WiFi Aggregation and Offload – Migrant User Support

In This Chapter

This section provides information about WiFi aggregation and offload for migrant user support configurations.

Topics in this section include:

Applicability

This example is applicable to all 7750 SR platforms supporting WLAN gateway (WLAN-GW) IOMs (IOM3-XP and 2xISAs). It provides a functional description of “migrant user” handling on 7750 WLAN-GW and the corresponding configuration. It assumes the user is aware of the general operations and configuration of the basic WLAN-GW function as already described in the 7750 SR OS Triple Play guide.

The configuration with migrant user support enabled was tested on release 11.0R4.

Overview

The term “Migrant user” refers to user equipment (UEs) that connects to a WiFi network service set identification (SSID) but moves out of the range of the access point before initiating or completing authentication. For open-SSIDs, a migrant user may stay in the range of the access point just long enough to get a DHCP lease from the WLAN-GW. In actual WiFi deployments with portal authentication, it has been observed that a large percentage of users are migrant such that they get a DHCP lease but do not initiate or complete authentication.

Prior to this feature, an Enhanced Subscriber Management (ESM) host is created when the DHCP process completes. This results in the consumption of resources on both the CPM and IOM, limiting the ESM scale and performance for fully authenticated active users. This feature adds support to create an ESM host only after a user has been fully authenticated, either via a web portal or with an AAA server based on completing EAP exchange. In addition, with this feature L2-aware NAPT is required, such that each UE gets the same shared configured inside IP address from the ISA via DHCP. Until a user is authenticated, forwarding of user traffic is constrained (via policy) to DNS and portal server access only.

Each user is allocated a small number of configured NAT outside ports to minimize public IP address consumption for unauthenticated users. Once the user is successfully authenticated, as indicated via a RADIUS Change of Authorization (COA) on successful portal authentication, an ESM host is created, and the L2-aware NAT is applied via a normal per-subscriber NAT policy. The inside IP address of the user does not change. The outside IP pool used is as per the NAT policy, and the L2-aware NAT could be 1:1 or NAPT with larger number of outside ports than in the un-authenticated phase. If a user is already pre-authenticated (for example if the RADIUS server remembers the MAC address of the UE from a previous successful portal authentication) then the initial access-accept from RADIUS will trigger the creation of the ESM host.

Migrant User Support for Open SSID Based on Portal Authentication

Sequence Of Events

1. DHCP Is Received From UE On ISA

   Based on the DHCP and L2-aware NAT configuration on the ISA, an IP address is assigned to the user via DHCP. The DHCP and L2-aware NAT configuration is under the soft-gre node under the group-interface, or under vlan-tag range under the soft-gre node on the group-interface.

   A different DHCP lease-time can be configured for an un-authenticated user (initial-lease-time) and an authenticated user (active-lease-time) for which an ESM host has been created. It is suggested that the initial lease be configured to a smaller value while the UE is migrant so that resources can be reclaimed quickly for a truly migrant user that will not complete authentication.

   In addition to lease-times, DHCP return options, for example primary and secondary DNS and NBNS server addresses, that can be configured. This configuration can be per soft-GRE group interface or per VLAN range (where a VLAN tag corresponds to an SSID).

   Up to 512 bytes of received DHCP options from clients are stored on the ISA. Once the DHCP ACK is sent back to the UE from the ISA, the UE will be created on the ISA in “migrant (or unauthenticated) state”.

   A configured L2-aware IP address is returned to each UE and a temporary L2-aware host is created on the anchor ISA for the UE. The NAT policy applicable to this L2-aware NAT for UE in migrant state is also configured under the group-interface (under soft-gre node or under vlan-tag range).

   ARP requests coming from the UE in migrant state will be responded to from the ISA. The authentication to RADIUS is triggered on receiving the first Layer 3 data packet as opposed to on a DHCP DISCOVER.

