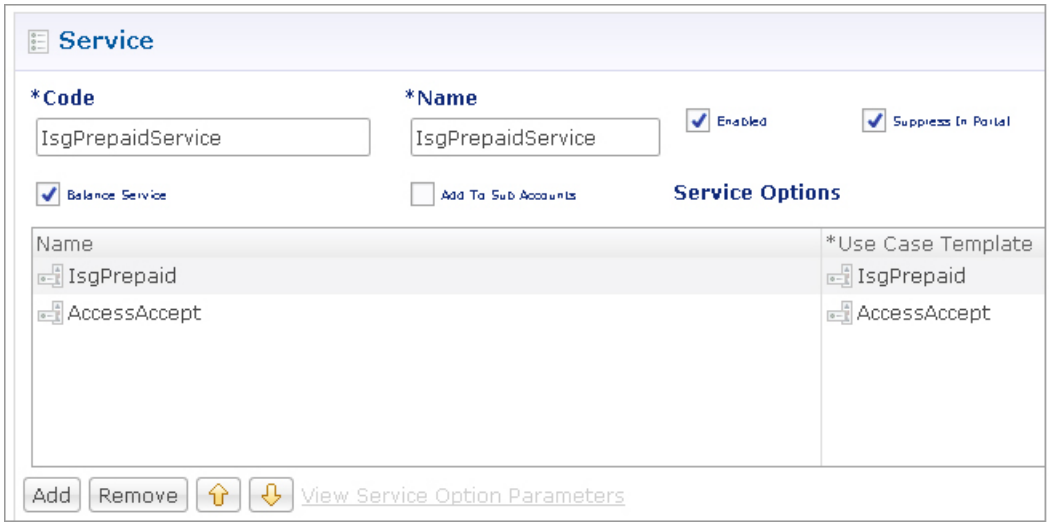


- **Service** is the ISG service defined above in the RADIUS Service Templates.
- The **Volume and Time Accounts** are the MsBM Account Balances used for the granted quota.
- **Volume and Time Dosages** are how much quota should be granted and consumed before the ISG should check back for status from the MsBM.
- **Validity Period** is the session timeout on the ISG.

Validation

Step 1 Create a new service that includes the IsgChargeConfiguration object along with an ISG Access Accept and optionally an Auto-Provision Quota. The quota can also be provisioned onto the customer account via the API or using the Control Center GUI.

Figure 7: Service



Step 2 Create a USuM Authorization domain to authorize a user account.

Step 3 Connect client to the ISG, log the client in so that the client is authorized on the ISG.

Step 4 After the client is authenticated and receives the 2M-UP-DOWN-PREPAID service, verify that the ISG sends an Access-Request on prepaid port 1814 to authenticate the user for the prepaid service.

```
*Apr 16 16:47:00.432: RADIUS(00000D93): Send Access-Request to 10.1.1.60:1814 id 1645/248, len 194
*Apr 16 16:47:00.432: RADIUS: authenticator 7C 4B 78 3A DE 2F 04 00 - 68 11 10 DE F3 00 4E F0
*Apr 16 16:47:00.432: RADIUS: User-Name           [1]   6   "test"
*Apr 16 16:47:00.432: RADIUS: User-Password       [2]   18  *
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  27
*Apr 16 16:47:00.432: RADIUS: ssg-service-info    [251] 21  "N2M-UP-DOWN-PREPAID"
*Apr 16 16:47:00.432: RADIUS: Framed-Protocol     [7]   6   PPP                       [1]
*Apr 16 16:47:00.432: RADIUS: Framed-IP-Address   [8]   6   192.168.11.7
*Apr 16 16:47:00.432: RADIUS: NAS-Port-Type       [61]  6   Virtual                   [5]
*Apr 16 16:47:00.432: RADIUS: NAS-Port            [5]   6   0
*Apr 16 16:47:00.432: RADIUS: NAS-Port-Id         [87]  9   "0/0/0/0"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  46
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair        [1]   40
"remote-id-tag=020a0000c0a80b0100000000"
*Apr 16 16:47:00.432: RADIUS: Service-Type        [6]   6   Framed [2]
*Apr 16 16:47:00.432: RADIUS: NAS-IP-Address      [4]   6   10.1.1.10
*Apr 16 16:47:00.432: RADIUS: Acct-Session-Id     [44]  10  "00000E40"
*Apr 16 16:47:00.432: RADIUS: Nas-Identifier      [32]  16  "csr1.cisco.com"
```

```
*Apr 16 16:47:00.432: RADIUS: Event-Timestamp     [55]  6   1397666820
```

The CPS will send a CoA message to log the prepaid user in:

```
SENT MESSAGES (synchronous - wait for response):

Sent:
com.broadhop.radius.actions.ICoARequest
SubstitutionValue: /synphaccountInfo 10.11.11.11:98
SubstitutionValue: /synphuserName test
SubstitutionValue: /synphuserPassword test
DestinationName:
CoaDeviceIp: 10.11.11.11
RadiusAvPairTemplateName: ISG_ACCOUNT_LOGIN
```

