Client Data Tunneling

Ethernet over GRE Tunnels

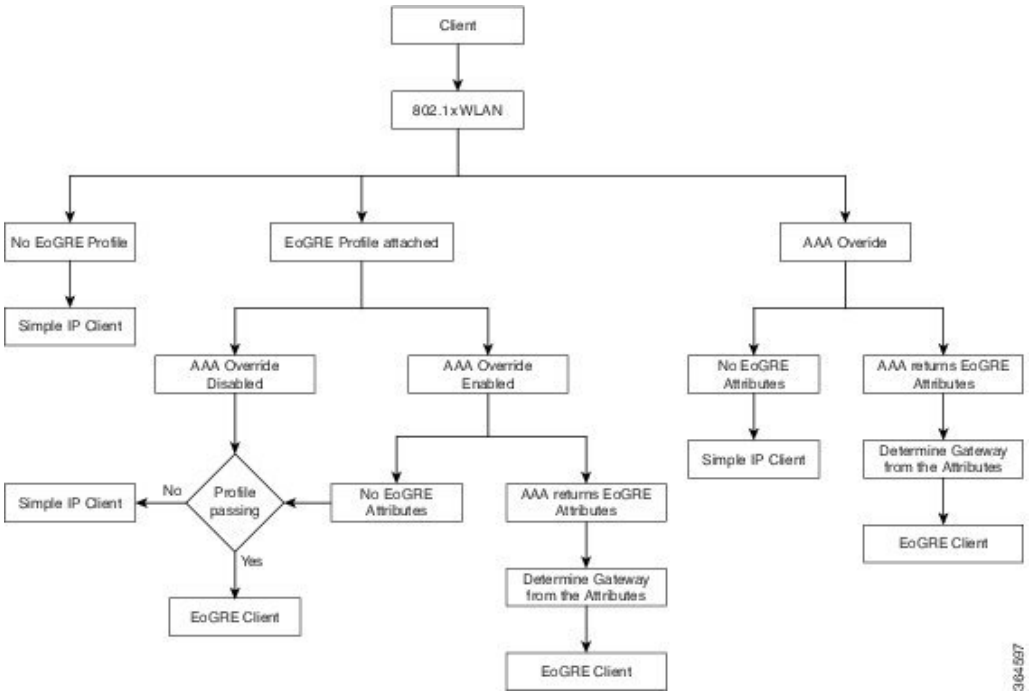
Ethernet over GRE (EoGRE) is an aggregation solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host's traffic is terminated and subscriber sessions are initiated for the end host.

High Availability (HA) is supported for EoGRE IPv4 and IPv6 tunnel configuration. In addition, Client SSO is supported for IPv4 and IPv6 EoGRE tunnel clients.

For more information about designing and deploying EoGRE on controller and Cisco FlexConnect APs, see the EoGRE Deployment Guide.

EoGRE on 802.1X Authentication-based WLANs

Figure 1: Workflow of EoGRE on 802.1X Authentication-based WLANs

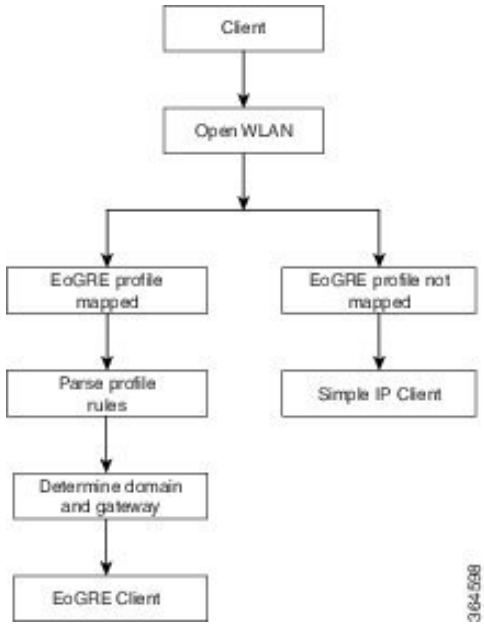


802.1X Authentication	Switching	AP Mode	EoGRE	SimpleIP
Central+No FlexConnect Backup RADIUS Server	Local	Connected	Clients can join as EoGRE.	Clients can join as SimpleIP.
Central+No FlexConnect Backup RADIUS Server	Local	Standalone	New clients cannot join; existing clients should work.	New clients cannot join; Existing clients should work.
Central+No FlexConnect Backup RADIUS Server	Local	Boot in standalone	Clients cannot join.	Clients cannot join.
Local AP Auth+No FlexConnect Backup RADIUS Server	Local	Connected	Clients become SimpleIP.	Clients join as SimpleIP.
Local AP Auth+No FlexConnect Backup RADIUS Server	Local	Standalone	Clients become SimpleIP.	Existing and new clients work as expected.
Local AP Auth+No FlexConnect Backup RADIUS Server	Local	Boot in standalone	Clients become SimpleIP.	Clients can join.