2. Layer 3 Data Packet Received on the ISA

   The first Layer 3 packet (other than DHCP) will trigger RADIUS authentication from the ISA based on configured **isa-radius-policy** in the **configure>aaa** context. The user-name in the access-request is as per the user-name-format configured in the isa-radius-policy. By default it is the MAC address of the UE. The isa-radius-policy can be configured as the authentication policy under the soft-gre group-interface, or under specific VLAN tag ranges on the soft-gre group-interface. The latter allows for the use of a different authentication policy per SSID.

   The RADIUS packets from the ISA are sourced with the IP address owned by the ISA. Each ISA in the WLAN-GW group gets an IP address from a set of contiguous addresses, the start of which is configurable in isa-radius-policy. The nas-ip-address sent in access-request message is configurable in the isa-radius-policy as the ISA's local IP address or the system IP address. In case the RADIUS server is behind a load-balancer which updates the source IP address of the RADIUS messages, the RADIUS server may use nas-ip-address to route the RADIUS response back. In this case the nas-ip-address should be configured as the ISA's IP address otherwise the response would incorrectly be routed to the CPM instead of the ISA.

The debug output below shows a RADIUS accept-request being sent to the RADIUS server on reception of first Layer 3 packet. The debug can be enabled by issuing:

```
   debug router "management" radius packet-type authentication | accounting | coa

253 2013/08/07 20:58:35.53 UTC MINOR: DEBUG #2001 Base WLAN-GW
"WLAN-GW: MDA 2/1, SeqNo 11830
   Info:     anchor egressing frame
             radius-auth-req

   IP/UDP:   from 192.168.0.2:1142 to 192.0.2.3:1812

RADIUS:   Access-Request (continued)
"

254 2013/08/07 20:58:35.53 UTC MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Transmit
  Access-Request(1) 192.168.0.2:1142 id 40 len 158 vrid 1
    NAS IP ADDRESS [4] 4 192.0.2.3
    NAS PORT TYPE [61] 4 Virtual(5)
    NAS PORT ID [87] 43 GRE rtr-3#lip-192.168.0.1#rip-192.0.2.1
    USER NAME [1] 17 00:0a:0a:00:01:00
    PASSWORD [2] 16 rCmhFboYeM2M8hOuBYJXJk
    CALLING STATION ID [31] 17 00:0a:0a:00:01:00
    VSA [26] 19 Alcatel(6527)
      CHADDR [27] 17 00:0a:0a:00:01:00
"
```

Received Layer 3 packets from the UE are handled as per the redirect-policy configured under the soft-gre group-interface or under applicable VLAN tag range on the soft-gre interface.

The redirect-policy is an IP ACL that should contain one more "forward rules" for traffic that should be forwarded while the UE is pending portal authentication. This typically should include traffic to and from DNS and web portal and is subjected to temporary L2-aware NAT. The redirect-policy also specifies the URL for redirecting triggered by http packets. The redirect-policy and/or the redirect URL can also be overridden via the RADIUS access-accept. Any other non-http traffic that does not match the forward rules is dropped.

While a UE is pending portal authentication no accounting messages are sent to the AAA server. Disconnect-Message from AAA server is supported while the UE is pending authentication.

3. Access-accept from RADIUS

   The access-accept is received on the ISA from which the access-request was generated. The initial access-accept from RADIUS can indicate if a user needs to be authenticated by the portal or is a pre-authenticated user. The indication is based on inclusion of a “redirect policy” applicable to the user in a vendor specific attribute (VSA) (Alc-Wlan-Portal-Redirect, type = string) received from the RADIUS server. The access-accept can also include a redirect URL VSA (Alc-Wlan-Portal-Url, type = string) for the user. An empty Alc-Wlan-Portal_redirect VSA forces the use of the redirect policy that is locally specified under the soft-gre interface or under vlan-tag ranges on soft-gre interface. The redirect-policy is created under sub-mgmt node.

   The UE state is changed to “portal” to indicate the UE is pending portal authentication and has limited access.

