Call Flows for 3G and 4G Mobile IP Users

This chapter provides various call flows for 3G and 4G mobile IP users, and contains the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

3G DHCP Discover Call Flow

In the 3G DHCP Discover authentication method, the DHCP Discover message carries the subscriber's MAC address that needs to be authenticated. The iWAG cannot handle inbound raw EAP authentication messages that are not encapsulated inside the RADIUS messages. Therefore, the EAP authentication messages are signaled with the AAA server without passing through the iWAG, that is, out-of-band authentication from the iWAG perspective.

The following figures and steps describe the call flow pertaining to DHCP Discover authentication for a 3G user:

Figure 1: 3G DHCP Discover Call Flow (Part 1)

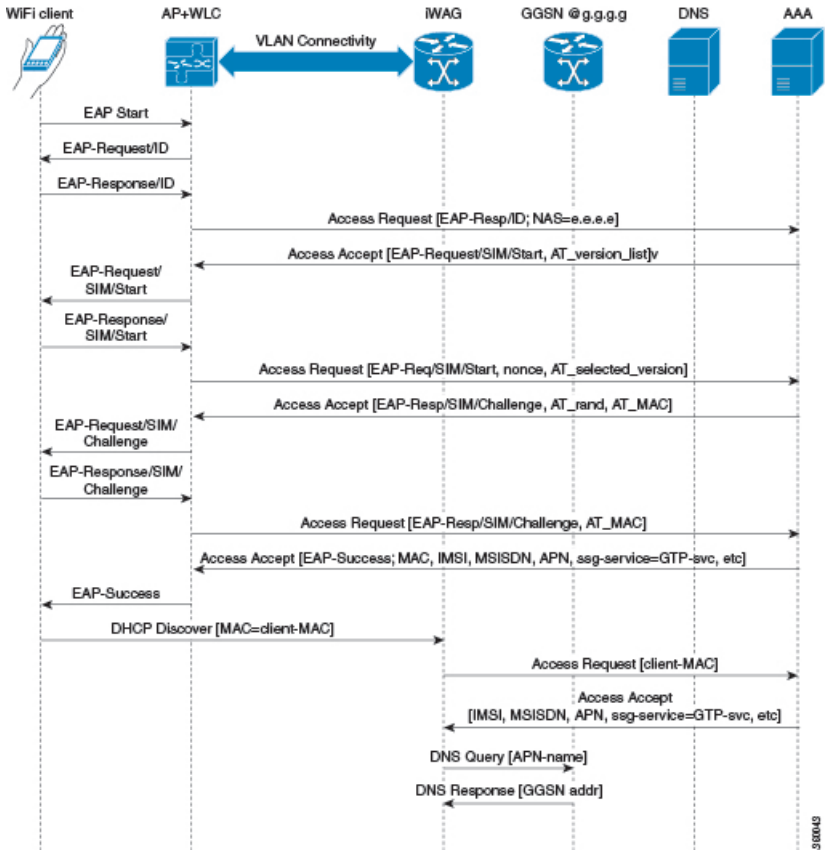
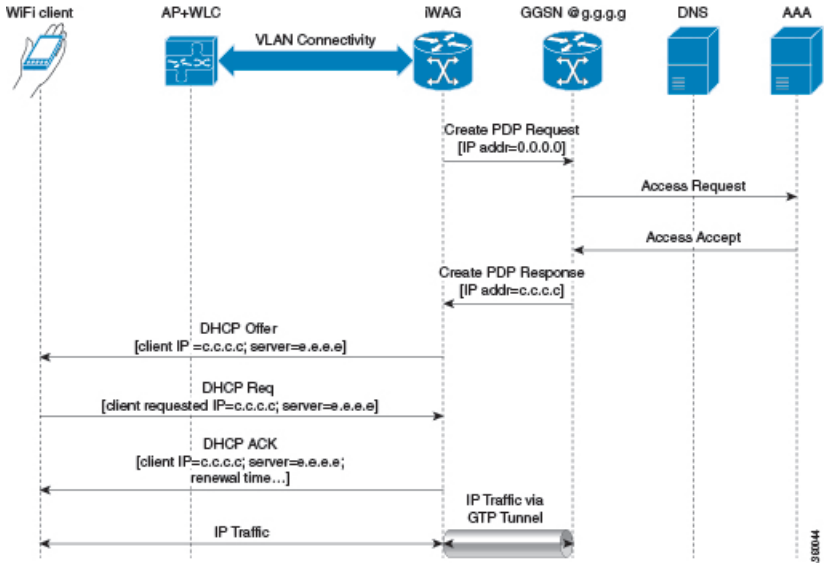


Figure 2: 3G DHCP Discover Call Flow (Part 2)



1 The mobile device is automatically associated to the SSID broadcast by the access points to establish and maintain wireless connectivity.

