Proxy Mobile IPv6: Network-Based Mobility Deployment Guide

Revised: April 28, 2016,

Proxy Mobile IPv6 Network-Based Mobility

Network-based mobility management enables IP mobility for a mobile node (MN) without requiring the MN to participate in any mobility-related signaling. IP mobility entities in the network are responsible for tracking the movements of the host or the MN and initiating the required mobility signaling on behalf of the host or the MN. Because the network is responsible for managing IP mobility on behalf of the MN, IP mobility is provided to any clientless MN, which is a node that does not run any mobile IP stack.

This guide provides deployment scenarios, configuration steps, call flows, and troubleshooting guidelines for deploying the network-based mobility Wi-Fi architecture by using Proxy Mobile IPv6 (PMIPv6).

Leveraging Wi-Fi Access Technology for Wi-Fi Offload

Service providers (SP) seek new ways to accommodate the surge in mobile data traffic and the variety of smart, portable devices coming onto their networks. As mobile devices proliferate, so do the opportunities to strengthen relationships with customers by delivering a superior subscriber or end-user experience.

Fixed and mobile operators are, therefore, looking at both licensed and unlicensed Wi-Fi technologies to meet the demand and to expand customer footprint. Trusted Wi-Fi hotspots can be integrated into the existing SP policy and accounting infrastructure, thereby allowing the SP to maintain subscriber accountability. At the same time, traffic from these trusted Wi-Fi hotspots can be integrated into the existing packet core of the SP by using the standard Proxy Mobile IPv6 (PMIPv6) (PMIPv6-S2a) interface to provide IP mobility across Wi-Fi and 4G networks to enhance subscriber experience.

We offer a comprehensive solution to SPs, mobile operators, Mobile Virtual Network Operators (MVNO) and cable operators to leverage Wi-Fi as an access technology for Wi-Fi offload.

Why PMIPv6

Proxy Mobile IPv6 (PMIPv6) is a mobility management protocol standardized by IETF (RFC 5213 and RFC 5844) for building a common network to accommodate various access technologies, such as Worldwide Interoperability for Microwave Access (WiMAX), 3rd Generation Partnership Project (3GPP), 3rd Generation Partnership Project 2 (3GPP2) and wireless LAN (WLAN).

Contrary to the Mobile IP approach, network-based mobility management enables IP mobility for an MN without requiring the MNs to participate in any mobility-related signaling. The mobility entities in the network are responsible for tracking the movements of the host or the MN and initiating the required mobility signaling on the MN's behalf. Because the network is responsible for managing IP mobility on behalf of the mobile node, IP mobility is provided to any clientless MN, which is a node without running any mobile IP stack, and this is the biggest advantage of PMIPv6 over other mobility technologies.

PMIPv6 is IP Version Agnostic

Both IPv4 and IPv6 protocols can be enabled over the same network infrastructure. Cisco PMIPv6 implementation is address-family agnostic, and it is capable of supporting the following combinations:

- Mobile Nodes (MNs) in a Proxy Mobile IPv6 (PMIPv6) domain operating in IPv4-only, IPv6-only, or in dual-stack mode
- The transport network between the mobile access gateway (MAG) and the local mobility anchor (LMA) is either IPv4-only, IPv6-only or dual-stack (where IPv4 is preferred)

Cisco Platforms that Support PMIPv6

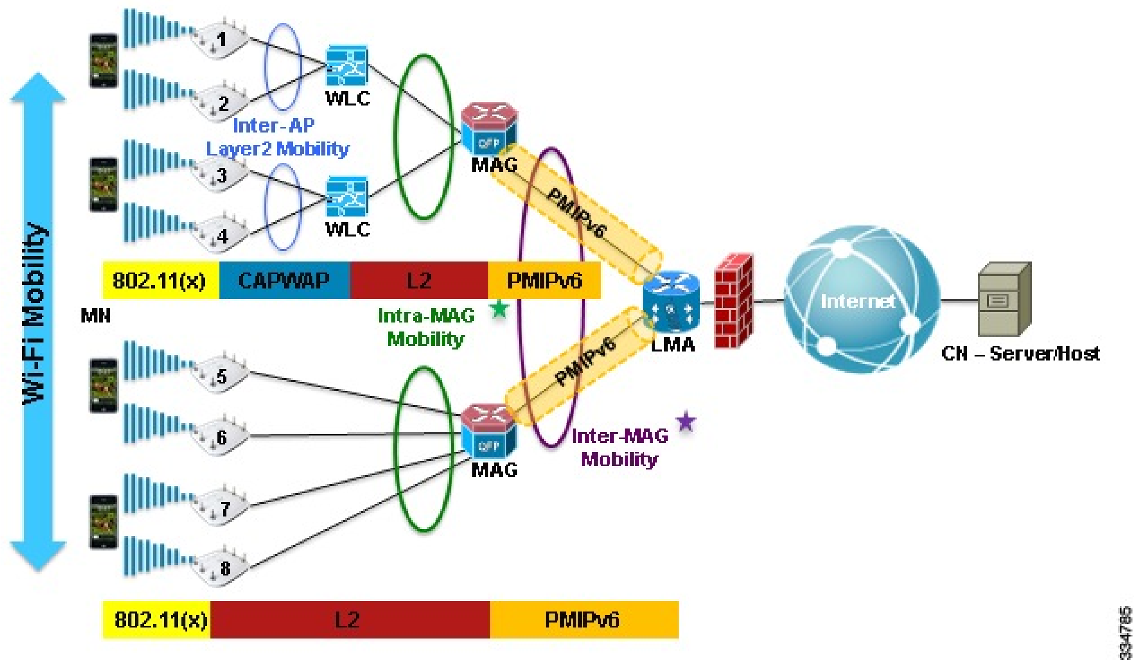
The following table provides information about the platforms that support PMIPv6:

Hardware Platform	Role	Minimum Supported Software	Recommended Software	Recommended Hardware
Cisco ASR 5000	LMA	12.2	14.0	See the product specification.
Cisco ASR 1000	MAG	15.1(3)S XE 3.4S	15.2(1)S XE 3.7S and later releases	Chassis ASR 1006 ASR1000-SIP20 ASR1000-RP2 (with 16GB RAM) ASR1000-ESP40
Cisco ISR-G2	MAG	15.2(4)	15.2(4)	See the product specification.
Cisco WLC	MAG	7.3	7.3	See the product specification.
Cisco ASR 1000	LMA	15.2(4)S XE 3.7S	15.2(4)S XE 3.7S	Chassis ASR 1006 ASR1000-SIP20 ASR1000-RP2 (with 16GB RAM) ASR1000-ESP40

Wi-Fi Mobility

Mobility Access Gateway (MAG) is agnostic to Wi-Fi access network deployment. The following figure shows Access Points (APs) operating in autonomous mode directly connected to MAG (AP 5 to AP 8) and light-weight APs (AP 1 to AP 4) connected to Wireless LAN Controllers (WLC), which in turn are connected to the MAG.