   The debug below shows the RADIUS accept-request being received from the RADIUS server and being processed by the WLAN-GW.

```
255 2013/08/07 20:58:35.61 UTC MINOR: DEBUG #2001 Base WLAN-GW
"WLAN-GW: MDA 2/1, SeqNo 11831
   Info:     anchor ingressing frame
             portal auth-accept

   IP/UDP:   from 192.0.2.3:1812 to 192.168.0.2:1142

RADIUS:   Access-Accept (continued)
"

256 2013/08/07 20:58:35.62 UTC MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Receive
  Access-Accept(2) id 40 len 64 from 192.0.2.3:1812 vrid 1
    VSA [26] 14 Alcatel(6527)
      SUBSC ID STR [11] 12 migrant_user
    VSA [26] 18 Alcatel(6527)
      WLAN PORTAL REDIRECT [172] 16 redirect-policy-1
"
```

The following command is used to display UE information on the ISA, including the state of the UE and the GRE tunnel to the AP through which the UE is connected.

```
*A:PE-1# tools dump wlan-gw ue
===============================================================================
Matched 1 session on Slot #2 MDA #1
===============================================================================
UE-Mac          : 00:0a:0a:00:01:00     UE-vlan         : N/A
UE IP Addr      : 10.0.0.10             Description     : Portal
UE timeout      : 288 sec               Auth-time       : 08/07/13 20:58:35
Tunnel MDA      : 2/2                   Tunnel Router   : 10
MPLS label      : 3000                  Shaper          : Default
GRE Src IP Addr : 192.0.2.2             GRE Dst IP Addr : 192.168.0.1
Anchor SAP      : 2/1/nat-out-ip:2049.1
Last-forward    : None                  Last-move       : None
Rx Frames       : 0                     Rx Octets       : 0
Tx Frames       : 0                     Tx Octets       : 0
```

```
-------------------------------------------------------------------------------
===============================================================================
No sessions on Slot #2 MDA #2 match the query
```

If neither of the two redirect related VSAs are included in access-accept, then this indicates a “pre-authenticated user”, and an ESM host is created for the subscriber with a subscriber-profile and other subscriber configuration from access-accept; from here normal ESM based forwarding occurs for the subscriber.

If a user is determined as a “pre-authenticated user”, a message is generated to the CPM to create an ESM host. The information received from RADIUS in the access-accept message (for example subscriber-profile, app-profile etc) and the information from DHCP (for example the DHCP options) are passed in this message.

4. COA from RADIUS

When user’s credentials entered on the portal are successfully verified, the portal triggers the AAA server to generate COA to WLAN-GW. The COA serves as a trigger to create an ESM host. The COA MUST contain the subscriber-id and user-name, which are used as a key to identify the UE pending portal authentication.

The following shows an example debug of a COA being received from the AAA server.

```
248 2013/08/07 19:12:38.29 UTC MINOR: DEBUG #2001 Base RADIUS
"RADIUS: Transmit
  Change of Authorization(43) 192.0.2.3:36776 id 124 len 96 vrid 1
    VSA [26] 19 Alcatel(6527)
      SUBSC ID STR [11] 17 00:0a:0a:00:01:00
    USER NAME [1] 17 00:0a:0a:00:01:00
    VSA [26] 10 Alcatel(6527)
      SLA PROF STR [13] 8 sla-profile-1
    VSA [26] 10 Alcatel(6527)
      SUBSC PROF STR [12] 8 sub-profile-1
"
```

When the COA is received and successfully processed, a COA-ACK is sent back to the AAA server. The COA message is passed to the CPM to create an ESM host. The information received in the COA, as well as stored information from DHCP (for example the DHCP options) are passed in this message. Once the ESM host is successfully created, the state of the UE on the ISA is changed accordingly to “ESM-user“, and can be seen in the output of **tools dump WLAN-GW UE** command, as shown below.