2 The AP or the WLC starts the EAP authentication process by sending an EAP Request ID to the mobile device.

3 The mobile device sends a response pertaining to the EAP Request ID back to the AP or the WLC.

4 The WLC sends a RADIUS Access Request to the AAA server asking it to authenticate the subscriber.

5 After the subscriber is authenticated, the AAA server caches its entire user profile that includes the information about IMSI, MSISDN, APN, and the Cisco AV pair having ssg-service-info set to GTP-service. The cached data also includes the client's MAC address, which is set as the calling-station-ID in the incoming EAP messages.

6 The AAA server sends the RADIUS Access Accept message to the AP or the WLC.

7 When the RADIUS Access Accept message comes back, the corresponding user profile in which the use of GTP-service is identified is obtained.

8 The WLC sends the successful EAP authentication message to the mobile device.

9 The mobile device sends a DHCP Discover message to the iWAG. In response to this DHCP Discover message, the DHCP goes into a new pending state to wait for the signaling on the MNO side to be completed, which assigns an IP address to the subscriber.

   In response to this DHCP Discover message, DHCP goes into a new pending state to wait for the signaling on the MNO side to be completed, which assigns an IP address to the subscriber.

10 The iWAG finds a session associated with the subscriber MAC address and retrieves the subscriber IP address from the session context.

11 The iWAG sends a RADIUS Access Request to the AAA server asking it to authenticate the subscriber using the MAC address in it as the calling-station-ID, while also providing all other known subscriber information, IDs, and IMSI in this Access Request message.

12 When the AAA server sends back the RADIUS Access Accept message to the iWAG, the user profile in which the use of GTP-service is identified is obtained.

13 The iWAG sends a query to the DNS server to resolve a given Access Point Name (APN) to a GGSN IP address.

14 The DNS server sends the DNS-resolved GGSN address back to the iWAG.

15 After receiving the DNS-resolved GGSN address, the iWAG sends the Create PDP Context Request, in which the PDP context address is set to 0, in order to request the GGSN for an IP address assignment.

16 The GGSN sends a RADIUS Access Request to the AAA server.

17 Based on the cached information obtained from the EAP-SIM authentication, the AAA server replies with a RADIUS Access Accept message to the GGSN.

18 The GGSN sends the Create PDP Context Response that carries the assigned IP address c.c.c.c for the subscriber, to the iWAG.

19 The iWAG sends a DHCP Offer message to the mobile device.

20 The mobile device sends a DHCP Request message to the iWAG, and the iWAG acknowledges this request by sending a DHCP ACK message to the mobile device.