802.1X Authentication	Switching	AP Mode	EoGRE	SimpleIP
Central+FlexConnect Backup RADIUS Server	Local	Connected	Clients join as EoGRE.	Existing and new clients work as expected.
Central+FlexConnect Backup RADIUS Server	Local	Standalone	Existing clients continue as EoGRE; new Client joins as SimpleIP.	Existing and new clients work as expected.
Central+FlexConnect Backup RADIUS Server	Local	Boot in standalone	Clients become SimpleIP.	Existing and new clients work as expected.

EoGRE on Open Authentication-based WLANs

Figure 2: Workflow of EoGRE on Open Authentication-based WLANs



Note For open WLANs, the EoGRE profile must have only one rule, which is a * rule. Mapping of a profile that has multiple rules to an open authentication WLAN is not supported. All clients should be EoGRE clients.

Open Authentication	Switching	AP Mode	EoGRE
Central	Local	Connected	Client will join as EoGRE.

Open Authentication	Switching	AP Mode	EoGRE
Central	Local	Standalone	New clients cannot join. Existing clients should work.
Central	Local	Boot in Standalone	Clients cannot join.

Changing the Tunnel Source

Prior to Release 8.2, the management IP address was used as the tunnel endpoint. Release 8.2 has enabled the specification of any L3 dynamic interface other than the management interface as a tunnel endpoint, if need be.

Support for IPv6

In Release 8.3, support is added for client IPv6 traffic and IPv6 address format for the EoGRE tunnel gateway. Client IPv6 traffic is supported on both IPv4 and IPv6 EoGRE tunnels. A maximum of eight different client IPv6 addresses are supported per client. Controllers send all the client IPv6 addresses that they have learned to the Accounting server in the accounting update message. All RADIUS or Accounting messages exchanged between controllers and tunnel gateways or RADIUS servers are outside the EoGRE tunnel.

CAPWAP	EoGRE	Remarks
CAPWAPv4	EoGREv4	Accounting IP expected to be CAPWAPv4 (controller IP)
CAPWAPv4	EoGREv6	Accounting IP expected to be CAPWAPv4 (controller IP)
CAPWAPv6	EoGREv4	Accounting IP expected to be CAPWAPv6 (controller IP)
CAPWAPv6	EoGREv6	Accounting IP expected to be CAPWAPv6 (controller IP)

One-to-One Mapping of WLAN with EoGRE VLAN

The EoGRE implementation for open WLANs is limited to 10 WLANs per VLAN per controller. This limitation can be overcome by having a one-to-one mapping between open WLANs and EoGRE VLANs.

A one-to-one mapping of a WLAN with an EoGRE VLAN can be achieved by overriding the EoGRE VLAN configuration within the WLAN. All the existing rules are still applicable, but when the EoGRE VLAN override option is enabled, the VLAN ID that you specify will be overridden with the EoGRE VLAN ID that is configured in the tunnel profile that is mapped to the WLAN.

The order of precedence is as follows:

1. If the AAA override option is enabled on the WLAN, the AAA values are applied.
2. If the EoGRE VLAN configuration override option is enabled, the EoGRE VLAN configuration values are applied on the VLAN ID that is specified.
3. Network Access Identifier (NAI) is matched in the EoGRE profile rule.

Related Documentation

- Ethernet over GRE Tunnels
- Service Provider Wi-Fi: Support for Integrated Ethernet Over GRE
- Intelligent Wireless Access Gateway Configuration Guide