The UE now has full access (and is not restricted by the original redirect-policy). The COA provides a reference to a subscriber profile that contains the NAT policy for an authenticated UE. The UE continues to keep the same inside L2-aware IP address that was provided originally via DHCP on the ISA. However, the NAT for an authenticated user could be an L2-aware 1:1 NAT or NAPT with a different outside pool and outside ports than the UE in migrant state. The ESM host that is created as described above will also result in the creation of a normal L2-aware host. The original temporary L2-aware host is retained for 10 seconds (and then deleted) to ensure the http response from the portal can be successfully routed back to the UE on the existing connection.

```
 A:PE-1# tools dump wlan-gw ue
===============================================================================
Matched 1 session on Slot #2 MDA #1
===============================================================================
UE-Mac          : 00:0a:0a:00:01:00     UE-vlan         : N/A
UE IP Addr      : N/A                   Description     : ESM-user
UE timeout      : N/A                   Auth-time       : 08/07/13 19:12:38
Tunnel MDA      : 2/2                   Tunnel Router   : 10
MPLS label      : 3000                  Shaper          : 1
GRE Src IP Addr : 192.0.2.2             GRE Dst IP Addr : 192.168.0.1
Anchor SAP      : 2/1/nat-out-ip:2049.1
Last-forward    : 08/07/13 19:12:25     Last-move       : None
Rx Frames       : 1                     Rx Octets       : 88
Tx Frames       : 1                     Tx Octets       : 222
-------------------------------------------------------------------------------
===============================================================================
No sessions on Slot #2 MDA #2 match the query
```

If UE goes out of range such that the idle timeout expires, the ESM host is deleted and an accounting-stop is sent to the AAA server. If a UE then comes back, and still has a valid DHCP lease, it may not send DHCP DISCOVER or REQUEST and continue to send data. The **data-triggered-ue-creation** command can be configured under soft-gre node on the group-interface (or under vlan-tag ranges on the group-interface) to trigger authentication and recreation of the ESM host for this UE.

The overall sequence of events to take a UE from migrant to authenticated state, where the forwarding of UE traffic is not restricted, is shown in Figure 412.