Figure 1: Wi-Fi Mobility



The Wi-Fi mobility can be of the following categories:

- **Inter-AP Mobility:** The Wi-Fi client can roam from one light-weight AP to another (for example, between AP 1 and AP 2), as long as these APs are connected to the same WLC. This move is completely transparent to the MAG.
- **Intra-MAG Mobility:** The Wi-Fi client can move either across light-weight APs that are attached to different WLCs (for example, between AP 2 and AP 3) or across autonomous APs (for example, between AP 5 and AP 6) or across light weight APs and autonomous APs, provided they are connected to the same MAG. The MAG takes appropriate actions to update the MN's binding locally and also performs PMIPv6 signaling with LMA on behalf of the MN.
- **Inter-MAG Mobility:** The Wi-Fi client can move across APs that are connected to different MAGs, for example, between AP 4 and AP 5. The MAG takes appropriate actions to create and maintain the MN's binding and also performs PMIPv6 signaling with the LMA on behalf of the MN.

SP Wi-Fi Mobility Deployment Scenarios

SPs providing wireline services, such as broadband, cable, Fiber to the x (FTTx) and so on, and wireless services, such as mobile network operator (MNO), mobile virtual network operator (MVNO) and so on, plan to rollout Wi-Fi services. Cisco supports various models for deploying service provider grade Wi-Fi. The following are the some of the most popular deployment models.

- Scenario 1: Wi-Fi Access Aggregation with a Standalone LMA
- Scenario 2: Wi-Fi Access Aggregation with an Evolved Packet Core
- Scenario 3: Wi-Fi Access Aggregation with multiple Mobile Operators
- Scenario 4: Residential and Community Wi-Fi Deployment

Commonalities Across all Deployment Scenarios

All deployment models requires that the MAC or hardware address of the Mobile Node (MN) is visible to the mobile access gateway (MAG). The Wi-Fi access network provides Layer 2 connection from the MN to the MAG, thus allowing the MAG to know the MAC address of the MN.

The MAG is a function on an access router that manages mobility-related signaling for the MN attached to its access link. MAG also acts as a proxy DHCP server for the MN and assigns IP addresses based on the PMIPv6 signaling between the MAG and the LMA.

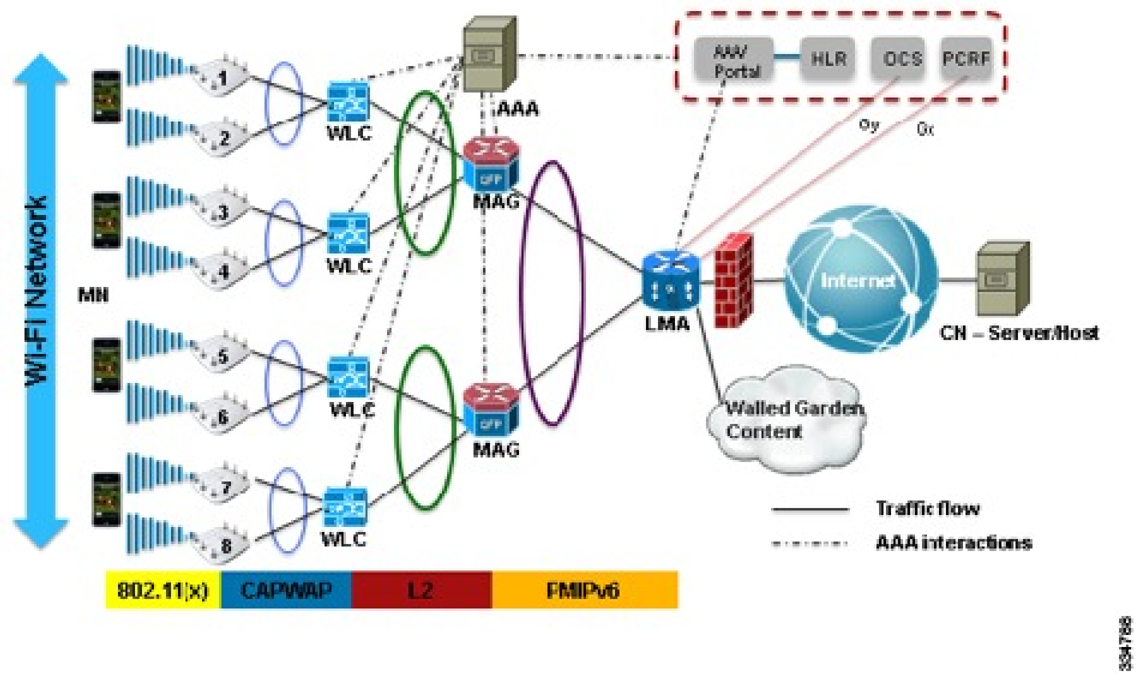
These deployment models facilitate service providers to reuse their existing subscriber credential database, Policy and Charging Rules Function (PCRF), Online Charging System (OCS), offline billing infrastructure and so on, by integrating all these functions with northbound interfaces of the LMA.

In all deployment models, we recommend you to use any one or a combination of the Extensible Authentication Protocol (EAP) methods, such as EAP-SIM, EAP-AKA, or EAP-TTLS, or PEAP encapsulation, as the mode of authentication for mobile subscriber; however, a combination of web-authentication and transparent auto-logon is also used in conjunction with EAP to support non-EAP capable MNs.

Scenario 1: Wi-Fi Access Aggregation with a Standalone LMA

This deployment scenario is also known as “standalone”, because there is no requirement of integrating the LMA with the Evolved Packet Core (EPC). The following figure shows how subscriber traffic from a Wi-Fi access network is integrated into a standalone LMA acting as the anchor point for the subscribers.