Restrictions for EoGRE Tunneling

- On Cisco vWLC, EoGRE tunneling is supported only in local switching mode.
- EoGRE feature is not supported in Cisco Aironet 702, 801, 802, 1520 Access Points.
- It is not possible to edit or delete a tunnel profile if the profile is associated with a WLAN. You must first dissociate the profile from the WLAN and then edit or delete the profile.
- It is not possible to edit or delete a tunnel gateway if the gateway is already associated with a domain. You must first dissociate the tunnel gateway from the domain and then edit or delete the tunnel gateway.
- It is not possible to edit or delete a domain if the domain is already associated with a tunnel profile rule. You must first dissociate the domain from the tunnel profile rule and then edit or delete the domain.
- If the domain is modified on the fly, the client associated with the domain is deauthenticated.
- We recommend that you do not have firewall that could block ICMP packets.
- Tunnel Gateway (TGW) as AAA and RADIUS realm feature on WLAN should not be used together.
- Tunnel Gateway (TGW) as AAA is not supported on EoGRE for FlexConnect APs.
- Tunnel EoGRE gateway statistics are not synced to the standby controller.
- Due to SNMP limitation, tunnel gateway names can be up to 127 characters only.
- For open WLANs, the profile must have only one rule, which is a * rule. Mapping of a profile that has multiple rules to an open authentication WLAN is not supported.
- EoGRE client gets IPV6 address from local switching VLAN.
- Broadcast/Multicast traffic on Local Switching VLAN reaches EoGRE clients.
- FlexConnect+Bridge Mode is not supported.
- Standalone mode: EoGRE client Fast Roaming is not supported.
- WebAuth is not supported.
- FlexConnect AP Local Authentication is not supported.
- FlexConnect AP Backup RADIUS server is not supported.
- EoGRE client with Static IP is not supported.
- FlexConnect ACL on the WLAN does not work for EoGRE clients.
- After Fault Tolerance, client type is SimpleIP. It is changed to EoGRE after a period of 30 seconds.
- MTU of AP gateway should be 1500 bytes.

- Lightweight APs support Path MTU only for EoGREv6. For EoGREv4, it is not supported.
- For EoGRE clients, the TrustSec SGT/Policy Enforcement might not work as expected because it is not supported for any tunneled traffic, including the Layer3 mobility tunnel.

  For tunneled traffic, the source SGT tag is not encoded in the CMD header (CMD header itself not added); the unknown SGACL policy (0,DGT) is applied at the policy enforcement point.
- EoGRE IPv6 Restrictions:
  - EoGRE client gets IPv6 address from local switching VLAN
  - DHCP Option 82 configuration is not supported on IPv6 clients.
  - Applications such as RADIUS, FTP, TFTP, SFTP, LDAP, SXP, syslog, and so on, are supported on only management IPv6 address.
  - Dynamic IPv6 AP-manager interface is not supported.
  - Dynamic interface with IPv6 supports only as tunnel interface.
  - Maximum number of dynamic interface to which IPv6 address can be assigned is16.
  - The IPv6 link local addresses are common for all switched virtual interfaces (SVI) on a switch. Due to this, configuring an IPv6 address on dynamic address fails. To overcome this issue, you must explicitly configure link local address on the uplink switch for SVI. Each SVI should have unique link local address configuration.
  - The IP packets on IPv6 tunnels has a maximum size limit of 1280 bytes on controller.
- When AAA override for a WLAN is enabled, the domain passed through AAA server should be attached to a second WLAN. This is applicable for APs that are in Local and FlexConnect modes. This is required so that the gateways mapped to the domain in AAA server become operational in Local mode in controller and are downloaded to AP in FlexConnect mode.
- Clients connecting to Wave 2 APs get an IP address from the native VLAN in the conditions described in CSCvu46349.

Configuring EoGRE on the Controller (GUI)

Procedure

Step 1 Create tunnel gateways and configure heartbeats:

a) Choose **Controller** > **Tunneling** > **EoGRE**.

b) Select the **Interface Name**.

Interface present on the controller to be used as a source of the tunnel.

c) Set the **Heartbeat Interval**. The default interval is 60 seconds.

The controller sends keepalive pings every 60 seconds.

d) Set **Max Heartbeat Skip Count**. The default value is set to 3.

If the TGW does not reply after three keepalive pings, the controller marks the TGW as nonoperational. The number of skip count decides how many times the TGW can skip consecutive replies, before the controller knows that the TGW is nonoperational.

e) Specify a **TGW Name**.
f) Specify the **TGW IP Address**.

Both IPv4 and IPv6 address formats are supported. You can create up to 10 such tunnel gateways.

g) Specify a **Domain Name**.
h) Specify the tunnel gateway that you created and its role as either primary/active or secondary/standby gateway, and click **Add**.

If the tunnel gateway is reachable, the state should be displayed as UP under the **TGW List**.

Click **Get Statistics** to view tunnel gateway statistics.

Domain represents a virtual collection of one or more tunnels used for redundancy purposes. Up to 16 tunnels can exist in a domain. If one tunnel fails, the traffic is redirected to another TGW.

In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active gateway. Clients will have to associate again with the secondary gateway. During and after failover, controller continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6.

Step 2 Create a tunnel profile:

a) Choose **Controller** > **Tunneling** > **Profiles**.
b) Specify a profile name and click **Add**.

The profile name is displayed under **Profile List**.