21 The WiFi subscriber traffic now has a data path through which it can flow.

3G DHCP Discover Call Flow Configuration

The following example shows a 3G DHCP Discover call flow configuration:

```
aaa new-model //authentication, authorization, and accounting configurations
!
!
aaa group server radius AAA_SERVER1
 server-private 99.0.7.10 auth-port 1812 acct-port 1813 key cisco
!
aaa authentication login default none
aaa authentication login WEB_LOGON group AAA_SERVER1
aaa authorization network ISG_PROXY_LIST group AAA_SERVER1
aaa authorization subscriber-service default local group AAA_SERVER1
aaa accounting network ISG_PROXY_LIST start-stop group AAA_SERVER1
aaa accounting network ACCT_SERVER
 action-type start-stop
 group AAA_SERVER1
!
!
!
!
!
aaa server radius dynamic-author
 client 99.0.7.10 server-key cisco
 auth-type any
 ignore server-key
!
aaa session-id common
aaa policy interface-config allow-subinterface
clock timezone EDT -4 0
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip domain name cisco.com
```

```
!
ip dhcp pool 2NETWORK
 network 10.0.0.0 255.0.0.0
 default-router 10.100.10.2
!
!
!
subscriber service multiple-accept
subscriber service session-accounting
subscriber service accounting interim-interval 1
subscriber redundancy dynamic periodic-update interval 15
subscriber authorization enable
!
!
spanning-tree extend system-id
!
username samipate nopassword
!
redundancy
 mode sso
redirect log translations extended exporter l4r-exporter
!
!
!
ip tftp source-interface GigabitEthernet0
ip tftp blocksize 8192
class-map type traffic match-any TC_TIMEOUT
 match access-group input name timeout_acl_in
 match access-group output name timeout_acl_out
!
class-map type traffic match-any TC_POSTPAID
 match access-group input name postpaid_acl_in
 match access-group output name postpaid_acl_out
!
class-map type traffic match-any TC_OPENGARDEN
 match access-group input name acl_in_opengarden
 match access-group output name acl_out_opengarden
!
policy-map type service OPENGARDEN_SERVICE
 10 class type traffic TC_OPENGARDEN
  accounting aaa list ACCT_SERVER
 !
 class type traffic default in-out
  drop
 !
!
policy-map type service SERVICE_POSTPAID
 20 class type traffic TC_POSTPAID
  police input 512000
 !
 class type traffic default in-out
  drop
 !
!
policy-map type service SERVICE_TIMEOUT
 25 class type traffic TC_TIMEOUT
  timeout absolute 10000
 !
 class type traffic default in-out
  drop
 !
!
policy-map type control ISG_GTP_CONTROL
 class type control always event service-stop
  1 service-policy type service unapply identifier service-name
 !
 class type control always event session-start
  10 service-policy type service name OPENGARDEN_SERVICE
  20 service-policy type service name SERVICE_POSTPAID
  25 service-policy type service name SERVICE_TIMEOUT
  30 authorize aaa list ISG_PROXY_LIST password lab1 identifier mac-address
 !
```

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

interface GigabitEthernet0/0/1
 description To interface g0/0/1
 ip address 99.0.7.11 255.255.255.0
 negotiation auto
!
interface GigabitEthernet0/0/2
 description To Client facing interface
 ip address 192.1.1.1 255.255.0.0
 negotiation auto
 service-policy type control ISG_GTP_CONTROL
 ip subscriber l2-connected # integration to ISG
  initiator unclassified mac-address # use this command to initiate unclassified mac
  initiator dhcp       # recognizes the incoming dhcp request. use this command to initiate
 DHCP discovery.
!
interface GigabitEthernet0/0/3
 description To Client facing interface
 ip address 192.2.1.1 255.255.0.0
 negotiation auto
 service-policy type control ISG_GTP_CONTROL
 ip subscriber l2-connected # integration to ISG
  initiator unclassified mac-address
  initiator dhcp      # recognizes the incoming dhcp request
!
interface GigabitEthernet0/3/0
 description To Client facing interface
 ip address 192.3.1.1 255.255.0.0
 negotiation auto
 service-policy type control ISG_GTP_CONTROL
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
!

interface GigabitEthernet1/3/0
 description To PGW/GGSN
 ip address 98.0.7.11 255.255.255.0
 negotiation auto
!

interface GigabitEthernet0
 description To Management Interface
 ip address 5.28.8.10 255.255.0.0
 negotiation auto
!
mcsa # enabling mobile client service abstraction
 enable sessionmgr
!
ip default-gateway 5.28.0.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 5.28.0.0 255.255.0.0 5.28.0.1
ip route vrf Mgmt-intf 5.28.0.0 255.255.0.0 5.28.0.1
ip route vrf Mgmt-intf 223.0.0.0 255.0.0.0 5.28.0.1
!
```

```
ip access-list extended acl_in_opengarden # enabling access lists
 permit udp any eq 5555 any
ip access-list extended acl_out_opengarden
 permit udp any eq 5555 any
ip access-list extended postpaid_acl_in
 permit udp any eq 181 any
ip access-list extended postpaid_acl_out
 permit udp any eq 181 any
ip access-list extended timeout_acl_in
 permit udp any eq 180 any
ip access-list extended timeout_acl_out
 permit udp any eq 180 any
!
!
!
!
radius-server attribute 44 include-in-access-req default-vrf
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 32 include-in-accounting-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server host 99.0.7.10 auth-port 1812 acct-port 1813
radius-server throttle accounting 300
radius-server key cisco
!
!
control-plane
!
 !
 !
 !
 !
!
line con 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
!
!