Figure 2: Wi-Fi Access Aggregation with a Standalone LMA

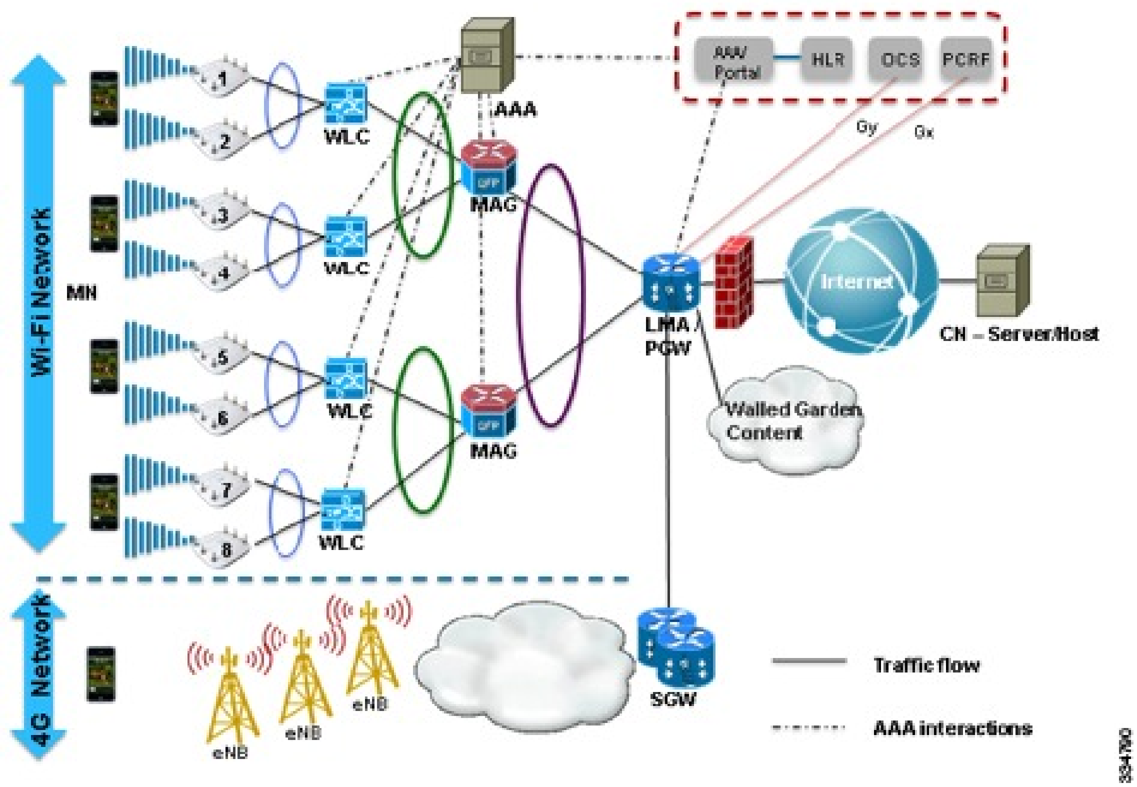


In this model, PMIPv6 facilitates IP mobility to a clientless MN when the clientless MN roams across a Wi-Fi access network.

Scenario 2: Wi-Fi Access Aggregation with the EPC

The following figure illustrates how the subscriber traffic from a Wi-Fi access network is integrated into an LMA which is colocated with a Packet Gateway (PGW) or an EPC. The trusted Wi-Fi traffic is integrated into the EPC via a standard PMIPv6-S2a interface; the Wi-Fi traffic is deemed trusted if both the access network and the core network are part of the SP network.

Figure 3: Wi-Fi Access Aggregation with EPC

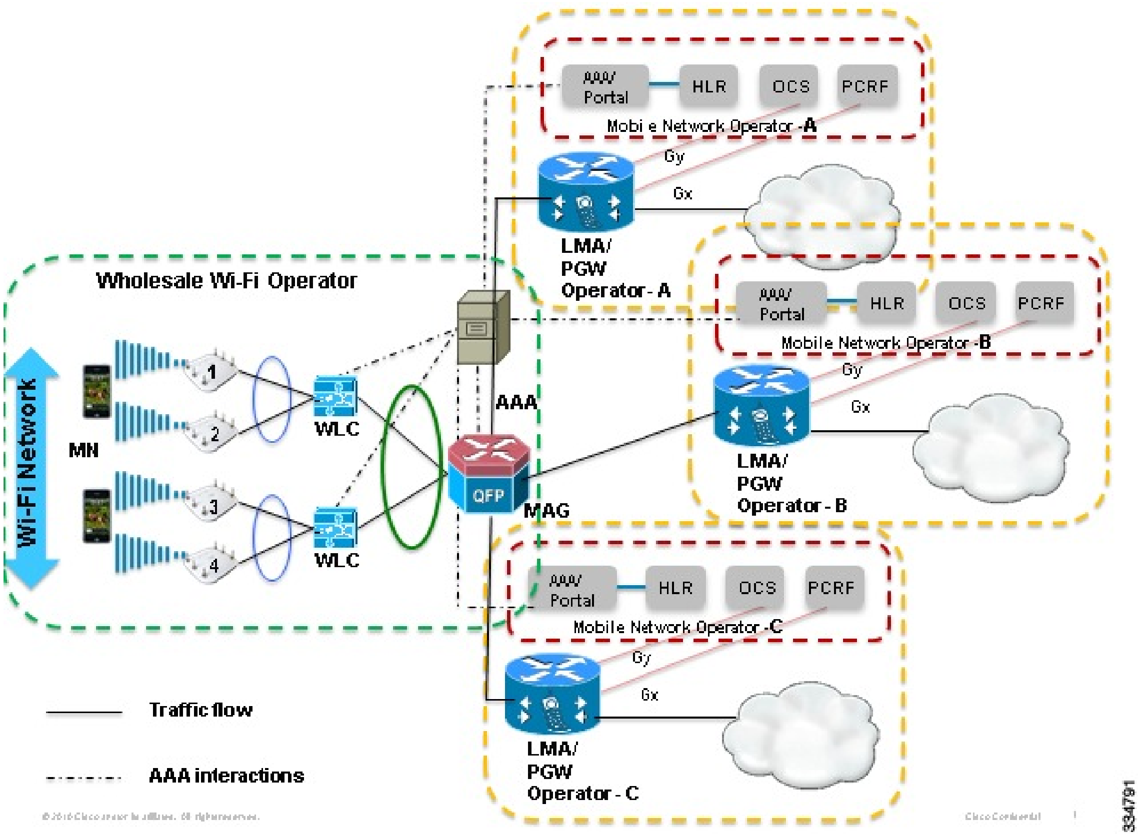


In this model, PMIPv6 facilitates IP mobility to a clientless MN not only while roaming across Wi-Fi access networks, but also while roaming across Wi-Fi and the fourth generation (4G)/Long Term Evolution (LTE) infrastructure because the subscriber session is anchored to the PGW or EPC.

Scenario 3: Wi-Fi Access Aggregation with Multiple Mobile Operators

This deployment model, illustrated in the following figure, is an extension of the Scenario 2 and was conceived for deploying Wi-Fi access as a Layer 2 wholesale service. Layer 2 wholesale allows a wireline or a wireless service provider who deploys a Wi-Fi access network, to partner with retail service providers, mobile network operators (MNOs), or mobile virtual network operator (MVNOs) for use of their Wi-Fi infrastructure. Retail SP, MNO, or MVNO have direct business relationship, such as accounting, billing, policy and so on, with the end subscribers while having service-level agreement with the Wi-Fi wholesale access provider.