Step 3 Define a tunnel profile rule:

a) Click the tunnel profile that you created.
b) Under the **Rule** tab, to map a specific realm to the profile, enter the realm name. A realm is a string after @, for example, user_name@realm. To match any **Realm**, use *, which means all realms are accepted.
c) Choose **Tunnel Type** as **EoGRE**.
d) Set **VLAN** to **0**.
e) Choose the **Gateway Domain** that you created in Step 1.
f) Click **Add** to add the rule to the tunnel profile.

Step 4 Specify tunnel parameters:

a) Under the **Tunnel Parameters** tab, check the **Gateway as AAA Proxy** and **Gateway as Accounting Proxy** (optional) check boxes to configure a tunnel gateway as a AAA proxy and as an Accounting proxy.
b) (Optional) Check the **DHCP Option-82** check box.

Note DHCP Option 82 configuration is not supported on IPv6 clients.

c) Choose the DHCP Option 82 format as either **Binary** or **ASCII**.
d) Specify the **DHCP Option 82 Delimiter**. The default is ;.
e) Specify the **Circuit-ID** and **Remote-ID** information. You can choose up to five fields each and sort them accordingly.
f) Click **Apply**.

Step 5 Create RADIUS Authentication or Accounting servers or both by specifying the tunnel gateway IP addresses that you specified in Step 1 as the server IP addresses, and enable **Tunnel Proxy**.

For instructions on how to create RADIUS servers, see the *Configuring RADIUS* chapter under *Security Solutions*.

Step 6 Associate the tunnel profile to the WLAN:

a) Choose **WLANs** and click the WLAN ID to which the tunnel profile has to be associated.
b) In the **Advanced** tab, under **Tunneling**, choose the **Tunnel Profile**.
c) (Optional) You can choose to enable AAA Override for the WLAN, which means that the controller is allowed to accept the attributes returned by the RADIUS server.
d) Save the configuration.

Step 7 Verify if the tunnel is correctly configured:

a) Choose **Controller** > **Tunneling** > **Profiles**.
b) Verify if the profile name is mapped to the correct WLAN.

Step 8 Verify the gateway statistics:

a) Choose **Controller** > **Tunneling** > **EoGRE**.
b) Click **Get Statistics**.

Configuring EoGRE on the Controller (CLI)

Procedure

- Configure keepalive ping parameters by entering these commands:
  - **config tunnel eogre heart-beat interval** *seconds*
  - **config tunnel eogre heart-beat max-skip-count** *number*
- Add new EoGRE tunnel gateways, or delete or modify existing gateways, by entering these commands:
  - **config tunnel eogre gateway add** *name* {**ipv4-address** | **ipv6-address**} *ip-addr*
  - **config tunnel eogre gateway delete** *name*
  - **config tunnel eogre gateway modify** *name* {**ipv4-address** | **ipv6-address**} *ip-addr*
- Configure EoGRE tunnel gateway domain by entering these commands:
  - **config tunnel eogre domain** {**create** | **delete**} *domain-name*
  - **config tunnel eogre domain** {**add** | **remove**} *domain-name gateway-name*
- Add primary gateway name to a domain by entering the following command. Secondary gateway is selected automatically after the primary gateway is added.
  - **config tunnel eogre domain primary** *domain-name gateway-name*

    In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active gateway. Clients will have to associate again with the secondary gateway. During and after failover, controller continues to ping the primary gateway.

When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6. This feature is supported on all Wave 1 and Wave 2 APs that are supported in this release.

- Configure tunnel profiles by entering these commands:
  - **config tunnel eogre profile** {**create** | **copy** | **delete** | **rule** | **eogre**}

  Follow the instructions displayed in the CLI to configure each parameter.
- Configure the gateway as AAA proxy by entering these commands:
  - **config tunnel profile eogre** *profile-name* **gateway-radius-proxy** {**enable** | **disable**}
  - **config tunnel profile eogre** *profile-name* **gateway-radius-proxy accounting** {**enable** | **disable**}
- Configure DHCP Option 82 for the tunnel profile by entering these commands:

Note DHCP Option 82 configuration is not supported on IPv6 clients.

  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82** {**enable** | **disable**}
  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82 format** {**binary** | **ascii**}
  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82 delimiter** *character*
  - **config tunnel profile eogre** *profile-name* **DHCP-Opt-82** {**circuit-id** | **remote-id**} *supported-parameter*
- Configure EoGRE tunnel interface by entering the following command:
  - **config tunnel eogre interface** *interface-name*

Note Before configuring the interface for the tunnel source, disable the WLAN associated with the interface.

- View details about EoGRE tunneling by entering these commands:
  - **show tunnel eogre** {**domain** | **gateway**} **summary**

Note The **show tunnel eogre gateway summary** command lists details of only the FlexConnect central switching clients and Local Mode AP clients. To view the details of FlexConnect local switching clients, use the **show ap eogre gateway** *ap-name* command.