#-----------------------------------------------
# Configuring GTP in IWAG
#-----------------------------------------------

gtp     # Make sure to configure mcsa before configuring GTP
 n3-request 7
 interval t3-response 1
 interval echo-request 64
 information-element rat-type wlan # RAT: Radio Access Technology
 interface local GigabitEthernet1/3/0 # Iwag access interfaces
 apn 1
  apn-name cisco.com  # you can have multiple APNs
  ip address ggsn 98.0.7.13 # details for the iWAG to reach the GGSN
  default-gw 192.168.0.1 prefix-len 16
  dns-server 192.168.255.253
  dhcp-lease 3000
 apn 2356
  apn-name cisco1.com   # you can have multiple APNs
  ip address ggsn 98.0.7.14
  default-gw 10.254.0.1 prefix-len 16
  dns-server 10.254.255.253
  dhcp-lease 3000
!
```

```
end
```

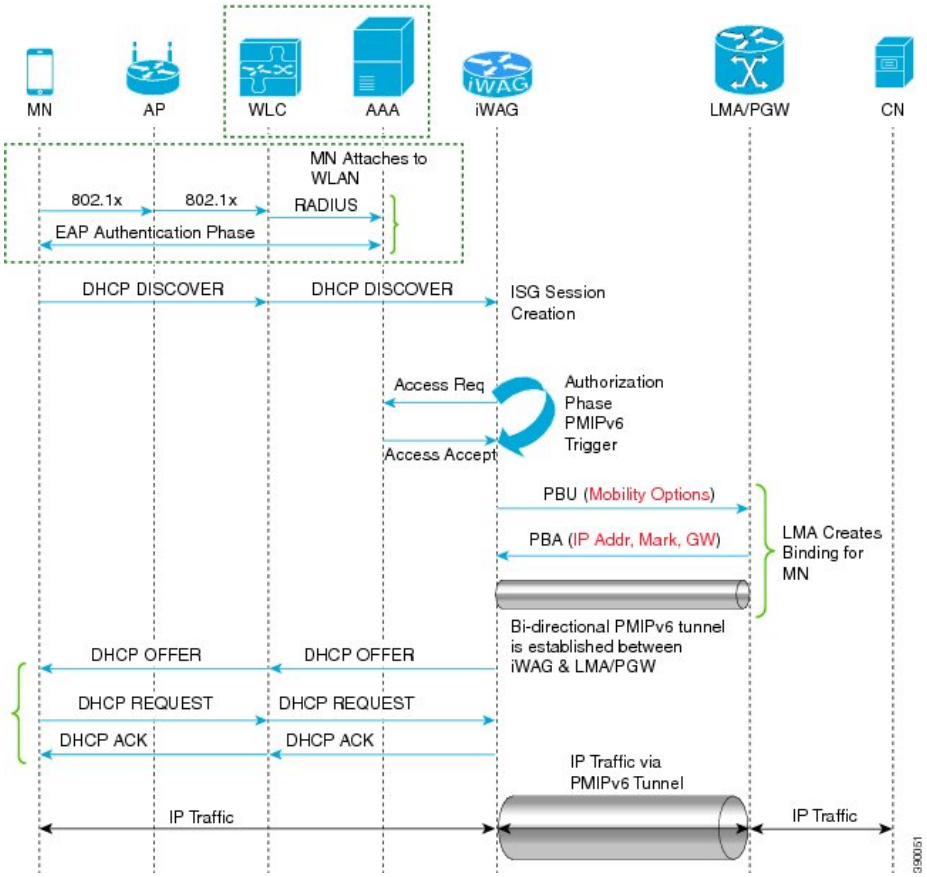
4G DHCP Discover Call Flow

The following is the overview of the 4G DHCP Discover call flow:

1. In the 4G DHCP Session Initiator use-case scenario, iWAG is configured only with DHCP as the session initiator.
2. On receiving the DHCP discover message from the AP or WLC, the iWAG creates the session.
3. The iWAG sends an Access Request message to the AAA server and downloads the mobility parameters through an Access Accept message.
4. After receiving the mobility parameters, the iWAG initiates PMIP signaling by sending a PBU message to the LMA.
5. The LMA responds with a PBA message that includes IP address, gateway, and mask.
6. Now the PMIP tunnel is established between the iWAG and the LMA.
7. The iWAG offers an IP address to the client and creates a binding.

The figure below shows the 4G DHCP session initiator call flow:

Figure 3: 4G DHCP Discover Call Flow



The following are the call flow steps for the 4G DHCP session initiator configuration:

1. The client sends an EAP authentication request to the AP or WLC.
2. The WLC sends an Access Request message to AAA server.
3. On receiving Access Accept message from the AAA server, the WLC authenticates the client or mobile node.
4. After successful authentication, the mobile node sends a DHCP DISCOVER message to the iWAG. The iWAG creates a session and sends Access Request message to the AAA server for user authorization.
5. After being authorized, the iWAG obtains the mobile node's profile parameters, such as LMA, LMA address, APN, and service type (IPv4, IPv6, or dual).
6. The iWAG triggers PMIPv6 signaling by sending a PBU message to the LMA based on the mobile node's profile obtained from the AAA server.
7. The LMA creates session binding, indicating the corresponding iWAG and IP address for the mobile node.
8. The LMA acknowledges by sending a PBA message containing the mobile node's IP address, network mask, and gateway address to the corresponding iWAG.

9 Now, a bidirectional PMIPv6 tunnel is set up between the iWAG and the LMA.

10 The iWAG offers an IP address to the mobile node through a DHCP OFFER message.

11 The mobile node accepts the IP address by sending a DHCP Request.

12 The iWAG, which also hosts the DHCP server, acknowledges the mobile node's request by sending a DHCP ACK message.

13 The iWAG finally creates a DHCP binding.

14 The mobile node configures the IP address that was offered on its wireless interface.

15 The mobile node seamlessly exchanges data traffic with the correspondent node.

4G DHCP Discover Call Flow Configuration

The following is a 4G DHCP session initiator configuration:

```
#-------------------------------------------
LMA (ASR 5000)
#-------------------------------------------

context pgw
    ip pool PMIP_POOL_TME 10.8.20.0 255.255.255.0 public 0 subscriber-gw-address 16.8.20.254

      ipv6 address 2001:DB8::1/64
      ip address 10.8.24.101 255.255.255.0 secondary
    subscriber default
    exit
    apn example.com
      pdp-type ipv4 ipv6
      selection-mode sent-by-ms
      accounting-mode none
      ip context-name pgw
      ip address pool name PMIP_POOL_TME
      ipv6 address prefix-pool v6_pool
      dns primary 198.0.100.250
    exit
    lma-service lma1
      no aaa accounting
      reg-lifetime 40000
      timestamp-replay-protection tolerance 0
      mobility-option-type-value standard
      revocation enable
      bind address 2001:DB8:0:1::1
    pgw-service pgw1
      plmn id mcc 100 mnc 200
      session-delete-delay timeout 60000
      associate lma-service lma1
    exit
    ipv6 route 2001:db8:cafe::/48 next-hop 2001:DB8:0:1:FFFF:1234::5 interface lma1
    ip route 10.8.0.0 255.255.0.0 10.8.24.8 lma1
  port ethernet 17/1
    boxertap eth3
    no shutdown
    bind interface lma1 pgw
end

#-------------------------------------------
IWAG (ASR 1000)
Local Profile without AAA (Simple Configuration using the MN's MAC)
#-------------------------------------------
!
ipv6 unicast-routing
!
```

```
 !
policy-map type control PROXYRULE
 class type control always event session-start
  10 proxy aaa list RP
 !
!
interface GigabitEthernet1/3/0
 ip address 10.27.52.1 255.255.0.0
 negotiation auto
 ipv6 address 2001:DB8:0:0:E000::F link-local
 ipv6 address 2001::1/64
 ipv6 nd ra suppress
 ipv6 eigrp 100
 service-policy type control PROXYRULE
 ip subscriber l2-connected
  initiator dhcp
  initiator unclassified-mac
!

ip dhcp pool pmipv6_dummy_pool
!
config terminal
 mcsa
enable sessionmgr
 ipv6 mobile pmipv6-domain D1
  replay-protection timestamp window 255
 lma lma1
  ipv6-address 2001:DB8:0:1::1
mag M1
ipv6-address 2001:DB8:0:1:FFFF:1234::5