Figure 4: Wi-Fi Access Aggregation with Multiple Mobile Operators



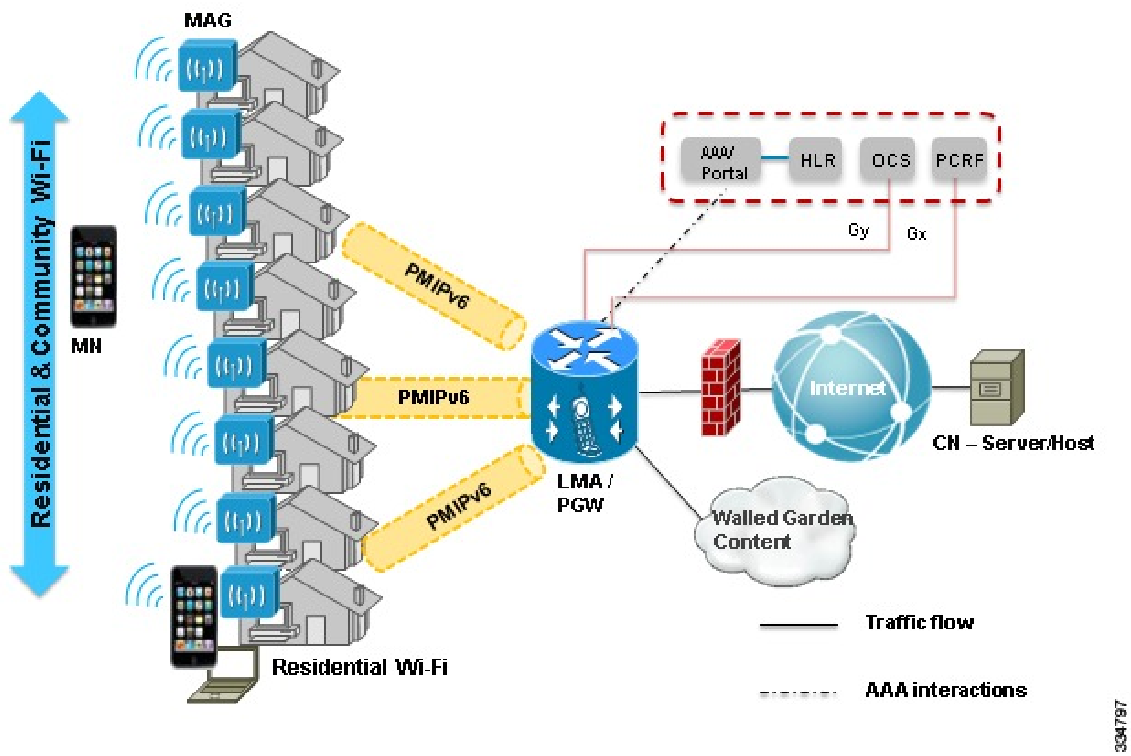
The subscriber traffic from wholesale Wi-Fi access networks is integrated into the respective MNO's LMA or MVNO's LMA, which is colocated with Packet Gateway (PGW) or an Evolved Packet Core (EPC). The authentication, authorization, and accounting (AAA) directs the MAG to integrate the subscriber's Wi-Fi traffic into a specific LMA based on the subscriber's credentials such as Network Access Identifier (NAI), International Mobile Subscriber Identity (IMSI), mobile Subscriber ISDN number (MSISDN) and so on.

In this model, PMIPv6 facilitates IP mobility to a clientless MN not only when roaming across Wi-Fi access network, but also when roaming across Wi-Fi and fourth generation (4G)/Long Term Evolution (LTE) infrastructure, because the subscriber session is anchored at the PGW or EPC.

Scenario 4: Residential and Community Wi-Fi Deployment

The Residential and Community Wi-Fi deployment model shows how residential and community Wi-Fi subscriber traffic is integrated into an LMA. The LMA either functions as a standalone entity or is colocated with a PGW or EPC. The MAG functionality is enabled on every residential or home gateway routers (for example, Cisco Integrated Service Routers [ISR]), thus tunneling all the residential subscriber traffic to the LMA via the PMIPv6 tunnel. The per-subscriber policy enforcement, quality of service (QoS), accounting and so on, is expected to occur in the LMA. The following figure illustrates the Residential and Community Wi-Fi deployment model:

Figure 5: Residential and Community Wi-Fi Deployment

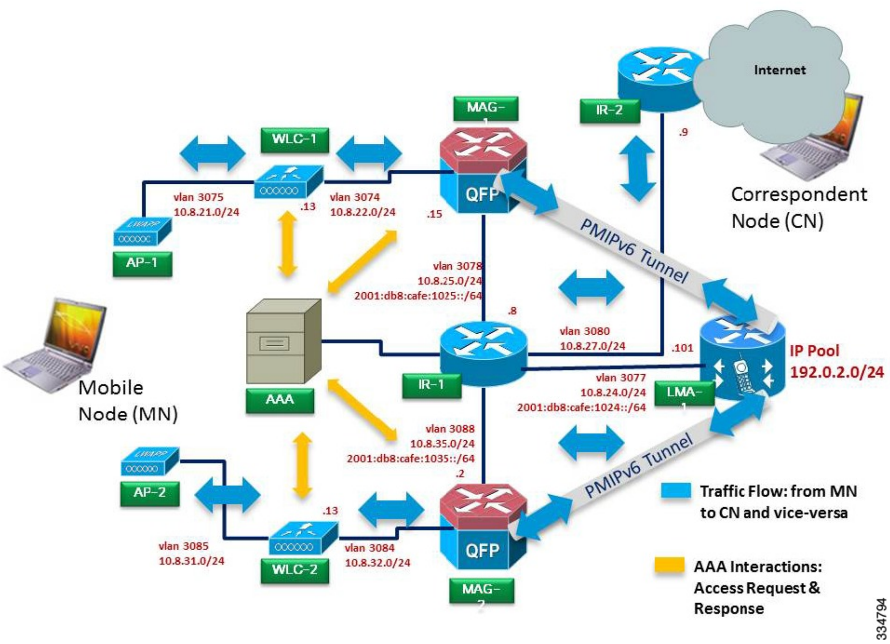


Similar to other deployment models, the trusted Wi-Fi traffic is integrated into the EPC via the standard PMIPv6-S2a interface. PMIPv6 facilitates IP mobility to a clientless MN not only when roaming across residential and community Wi-Fi access networks but also when roaming across Wi-Fi and fourth generation (4G)/Long Term Evolution (LTE) infrastructure, because the subscriber session is anchored at the PGW or EPC.

Configuration Examples

This section explains how to configure PMIPv6 mobility-based SP Wi-Fi networks. The configuration examples provided in this section applies to all the deployment scenarios discussed in this document. The following figure is the network topology diagram for PMIPv6—Network-Based Mobility and it serves as a reference for all of the deployment scenarios discussed in this guide.

Figure 6: Network Topology for PMIPv6 Network-Based Mobility Deployment



Prerequisites for PMIPv6 Network-Based Mobility Deployment

The following prerequisites for Cisco MAG implementation on Cisco ASR 1000 and Cisco ISR devices apply only to the scenarios discussed in this deployment guide:

- The access technology that is supported on the access link shared with an MN is IEEE 802.11 a/b/g/n.
- The service offered to an MN is IPv4-only; therefore, only IPv4 addresses are assigned to the MN.
- The MAG and the MN are connected over an L2 network so that the MAG is aware of the MAC or hardware address of the MN.
- The subnet-mask length for the IPv4 home address assigned to an MN must be a non-32-bit subnet mask; typically it is /24.
- The transport network of the MAG, the intermediate-router (IR) and the LMA is dual-stack; however the MAG and LMA are connected over IPv6 transport.

Software and Hardware Details

The following table lists the software and hardware details required for deployment of PMIPv6 Network-based Mobility, and it serves as a reference for all of the deployment scenarios discussed in this guide.

Network Element	Role	Software Version	Quantity Used
Cisco AIR-LAP1142N-K-K9	Light-weight AP	—	2
Cisco 5508 Series Wireless Controller	WLC	7.2	2
Cisco ASR 1000 Series Aggregation Services Routers	MAG	XE 3.7S	2
Cisco ASR 5000 Series Aggregation Services Routers	LMA	14.0	1
Cisco 3925 Integrated Services Routers	IR	—	2
Cisco Catalyst 4500 Series Switches or Cisco Catalyst 3750 Series Switches	Access Switch	—	1
Personal computer	The MN in which the MAC address is 0024.d78e.21a4	—	1

Cisco APs

No configuration is required if Cisco light-weight Access Points (APs) are used. The light-weight APs function as plug-and-play network elements. They also act as DHCP clients to the connected Wireless LAN Controllers (WLC), which, in turn, acts as the DHCP server and downloads the required image and configuration from the WLC.

