Use Case Scenarios

First Published: December 5, 2006
Revised: December 23, 2006,

This chapter provides examples of use case scenarios which you can use to observe typical system behaviors and RADIUS interactions for various conditions. In the first use case, debugs for all RADIUS messages are shown. In the other use cases, all message flows are listed but only RADIUS debugs of interest are shown.

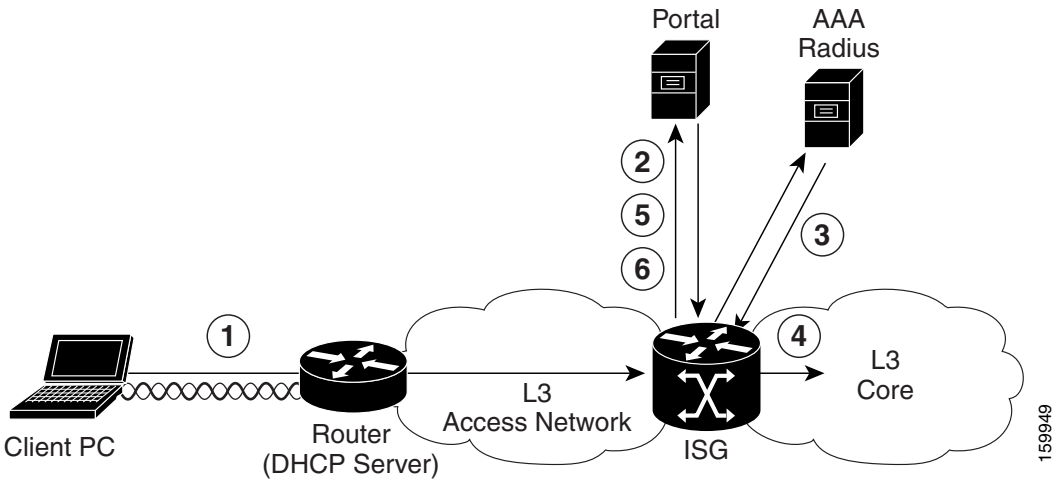
This chapter includes the following topics:

Case 1: Portal Login

This use case is typical of public access control as used in PWLAN applications. In this scenario, an IP subscriber obtains an IP address and is then routed to ISG over a L3 access network. The ISG redirects the subscriber to a portal for authentication and then activate services as per the subscriber profile stored in RADIUS. An architecture as shown in Figure 1 is assumed. In this example, each numbered item matches the numbers inFigure 1 :

1. A user session is created upon detection of a new IP source address. Some default services are applied.
2. ISG redirects the user to a portal. The user enters his username and password and the user credentials are sent to ISG.
3. The user is authenticated at AAA server and his user profile is retrieved from RADIUS which dictates what features and service are applied to the newly created session.
4. The user has now access to the network.
5. Some time later, the user returns to the portal and modifies his service to obtain more bandwidth. New policing parameters are pushed from the portal via CoA.
6. Some time later, the user disconnects from the portal and the session is terminated.

Figure 1 Portal Login Routing Diagram



ISG Configuration

The ISG access interface is configured as "routed" and to identify new session based on a new IP address as shown in the following example:

```
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip address 10.1.1.1 255.255.255.0
  service-policy type control RULE_IP_SESSION1
  ip subscriber routed
     initiator unclassified ip-address
```

The ISG Control Policy for this use case is shown in the following example:

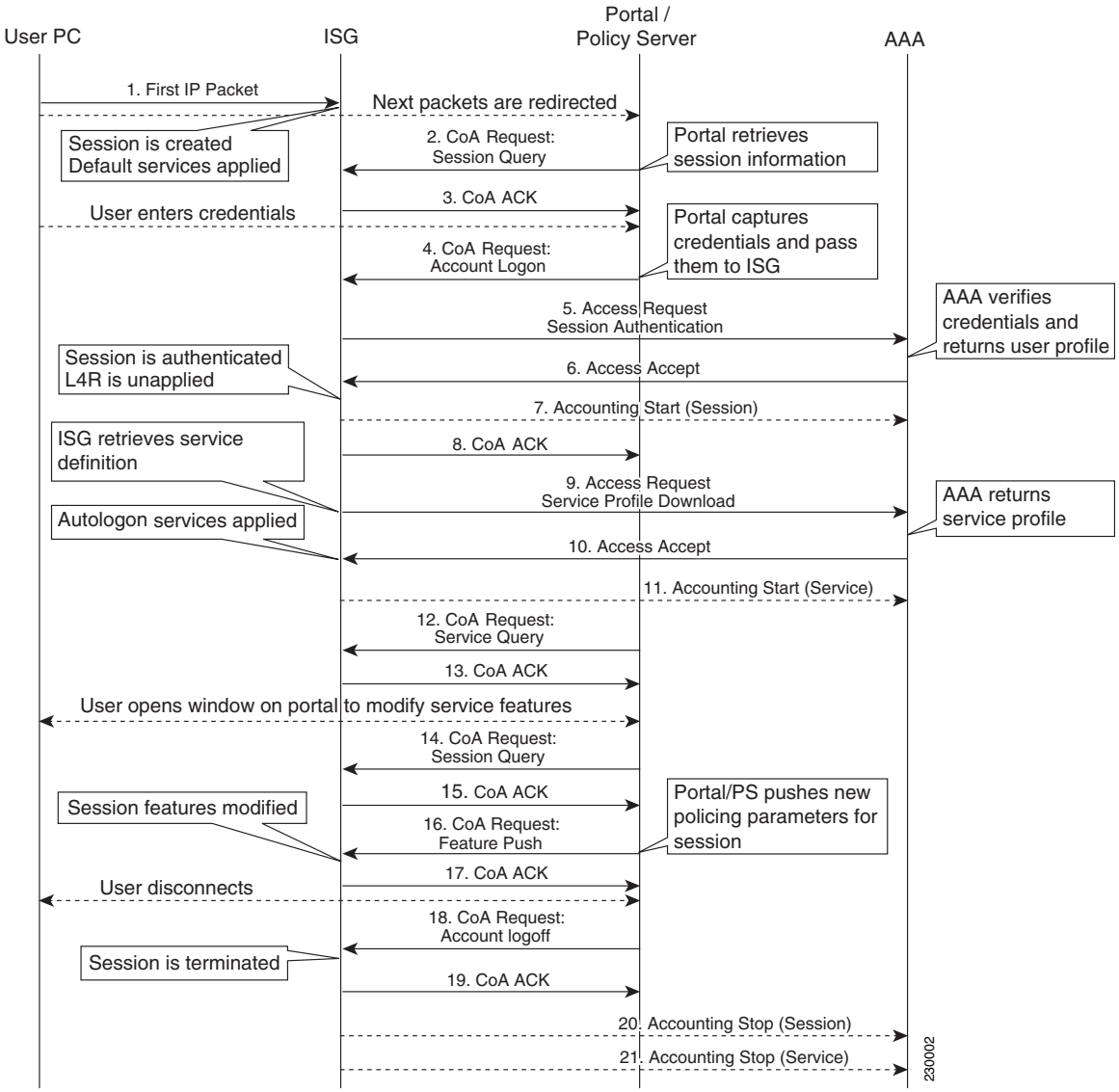
```
policy-map type control RULE_IP_SESSION1
 class type control IP_UNAUTH_COND event timed-policy-expiry
  1 service disconnect
 !
 class type control always event session-start
  10 service-policy type service name PBHK_SERVICE
  20 service-policy type service name L4REDIRECT_SERVICE
  30 service-policy type service name OPENGARDEN_SERVICE
  40 set-timer IP_UNAUTH_TIMER 10
 !

 class type control always event account-logon
  10 authenticate aaa list WEB_LOGON
  20 service-policy type service unapply name L4REDIRECT_SERVICE
 !
!
```

Case 1: Call Flow

Figure 2 shows the sequence diagram for Use Case 1. See Case 1: Details for more information on each numbered item.

Figure 2 Sequence Diagram for Use Case



Case 1: Details

Each numbered item below matches the numbers in Figure 2

1. ISG interface is configured to identify individual IP addresses as new session:

```
ip subscriber routed
identifier unclassified ip-address
```

On a new session start, ISG is configured to apply default services (in this case PBHK, L4-redirect and Open_Garden). These services can be defined locally on ISG (as assumed in this use case) or could be defined on an external AAA server.

```
class type control always event session-start
10  service-policy type service name PBHK_SERVICE
20  service-policy type service name L4REDIRECT_SERVICE
30  service-policy type service name OPEN_GARDEN_SERVICE
```

2. Portal request session information via a CoA Session Query. It uses using the PBHK identifier as the session identifier.

```
RADIUS: COA  received from id 4 192.168.1.100:32777, CoA Request, len 54
COA: 192.168.1.100 request queued
RADIUS:  authenticator 8C 21 98 CF BF 15 D8 61 - EA A9 2C C5 2D C6 AF BF
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"          PBHK identifier

RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-command-code   [252] 5
RADIUS:   04 20 26               [Account-Ping  &]
```

3. ISG replies with CoA ACK. Information of interest includes the client's IP addresses as well as the session's state (in this case "unautenticated").

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 4, len 118
RADIUS:  authenticator 04 18 EA 0B A4 77 37 32 - 56 60 F7 31 CD 26 86 01
RADIUS:  Vendor, Cisco       [26]  10
RADIUS:   ssg-command-code   [252] 4
RADIUS:   04 30                 [Account-Ping 0]    "0" means session is not
authenticated
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"        PBHK identifier
RADIUS:  Vendor, Cisco       [26]  22
RADIUS:   Cisco AVpair       [1]   16  "sg-version=1.0"
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  31  "nas-port:10.10.10.11:0/0/1/70"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2             Client's IP address
```

4. PS issues CoA Account Logon that includes user's username/password. ISG is configured to authenticate session on this event. Note that the second action to remove the redirect service is only executed if authentication is successful.

```
class type control always event account-logon
   10 authenticate aaa list IP_AUTHEN_LIST
   20 service-policy type service unapply name L4REDIRECT_SERVICE

RADIUS: COA  received from id 5 192.168.1.100:32777, CoA Request, len 84
COA: 192.168.1.100 request queued
RADIUS:  authenticator BF 62 14 C1 6F DE 76 61 - 84 D8 D5 01 14 F8 52 80
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-command-code   [252] 9
```

```
RADIUS:   01 49 50 5F 55 43 31            [Account-Log-On IP_UC1]
```

5. ISG issues an Accept Request to authenticate the session at AAA, it includes the client's username and password.

```
Send Access-Request to 192.168.1.100:1812 id 1645/16, len 115
RADIUS:  authenticator F4 2C 9B 48 FF 83 A7 5A - 0F 5C 83 FE 5C E8 DE C0
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Login                     [1]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Event-Timestamp     [55]  6   1159320597
```

6. Upon successful credential verification, AAA responds with Access Accept which includes the user profile listing the services to be activated. Since the authentication was successful, the L4-redirect service is unapplied (action 20 of session's control policy).

```
RADIUS: Received from id 1645/16 192.168.1.100:1812, Access-Accept, len 193
RADIUS:  authenticator CA E9 E3 20 57 05 06 01 - AD FF F7 86 07 43 33 73
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-account-info   [250] 23  "AINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-account-info   [250] 19  "NCOA_BOD_1Meg_UC1"
RADIUS:  Idle-Timeout        [28]  6   300
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   ssg-account-info   [250] 34  "QU;512000;256000;D;512000;256000"
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "subscriber:accounting-list=BH_ACCNT_LIST1"
```

7. ISG signals the session start by sending an accounting message to the accounting server.

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/203, len
180
RADIUS:  authenticator 23 80 8E 14 C7 0F 00 BD - 05 3E 5D 73 D9 84 D3 6A
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Acct-Status-Type    [40]  6   Start                     [1]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43          [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320597
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

8. ISG responds to PS with CoA ACK to signal successful account logon and includes subscriber information and subscriber services information.

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 5, len 220
RADIUS:  authenticator C2 9C AB 02 5F 97 DA 2F - E3 B1 F6 E0 4D 7B 9A 77
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-command-code   [252] 9
RADIUS:   01 49 50 5F 55 43 31            [Account-Log-On IP_UC1]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-account-info   [250] 23  "AINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-account-info   [250] 19  "NCOA_BOD_1Meg_UC1"
RADIUS:  Idle-Timeout        [28]  6   300
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   ssg-account-info   [250] 34  "QU;512000;256000;D;512000;256000"
RADIUS:  Vendor, Cisco       [26]  38
RADIUS:   Cisco AVpair       [1]   32  "accounting-list=BH_ACCNT_LIST1"
```

9. Assuming that services to be activated for session are not already cached on ISG, ISG sends Access Request to AAA to download service definition.

```
RADIUS(00000027): Send Access-Request to 192.168.1.100:1812 id 1645/17, len 117
RADIUS:  authenticator 6F 50 DA 86 D4 77 5A B1 - 2E 7E 18 AD 68 2B 6F B8
RADIUS:  User-Name           [1]   22  "INTERNET_SERVICE_UC1"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Outbound                  [5]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Event-Timestamp     [55]  6   1159320597
```

10. Server responds with the service definition (service profile) and ISG applies service(s) to the session.

```
RADIUS: Received from id 1645/17 192.168.1.100:1812, Access-Accept, len 312
RADIUS:  authenticator 28 44 E2 8C DC 5B 8B 3B - 8B 5F 0F 2F 7C D4 4C 71
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   Cisco AVpair       [1]   34  "ip:traffic-class=in default drop"
RADIUS:  Vendor, Cisco       [26]  49
RADIUS:   Cisco AVpair       [1]   43  "subscriber:accounting-list=BH_ACCNT_LIST1"
RADIUS:  Vendor, Cisco       [26]  80
RADIUS:   Cisco AVpair       [1]   74  "ip:traffic-class=input access-group name
ACL_IN_INTERNET_UC1 priority 30"
RADIUS:  Vendor, Cisco       [26]  82
RADIUS:   Cisco AVpair       [1]   76  "ip:traffic-class=output access-group name
ACL_OUT_INTERNET_UC1 priority 30"
RADIUS:  Vendor, Cisco       [26]  41
RADIUS:   Cisco AVpair       [1]   35  "ip:traffic-class=out default drop"
```

11. ISG signals service start by sending accounting message for BASIC_INTERNET_SERVICE_UC1. The accounting-ID for the service is tied to the session via the parent-session-id attribute.

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/204, len
205
RADIUS:  authenticator D3 EE 5E 20 AB D1 9A 2A - A8 7B C4 12 BA 78 29 39
RADIUS:  Acct-Session-Id     [44]  10  "00000033"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
```

```
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "NINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "parent-session-id=00000032"
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Acct-Status-Type    [40]  6   Start                    [1]
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                  [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                   [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43          [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320597
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

12. Portal/PS queries ISG to determine if the Auto-logon service was successfully activated using a "CoA Session Query for Service Status".

```
RADIUS: COA  received from id 8 192.168.1.100:32777, CoA Request, len 72
COA: 192.168.1.100 request queued
RADIUS:  authenticator B6 C5 2C D4 AB CB 3E CD - 9D 91 E9 7D 45 B8 AF 88
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-command-code   [252] 23
RADIUS:   04 49 4E 54 45 52 4E 45 54 5F 53 45 52 56 49 43 45  [INTERNET_SERVICE]
RADIUS:   5F 55 43 31              [Account-Ping _UC1]
```

13. ISG returns session's service info to Portal/PS.

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 8, len 151
RADIUS:  authenticator 67 44 50 B7 D6 89 4A 0A - 23 C9 4E 3A E1 5F A6 4C
RADIUS:  Vendor, Cisco       [26]  39
RADIUS:   ssg-account-info   [250] 33  "N1INTERNET_SERVICE_UC1;6;IP_UC1"
RADIUS:  Vendor, Cisco       [26]  10
RADIUS:   ssg-command-code   [252] 4
RADIUS:   04 31                 [Account-Ping 1]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  22
RADIUS:   Cisco AVpair       [1]   16  "sg-version=1.0"
RADIUS:  NAS-Port-Id         [87]  31  "nas-port:10.10.10.11:0/0/1/70"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
```

14. When user opens new window at portal, Portal/PS may require session information and uses CoA Account Query to get information.

```
RADIUS: COA  received from id 10 192.168.1.100:32777, CoA Request, len 54
COA: 192.168.1.100 request queued
RADIUS:  authenticator F6 CD 8A 1A 2E 99 B2 B6 - 98 1A 81 70 C2 F5 15 42
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  11
RADIUS:   ssg-command-code   [252] 5
RADIUS:   04 20 26                [Account-Ping  &]
```

15. ISG responds with session and service information.

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 10, len 444
RADIUS:  authenticator E7 64 D2 F5 96 E0 76 2D - D1 AD ED 79 F7 2E 99 C9
```

```
RADIUS:  Vendor, Cisco       [26]  60
RADIUS:   ssg-account-info   [250] 54
"N1OPENGARDEN_SERVICE;277;IP_UC1;139;179;24236;213422"
RADIUS:  Vendor, Cisco       [26]  48
RADIUS:   ssg-account-info   [250] 42  "N1INTERNET_SERVICE_UC1;96;IP_UC1;0;0;0;0"
RADIUS:  Vendor, Cisco       [26]  54
RADIUS:   ssg-account-info   [250] 48
"N1PBHK_SERVICE;277;IP_UC1;139;179;24236;213422"
RADIUS:  Vendor, Cisco       [26]  10
RADIUS:   ssg-command-code   [252] 4
RADIUS:   04 31                 [Account-Ping 1]
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-account-info   [250] 23  "AINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  25
RADIUS:   ssg-account-info   [250] 19  "NCOA_BOD_1Meg_UC1"
RADIUS:  Idle-Timeout        [28]  6   300
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   ssg-account-info   [250] 34  "QU;512000;256000;D;512000;256000"
RADIUS:  Vendor, Cisco       [26]  38
RADIUS:   Cisco AVpair       [1]   32  "accounting-list=BH_ACCNT_LIST1"
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  22
RADIUS:   Cisco AVpair       [1]   16  "sg-version=1.0"
RADIUS:  NAS-Port-Id         [87]  31  "nas-port:10.10.10.11:0/0/1/70"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
```

16. User modifies service features from Portal. PS issues a CoA Feature Push to modify features, in this case the policing rate went to 1024K and idle timeout is changed to 2000 seconds.

```
RADIUS: COA  received from id 16 192.168.1.100:32777, CoA Request, len 77
COA: 192.168.1.100 request queued
RADIUS:  authenticator C4 14 F5 2F FF BE 68 4D - 60 8E AA 49 7D AA 2C 4F
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  28
RADIUS:   ssg-service-info   [251] 22  "QU;1024000;D;1024000"
RADIUS:  Idle-Timeout        [28]  6   2000
```

17. ISG acknowledge that feature(s) were modified.

```
RADIUS(00000000): Send CoA Ack Response to 192.168.1.100:32777 id 16, len 26
RADIUS:  authenticator 53 5E 5D 13 AF 1A 1C 53 - 75 CD FF 3B C9 01 D5 4C
RADIUS:  Dynamic-Author-Error[101] 6   Success
```

18. User disconnects (logs off) from Portal. Portal/PS sends a CoA Request : Account Logoff to terminate the session.

```
RADIUS: COA  received from id 18 192.168.1.100:32777, CoA Request, len 58
COA: 192.168.1.100 request queued
RADIUS:  authenticator 5B 9E A9 CA EA 1A C2 AC - 1B 4A 89 40 E2 ED E9 F2
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  Vendor, Cisco       [26]  15
RADIUS:   ssg-command-code   [252] 9
RADIUS:   02 49 50 5F 55 43 31            [Account-Log-Off IP_UC1]
```

19. ISG responds with CoA ACK.

```
RADIUS(00000027): Send CoA Ack Response to 192.168.1.100:32777 id 18, len 52
```

```
RADIUS:  authenticator D2 D8 A2 19 19 FD E6 C3 - BA 9D 70 5D 58 F6 0A 85
RADIUS:  Vendor, Cisco       [26]  9
RADIUS:   ssg-command-code   [252] 3
RADIUS:   02
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
```

20. ISG signals that the session is terminated using Accounting Stop.

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/205, len
251
RADIUS:  authenticator 90 CB DD 33 73 11 0A 24 - A3 22 F1 08 83 E5 40 9A
RADIUS:  Acct-Session-Id     [44]  10  "00000032"
RADIUS:  Framed-IP-Address   [8]   6   10.10.14.2
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Acct-Authentic      [45]  6   RADIUS                    [1]
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "connect-progress=Call Up"
RADIUS:  Acct-Session-Time   [46]  6   197
RADIUS:  Acct-Input-Octets   [42]  6   88902
RADIUS:  Acct-Output-Octets  [43]  6   752244
RADIUS:  Acct-Input-Packets  [47]  6   476
RADIUS:  Acct-Output-Packets [48]  6   621
RADIUS:  Acct-Terminate-Cause[49]  6   user-request              [1]
RADIUS:  Vendor, Cisco       [26]  35
RADIUS:   Cisco AVpair       [1]   29  "disc-cause-ext=TS User Exit"
RADIUS:  Acct-Status-Type    [40]  6   Stop                      [2]
RADIUS:  Vendor, Cisco       [26]  23
RADIUS:   ssg-account-info   [250] 17  "S10.10.10.11:85"
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43          [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320794
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

21. ISG signals that the service is terminated using Accounting Stop.

```
RADIUS(00000027): Send Accounting-Request to 192.168.1.100:1813 id 1646/206, len
247
RADIUS:  authenticator 6E 86 93 CD 6A 60 D8 43 - 57 2F B6 9B 84 98 87 AA
RADIUS:  Acct-Session-Id     [44]  10  "00000033"
RADIUS:  Framed-Protocol     [7]   6   PPP                       [1]
RADIUS:  Vendor, Cisco       [26]  29
RADIUS:   ssg-service-info   [251] 23  "NINTERNET_SERVICE_UC1"
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "parent-session-id=00000032"
RADIUS:  User-Name           [1]   8   "IP_UC1"
RADIUS:  Acct-Input-Packets  [47]  6   46
RADIUS:  Acct-Output-Packets [48]  6   59
RADIUS:  Acct-Input-Octets   [42]  6   9764
RADIUS:  Acct-Output-Octets  [43]  6   12622
RADIUS:  Acct-Session-Time   [46]  6   197
RADIUS:  Acct-Terminate-Cause[49]  6   user-request              [1]
RADIUS:  Vendor, Cisco       [26]  35
RADIUS:   Cisco AVpair       [1]   29  "disc-cause-ext=TS User Exit"
RADIUS:  Acct-Status-Type    [40]  6   Stop                      [2]
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  NAS-Port-Id         [87]  10  "0/0/1/70"
RADIUS:  Service-Type        [6]   6   Framed                    [2]
```

```
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Unsupported         [151] 10
RADIUS:   42 44 42 39 32 42 45 43          [ BDB92BEC]
RADIUS:  Event-Timestamp     [55]  6   1159320794
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Acct-Delay-Time     [41]  6   0
```

Case 2: Transparent Auto-Logon

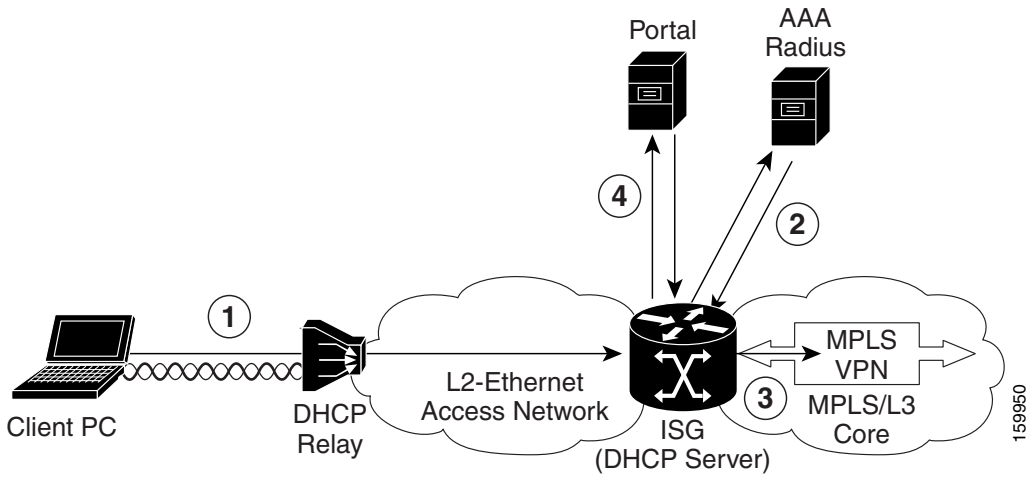
The Transparent Auto-Logon (TAL) capability allows the delivery of "always-on access to services". This means the session is authorized based on network identifiers and no subscriber authentication is required to gain access.

This use case is typical of broadband residential access where many IP sessions are aggregated on a single VLAN at the BRAS. To achieve a service similar to PPP, service providers would identify the end users based on location information that is popoulated by the DSLAM in the DHCP Option-82 field.

Figure 3 shows the architecture used for this use case. In this example, each numbered item below matches the numbers inFigure 3 :

1. A user session is created upon detection of new DHCP interaction (ISG is DHCP Server or Relay). An assumption is that a downstream switch or DSLAM populates DHCP Option-82 with the subscriber's physical location
2. The user is authorized at AAA server based on his MAC address + DHCP Option 82 info. The AAA server authorizes the user and returns the user profile listing the features and services to be applied to the session . One of the service is a primary service that includes a vrf-id and DHCP class to make sure an IP address routable through the VRF is assigned.
3. The user can access his services through through the MPLS VPN.
4. Some time later, the user accesses the portal and subscribes to a “turbo-button” type service where the bandwidth is increased.Still later, the user accesses the portal and de-activates “turbo-button” type service to return to normal service.

Figure 3 Transparent Auto-Logon Routing Diagram



ISG Configuration

This section has the following topics:

Interface Configuration

An example of the Interface Configuration is shown below:

```
!!! Interface Configuration

interface GigabitEthernet0/1.22
 encapsulation dot1Q 22
 ip address 10.3.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_IP_SESSION2a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
```

Control Policy Configuration

An example of the Control Policy Configuration is shown below:

```
!!! Control Policy Configuration

policy-map type control RULE_IP_SESSION2a
 class type control IP_UNAUTH_COND event timed-policy-expiry
  10 service disconnect
 !
 class type control BOD1M_CLASS event service-start
  10 service-policy type service unapply name DEFAULT_BW_512K_UC2
  20 service-policy type service identifier service-name
 !
 class type control BOD1M_CLASS event service-stop
  10 service-policy type service unapply identifier service-name
  20 service-policy type service name DEFAULT_BW_512K_UC2
 !
 class type control always event session-start
  10 service-policy type service name PBHK_SERVICE
  20 service-policy type service name OPENGARDEN_SERVICE2
  30 authorize aaa list AUTHOR_LIST1 password cisco123 identifier remote-id plus
circuit-id plus mac-address
  40 service-policy type service name L4REDIRECT_SERVICE2
  50 set-timer IP_UNAUTH_TIMER 5
 !
 class type control always event account-logon
  10 authenticate aaa list AUTHEN_LIST1
  20 service-policy type service unapply name L4REDIRECT_SERVICE2
 !
!
```

Policy Control Class-Map

An example of the Policy Control Class-Map configuration is shown below:

```
!!! Policy Control class-map

class-map type control match-all BOD1M_CLASS
 match service-name BOD1M_SERVICE_UC2
!
class-map type control match-all IP_UNAUTH_COND
 match timer IP_UNAUTH_TIMER
 match authen-status unauthenticated
!
```

DHCP Pools

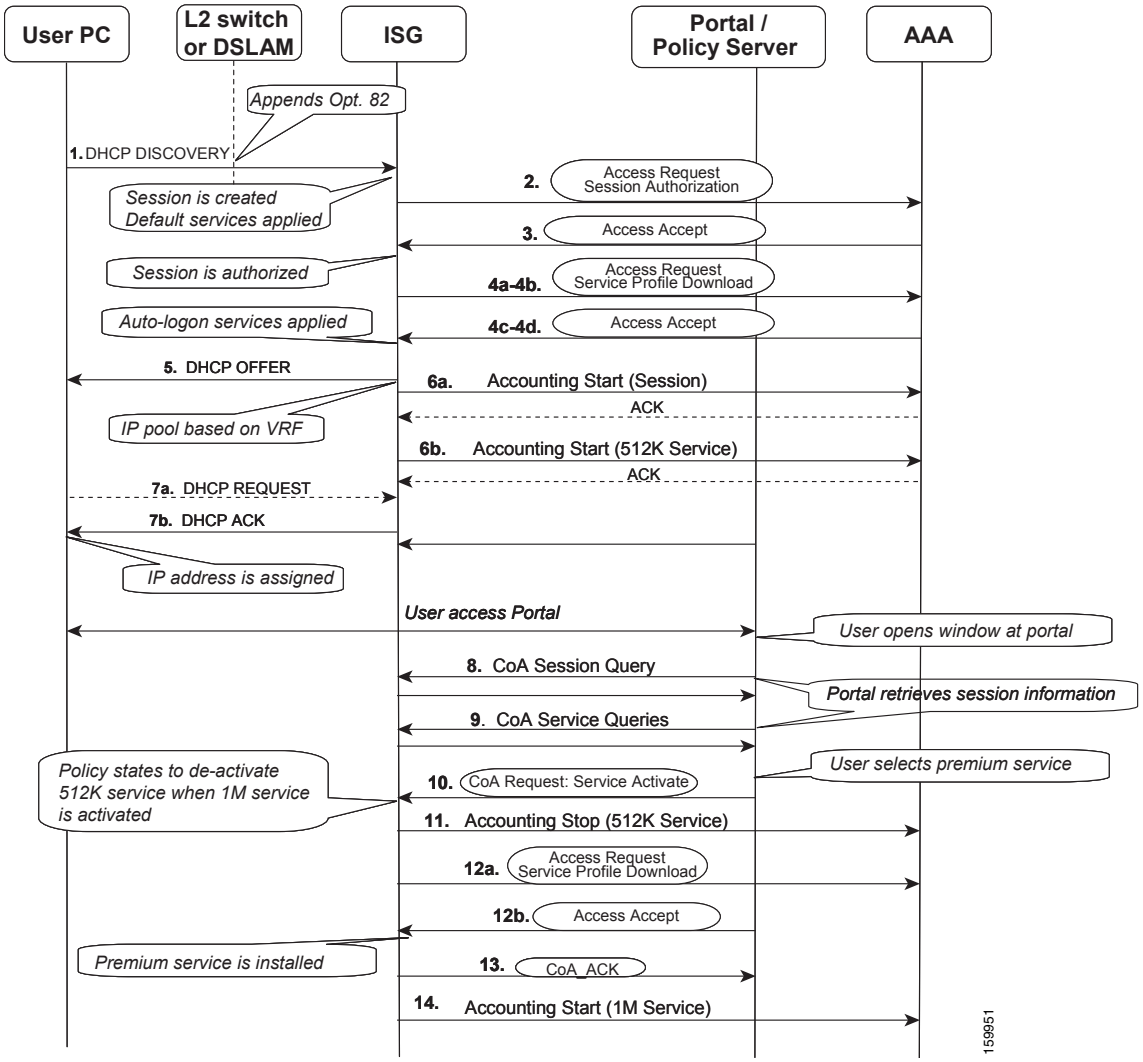
An example of the DHCP Pools configuration is shown below:

```
!!! DHCP POOLS..
ip dhcp excluded-address 10.3.10.1
ip dhcp excluded-address 10.3.11.1
!
ip dhcp pool VPN_UC2_POOL1
   vrf VPN_ISP1
   network 10.3.11.0 255.255.255.0
   default-router 10.3.11.1
   domain-name isgtest.com
   class CLASS1
!
ip dhcp pool DHCP_POOL1
   network 10.3.10.0 255.255.255.0
   default-router 10.3.10.1
   lease 0 0 30
   class default
!
ip dhcp class CLASS1
Ip dhcp class default
!
```

Case 2: Call Flow

Figure 4 shows the sequence diagram for Use Case 2. See Case 2: Details for more information on each numbered item.

Figure 4 Sequence Diagram for Use Case 2



Case 2: Details

Each numbered item corresponds to the numbers in Figure 4.

1. A DHCP DISCOVERY message is initiated by the subscriber. An assumption is made that an intermediate device (DSLAM or switch) populates DHCP Option-82 information to identify the subscriber's physical location. The ISG interface is configured to start a new session on DHCP control traffic.

   On the new session, ISG is configured to apply default services (in this case PBHK) and authorize session based on MAC address and DHCP Option-82 info.

2. ISG issues an Accept Request to authorize the session at AAA. The Accept Request includes the MAC address and option-82 information as username and uses the password defined in the policy. In this example, "cisco" is used.

```
Send Access-Request to 192.168.1.100:1812 id 1645/149, len 244
RADIUS:  authenticator A8 6C 11 8C C3 60 7F 67 - 21 C1 07 89 ED 12 2B E9
RADIUS:  User-Name           [1]   47  "0|6|000d.edc0.3f80:0|4|22|1|15:0050.5607.0103"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port-Type       [61]  6   Virtual                   [5]
RADIUS:  Vendor, Cisco       [26]  34
RADIUS:   Cisco AVpair       [1]   28  "circuit-id-tag=0|4|22|1|15"
RADIUS:  Vendor, Cisco       [26]  40
RADIUS:   Cisco AVpair       [1]   34  "remote-id-tag=0|6|000d.edc0.3f80"
RADIUS:  NAS-Port            [5]   6   0
RADIUS:  NAS-Port-Id         [87]  32  "0|6|000d.edc0.3f80:0|4|22|1|15"
RADIUS:  Service-Type        [6]   6   Outbound                  [5]
RADIUS:  NAS-IP-Address      [4]   6   10.10.10.11
RADIUS:  Acct-Session-Id     [44]  10  "00000381"
RADIUS:  Nas-Identifier      [32]  13  "c7301-d19-2"
RADIUS:  Event-Timestamp     [55]  6   1159560540
```

3. Upon successful identity verification, AAA responds with Access Accept which includes the user profile and services to be activated. In this example, "DEFAULT_BW_512K_UC2" and "VPN1_UC2" are used.

```
Received from id 1645/149 192.168.1.100:1812, Access-Accept, len 173
RADIUS:  authenticator AF 6C 9C AB 5A D4 F2 E3 - A4 25 BD 89 96 8F 17 93
RADIUS:  Vendor, Cisco       [26]  28
RADIUS:   ssg-account-info   [250] 22  "ADEFAULT_BW_512K_UC2"
RADIUS:  Vendor, Cisco       [26]  17
RADIUS:   ssg-account-info   [250] 11  "AVPN1_UC2"
RADIUS:  Reply-Message       [18]  16
RADIUS:   57 65 6C 63 6F 6D 65 20 54 6F 20 49 53 47    [ Welcome To ISG]
RADIUS:  Vendor, Cisco       [26]  26
RADIUS:   ssg-account-info   [250] 20  "NBOD1M_SERVICE_UC2"
RADIUS:  Session-Timeout     [27]  6   180000
RADIUS:  User-Name           [1]   47   "
0|6|000d.edc0.3f80:0|4|22|1|15:0050.5607.0103 "
RADIUS:  Idle-Timeout        [28]  6   600
RADIUS:  Vendor, Cisco       [26]  46
RADIUS:   Cisco AVpair       [1]   40  "subscriber:accounting-list=ACCNT_LIST1"
```

4. **4a-4b**. Since the services are not cached on ISG, ISG needs to retrieve them from AAA.

   4c-4d. Both services' definitions are retrieved and the services are applied. This example is the service definitions as they appear on the AAA server.

```
Service Name = "VPN1_UC2"
 CiscoAVPair: ip:vrf-id=VPN_ISP1
 CiscoAVPair: subscriber:classname=CLASS1
```

```
 CiscoAVPair: subscriber:sg-service-type=primary

Service Name = "DEFAULT_BW_512K_UC2"
 CiscoAVPair: ip:traffic-class=output access-group name ACL_OUT_DEFAULT_BW priority 50
 SERVICE INFO: QU;512000;256000;D;512000;256000
 CiscoAVPair: subscriber:accounting-list=ACCNT_LIST1
 CiscoAVPair: ip:traffic-class=input access-group name ACL_IN_DEFAULT_BW priority 50
```

5. ISG offers an IP address, based on the DHCP class, that is routable within the customer-assigned VRF.
6. **6a-6b**. An Accounting Request is sent to signal the user session start and another to signal the service start.
7. **7a-7b**. The user request, the offered address, and the address are handed out by ISG.
8. **8a-9b**. Some time later, an assumption is made that the user signs on to the portal. The Portal/PS issues one or more CoA Request:Account Query to obtain subscriber information and service status. ISG responds to the Portal/PS with a CoA ACK that includes subscriber information and subscriber service information.
9. **9a-9b**. These steps handle service queries similar to those in the previous steps.
10. Assuming that the user selects a new service "BOD1M_SERVICE_UC2", the Portal/PS issues a CoA Request:Service Activate message that includes a new service name.

```
RADIUS: COA  received from id 131 192.168.1.100:32777, CoA Request, len 70
Sep 29 20:14:08.456: COA: 192.168.1.100 request queued
Sep 29 20:14:08.456: RADIUS:  authenticator 12 01 8B 5A 1E 69 13 18 - 05 C2 AC 26 EE
00 E2 3B
Sep 29 20:14:08.456: RADIUS:  Vendor, Cisco       [26]  24
Sep 29 20:14:08.456: RADIUS:   ssg-account-info   [250] 18  "S10.10.10.11:110"
Sep 29 20:14:08.456: RADIUS:  Vendor, Cisco       [26]  26
Sep 29 20:14:08.456: RADIUS:   ssg-command-code   [252] 20
RADIUS:   0B 42 4F 44 31 4D 5F 53 45 52 56 49 43 45 5F 55 43  [BOD1M_SERVICE_UC]
RADIUS:   32                [Service-Log-On 2]
```

11. The control policy specifies to disconnect the 512K service if the 1M service is activated. Disconnecting the 512K service triggers the ISG to send an Accounting Request to signal a service stop for the 512K service.
12. **12a-12b**. Since an assumption is made that the 1M service definition is not already cached on ISG, ISG needs to retrieve the 1M service definition from AAA. Below is an example of what the service definition looks like at the AAA.

```
Service Name = "BOD1M_SERVICE_UC2"
CiscoAVPair: ip:traffic-class=in default drop
CiscoAVPair: ip:traffic-class=output access-group name ACL_OUT_BOD1M priority 30
SERVICE INFO: QU;1024000;512000;D;1024000;512000
CiscoAVPair: ip:traffic-class=input access-group name ACL_IN_BOD1M priority 30
CiscoAVPair: subscriber:accounting-list=ACCNT_LIST1
CiscoAVPair: ip:traffic-class=out default drop
```

13. ISG acknowledges that 1M service was installed.
14. ISG sends an Accounting Request to signal that 1M service has started.

Case 3: Service Authentication

In this use case, service authentication is required at an application server before user can access this service. When the service profile is retrieved by ISG, it is identified (within a policy directive VSA) that additional authentication is required at a specified server. In that case, the username and password retrieved within the user profile is used for logging onto the service. Figure 5 shows the sequence diagram for Service Authentication.

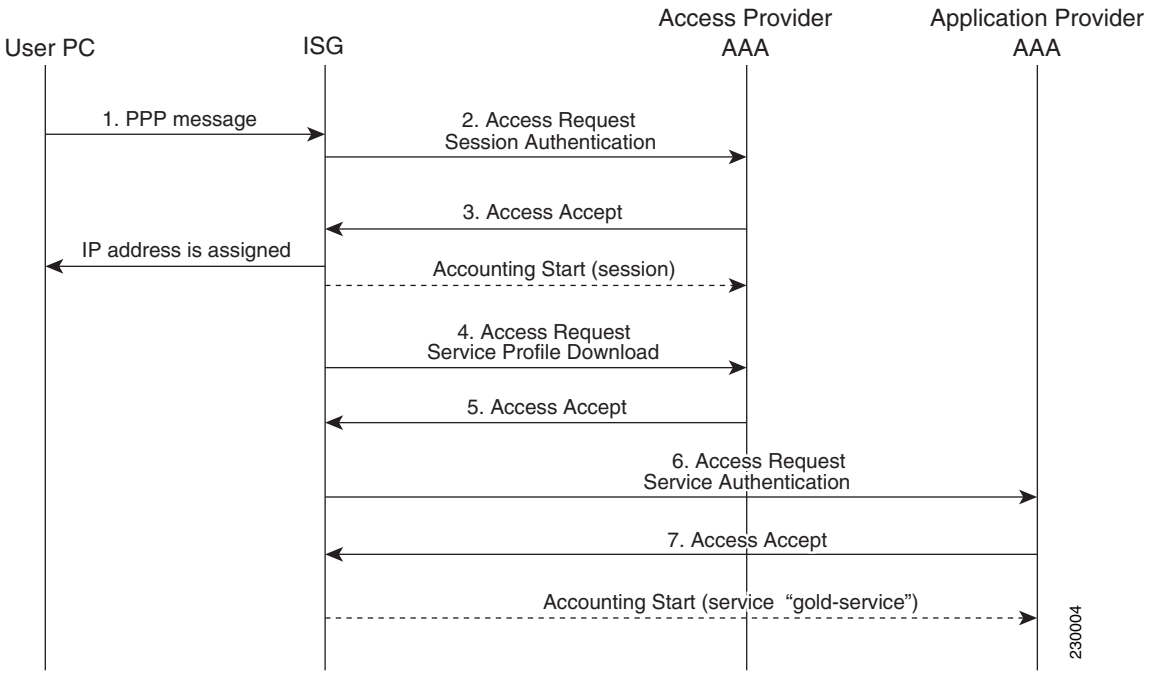
In this example:

- A PPP user session is created upon detection of PPP control traffic.
- The user is authorized at AAA server.
- User profile contains autologon service that requires authentication.
- ISG authenticates service before granting access.

Case 3: Detailed Call Flow

Figure 5 shows the sequence diagram for Use Case 2. See Case 3 Details: for more information on each numbered item.

Figure 5 Service Authentication Sequence Diagram



Case 3 Details:

Each numbered item corresponds to the numbers in Figure 5.

1. A PPP control message is initiated by the subscriber. For PPP sessions, the ISG interface does not need to be configured because PPP sessions are created automatically. In this use case, an assumption is made that sessions require authentication. This authentication is enabled using the command:

   ```
   ppp authentication chap PPP_LIST
   ```

2. ISG issues an Accept Request to authenticate the session at the access provider AAA which includes the user's username and password
3. Upon successful identity verification, AAA responds with Access Accept which includes the user profile and service to be activated (in this case “goldservice”). The service name VSA with the user profile will contain an additional username and password, for example:

   ```
   "Agoldservice;myusername;mypassword"
   ```

4. Assuming that service “goldservice” is not already cached on ISG, ISG send Access Request to AAA to download service definition.
5. The server responds with service definition. Within the service definition, there is a policy-directive VSA that indicates that further authentication is required at a specific application server.

   ```
   “policy-directive=authenticate aaa list auth-list”
   ```

6. ISG initiates an Access-Request to specified server for Service Authentication
7. Upon successful credential verification, application server responds with Access-Accept and user can access his service