  - **show tunnel eogre summary**
  - **show tunnel eogre statistics**

- **show tunnel eogre gateway statistics**
- **show tunnel profile summary**
- **show tunnel profile detail** *profile-name*

Configuring EoGRE for FlexConnect APs (GUI)

- Ensure that the APs are in FlexConnect mode.
- The tunnel configurations made for the controller also applies to Cisco FlexConnect APs when the tunnel profile is associated with a WLAN.
- Path MTU discovery is supported on FlexConnect APs

Procedure

Step 1 Choose **WLANs** > **WLANs**.

Step 2 Click the WLAN ID.

Step 3 In the **Advanced** tab under **FlexConnect**, enable **FlexConnect Local Switching**.

Note Only FlexConnect Local Switching option has to be configured on the FlexConnect AP or FlexConnect Group to enable FlexConnect AP tunnel.

Step 4 Save the configuration.

Step 5 To view the statistics per gateway, choose **Wireless** > **All APs** > **AP name** > **FlexConnect** > **Tunnel Gateway List** and click **Get Statistics**.

Configuring EoGRE for FlexConnect APs (CLI)

- Ensure that the APs are in FlexConnect mode.
- The tunnel configurations made for controller also applies to Cisco FlexConnect APs when the tunnel profile is associated with a WLAN.

Procedure

Step 1 Enable Local Switching on FlexConnect APs associated with a WLAN by entering this command:
config wlan flexconnect local-switching *wlan-id* **enable**

Step 2 Monitor the EoGRE configurations by entering this command:
show ap eogre {**domain** | **gateway**} *ap-name*

Note The **show ap eogre gateway** *ap-name* command lists details of FlexConnect local switching clients. To view the details of FlexConnect central switching clients and Local Mode AP clients, use the **show tunnel eogre gateway summary** command.

To see the tunnel gateway statistics in controller, use the **show tunnel eogre gateway statistics** command.

To see the tunnel gateway statistics in AP, use the **show ap eogre statistics** *ap-name* command.

One-to-One Mapping of WLAN with EoGRE VLAN (GUI)

Before you begin

- Ensure that you have created an EoGRE tunnel profile.
- Ensure that the WLAN is in disabled state before you proceed with this procedure.

Procedure

Step 1 Choose **WLANs** and click the WLAN ID.

Step 2 Click the **Advanced** tab and scroll down to the **Tunneling** section.

Step 3 Select the tunnel profile.

Step 4 Check the **EoGRE VLAN Override** check box to enable the EoGRE VLAN override feature on the WLAN.

Step 5 In the **EoGRE VLAN Override ID** field, enter the VLAN ID that should be overridden with the EoGRE VLAN ID configured in the tunnel profile.

Step 6 Save the configuration.

One-to-One Mapping of WLAN with EoGRE VLAN (CLI)

Before you begin

- Ensure that you have created an EoGRE tunnel profile.
- Ensure that the WLAN is in disabled state before you proceed with this procedure.

Procedure

Step 1 Enable the EoGRE VLAN override feature on a WLAN by entering this command:

config wlan tunnel eogre-vlan-override *wlan-id* **enable**

Step 2 Configure the VLAN ID that should be overridden with the EoGRE VLAN ID configured in the tunnel profile by entering this command:

config wlan tunnel eogre-vlan-override *wlan-id vlan-id*

Step 3 Monitor the configuration on the WLAN by entering this command:

show wlan *wlan-id*

Step 4 View the client details, including the EoGRE VLAN ID being used, by entering this command:

show client detail *client-mac-addr*

What to do next

You can troubleshoot issues related to this feature by using the **debug client** *client-mac-addr* command:

Proxy Mobile IPv6

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in an IP mobility-related signaling scenario. The mobility entities in the network track the movements of the mobile node, initiate mobility signaling, and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The Cisco Wireless Controller implements the MAG functionality.

For PMIPv6 clients, the controller supports both central web authentication and local web authentication.

PMIPv6 is supported for clients with 802.1X authentication. After the 802.1X authentication is complete, a Cisco AP starts PMIPv6 signaling for the corresponding client.

MAG on AP is supported on FlexConnect mode APs in a locally switched WLAN. For PMIPv6 clients, all the data traffic from clients is tunneled to the LMA in the Generic Routing Encapsulation (GRE) tunnel established between the MAG and the LMA. Similarly, all the packets received from the LMA in the GRE tunnel are routed to the wireless client.