Cisco Wireless LAN Controller

No PMIPv6-specific configuration is required on WLC. For information on configuring a Cisco WLC, see the *Cisco Wireless LAN Controller Configuration Guide*.

LMA Support for Cisco ASR 5000 Series Aggregation Services Routers

The following example shows how to configure an LMA in Cisco ASR 5000 Series Aggregation Services Routers:

```
context pgw
    ip pool PMIP_IPv4_POOL 192.0.2.0 255.255.255.0 public 0
subscriber-gw-address 192.0.2.254
    ipv6 pool PMIP_IPv6_POOL prefix 2001:db8:f00d::/48
public 0 policy allow-static-allocation
!
```

```
    interface lma1
      ipv6 address 2001:db8:cafe:1024::101/64
      ip address 10.8.24.101 255.255.255.0 secondary
      subscriber default
    exit
!
    apn example.com
      selection-mode sent-by-ms
      accounting-mode none
      ip context-name pgw
      ip address pool name PMIP_IPv4_POOL
      ipv6 address prefix-pool PMIP_IPv6_POOL
      dns primary 198.51.100.250
      dns secondary 198.51.100.251
    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:cafe:1024::101
!
    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:cafe:1024::8 interface lma1
    ip route 0.0.0.0 0.0.0.0 10.8.24.8 lma1
!
  port ethernet 17/1
    boxertap eth3
    no shutdown
    bind interface lma1 pgw
  end
!
```

MAG Support for Cisco ASR 1000 Series Aggregation Services Routers

The Cisco MAG feature supports various configuration options that enable the MAG to extract an MN profile. The following examples show how to enable MAG on Cisco ASR 1000 Series Aggregation Services Routers and Cisco Integrated Service Routers.

Configuring MN Profiles locally on a MAG

This configuration option is used for proof of concept, laboratory demonstration, and testing. The following example shows how the MN profile is locally configured on the MAG, so that an external radius server is not required. It is assumed that the MN MAC address or the DHCP client-identifier is already known and it can be configured locally as the NAI.

```
!
ipv6 unicast-routing
!
ip dhcp pool pmipv6_dummy_pool
!
ipv6 mobile pmipv6-domain D1
 replay-protection timestamp window 200
 lma lma1
  ipv6-address 2001:DB8:CAFE:1024::101
 nai mn0@example.com
  apn example.com
  lma lma1
  int att WLAN l2-addr 0024.d78e.21a4
!
ipv6 mobile pmipv6-mag M1 domain D1
```

```
 role 3GPP
 address ipv6 2001:DB8:CAFE:1025::15
 interface GigabitEthernet 0/1/0.3074
 interface GigabitEthernet 0/1/0.4001
!
interface GigabitEthernet 0/1/0.3074
 description => Connected to access network
 encapsulation dot1Q 3074
 ip address 10.8.22.15 255.255.255.0
!
interface GigabitEthernet 0/1/0.4001
 description => Connected to access network
 encapsulation dot1Q 4001
 ip address 10.8.51.15 255.255.255.0
!
```

Sample Output for the show ipv6 mobile pmipv6 mag binding Command

```
MAG1# show ipv6 mobile pmipv6 mag binding
----------------------------------------------------------
Total number of bindings: 1
[Binding][MN]: Domain: D1, Nai: mn0@example.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/1/0.3074
        [Binding][MN]: Hoa: 192.0.2.1, att: 4, llid: 0024.d78e.21a4
        [Binding][MN]: HNP: 0
        [Binding][MN][LMA]: Id: lma1
        [Binding][MN][LMA]: lifetime: 3600
        [Binding][MN][GREKEY]: Upstream: 5, Downstream: 5
```

Configuring a Default MN Profile on the MAG

The following is the simplest form of configuration; the MAG applies the default profile configured on the MAG access interface that connects with the MN. This form of configuration is useful for a proof of concept, laboratory demonstration, or testing, without requiring an external radius server for extracting the MN's profile. When using the default profile, the MAG considers the Network Access Identifier (NAI) as the client's MAC address.

```
!
ipv6 unicast-routing
!
ip dhcp pool pmipv6_dummy_pool
!
ipv6 mobile pmipv6-domain D1
 replay-protection timestamp window 200
 lma lma1
  ipv6-address 2001:DB8:CAFE:1024::101
 nai default_subscriber_profile_A
  apn example_A.com
  lma lma1
 nai default_subscriber_profile_B
  apn example_B.com
  lma lma1
!
ipv6 mobile pmipv6-mag M1 domain D1
 role 3GPP
 discover-mn-detach poll interval 3600 timeout 10 retries 10
 address ipv6 2001:DB8:CAFE:1025::15
 interface GigabitEthernet 0/1/0.4001
  enable pmipv6 default default_subscriber_profile_B
 interface GigabitEthernet 0/1/0.3074
  enable pmipv6 default default_subscriber_profile_A
!
interface GigabitEthernet 0/1/0.3074
 description => Connected to access network
 encapsulation dot1Q 3074
 ip address 10.8.22.15 255.255.255.0
!
interface GigabitEthernet 0/1/0.4001
 description => Connected to access network
```

```
 encapsulation dot1Q 4001
 ip address 10.8.51.15 255.255.255.0
!
```

Sample Output for the show ipv6 mobile pmipv6 mag binding Command

```
MAG1# show ipv6 mobile pmipv6 mag binding

Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, Nai: 0024.d78e.21a4
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/1/0.3074
        [Binding][MN]: Hoa: 192.0.2.1, att: 4, llid: 0024.d78e.21a4
        [Binding][MN]: HNP: 0
        [Binding][MN][LMA]: Id: lma1
        [Binding][MN][LMA]: lifetime: 3600
        [Binding][MN][GREKEY]: Upstream: 8, Downstream: 8
```

Configuring an MN Profile on the External RADIUS Server

In a typical commercial deployment, MN profiles are configured on a centralized external radius server. The MAG extracts the MN profile based on the MN or subscriber radius calling-station-id attribute, which is expected to be either subscriber MAC address or the NAI carried via the DHCP client-identifier (DHCP option 61).

```
!
ipv6 unicast-routing
!
ip dhcp pool pmipv6_dummy_pool
!
ipv6 mobile pmipv6-domain D1
 replay-protection timestamp window 200
 mn-profile-load-aaa
 lma lma1
  ipv6-address 2001:DB8:CAFE:1024::101
!
ipv6 mobile pmipv6-mag M1 domain D1
 role 3GPP
 address ipv6 2001:DB8:CAFE:1025::15
 interface GigabitEthernet 0/1/0.3074
 interface GigabitEthernet 0/1/0.4001
!
interface GigabitEthernet 0/1/0.3074
 description => Connected to access network
 encapsulation dot1Q 3074
 ip address 10.8.22.15 255.255.255.0
!
interface GigabitEthernet 0/1/0.4001
 description => Connected to access network
 encapsulation dot1Q 4001
 ip address 10.8.51.15 255.255.255.0
!
aaa new-model
!
aaa group server radius CAR-AAA
 server 203.0.113.115 auth-port 1812 acct-port 1813
!
aaa authentication login default none
aaa authorization ipmobile default group CAR-AAA
!
aaa session-id common
!
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 attribute 31 mac format ietf lower-case
```

```
radius-server attribute 31 send nas-port-detail mac-only
radius-server retransmit 2
radius-server timeout 3
radius-server vsa send accounting
radius-server vsa send authentication
!
radius-server host 203.0.113.115 auth-port 1812 acct-port 1813 key aaacisco
!
```

Sample Output for the show ipv6 mobile pmipv6 mag binding Command

```
MAG1# show ipv6 mobile pmipv6 mag binding

Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, Nai: mn0@example.com
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/1/0.3074
        [Binding][MN]: Hoa: 192.0.2.1, att: 4, llid: 0024.d78e.21a4
        [Binding][MN]: HNP: 0
        [Binding][MN][LMA]: Id: lma1
        [Binding][MN][LMA]: lifetime: 3600
        [Binding][MN][GREKEY]: Upstream: 5, Downstream: 5
```

Configuring an MN Profile as a Combination of the External Radius Server and the Default Profile

Cisco MAG provides the flexibility to define MN profiles as a combination of the external radius server configuration and the default profile configuration. This is useful in scenarios where a service provider (SP) must apply default profiles to the subscribers for whom there are no profiles defined on the external radius server.