!
ipv6 mobile pmipv6-mag M1 domain D1
 no discover-mn-detach
 sessionmgr
 role 3GPP
 apn example.com
 address ipv6 2001:0DB8:2:4::2
 interface GigabitEthernet0/1/1
  lma lma1 D1
ipv6-address 2001:DB8:0:1::2


!
```

4G Roaming Call Flow

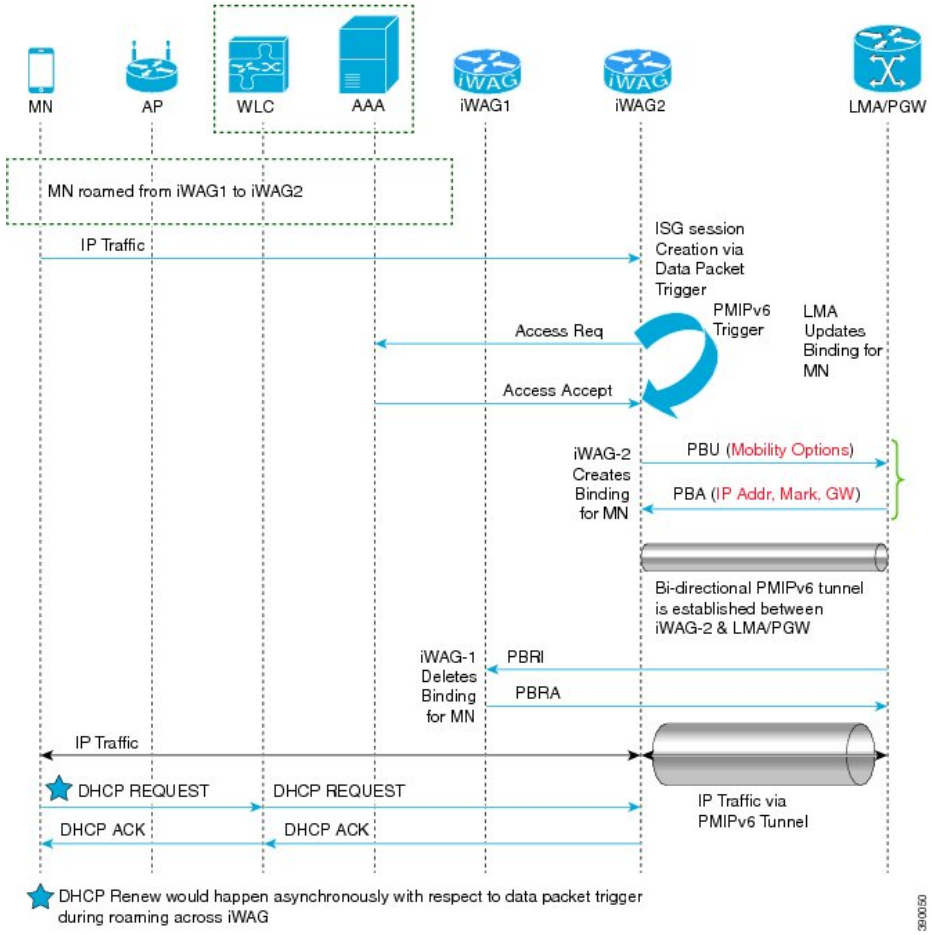
After roaming from one iWAG to another, the mobile node sends traffic to the iWAG. On receiving the unclassified MAC address, the iWAG creates a session and sends an Access Request message to the AAA server. The iWAG downloads mobility parameters from the AAA server through an Access Accept message. The iWAG initiates PMIP signaling by sending a PBU message. The LMA responds with a PBA message. In this case, the LMA provides the same IP address to iWAG 2 to enable the mobile node to maintain the same IP address after roaming. The LMA sends a Proxy Binding Revocation Indication (PBRI) message to iWAG 1 to delete the binding for the mobile node.

This call flow covers the following:

- Session roaming from iWAG 1 to another iWAG 2
- PMIP tunnel creation between LMA and iWAG 2
- Assigning same IP address to the MN after roaming
- Session termination

The figure below describes the call flow for 4G roaming involving a DHCP session. Here, DHCP and the unclassified MAC address together indicate First Sign of Life (FSOL) on the iWAG access interface.

Figure 4: 4G Roaming Call Flow



The following are the call flow steps for the 4G roaming configuration:

1. A mobile node roams from iWAG 1 to iWAG 2. The mobile node directly sends the IP packet to iWAG 2. The iWAG 2 creates sessions and send access request to the AAA server.
2. The iWAG 2 downloads mobility parameters from the AAA server through an Access Accept message.
3. On receiving mobility parameters from the AAA server, the iWAG 2 initiates PMIP signaling by sending a Proxy Binding Update (PBU) message to the LMA. The LMA responds with the PBA message that contains the IP address, mask, and gateway. Now a PMIP tunnel is established between iWAG 2 and the LMA.
4. The LMA sends a PBRI message to iWAG 1 to delete the binding from iWAG 1. iWAG 1 deletes the binding for mobile node and responds with a PBRA message.
5. iWAG 2 acknowledges the same IP address to the MN through a DHCP ACK message.
6. The MN seamlessly exchanges data traffic with the correspondent node.

4G Roaming Call Flow Configuration

The following is a 4G Roaming call flow configuration:

```
#-------------------------------------------
LMA (ASR 5000)
#-------------------------------------------
context pgw
    ip pool PMIP_POOL_TME 10.8.20.0 255.255.255.0 public 0 subscriber-gw-address 209.165.201.1

      ipv6 address 2001:DB8::1/64
      ip address 10.8.24.101 255.255.255.0 secondary
    subscriber default
    exit
    apn serviceprovider.com
      selection-mode sent-by-ms
      accounting-mode none
      ip context-name pgw
      ip address pool name PMIP_POOL_TME
      ipv6 address prefix-pool v6_pool
    exit
    lma-service lma1
      no aaa accounting
      reg-lifetime 40000
      timestamp-replay-protection tolerance 0
      mobility-option-type-value standard
      revocation enable
      bind address 2001:DB8:0:0:E000::F
    pgw-service pgw1
      plmn id mcc 100 mnc 200
      session-delete-delay timeout 60000
      associate lma-service lma1
    exit
    ipv6 route 2001:DB8::/48 next-hop 2001:DB8:0:ABCD::1 interface lma1
    ip route 10.8.0.0 255.255.0.0 10.8.24.8 lma1
  port ethernet 17/1
    boxertap eth3
    no shutdown
    bind interface lma1 pgw
end
#-------------------------------------------
IWAG2 (ASR 1000)
Local Profile without AAA (Simple Configuration using the MN's MAC)
#-------------------------------------------
!
ipv6 unicast-routing
! !
policy-map type control PROXYRULE
 class type control always event session-start
  10 proxy aaa list RP
 !
ip dhcp pool pmipv6_dummy_pool
!
ipv6 mobile pmipv6-domain D1
 replay-protection timestamp window 200
 lma lma1
  ipv6-address 2001:DB8:0:0:E000::F
 nai mn1@example.com
  apn example.com
  lma lma1
  int att WLAN l2-addr 0024.d78e.21a4
!
ipv6 mobile pmipv6-mag M1 domain D1
 discover-mn-detach 100 10
 role 3GPP
 address ipv6 2001:DB8:0:1:FFFF:1234::5
 interface GigabitEthernet 0/1/0.3074
!
interface GigabitEthernet1/3/0
```

```
 ip address 10.27.52.1 255.255.0.0
 negotiation auto
 ipv6 address 2001:DB8:0:1::1 link-local
 ipv6 address 2001:DB8::1
 ipv6 nd ra suppress
 ipv6 eigrp 100
 service-policy type control PROXYRULE
 ip subscriber l2-connected
  initiator dhcp
  initiator unclassified-mac
!
```

Note In 4G roaming involving a DHCP + RADIUS proxy-initiated session, DHCP, RADIUS proxy, and unclassified MAC address together indicate FSOL on the iWAG access interface.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
iWAG commands	Cisco IOS Intelligent Wireless Access Gateway Command Reference

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Call Flows for 3G and 4G Mobile IP Users

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Call Flows for 3G and 4G Mobile IP Users

Feature Name	Releases	Feature Information
Call Flows for 3G and 4G Mobile IP Users	Cisco IOS XE Release 3.11	In Cisco IOS XE Release 3.11S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.