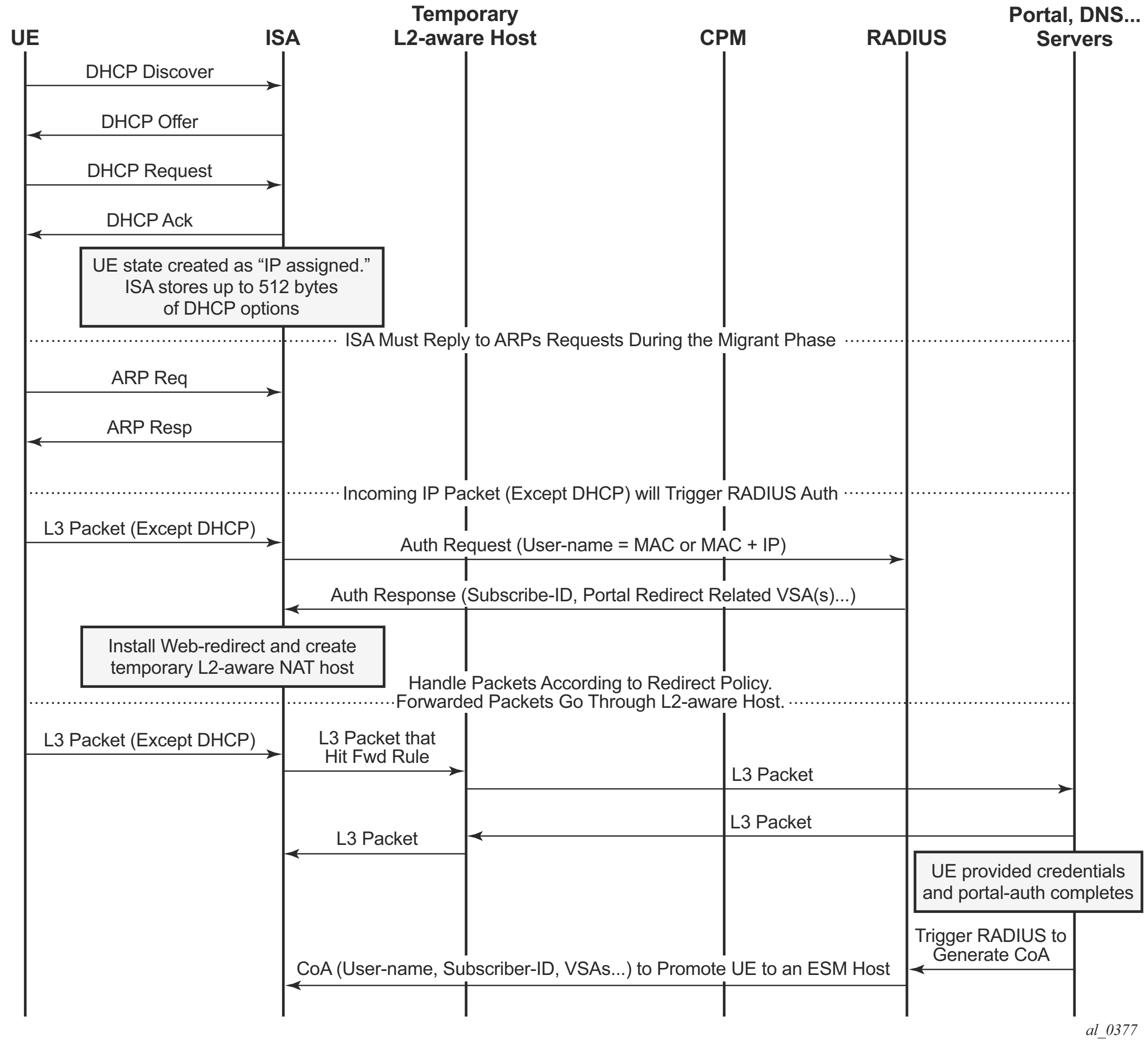
UE
ISA
Temporary L2-aware Host
CPM
RADIUS
Portal, DNS... Servers
DHCP Discover
DHCP Offer
DHCP Request
DHCP Ack
UE state created as "IP assigned." ISA stores up to 512 bytes of DHCP options
ISA Must Reply to ARPs Requests During the Migrant Phase
ARP Req
ARP Resp
Incoming IP Packet (Except DHCP) will Trigger RADIUS Auth
L3 Packet (Except DHCP)
Auth Request (User-name = MAC or MAC + IP)
Auth Response (Subscribe-ID, Portal Redirect Related VSA(s)...)
Install Web-redirect and create temporary L2-aware NAT host
Handle Packets According to Redirect Policy. Forwarded Packets Go Through L2-aware Host.
L3 Packet (Except DHCP)
L3 Packet that Hit Fwd Rule
L3 Packet
L3 Packet
L3 Packet
UE provided credentials and portal-auth completes
Trigger RADIUS to Generate CoA
CoA (User-name, Subscriber-ID, VSAs...) to Promote UE to an ESM Host
al_0377

Figure 412: Sequence of Events to Establish and Authenticate a Migrant User (continued)