The MAG attempts to extract the MN profile from the external radius server by sending an access-request message to the radius server. If the access-request message times out or if the radius server responds with an access-reject message, indicating that there is no profile for the requested MN, the MAG then applies the default profile configured on the MAG's access interface that connects to the MN.

```
!
ipv6 unicast-routing
!
ip dhcp pool pmipv6_dummy_pool
!
ipv6 mobile pmipv6-domain D1
 replay-protection timestamp window 200
 mn-profile-load-aaa
 lma lma1
  ipv6-address 2001:DB8:CAFE:1024::101
 nai default_subscriber_profile_A
  apn example_A.com
  lma lma1
 nai default_subscriber_profile_B
  apn example_B.com
  lma lma1
!
ipv6 mobile pmipv6-mag M1 domain D1
 discover-mn-detach poll interval 3600 timeout 10 retries 10
 address ipv6 2001:DB8:CAFE:1025::15
 interface GigabitEthernet 0/1/0.4001
  enable pmipv6 default default_subscriber_profile_B
 interface GigabitEthernet 0/1/0.3074
  enable pmipv6 default default_subscriber_profile_A
!
interface GigabitEthernet 0/1/0.3074
 description => Connected to access network
 encapsulation dot1Q 3074
 ip address 10.8.22.15 255.255.255.0
!
interface GigabitEthernet 0/1/0.4001
 description => Connected to access network
 encapsulation dot1Q 4001
 ip address 10.8.51.15 255.255.255.0
```

```
!
```

Sample Output for the show ipv6 mobile pmipv6 mag binding Command

```
MAG1# show ipv6 mobile pmipv6 mag binding

Total number of bindings: 1
----------------------------------------
[Binding][MN]: Domain: D1, Nai: 0024.d78e.21a4
        [Binding][MN]: State: ACTIVE
        [Binding][MN]: Interface: GigabitEthernet0/1/0.3074
        [Binding][MN]: Hoa: 192.0.2.1, att: 4, llid: 0024.d78e.21a4
        [Binding][MN]: HNP: 0
        [Binding][MN][LMA]: Id: lma1
        [Binding][MN][LMA]: lifetime: 3600
        [Binding][MN][GREKEY]: Upstream: 8, Downstream: 8
```

AAA Attributes in the Cisco Access Register

The following RADIUS attributes must be configured on the external RADIUS server to enable the deployment of PMIPv6 network-based mobility.

```
 Cisco-AVPair = mn-nai=mn0@example.com
 Cisco-AVPair = mn-service=ipv4
 Cisco-AVPair = home-lma-ipv6-address=2001:db8:cafe:1024::101
 Cisco-AVPair = home-lma-ipv4-address=10.8.24.101
 Cisco-AVPair = home-lma=lma1
 Cisco-AVPair = mn-apn=example.com
 Cisco-AVPair = cisco-mpc-protocol-interface=pmipv6
```

PMIPv6 Signaling and Call Flow

The following figures (figures 7, 8, 9, and 10) summarize the PMIPv6 signaling call flow that occurs when the MN performs the following actions:

- Authenticates in a Wi-Fi network
- Attaches to a MAG
- Obtains an IP address
- Sends traffic
- Performs inter-MAG mobility when retaining IP address continuity