The ISG will send the CoA Ack and begin the Prepaid Accounting on port 1815:

```
*Apr 16 16:47:00.432: RADIUS(00000D93): Send CoA Ack Response to 10.1.1.60:53211 id 133, len 180
*Apr 16 16:47:00.432: RADIUS: authenticator 13 34 51 7E 42 77 4C 00 - F0 DA B2 C6 4F DA 81 4B
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  13
*Apr 16 16:47:00.432: RADIUS: ssg-command-code    [252] 7
*Apr 16 16:47:00.432: RADIUS: 01 74 65 73 74              [Account-Log-On test]
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  24
*Apr 16 16:47:00.432: RADIUS: ssg-account-info    [250] 18  "S10.11.11.11:210"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  25
*Apr 16 16:47:00.432: RADIUS: ssg-account-info    [250] 19  "/synphMA0050.56ab.2983"
*Apr 16 16:47:00.432: RADIUS: Idle-Timeout        [28]  6   600
*Apr 16 16:47:00.432: RADIUS: Session-Timeout     [27]  6   3600
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  27
*Apr 16 16:47:00.432: RADIUS: ssg-account-info    [250] 21  "A2M-UP-DOWN-PREPAID"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  37
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair        [1]   31  "accounting-list=QPS_ACCT_LIST"
*Apr 16 16:47:00.432: RADIUS: Session-Timeout     [27]  6   3600
*Apr 16 16:47:00.432: RADIUS: Calling-Station-Id  [31]  16  "0050.56ab.2983"
*Apr 16 16:47:00.432: RADIUS/ENCODE: Best Local IP-Address 10.1.1.10 for Radius-Server 10.1.1.60
*Apr 16 16:47:00.432: RADIUS(00000D93): Send Accounting-Request to 10.1.1.60:1815 id 1646/42, len
297
*Apr 16 16:47:00.432: RADIUS: authenticator 63 4E 5F 24 C0 1A DF 8E - 83 58 AE 4B BF 53 9C 8D
*Apr 16 16:47:00.432: RADIUS: Acct-Session-Id     [44]  10  "00000E40"
*Apr 16 16:47:00.432: RADIUS: Framed-Protocol     [7]   6   PPP                       [1]
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  27
*Apr 16 16:47:00.432: RADIUS: ssg-service-info    [251] 21  "N2M-UP-DOWN-PREPAID"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  34
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair        [1]   28  "parent-session-id=00000E3F"
*Apr 16 16:47:00.432: RADIUS: User-Name           [1]   6   "test"
*Apr 16 16:47:00.432: RADIUS: Acct-Status-Type    [40]  6   Start                     [1]
*Apr 16 16:47:00.432: RADIUS: Framed-IP-Address   [8]   6   192.168.11.7
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  25
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair        [1]   19  "portbundle=enable"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  24
*Apr 16 16:47:00.432: RADIUS: ssg-account-info    [250] 18  "S10.11.11.11:210"
*Apr 16 16:47:00.432: RADIUS: Calling-Station-Id  [31]  16  "0050.56ab.2983"
*Apr 16 16:47:00.432: RADIUS: NAS-Port-Type       [61]  6   Virtual                   [5]
*Apr 16 16:47:00.432: RADIUS: NAS-Port            [5]   6   0
```

```
*Apr 16 16:47:00.432: RADIUS: NAS-Port-Id         [87]  9   "0/0/0/0"
*Apr 16 16:47:00.432: RADIUS: Vendor, Cisco       [26]  46
*Apr 16 16:47:00.432: RADIUS: Cisco AVpair        [1]   40
"remote-id-tag=020a0000c0a80b0100000000"
*Apr 16 16:47:00.432: RADIUS: Service-Type        [6]   6   Framed                    [2]
*Apr 16 16:47:00.432: RADIUS: NAS-IP-Address      [4]   6   10.1.1.10
*Apr 16 16:47:00.432: RADIUS: home-hl-prefix      [151] 10  "1577E053"
*Apr 16 16:47:00.432: RADIUS: Event-Timestamp     [55]  6   1397666820
*Apr 16 16:47:00.432: RADIUS: Nas-Identifier      [32]  16  "csr1.cisco.com"
*Apr 16 16:47:00.432: RADIUS: Acct-Delay-Time     [41]  6   0
```

Verify prepaid accounting messages are being passed on ISG Prepaid accounting port 1815 and that quota is being debited from the CPS MsBM. Taking the tcpdump on ports 1814, 1815 and 1700 and analyzing the results in Wireshark can help verify proper transaction flow:

```
tcpdump -i any port 1700 or 1814 or 1815 -s0 -w pp.pcap
```