After the 802.1X authentication is complete, the Cisco AP starts PMIPv6 signaling for the client. In a MAG-on-AP scenario, the Cisco AP starts PMIPv6 signaling. In a MAG-on-controller scenario, the controller starts PMIPv6 signaling.

Fast Roaming with Central Association

Fast roaming is supported when central association is enabled on WLANs. When central association is enabled, all key cachings occur on the controller. When a PMIPv6 client roams from one AP to another on the same mobility domain, the controller sends the PMIPv6 parameters of the client to a new AP in PMIPv6 tunnel payload to start PMIPv6 signaling. Also, the controller sends the PMIPv6 tunnel payload to the old AP to tear down the Generic Routing Encapsulation (GRE) tunnel for the client with the LMA. Fast roaming is supported in both intra-controller and inter-controller roaming scenarios and mobility messages are added to send PMIPv6 parameters from one controller to another during roaming.

Client roaming from third-party MAG to Cisco AP-MAG is similar to a new client joining; a client roaming away from a Cisco AP-MAG to a third-party MAG is similar to a client leaving, and therefore, requires no special handling.

With Cisco APs in FlexConnect mode, all reassociation requests from clients are handled by the Cisco APs themselves. However, if central association is enabled, all reassociation requests are handled by the controller.

Dynamic AAA Attributes

The dynamic AAA attributes that are supported are listed below:

Type	Attribute	Value	Description	Controller Behavior
89	Chargeable-User-Identity	String	Chargeable User Identity RFC-4372	If present, the attribute is copied into the MSCB and used in accounting reports; no other usage.
26/104 15/13	3GPP-Charging-Characteristics	String	Rules for producing charging information	If present, the attribute is copied to the MSCB and passed to the L2 attach triggers to the MAG. The attribute is used to send to the local mobility anchor (LMA) as an option in the proxy binding update (PBU).
26/9/1	Cisco-Service-Selection	String	Service Identifier (APN)	If present, the attribute overrides the locally configured APN.
26/9/1	Cisco-Mobile-Node-Identifier	String	Mobile Node Identifier	If present, the attribute is used for the network access identifier (NAI).
26/9/1	Cisco-MSISDN	String	Mobile Subscriber ISDN Number	If present, the attribute is used to pass to MAG code with a new parameter in the L2 attach trigger.
26/9/1	Cisco-MPC-Protocol-Interface	ENUM: "none" "PMIPv6" "GTPv1" "PMIPv4"	Mobile Node Service Type	Only IPv4 and simple IP clients are supported.
26/9/1	Cisco-URL-REDIRECT	String	HTTP URL of the Captive Portal	Existing attribute used for web authentication; no changes required.
26/9/1	Cisco-URL-REDIRECT-ACL	String	Specific Redirect Rule	Existing attribute used for web authentication; no changes required.
26/9/1	Cisco-Home-LMA-IPv4-Address	IP Address	Mobile node's Home LMA IPv4 address	If present, this attribute is used as the LMA for the client. **Note** The GRE tunnel creation is still static.

PMIPv6 AAA Attributes

The PMIPv6 AAA attributes that are supported are listed below:

Type	Attribute	Value	Description	Controller Behavior
89	Chargeable-User-Identity	String	Chargeable User Identity RFC-4372	If present, the attribute is copied into the MSCB and used in accounting reports; no other usage.
26/104 15/13	3GPP-Charging-Characteristics	String	Rules for producing charging information	If present, the attribute is copied to the MSCB and passed to the L2 attach triggers to the MAG. The attribute is used to send to the local mobility anchor (LMA) as an option in the proxy binding update (PBU).
26/9/1	mn-network	String	Service Identifier (APN)	If present, the attribute overrides the locally configured APN (Mandatory)
26/9/1	mn-nai	String	Mobile Node Identifier	If present, the attribute is used for the network access identifier (NAI).
26/9/1	cisco-msisdn	String	Mobile Subscriber ISDN Number	If present, the attribute is used to pass to MAG code with a new parameter in the L2 attach trigger.
26/9/1	cisco-mpc-protocol-interface	ENUM: "None" "PMIPv6"	Mobile Node Service Type	Only PMIPv6 clients are supported. (Mandatory)
26/9/1	home-lma-ipv4-address	IPv4 Address	Mobile node's Home LMA IPv4 address	If present, this attribute is used as the LMA for the client. The LMA should also be configured in controller (Mandatory). **Note** The GRE tunnel creation is still static.
26/9/1	mn-service	ENUM: "IPv4"	Type of client	Only IPv4 is supported.

Changing the Tunnel Endpoint

In releases prior to Release 8.2, the management IP address was used as the tunnel endpoint. Release 8.2 added the capability to specify a tunnel endpoint, other than management interface.

Note This feature currently supports EoGRE and PMIPv6 types of tunnels for mobility tunnel termination.

Restrictions on Proxy Mobile IPv6

- IPv6/dual stack clients are not supported. Only IPv4 is supported with PMIPv6.
- You must enable DHCP Proxy before you can connect to a PMIPv6-enabled WLAN.

- PMIPv6 is not supported on local switching WLANs with FlexConnect mode APs. PMIPv6 MAG on AP is supported only when AP is in FlexConnect mode and WLAN is configured for FlexConnect Local Switching. If the WLAN is configured for Central Switching, MAG on controller is used.
- PMIPv6 on FlexConnect ACL with local switching is not supported.
- MAG on AP is not supported for clients in a centrally switched WLAN.
- IPv6 addresses on dynamic interfaces are not supported.
- Intercontroller roaming from PMIPv6 to non-PMIPv6 WLANs is not supported.

Configuring Proxy Mobile IPv6 (GUI)

Procedure

Step 1 Choose **Controller > PMIPv6 > General**. The **PMIPv6 General**window is displayed.

Step 2 Enter the values for the following parameters:

- **Domain Name**—Name of the PMIPv6 domain. The domain name can be up to 127 case-sensitive, alphanumeric characters.
- **MAG Name**—Name of the MAG.
- **Interface**—Interface on the the controller used as a source for PMIPv6 tunneling.
- **MAG APN**—Access Point Name (APN) if you have subscribed to a MAG.

  MAG can be configured for one of the following roles:

  - 3gpp—Specifies the role as 3GPP (Third Generation Partnership Project standard)
  - lte—Specifies the role as Long Term Evolution (LTE) standard
  - wimax—Specifies the role as WiMax
  - wlan—Specifies the role as WLAN

  By default, the MAG role is WLAN. However, for lightweight access points, the MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.
- **Maximum Bindings Allowed**—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 and 40000.
- **Binding Lifetime**—Lifetime, in seconds, of the binding entries in the controller. The valid range is between 10 and 65535. The default value is 3600. The binding lifetime should be a multiple of 4.
- **Binding Refresh Time**—Refresh time, in seconds, of the binding entries in the controller. The valid range is between 4 and 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4.
- **Binding Initial Retry Timeout**—Initial timeout, in milliseconds, between the Proxy Binding Updates (PBUs) when the controller does not receive the Proxy Binding Acknowledgments (PBAs). The valid range is between 100 and 65535. The default value is 1000.
- **Binding Maximum Retry Timeout**—Maximum timeout between the PBUs when the controller does not receive the PBAs. The valid range is between 100 and 65535. The default value is 32000.

- **Replay Protection Timestamp**—Maximum amount of time, in milliseconds, difference between the timestamp in the received PBA and the current time of the day. The valid range is between 1 and 255. The default value is 7.
- **Minimum BRI Retransmit Timeout**—Minimum amount of time, in milliseconds, that the controller waits for before retransmitting the BRI message. The valid range is between 500 and 65535. The default value is 1000.
- **Maximum BRI Retransmit Timeout**—Maximum amount of time, in milliseconds, that the controller waits for before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 and 65535. The default value is 2000.
- **BRI Retries**—Maximum number of times that the controller retransmits the BRI message before receiving the Binding Revocation Acknowledgment (BRA) message. The valid range is between 1 to 10. The default value is 1.

Step 3 Click **Apply**.

Note To clear your configuration, click **Clear Domain**.

Step 4 To create the LMA, follow these steps:

a) Choose **Controller > PMIPv6 > LMA** and click **New**.
b) Enter the values for the following parameters:
   - **Member Name**—Name of the LMA connected to the controller.
   - **Member IP Address**—IP address of the LMA connected to the controller.
c) Click **Apply**.

Step 5 To create a PMIPv6 profile, follow these steps:

a) Choose **Controller > PMIPv6 > Profiles** and click **New**.
b) In the **PMIPv6 Profile > New** window, enter the values for the following parameters:
   - **Profile Name**—Name of the profile.
   - **Network Access Identifier**—Name of the Network Access Identifier (NAI) associated with the profile.
   - **LMA Name**—Name of the LMA to which the profile is associated.
   - **Access Point Node**—Name of the access point node; APN identifies a particular routing domain for user traffic.
c) Click **Apply**.

Step 6 To configure PMIPv6 parameters for a WLAN, follow these steps:

a) Choose **WLANs > WLAN ID**. The **WLANs > Edit** window is displayed.
b) Click the **Advanced** tab.
c) Under **PMIP**, from the **PMIP Mobility Type** drop-down list, choose the mobility type from the following options:
   - **None**—Configures the WLAN with simple IP
   - **PMIPv6**—Configures the WLAN with only PMIPv6

d) From the **PMIP Profile** drop-down list, choose the PMIP profile for the WLAN.
e) In the **PMIP Realm** field, enter the default realm for the WLAN.
f) Click **Apply**.