- Detaches from the MAG when moving out of the Wi-Fi network

Figure 7: PMIPv6 Signaling for MN Attachment

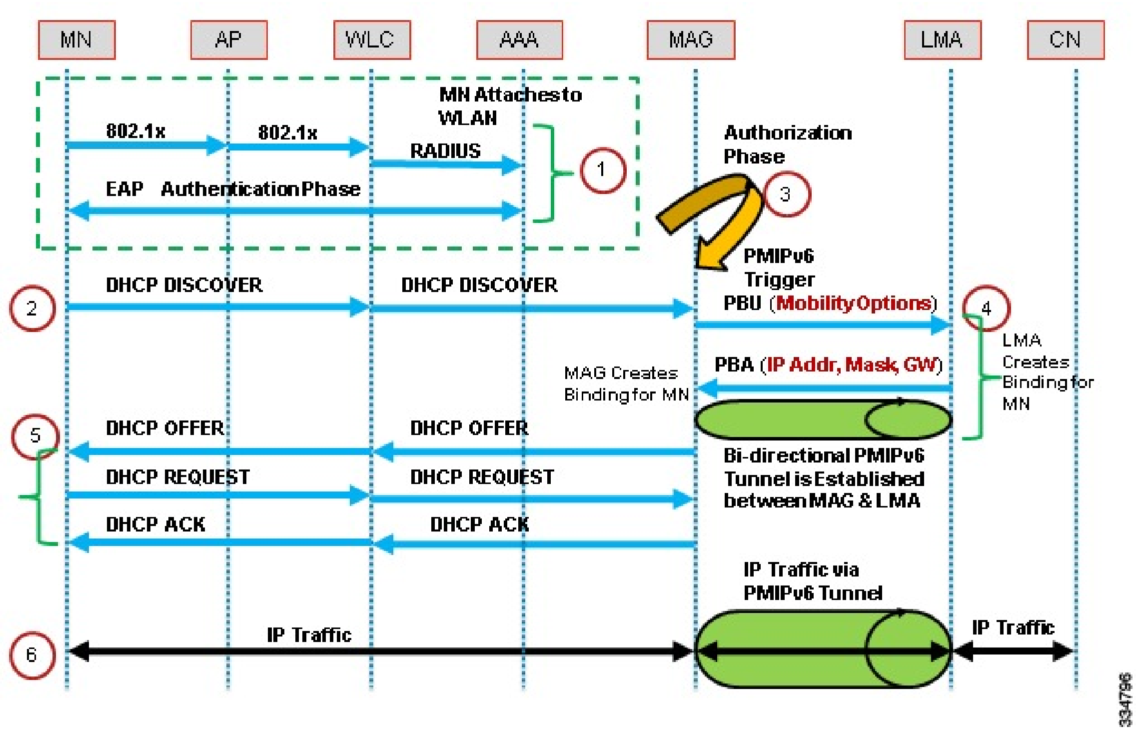


Figure 8: PMIPv6 Signaling for Session Maintenance

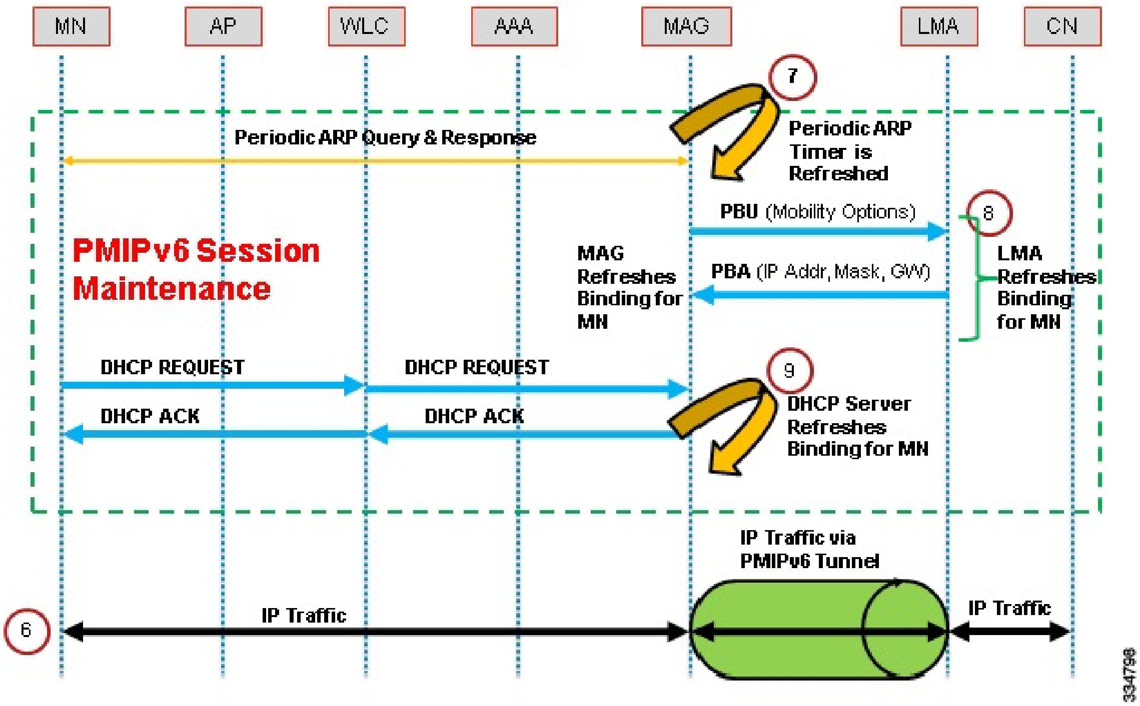


Figure 9: PMIPv6 Signaling for MN Detachment

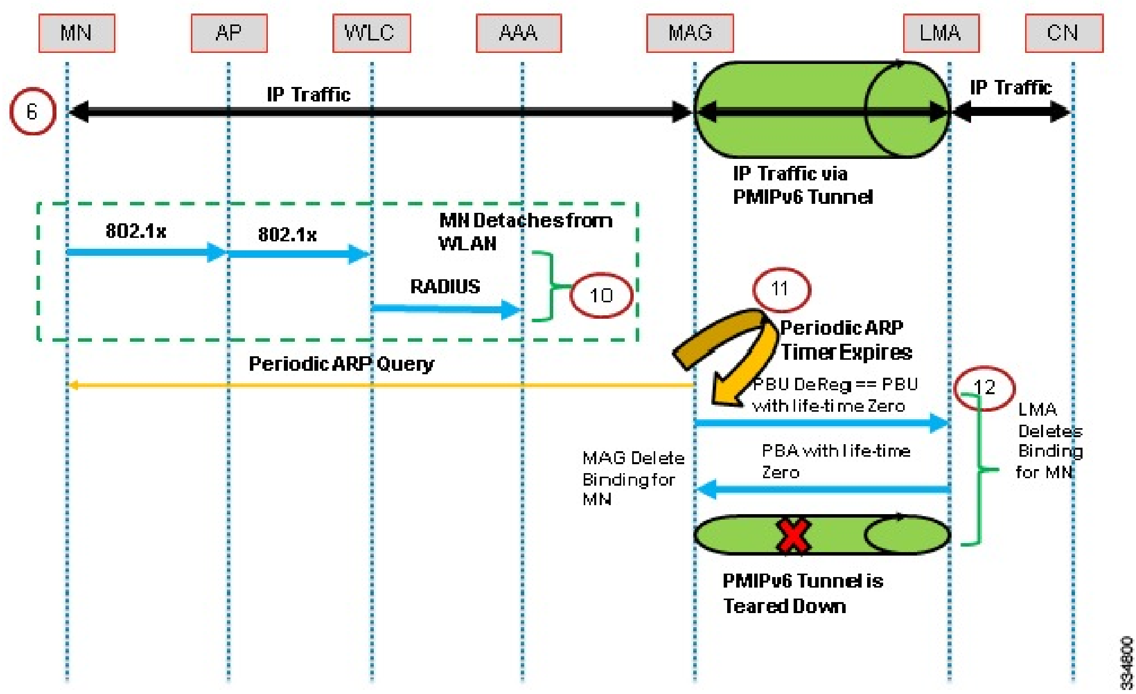
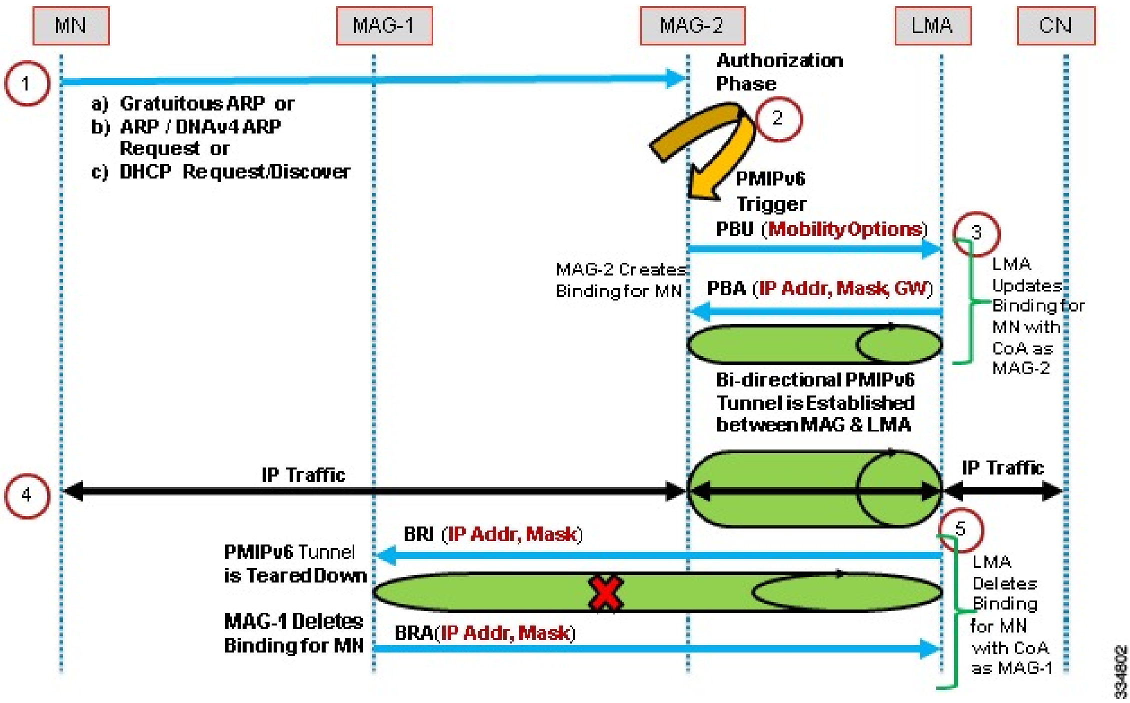