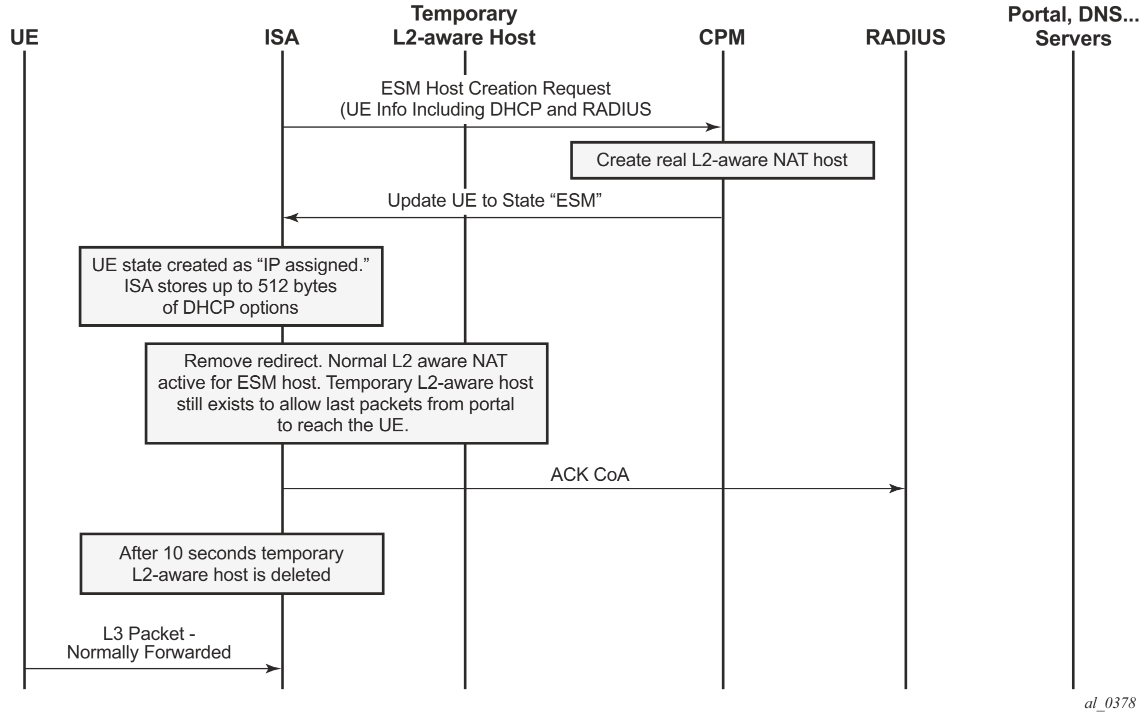
UE
ISA
Temporary L2-aware Host
CPM
RADIUS
Portal, DNS... Servers
ESM Host Creation Request (UE Info Including DHCP and RADIUS
Create real L2-aware NAT host
Update UE to State "ESM"
UE state created as "IP assigned." ISA stores up to 512 bytes of DHCP options
Remove redirect. Normal L2 aware NAT active for ESM host. Temporary L2-aware host still exists to allow last packets from portal to reach the UE.
ACK CoA
After 10 seconds temporary L2-aware host is deleted
L3 Packet - Normally Forwarded
al_0378

Figure 413: Sequence of Events to Establish and Authenticate a Migrant User

Configuration

The authentication-policy as shown below is used to configure a RADIUS server, and is applicable to the UEs in authenticated state.

```
subscriber-mgmt
    authentication-policy "authentication-1" create
     password "E40PedK6aqrEIpr2DEoJyVR8PQ3XkFF7" hash2
      radius-authentication-server
               source-address 192.0.2.1
               router "management"
               server 1 address 192.0.2.3 secret "6uuGli25Vtl49q0." hash2
      exit
      accept-authorization-change
      include-radius-attribute
               acct-session-id
               circuit-id
               remote-id
               nas-port-id
               nas-identifier
               nas-port-type
               pppoe-service-name
               dhcp-options
               dhcp-vendor-class-id
               access-loop-options
               mac-address
               called-station-id
               calling-station-id sap-string
               tunnel-server-attrs
```

An isa-radius-policy is required for authentication from the ISA, as below – this contains the attributes to be sent in the access request message to the RADIUS server, which is also configured in this policy.

```
aaa
   isa-radius-policy "isa-policy-1" create
       nas-ip-address-origin isa-ip
       password "CAO6ALDnhyBJERE4xnXoW15MQ/hu74x5nDE7F.OJxHM" hash2
       auth-include-attributes
            called-station-id
            calling-station-id
            circuit-id
            dhcp-options
            dhcp-vendor-class-id
            mac-address
            nas-identifier
            nas-port-id
            nas-port-type
            remote-id
       exit
       servers
            router 1
            source-address-range 192.168.0.2
            server 1 create
                authentication
                coa
                ip-address 192.0.2.3
                secret "CAO6ALDnhyBJERE4xnXoW15MQ/hu74x5nDE7F.OJxHM" hash2
                no shutdown
            exit
       exit
  exit
exit
```

The HTTP redirect policy is shown below, this is enforced on ISA while a UE is migrant and contains the configurations defining the forwarding of traffic in this state.

```
subscriber-mgmt
    http-redirect-policy "redirect-policy-1" create
 url "http://66.185.84.163"
 forward-entries
     dst-ip 192.168.1.1 protocol udp dst-port 53
     dst-ip 192.168.1.2 protocol udp dst-port 53
     dst-ip 66.185.84.163 protocol tcp dst-port 80
     dst-ip 10.0.0.1 protocol udp dst-port 67
     dst-ip 10.0.0.1 protocol udp dst-port 68
  exit
     exit
exit
```

The NAT pool configuration for migrant and authenticated UEs is shown below.

```
vprn 10 customer 1 create
   nat
      inside
          l2-aware
              address 10.0.0.1/24
          exit
      exit
      outside
           pool "migrant-pool-1" nat-group 1 type wlan-gw-anchor create
                 address-range 192.168.2.0 192.168.2.255 create
                 exit
                 no shutdown
           exit
           pool "auth-pool-1" nat-group 1 type l2-aware create
                address-range 192.168.3.0 192.168.3.255 create
                exit
                no shutdown
           exit
       exit
   exit
exit
```

The NAT policy for migrant UEs is as follows.

```
service
   nat
        nat-policy "migrant-policy" create
           pool "migrant-pool-1" router 1
           timeouts
              tcp-established min 1
           exit
        exit
    exit
exit
```

Below is the NAT policy for authenticated UEs.

```
service
    nat
         nat-policy "nat-auth-policy-1" create
            pool "auth-pool-1" router 10
         exit
    exit
exit
```

The migrant user configuration under the soft-gre group-interface within the VPRN service is shown below. This includes configuration for authentication, DHCP, and forwarding from the ISA, as defined in the sections above. The migrant user related configuration can be specified per VLAN tag (or range) under soft-gre interface, where each VLAN tag represents an SSID.

```
vprn 1 customer 1 create
   subscriber-interface "sub-int-1" create
         address 10.0.0.1/24
         group-interface "soft-gre-1" softgre create
             sap-parameters
                  sub-sla-mgmt
                       def-sla-profile "sla-profile-1"
                       def-sub-id use-auto-id
                       def-sub-profile "sub-profile-1"
                       sub-ident-policy "sub_ident"
                   exit
              exit
              dhcp
                  proxy-server
                       emulated-server 10.0.0.1
                       lease-time hrs 1
                       no shutdown
                  exit
                  trusted
                  lease-populate 32767
                  gi-address 10.0.0.1
                  no shutdown
              exit
```

```
          authentication-policy "authentication-1"
          host-connectivity-verify

          soft-gre
               authentication
                   authentication-policy "isa-policy-1"
               exit
               gw-address 192.168.0.1
               mobility
                   hold-time 0
                   trigger data iapp
               exit
               router 1
               wlan-gw-group 1
               vlan-tag-ranges
                   range start 100 end 100
                       authentication
                            authentication-policy "isa-policy-1"
                       exit
                       data-triggered-ue-creation
                       dhcp
                            active-lease-time min 12
                            initial-lease-time min 5
                            l2-aware-ip-address 10.0.0.10
                            primary-dns 192.168.1.1
                            secondary-dns 192.168.1.2
                            no shutdown
                       exit
                       http-redirect-policy "redirect-policy-1"
                       nat-policy "migrant-policy"
            exit
              exit
              no shutdown
          exit
       exit
    exit
exit
```

Conclusion

Migrant user support is a useful feature that optimizes system resources (public IP addresses, ESM hosts, CPU processing, etc.) to provide the scale and performance required in live hot-spot and home-spot WiFi deployments at peak times.