Step 7 Click **Save Configuration**.

Configuring Proxy Mobile IPv6 (CLI)

Procedure

Step 1 Configure a PMIPv6 domain name by entering this command:

config pmipv6 domain *domain-name*

Note This command also enables the MAG functionality on the Cisco Wireless Controller.

Step 2 Configure MAG by using these commands:

- Configure the maximum binding update entries that are allowed by entering this command:

  config pmipv6 mag binding maximum *units*

- Configure the binding entry lifetime by entering this command:

  config pmipv6 mag lifetime *units*

- Configure the binding refresh interval by entering this command:

  config pmipv6 mag refresh-time *units*

- Configure the initial timeout between PBUs if PBA does not arrive by entering this command:

  config pmipv6 mag init-retx-time *units*

- Configure the maximum initial timeout between PBUs if PBA does not arrive by entering this command:

  config pmipv6 mag max-retx-time *units*

- Configure the replay protection mechanism by entering this command:

  config pmipv6 mag replay-protection {**timestamp window** *units* | **sequence-no** | **mobile-node-timestamp**}

- Configure the minimum or maximum amount of time, in seconds, that the MAG should wait for before it retransmits the binding revocation indication (BRI) message by entering this command:

  config pmipv6 mag bri delay {**min** | **max**} *units*

- Configure the maximum number of times the MAG should retransmit the BRI message before it receives the binding revocation acknowledgment (BRA) message by entering this command:

  config pmipv6 mag bri retries *units*

- Configure the list of LMAs for the MAG by entering this command:

  config pmipv6 mag lma *lma-name* **ipv4-address** *ip-address*

- Add an APN for a MAG by entering this command:

  config pmipv6 mag apn *apn-name*

  A MAG can be configured for one of the different roles:

  - 3gpp—Specifies the role as 3GPP (Third Generation Partnership Project standard)
  - lte—Specifies the role as Long Term Evolution (LTE) standard
  - wimax—Specifies the role as WiMax
  - wlan—Specifies the role as WLAN

  Note By default, the MAG role is WLAN. However, for the lightweight access points, the MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.

- Delete an APN by entering this command:

  config pmipv6 delete mag apn *apn-name*

Step 3 Add a profile to a PMIPv6 domain by entering this command:

config pmipv6 add profile *profile-name* **nai** {*user@realm* | *@realm* | *} **lma** *lma-name* **apn** *apn-name*

Note nai stands for network access identifier, while apn stands for access point name.

Step 4 Delete a PMIPv6 entity by entering this command:

config pmipv6 delete {**domain** *domain-name* | **lma** *lma-name* | **profile** *profile-name* **nai** {*user@realm* | *@realm* | *}}

Step 5 Configure the PMIPv6 parameters for the WLAN by using these commands:

- Configure the default realm for the WLAN by entering this command:

  config wlan pmipv6 default-realm {*realm-name* | **none**} *wlan-id*

- Configure the mobility type for a WLAN or for all WLANs by entering this command:

  config wlan pmipv6 mobility-type {**enable** | **disable**} {*wlan-id* | **all**}

- Configure the profile name for a PMIPv6 WLAN by entering this command:

  config wlan pmipv6 profile-name {**none** | *name*} *wlan-id*

Step 6 Configure a PMIPv6 interface name by entering this command:

config pmipv6 interface *interface-name*

Note Before configuring the interface for the tunnel source, you should disable the WLAN associated with the interface.

Step 7 Save your changes by entering this command:

save config

Step 8 See the PMIPv6 configuration details by using the following **show** commands:

- See the details of a profile of a PMIPv6 domain by entering this command:

  show pmipv6 domain *domain-name* **profile** *profile-name*

- See a summary of all the PMIPv6 profiles by entering this command:

  show pmipv6 profile summary
- See global information about the PMIPv6 for a MAG by entering this command:

  show pmipv6 mag globals
- See information about MAG bindings for LMA or NAI by entering this command:

  show pmipv6 mag bindings {**lma** *lma-name* | **nai** *nai-name*}
- See statistical information about MAG by entering this command:

  show pmipv6 mag stats domain *domain-name* **peer** *peer-name*
- See information about PMIPv6 for all clients by entering this command:

  show client summary
- See information about PMIPv6 for a client by entering this command:

  show client details *client-mac-address*
- See information about PMIPv6 for a WLAN by entering this command:

  show wlan *wlan-id*