Figure 10: PMIPv6 Signaling for Inter-MAG Roaming



PMIPv6 MAG-Related Timers

The following table provides information about PMIPv6 MAG-related timers

Timer	**Default Value, in seconds**	**Purpose**	**Commands**
Detach Query Period	10	Specifies the Periodicity (X) of Address Resolution Protocol (ARP) Pooling. Periodic ARP query timer (X) is used to keep track of the MN attachment with MAG.	(config-ipv6-pmipv6-mag)# **discover-mn-detach** *seconds* *timeout-seconds* For example, the value of *seconds* is 100 and that of *timeout-seconds* is 10.
Detach Query Response Time	2	Specifies the ARP query response timeout (Y). The ARP query timeout period (Y) is used to keep track of the MN attachment with MAG.	(config-ipv6-pmipv6-mag)# **discover-mn-detach** *seconds* *timeout-seconds* For example, the value of *seconds* is 100 and that of *timeout-seconds* is 10.

Timer	Default Value, in seconds	Purpose	Commands
Registration Life Time	3600	Specifies the maximum lifetime permitted for a PBU entry on the MAG. However, the actual lifetime assigned to an MN is the minimum negotiated value between the LMA and the MAG. Note: The MAG also uses the negotiated value as the DHCP lease time when assigning an IP address to the MN.	(config-ipv6-pmipv6-mag)# **binding lifetime** *seconds*
BRI Init Delay Time	1	Specifies the minimum time for which an MAG must wait before retransmitting the Binding Revocation Indication (BRI) message. **Note** This timer is used for bulk revocation.	(config-ipv6-pmipv6-mag)# **bri delay min** *milliseconds*
BRI Max Delay Time	2	Specifies the maximum time for which a MAG must wait for the Binding Revocation Acknowledgment (BRA) message before retransmitting the BRI message.	(config-ipv6-pmipv6-mag)# **bri delay max** *milliseconds*
Refresh Time	300	Specifies the PBU entry refresh interval.	(config-ipv6-pmipv6-mag)# **binding refresh-time** *seconds*
Refresh Retransmit Init time	1	Specifies the minimum time for which an MAG must wait before retransmitting the PBU.	(config-ipv6-pmipv6-mag)# **binding max retx-time** *seconds*
Refresh Retransmit Max time	32	Specifies the maximum time for which a MAG must wait for the PBA.	(config-ipv6-pmipv6-mag)# **binding max-retx-time** *seconds*

Troubleshooting Commands

Use the following commands to troubleshoot LMA problems in Cisco ASR 5000 Series Aggregation Services Routers:

- **monitor protocol** (select “48” for Mobile IPv6, and 5 for Verbosity Level

- See the *Cisco ASR 5000 Command Reference Guide* for more debug commands.

Use the following commands to troubleshoot MAG problems in Cisco ASR 1000 Series Aggregation Services Routers and Cisco Integrated Service Routers:

- The following are the control plane **debug** commands:
  - **debug ipv6 mobile mag info**
  - **debug ipv6 mobile mag event**
  - **debug ip dhcp server events**
  - **debug ipv6 mobile packets**
  - **debug ip dhcp server packet detail**
  - **debug arp**
  - **debug radius**
- The following are the date plane **debug** commands:
  - **debug tunnel**
  - **debug ip cef packet** *interface* input rate 0
  - **debug ip cef packet** *interface* output rate 0

Use the following commands to troubleshoot problems in Cisco 5508 WLC:

- **debug dhcp message enable**
- **debug dhcp packet enable**
- **debug arp all enable**
- **debug dot1x events**

Show Commands

You can use the following **show** commands to troubleshoot LMA problems in Cisco ASR 5000 Series Aggregation Services Routers:

- **show ipv6 interface**
- **show lma-service session**
- **show lma statistics**

You can use the following **show** commands to troubleshoot MAG problems in MAG in Cisco ASR 1000 Series Aggregation Services Routers and Cisco Integrated Service Routers:

- **show ip dhcp binding**
- **show ipv6 mobile pmipv6 mag binding**
- **show ipv6 mobile pmipv6 mag tunnel**
- **show ipv6 mobile pmipv6 mag globals**

- **show ipv6 mobile pmipv6 mag stats**
- **show route-map dynamic**
- **show platform software route-map RP active map (ASR1000)**

You can use the following **show** commands troubleshoot problems in Cisco 5506 WLC:

- **show interface summary**
- **show route summary**
- **show dhcp proxy**

Additional References

The following sections provide references related to the GRE for Mobile Networks feature.

Related Documents

Related Topic	Document Title
Mobile IP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility , Release 12.3 T
Mobile IP commands and configuration tasks related to mobile networks	http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftmbrout.htm Cisco Mobile Networks feature document, Release 12.2(4)T and 12.2(13)T
Additional information about GRE keepalives	*Generic Routing Encapsulation (GRE) Tunnel Keepalive* feature document, Release 12.2(8)T
Information on configuring quality of service (QoS) with GRE	Quality of Service Options on GRE Tunnel Interfaces

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Glossary

CN—Correspondent Node. The device that the mobile node (MN) is communicating with, such as a web server. A correspondent node may either be mobile (for example, another mobile node [MN]), or be stationary (for example, a server).

LMA—Local Mobility Anchor. LMA is the home agent for the mobile node (MN) in a PMIPv6 domain. LMA is the topological anchor point for the MN's home network prefix and is the entity that manages the MN's binding state.

MAG—Mobile Access Gateway. MAG is a function on an access router that manages mobility-related signaling for an MN that is attached to its access link. The MAG is responsible for tracking MN movements to and from the access link.

NAI—Network Access Identifier. A NAI is the user identity submitted by the client during network access authentication. When roaming, the purpose of the NAI is to identify the user as well as to assist in the routing of the authentication request. The standard syntax is "user@realm" or as defined in RFC 4282.

MN—Mobile Node. MN is an IP host, an MN, or a router, whose mobility is managed by the network. The MN can be an IPv4-only node, IPv6-only node, or a dual-stack node. The MN is not required to participate in any IP mobility-related signaling for achieving mobility for an IP address that is obtained in that PMIPv6 domain.

PMIPv6 domain—Proxy Mobile IPv6 domain. A network where the mobility management of an MN is handled using the PMIPv6 protocol. The domain consists of network entities, such as MAGs and LMAs, between which Proxy Binding is maintained on behalf of the MNs.

PBU—Proxy Binding Update. PBU is the request message sent by a MAG to an LMA for establishing a binding between an MN's home network prefix and the MAG to which the MN is attached.

PBA—Proxy Binding Acknowledgement. PBU is the reply message from an LMA in response to a PBU from the MAG.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands