Intelligent Wireless Gateway Configuration Guide Cisco IOS Release 3S

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Intelligent Wireless Access Gateway

The Intelligent Wireless Access Gateway (iWAG) is a Cisco software feature set that supports clientless integration into the existing Gateway General Packet Radio Service (GPRS) Support Node (GGSN). iWAG provides a WiFi offload option to 3G service providers by enabling a single-box solution of that provides the combined functionality of Proxy Mobile IPv6 (PMIPv6) and GPRS Tunneling Protocol (GTP) on the Intelligent Services Gateway (ISG) framework. This document provides information about iWAG and how to configure it.

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.

Information About Intelligent Wireless Access Gateway

ISG Overview

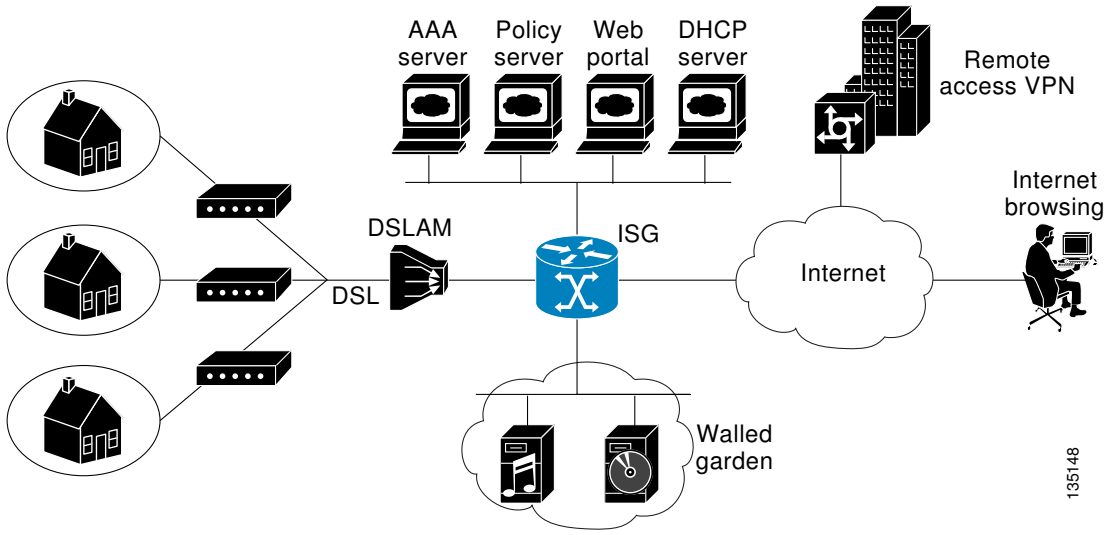
Intelligent Services Gateway (ISG) is a structured framework in which edge access devices deliver flexible and scalable services to subscribers. ISG handles the following key aspects of subscriber management:

- Subscriber identification
- Service and policy determination
- Session policy enforcement
- Session life-cycle management
- Accounting for access and service usage
- Session state monitoring

In addition, ISG introduces a dynamic element to the provisioning and activation of services through control policies and Change of Authorization (CoA) extensions to the RADIUS protocol.

An ISG-enabled device may be deployed at the access edge and service edge of a network and is applicable to a range of subscriber network environments, such as digital subscriber line (DSL), public wireless LAN (PWLAN), and mobile wireless network. Moreover, ISG has been designed to accommodate a flexible distribution of subscriber and service information within a given solution. The figure below illustrates a typical DSL deployment for which service profile data may be stored in an authentication, authorization, and accounting (AAA) database and retrieved and cached on demand.

Figure 1 Sample Topology for a DSL Deployment



It is also possible to define services directly on an ISG. In all cases, service activation may be triggered as a result of a locally defined control policy, user profile associations, or CoA commands from an external policy server or portal application.

Proxy Mobile IPv6 Overview

Proxy Mobile IPv6 (PMIPv6) provides network-based IP Mobility management to a mobile node (MN), without requiring the participation of the MN in any IP mobility-related signaling. The mobility entities in the network track the movements of the MN, initiate the mobility signaling, and set up the required routing state.

The major functional entities of PMIPv6 are Mobile Access Gateways (MAGs), Local Mobility Anchors (LMAs), and MNs.

Mobile Access Gateways

A Mobile Access Gateway (MAG) performs mobility-related signaling on behalf of the mobile nodes (MN) attached to its access links. MAG is the access router for the MN; that is, the MAG is the first-hop router in the localized mobility management infrastructure.

A MAG performs the following functions:

- Obtains an IP address from a Local Mobility Anchor (LMA) and assigns it to an MN
- Retains the IP address of an MN when the MN roams across MAGs
- Tunnels traffic from an MN to LMA

Local Mobility Anchor

Local Mobility Anchor (LMA) is the home agent for a mobile node (MN) in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for MN home network prefixes and manages the binding state of an MN. An LMA has the functional capabilities of a home agent as defined in the Mobile IPv6 base specification (RFC 3775) along with the capabilities required for supporting the PMIPv6 protocol.

Note Use an **dynamic mag learning** command to enable an LMA to accept Proxy Mobile IPv6 (PMIPv6) signaling messages from any Mobile Access Gateway (MAG) that is not locally configured.

Mobile Node

A mobile node (MN) is an IP host whose mobility is managed by the network. An MN can be an IPv4-only node, an IPv6-only node, or a dual-stack node, which is a node with IPv4 and IPv6 protocol stacks. An MN is not required to participate in any IP mobility-related signaling for achieving mobility for an IP address or a prefix that is obtained in the Proxy Mobile IPv6 (PMIPv6) domain.

AAA Server Attributes for Proxy Mobile IPv6

If an authentication, authorization, and accounting (AAA) server is available, a Mobile Access Gateway (MAG) obtains the profile information of the Proxy Mobile IPv6 (PMIPv6) domain and the mobile node (MN) from the server during the configuration and call-flow time, respectively.

The following are the AAA attributes required for configuring the PMIPv6 domain and the MN are:

- PMIPv6 domain-specific AAA attributes:
  - cisco-mpc-protocol-interface
  - lma-identifier
  - mag-identifier
  - mag-v4-address
  - mag-v6-address
  - pmip6-domain-identifier
  - pmip6-fixed-l1-address

    - pmip6-fixed-l2-address
    - pmip6-timestamp-window
    - pmip6-replay-protection
    - pmip6-spi-key
    - pmip6-spi-value
- MN-specific AAA attributes:
    - home-lma
    - home-lma-ipv6-address
    - mn-apn
    - mn-nai
    - mn-network
    - mn-service
    - multihomed

Mobile Client Service Abstraction

Mobile Client Service Abstraction (MCSA) is a uniform mechanism that detects the MNs network events that avoid being detected by mobility protocols. MCSA provides interfaces through which the MAG, General Packet Radio Service (GPRS) Tunneling Protocol (GTP) and ISG receive or send event notifications. MCSA delivers discovery event notifications and service event notifications from mobile nodes (MNs) to the appropriate protocol module. When the Intelligent Services Gateway (ISG) is not available, MCSA performs authentication, authorization, and accounting (AAA). MCSA consists of the following three interfaces through which the protocol modules interact:

- MCSA Client Interface, page 4
- MCSA Service Interface, page 4
- LMA Interface, page 4

MCSA Client Interface

The MCSA client interface exists between the Mobile Access Gateway (MAG) or General Packet Radio Service (GPRS) Tunneling Protocol (GTP) and mobile client service abstraction (MCSA). The mobility protocol modules that provide various services to the MAG or GTP register themselves with the MCSA at the MCSA client interface. The MCSA provides client session discovery notifications to appropriate protocol modules through the MCSA client interface.

MCSA Service Interface

The MCSA service interface exists between the Mobile Client Service Abstraction (MCSA) and Intelligent Services Gateway (ISG). The ISG provides session event notifications to MCSA through the MCSA service interface. The MCSA delivers these event notifications to specific mobility or tunneling protocols modules, such as Mobile Access Gateway (MAG) or the General Packet Radio Service (GPRS) Tunneling Protocol (GTP).

LMA Interface

LMA interface exists between the Local Mobility Anchor (LMA) and Mobile Client Access Abstraction (MCSA). The LMA sends the binding event notifications to the LMA interface, which informs the Intelligent Service Gateway (ISG) about the notifications.

How to Configure Intelligent Wireless Access Gateway

Configuring ISG for iWAG

Creating ISG Sessions for IP Subscribers

An Intelligent Services Gateway (ISG) device creates IP sessions for IP traffic on subscriber-side interfaces. The tasks in the following sections enable IP sessions and indicate how sessions are identified:

Creating ISG IP Interface Sessions

An ISG IP interface session encompasses all IP packets that cross the specified interface or subinterface. Perform this task to create an ISG IP interface session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*[**.** *subinterface-number*]
4. **ip subscriber interface**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number*[**.** *subinterface-number*] **Example:** Device(config)# interface GigabitEthernet 0/0/0.1	Specifies an interface or subinterface and enters interface or subinterface configuration mode.
Step 4	**ip subscriber interface** **Example:** Device(config-subif)# ip subscriber interface	Specifies the type of IP subscriber to be hosted on the interface. **Note** The **ip subscriber interface** command cannot be configured if the **service-policy input** or **service-policy output** command is already configured on the interface; these commands are mutually exclusive.
Step 5	**end** **Example:** Device(config-subif)# end	(Optional) Returns to privileged EXEC mode.

Creating ISG Static Sessions

An Intelligent Services Gateway (ISG) static session enables you to configure static IP sessions by configuring a group of server addresses. Perform the following task to create ISG static sessions.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip subscriber list** *list-name*
4. **ip source** *ip-address* {**mac** *mac-address* | **mask** *subnet-mask*}
5. **exit**
6. **interface** *type number*
7. **ip subscriber** {**l2-connected** | **routed**}
8. **initiator static ip subscriber list** *list-name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ip subscriber list** *list-name* **Example:** Device(config)# ip subscriber list mylist	Specifies the IP subscriber list name and enters server list configuration mode.
Step 4	**ip source** *ip-address* {**mac** *mac-address* | **mask** *subnet-mask*} **Example:** Device(config-server-list)# ip source 209.165.200.225 mac 0.7.f	Specifies the static server IP address and MAC address (in case of Layer 2-connected subscribers) or subnet mask (in the case of routed interfaces).
Step 5	**exit** **Example:** Device(config-server-list)# exit	Exits server list configuration mode and returns to global configuration mode.
Step 6	**interface** *type number* **Example:** Device(config)# interface GigabitEthernet 2/0/0	Specifies an interface and enters interface configuration mode.
Step 7	**ip subscriber** {**l2-connected** | **routed**} **Example:** Device(config-if)# ip subscriber l2-connected	Specifies the type of IP subscriber to be hosted on the interface and enters ISG IP subscriber configuration mode. **Note** IP sessions for Layer 2-connected subscribers should be configured using the **ip subscriber l2-connected** command. However, the **ip subscriber routed** command can also be used if subscriber IP addresses are routable in the access domain.

	Command or Action	Purpose
Step 8	**initiator static ip subscriber list** *list-name* **Example:** Device(config-subscriber)# initiator static ip subscriber list mylist	Creates an IP subscriber session with the packet type as static and attaches the session to the list.
Step 9	**end** **Example:** Device(config-subscriber)# end	(Optional) Returns to privileged EXEC mode.

Creating ISG IP Subnet Sessions

An IP subnet session represents all the traffic that is associated with a single IP subnet. IP subnet sessions are used to apply uniform edge processing to packets associated with a particular IP subnet. When an IP subnet session is configured, ISG treats the subnet as a single subscriber, which means that ISG features and functionality are applied to the subnet traffic as an aggregate. Perform this task to create an IP subnet session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip subscriber routed**
5. **initiator unclassified ip-address** [**ipv4** | [**ipv6**] [**list** *list-name*]]
6. **end**
7. Add the Framed-IP-Netmask attribute to the service or user profile.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** Device(config)# interface gigabitethernet 0/0/0	Specifies an interface and enters interface configuration mode.
Step 4	**ip subscriber routed** **Example:** Device(config-if)# ip subscriber routed	Specifies the type of IP subscriber to be hosted on the interface, and enters ISG IP subscriber configuration mode.
Step 5	**initiator unclassified ip-address** [**ipv4** | [**ipv6**] [**list** *list-name*]] **Example:** Device(config-subscriber)# initiator unclassified ip-address	Configures ISG to create an IP subscriber session when an IP packet with an unclassified IP source address is received.
Step 6	**end** **Example:** Device(config-subscriber)# end	(Optional) Returns to privileged EXEC mode.
Step 7	Add the Framed-IP-Netmask attribute to the service or user profile.	Enables an IP subnet session for the subscriber. • When a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute.

Configuring IP Session Recovery for DHCP-Initiated IP Sessions

Perform this task to configure Intelligent Services Gateway (ISG) to take specific actions after the recovery of an IP session when ISG has terminated or reloaded the session. This task applies to DHCP-initiated IP sessions only.

If a policy for session recovery is not configured, ISG applies the following default policy:

```
policy-map type control GLOBAL
 class type control always event session-restart
  1 service disconnect delay 60
```

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type control** *policy-map-name*
4. **class type control** {*control-class-name* | **always**} **event session-restart**
5. *action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}
6. *action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}}
7. *action-number* **set-timer** *name-of-timer minutes*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**policy-map type control** *policy-map-name* **Example:** Device(config)# policy-map type control MY-POLICY	Creates or modifies a control policy map, which is used to define a control policy, and enters control policy-map configuration mode.
Step 4	**class type control** {*control-class-name* | **always**} **event session-restart** **Example:** Device(config-control-policymap)# class type control always event session-restart	Specifies a control class that is evaluated when the session-restart event occurs and enters policy-map class control configuration mode. • A policy rule for which the control class is **always** will always be treated as the lowest priority rule within the control policy map.

	Command or Action	Purpose
Step 5	*action-number* **authorize** [**aaa list** *list-name*] [**password** *password*] [**upon network-service-found** {**continue** | **stop**}] **identifier** {**authenticated-domain** | **authenticated-username** | **auto-detect** | **circuit-id** [**plus remote-id**] | **dnis** | **mac-address** | **nas-port** | **remote-id** [**plus circuit-id**] | **source-ip-address** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**} **Example:** Device(config-control-policymap-class-control)# 1 authorize identifier source-ip-address	(Optional) Initiates a request for authorization on the basis of the specified identifier.
Step 6	*action-number* **service-policy type service** [**unapply**] [**aaa list** *list-name*] {**name** *service-name* | **identifier** {**authenticated-domain** | **authenticated-username** | **dnis** | **nas-port** | **tunnel-name** | **unauthenticated-domain** | **unauthenticated-username**}} **Example:** Device(config-control-policymap-class-control)# 1 service-policy type service aaa list LISTA name REDIRECT	(Optional) Activates an ISG service. • Specifying an identifier instead of a service name activates a service that has the same name as the specified identifier.
Step 7	*action-number* **set-timer** *name-of-timer minutes* **Example:** Device(config-control-policymap-class-control)# 1 set-timer TIMERA 5	(Optional) Starts a named policy timer. • Expiration of the timer generates the event timed-policy expiry.
Step 8	**end** **Example:** Device(config-control-policymap-class-control)# end	(Optional) Returns to privileged EXEC mode.

Verifying ISG IP Subscriber Sessions

Perform this task to verify IP subscriber session configuration and creation. The **show** commands can be used in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session** [**detailed**] [**identifier** *identifier* \| **uid** *session-id* \| **username** *name*]
3. **show ip subscriber** [**mac** *mac-address* \| [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] \| **interface** *interface-name* [**detail** \| **statistics**] \| **ip** *ip-address* \| **static list** *listname* \| **statistics** {**arp** \| **dangling**}]]
4. **show platform isg session-count** {**all** \| *slot*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show subscriber session** [**detailed**] [**identifier** *identifier* | **uid** *session-id* | **username** *name*] **Example:** Device# show subscriber session detailed	Displays information about ISG policies and features for subscriber sessions.
Step 3	**show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **Example:** Device# show ip subscriber ip 10.10.10.10	Displays information about ISG IP subscriber sessions.
Step 4	**show platform isg session-count** {**all** | *slot*} **Example:** Device# show platform isg session-count all	Displays the number of active ISG subscriber sessions by line card.

Clearing ISG IP Subscriber Sessions

SUMMARY STEPS

1. **enable**
2. **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]]
3. **clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

Command or Action	Purpose
Step 2 **show ip subscriber** [**mac** *mac-address* | [**vrf** *vrf-name*] [[**dangling** *seconds*] [**detail**] | **interface** *interface-name* [**detail** | **statistics**] | **ip** *ip-address* | **static list** *listname* | **statistics** {**arp** | **dangling**}]] **Example:** Device# show ip subscriber ip 10.10.10.10	(Optional) Displays information about ISG IP subscriber sessions.
Step 3 **clear ip subscriber** [**interface** *interface-name* | **mac** *mac-address* | **slot** *slot-number* **no-hardware** | [**vrf** *vrf-name*] [**dangling** *seconds* | **ip** *ip-address* | **statistics**]] **Example:** Device# clear ip subscriber ip 10.10.10.10	Clears ISG IP subscriber sessions.

Troubleshooting ISG IP Subscriber Sessions

Use the following commands to troubleshoot ISG IP subscriber sessions. You can use the **debug** commands in any order.

SUMMARY STEPS

1. **enable**
2. **debug ip subscriber packet**
3. **debug condition username** *username*

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** Device# enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 **debug ip subscriber packet** **Example:** Device# debug ip subscriber packet	Enables ISG IP subscriber session debugging.

Command or Action	Purpose
Step 3 **debug condition username** *username* **Example:** Device# debug condition username user1	Filters debugging output for certain debug commands on the basis of specified conditions.

Assigning ISG Subscriber IP Addresses by Using DHCP

Configure DHCP support in your network before performing the tasks in this section.

Configuring an ISG Interface for Dynamic DHCP Class Association

Perform this task to enable ISG to influence the assignment of IP addresses to subscribers on the interface by providing the local DHCP component with a class name. The class name refers to a class configured using the **ip dhcp pool** command and can reference a pool of addresses or a relay destination.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask* [**secondary**]
5. **ip subscriber** [**l2-connected** | **routed**]
6. **initiator dhcp class-aware**
7. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Device(config)# interface gigabitethernet 0/0/0	Specifies an interface for configuration and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** Device(config-if)# ip address 10.1.0.1 255.255.0.0	Sets a primary or secondary IP address for an interface.
Step 5	**ip subscriber** [**l2-connected** | **routed**] **Example:** Device(config-if)# ip subscriber	Enables ISG IP subscriber configuration mode.
Step 6	**initiator dhcp class-aware** **Example:** Device(config-subscriber) initiator dhcp class-aware	Configures ISG to create IP sessions upon receipt of DHCP DISCOVER packets. • The **class-aware** keyword allows ISG to influence the IP address assigned by DHCP by providing DHCP with a class name.
Step 7	**end** **Example:** Device(config-if)# end	(Optional) Returns to privileged EXEC mode.

Configuring DHCP Server User Authentication

Perform this task to authenticate the DHCP clients on the server.

You need to use the ISG framework to enable DHCP server user authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name* **local**
5. **ip dhcp pool** *pool-name*
6. **network** *network-number mask*
7. **exit**
8. **interface** *type number*
9. **ip subscriber l2-connected**
10. **initiator dhcp class-aware**
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** Device(config)# aaa new model	Enables authentication, authorization, and accounting (AAA).
Step 4	**aaa authentication login** *list-name* **local** **Example:** Device(config)# aaa authentication login mylist local	Sets the AAA authentication at login.
Step 5	**ip dhcp pool** *pool-name* **Example:** Device(config)# ip dhcp pool testpool	Creates a name for the DHCP server address pool and enters DHCP pool configuration mode.

	Command or Action	Purpose
Step 6	**network** *network-number mask* **Example:** Device(dhcp-config)# network 172.16.0.0 255.240.0.0	Configures the network number and mask for a DHCP address pool primary or secondary subnet on a Cisco DHCP server.
Step 7	**exit** **Example:** Device(dhcp-config)# exit	Exits DHCP pool configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** Device(config)# interface GigabitEthernet 0/0	Enters interface configuration mode.
Step 9	**ip subscriber l2-connected** **Example:** Device(config-if)# ip subscriber l2-connected	Configures a Layer 2-connected IP session on the interface and enters IP subscriber configuration mode.
Step 10	**initiator dhcp class-aware** **Example:** Device(config-subscriber)# initiator dhcp class-aware	Initiates a class for DHCP for an IP session initiated by DHCP.
Step 11	**end** **Example:** Device(config-subscriber)# end	Returns to privileged EXEC mode.

Configuring a DHCP Class in a Service Policy Map

Perform this task to assign a DHCP class to a service policy map. Subscribers for which this service policy map is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

Before configuring a DHCP class in a service policy map, you must configure a DHCP pool and the classes configured within the DHCP pool must match the DHCP classes configured in the service policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-name*
4. **classname** *class-name*
5. **end**
6. **show policy-map type service**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**policy-map type service** *policy-name* **Example:** Device(config)# policy-map type service service1	Creates a service policy map or specifies an existing service policy map for configuration, and enters service policy-map configuration mode.
Step 4	**classname** *class-name* **Example:** Device(config-service-policymap)# classname class1	Associates a DHCP pool with a service policy map.
Step 5	**end** **Example:** Device(config-service-policymap)# end	(Optional) Returns to privileged EXEC mode.
Step 6	**show policy-map type service** **Example:** Device# show policy-map type service	(Optional) Displays the contents of all service policy maps. • Use this command to verify that the DHCP class is associated with the service policy map.

- What to Do Next, page 19

What to Do Next

After you have configured the DHCP address pool class in a service policy map, you may want to configure a method of activating the service policy map; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Configuring a DHCP Class in a Service Profile or User Profile on the AAA Server

Perform this task to add the vendor-specific attribute (VSA) for a DHCP class to a user profile or service profile on the AAA server. Subscribers for whom the user or service profile is activated will be assigned IP addresses from the DHCP pool or the remote server that is associated with the class.

Before configuring a DHCP class in a service profile or user profile on the AAA Server, a DHCP address pool must be configured. Classes configured within the DHCP address pool must match the DHCP address pool classes configured in the service or user profile. To associate a DHCP address pool with a service or specific subscriber, add the DHCP class attribute to the user or service profile. For example:
26,9,1 = "subscriber:classname=class-name "

After associating a DHCP address pool with a service or specific subscriber, you may want to configure a method of activating the service policy map or service profile; for example, control policies can be used to activate services. For more information about methods of service activation, see the module "Configuring ISG Subscriber Services."

Configuring a DHCP Server IP Address

Perform this task to either specify which DHCP servers to use on your network or to configure the IP address of one or more DHCP servers available on the network, and to specify the DHCP Lease Query for routed IP sessions.

Note The DHCP server IP address needs to be configured for routed IP sessions if the DHCP Lease Query is performed.

The following prerequisites apply for this task:

- The DHCP server must support the DHCP lease protocol.
- The IP address of the phone must be assigned by DHCP address assignments.
- The traffic must be classified as Layer 3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}}
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ip dhcp-server** {*ip-address* | **query lease** {**retries** *max-retransmissions* | **timeout** *timeout-query-seconds*}} **Example:** Device(config)# ip dhcp-server query lease retries 3	Configures the IP address of one or more DHCP servers available on the network, and specifies the DHCP Lease Query for routed IP sessions.
Step 4	**end** **Example:** Device(config)# end	Exits global configuration mode.

Configuring ISG Dynamic VPN Selection

Configuring a Multiservice Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface multiservice** *interface-number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**interface multiservice** *interface-number* **Example:** Device(config)# interface multiservice 1	Creates a multiservice interface, which enables dynamic VPN selection, and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name* **Example:** Device(config-if)# ip vrf forwarding vrf1	Associates a VPN VRF with an interface or subinterface.
Step 5	**ip address** *ip-address mask* **Example:** Device(config-if)# ip address 172.16.0.0 255.255.255.0	Sets the primary IP address for an interface. • Specifies the IP address of the VPN.
Step 6	**end** **Example:** Device(config-if)# end	(Optional) Returns to privileged EXEC mode.

Specifying a VRF in a Service Policy Map

VPN routing and forwarding (VRF) transfer occurs when a new primary service is activated for a session, causing the session to transfer from one VRF to another. Services can be configured in service profiles on an external authentication, authorization, and accounting (AAA) server or they can be configured on the ISG device in service policy maps. Perform this task to configure a VRF in a service policy map on the ISG device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type service** *policy-map-name*
4. **ip vrf forwarding** *name-of-vrf*
5. **sg-service-type primary**
6. **sg-service-group** *service-group-name*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**policy-map type service** *policy-map-name* **Example:** Device(config)# policy-map type service service1	Creates or modifies a service policy map, which is used to define an ISG service, and enters service policy-map configuration mode.
Step 4	**ip vrf forwarding** *name-of-vrf* **Example:** Device(config-service-policymap)# ip vrf forwarding vrf1	Associates the service with a VRF.
Step 5	**sg-service-type primary** **Example:** Device(config-service-policymap)# sg-service-type primary	Defines the service as a primary service. • A primary service contains a network-forwarding policy. A service must be defined as a primary service by using the **sg-service-type primary** command. Any service that is not a primary service is defined as a secondary service by default.

Command or Action	Purpose
Step 6 **sg-service-group** *service-group-name* **Example:** Device(config-service-policymap)# sg-service-group group1	(Optional) Associates an ISG service with a service group. • A service group is a group of services that may be active simultaneously for a given session. Typically, a service group includes one primary service and one or more secondary services.
Step 7 **end** **Example:** Device(config-service-policymap)# end	(Optional) Returns to privileged EXEC mode.

Verifying VRF Transfer for IP Sessions

Perform the following task as needed to verify VRF transfer for IP sessions. You can use the **show** commands in this task in any order.

SUMMARY STEPS

1. **enable**
2. **show subscriber session uid** *session-identifier* **detail**
3. **show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]]
4. **show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**}
5. **show ip route** [**vrf** *vrf-name*]
6. **show ip dhcp binding** [**ip-address**]

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 **show subscriber session uid** *session-identifier* **detail** **Example:** Device# show subscriber session uid 4 detail	Displays information about ISG subscriber sessions with a specific session identifier.

	Command or Action	Purpose
Step 3	**show ip subscriber** [**dangling** *seconds* | **detail** | **ip** *ip-address* | **mac** *mac-address* | **vrf** *vrf-name* [**dangling** *seconds* | **detail** | **ip** *ip-address*]] **Example:** Device# show ip subscriber vrf vrf1	Displays information about ISG IP subscriber sessions.
Step 4	**show idmgr** {**memory** [**detailed** [**component** [*substring*]]] | **service key session-handle** *session-handle-string* **service-key** *key-value* | **session key** {**aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string*} | **statistics**} **Example:** Device# show idmgr session key nativeip-vrf ip-address 209.165.200.225	Displays information related to ISG session and service identity.
Step 5	**show ip route** [**vrf** *vrf-name*] **Example:** Device# show ip route	Displays the current state of the routing table.
Step 6	**show ip dhcp binding** [**ip-address**] **Example:** Device# show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

Troubleshooting VRF Transfer for IP Sessions

The commands in this task can be used to troubleshoot VRF transfer of IP sessions. The **debug** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **debug subscriber** {**event** | **error** | **packet** | **policy** | **service**}
3. **debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**}
4. **debug subscriber policy dpm** {**error** | **event**}
5. **debug ip dhcp server** {**events** | **packets** | **linkage** | **class**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug subscriber** {**event** | **error** | **packet** | **policy** | **service**} **Example:** Device# debug subscriber service	Displays debugging messages pertaining to subscriber policies, policy server events, and changes to service.
Step 3	**debug ip subscriber** {**event** | **error** | **packet** | **fsm** | **all**} **Example:** Device# debug ip subscriber error	Displays debugging messages pertaining to an IP session created on the service gateway.
Step 4	**debug subscriber policy dpm** {**error** | **event**} **Example:** Device# debug subscriber policy dpm event	Displays diagnostic information about policy execution that is related to DHCP events.
Step 5	**debug ip dhcp server** {**events** | **packets** | **linkage** | **class**} **Example:** Device# debug dhcp ip dhcp server events	Enables Cisco IOS DHCP server debugging.

Configuring PMIPv6 Support for iWAG

Configuring the Minimum Configuration for a MAG to Function

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mobile pmipv6-domain** *domain-name*
4. **lma** *lma-id*
5. **ipv6-address** *ipv6-address*
6. **exit**
7. Repeat Steps 5 to 8 to configure the second LMA.
8. **nai** [*user*]*@realm*
9. **lma** *lma-id*
10. **service** {**dual** | **ipv4** | **ipv6**}
11. **exit**
12. Repeat Steps 10 to 11 to configure the second MN.
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ipv6 mobile pmipv6-domain** *domain-name* **Example:** Device(config)# ipv6 mobile pmipv6-domain dn1	Creates the Proxy Mobile IPv6 (PMIPv6) domain and enters PMIPv6 domain configuration mode.
Step 4	**lma** *lma-id* **Example:** Device(config-ipv6-pmipv6-domain)# lma lma1	Configures an Local Mobility Anchor (LMA) within the PMIPv6 domain and enters PMIPv6 domain LMA configuration mode.

	Command or Action	Purpose
Step 5	**ipv6-address** *ipv6-address* **Example:** Device(config-ipv6-pmipv6-domain-lma)# ipv6-address 2001:DB8::1	Configures an IPv6 address for the LMA within the PMIPv6 domain.
Step 6	**exit** **Example:** Device(config-ipv6-pmipv6-domain-lma)# exit	Exits PMIPv6 domain LMA configuration mode and returns to PMIPv6 domain configuration mode.
Step 7	Repeat Steps 5 to 8 to configure the second LMA.	—
Step 8	**nai** [*user*]*@realm* **Example:** Device(config-ipv6-pmipv6-domain)# nai user1@example.com	Configures a network access identifier for the mobile node (MN) within the PMIPv6 domain and enters PMIPv6 domain mobile node configuration mode.
Step 9	**lma** *lma-id* **Example:** Device(config-ipv6-pmipv6-domain-mn)# lma lma1	Configures an LMA for the MN.
Step 10	**service** {**dual** | **ipv4** | **ipv6**} **Example:** Device(config-ipv6-pmipv6-domain-mn)# service ipv4	Configures the service provided to the MN within the PMIPv6 domain. The type of services provided to the MN are as follows: • **dual**—Specifies both IPv4 and IPv6 services for an MN. • **IPv4**—Specifies IPv4 service for an MN. • **IPv6**—Specifies IPv6 service for an MN.
Step 11	**exit** **Example:** Device(config-ipv6-pmipv6-domain-mn)# exit	Exits PMIPv6 domain mobile node configuration mode and returns to PMIPv6 domain configuration mode.
Step 12	Repeat Steps 10 to 11 to configure the second MN.	—

Command or Action	Purpose
Step 13 **end** **Example:** Device(config-ipv6-pmipv6-domain)# end	Exits PMIPv6 domain configuration mode and returns to privileged EXEC mode.

Configuring a Detailed Configuration for a MAG When an AAA Server Is Not Available

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mobile pmipv6-domain** *domain-name*
4. **replay-protection timestamp** [**window** *seconds*]
5. **auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** *ascii-string* | **hex** *hex-string*}
6. **encap** {**gre-ipv4** | **ipv6-in-ipv6**}
7. **local-routing-mag**
8. **lma** *lma-id*
9. **ipv6-address** *ipv6-address*
10. **exit**
11. Repeat Steps 10 to 12 to configure each LMA.
12. **mag** *mag-id*
13. **ipv6-address** *ipv6-address*
14. **exit**
15. **mn-profile-load-aaa**
16. **nai** [*user*]*@realm*
17. **lma** *lma-id*
18. **int att** *interface-access-type* **l2-addr** *mac-address*
19. **gre-encap-key** [**down** | **up**] *key-value*
20. **service** {**dual** | **ipv4** | **ipv6**}
21. **apn** *apn-name*
22. **exit**
23. Repeat Steps 20 to 24 to configure each MN.
24. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ipv6 mobile pmipv6-domain** *domain-name* **Example:** Device(config)# ipv6 mobile pmipv6-domain dn1	Creates a Proxy Mobile IPv6 (PMIPv6) domain and enters PMIPv6 domain configuration mode.
Step 4	**replay-protection timestamp** [**window** *seconds*] **Example:** Device(config-ipv6-pmipv6-domain)# replay-protection timestamp window 200	Configures the replay protection mechanism within the PMIPv6 domain.
Step 5	**auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** *ascii-string* | **hex** *hex-string*} **Example:** Device(config-ipv6-pmipv6-domain)# auth-option spi 67 key ascii key1	Configures authentication for the PMIPv6 domain.
Step 6	**encap** {**gre-ipv4** | **ipv6-in-ipv6**} **Example:** Device(config-ipv6-pmipv6-domain)# encap gre-ipv4	Configures the tunnel encapsulation mode type between the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA).
Step 7	**local-routing-mag** **Example:** Device(config-ipv6-pmipv6-domain)# local-routing-mag	Enables local routing for the MAG.

	Command or Action	Purpose
Step 8	**lma** *lma-id* **Example:** Device(config-ipv6-pmipv6-domain)# lma lma1	Configures LMA within the PMIPv6 domain and enters PMIPv6 domain LMA configuration mode.
Step 9	**ipv6-address** *ipv6-address* **Example:** Device(config-ipv6-pmipv6-domain-lma)# ipv6-address 2001:0DB8:2:3::1	Configures an IPv6 address for the LMA within the PMIPv6 domain.
Step 10	**exit** **Example:** Device(config-ipv6-pmipv6-domain-lma)# exit	Exits PMIPv6 domain LMA configuration mode and returns to PMIPv6 domain configuration mode.
Step 11	Repeat Steps 10 to 12 to configure each LMA.	—
Step 12	**mag** *mag-id* **Example:** Device(config-ipv6-pmipv6-domain)# mag mag1	Configures a MAG within the PMIPv6 domain and enters PMIPv6 domain MAG configuration mode.
Step 13	**ipv6-address** *ipv6-address* **Example:** Device(config-ipv6-pmipv6-domain-mag)# ipv6-address 2001:0DB8:2:4::1	Configures an IPv6 address for the MAG within the PMIPv6 domain.
Step 14	**exit** **Example:** Device(config-ipv6-pmipv6-domain-mag)# exit	Exits PMIP domain MAG configuration mode and returns to PMIPv6 domain configuration mode.

	Command or Action	Purpose
Step 15	**mn-profile-load-aaa** **Example:** Device(config-ipv6-pmipv6-domain)# mn-profile-load-aaa	(Optional) Loads the profile configuration from AAA to the mobile node (MN) within the PMIPv6 domain. **Note** Steps 20 to 24 need not be entered if the MN is configured using the configuration from AAA. You can use the specific command to override the configuration for a specific mobile node (MN) parameter.
Step 16	**nai** [*user*]*@realm* **Example:** Device(config-ipv6-pmipv6-domain)# nai user1@example.com	Configures the network address identifier (NAI) for the MN within the PMIPv6 domain and enters PMIPv6 domain MN configuration mode.
Step 17	**lma** *lma-id* **Example:** Device(config-ipv6-pmipv6-domain-mn)# lma lma1	Configures the LMA for the MN.
Step 18	**int att** *interface-access-type* **l2-addr** *mac-address* **Example:** Device(config-ipv6-pmipv6-domain-mn)# int att Gigabitethernet l2-addr 02c7.f800.0422	Configures the access technology type, interface, and MAC address of the MN interface within the PMIPv6 domain.
Step 19	**gre-encap-key** [**down** | **up**] *key-value* **Example:** Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key down 45	Configures a generic routing encapsulation (GRE) key for the MN within the PMIPv6 domain.
Step 20	**service** {**dual** | **ipv4** | **ipv6**} **Example:** Device(config-ipv6-pmipv6-domain-mn)# service ipv4	Configures the service provided to the MN within the PMIPv6 domain. The type of services provided to the MN are as follows: • **dual**—Specifies both IPv4 and IPv6 services for an MN. • **IPv4**—Specifies an IPv4 service for an MN. • **IPv6**—Specifies an IPv6 service for an MN.
Step 21	**apn** *apn-name* **Example:** Device(config-ipv6-pmipv6-domain-mn)# apn apn1	Specifies an access point name (APN) to the MN subscriber within the PMIPv6 domain.

	Command or Action	Purpose
Step 22	**exit** **Example:** Device(config-ipv6-pmipv6-domain-mn)# exit	Exits PMIP domain MN configuration mode and returns to PMIPv6 domain configuration mode.
Step 23	Repeat Steps 20 to 24 to configure each MN.	—
Step 24	**end** **Example:** Device(config-ipv6-pmipv6-domain)# end	Exits PMIPv6 domain configuration mode and returns to privileged EXEC mode.

Configuring Mobile Client Service Abstraction

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mcsa**
4. **enable sessionmgr**
5. **end**
6. **show mcsa statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**mcsa** **Example:** Device(config) mcsa	Enables the mobile client service abstraction (MCSA) and enters MCSA configuration mode.
Step 4	**enable sessionmgr** **Example:** Device(config-mcsa) enable sessionmgr	Enables the mobile client service abstraction (MCSA) to receive notifications from the Intelligent Services Gateway (ISG).
Step 5	**end** **Example:** Device(config-mcsa) end	Exits MCSA configuration mode and returns to privileged EXEC mode.
Step 6	**show mcsa statistics** **Example:** Device# show mcsa statistics	Displays the MCSA notification statistics.

Configuring a Minimum Configuration for a MAG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name*
4. **address ipv6** *ipv6-address*
5. **sessionmgr**
6. **generate grekey**
7. **interface** *type number*
8. **role** {**3gpp** | **lte** | **wimax** | **wlan**}
9. **apn** *apn-name*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name* **Example:** Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1	Enables the MAG service on a device, configures the PMIPv6 domain for the MAG, and enters MAG configuration mode.
Step 4	**address ipv6** *ipv6-address* **Example:** Device(config-ipv6-pmipv6-mag)# address ipv6 2001:0DB8:2:4::1	Configures an IPv6 address for the MAG.
Step 5	**sessionmgr** **Example:** Device(config-ipv6-pmipv6-mag)# sessionmgr	Enables the MAG to process the the notification it receives through the mobile client service abstraction (MCSA) from the Intelligent Services Gateway (ISG).
Step 6	**generate grekey** **Example:** Device(config-ipv6-pmipv6-mag)# generate grekey	Enables dynamic generation of upstream generic routing encapsulation keys for mobile nodes in an LMA.
Step 7	**interface** *type number* **Example:** Device(config-ipv6-pmipv6-mag)# interface gigabitethernet 0/0/0	Enables an interface for the MAG.

	Command or Action	Purpose
Step 8	**role** {**3gpp** | **lte** | **wimax** | **wlan**} **Example:** Device(config-ipv6-pmipv6-mag)# role lte	Configures a role for the MAG. The keywords are as follows: • **3gpp**—Specifies the role as the 3rd Generation Partnership Project (3GPP). • **lte**—Specifies the role as Long Term Evaluation (LTE). • **wimax**—Specifies the role as wimax. • **wlan**—Specifies the role as wireless LAN (WLAN).
Step 9	**apn** *apn-name* **Example:** Device(config-ipv6-pmipv6-mag)# apn apn2	Specifies an access point name (APN) to the subscriber of the MAG. **Note** Specifying an APN is mandatory if the role of the MAG is 3GPP.
Step 10	**end** **Example:** Device(config-ipv6-pmipv6-mag)# end	Exits MAG configuration mode and returns to privileged EXEC mode.

Configuring a Detailed Configuration for a MAG

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **exit**
5. **ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name*
6. **role** {**3gpp** | **wlan**}
7. **apn** *apn-name*
8. **local-routing-mag**
9. **discover-mn-detach poll interval** *seconds* **timeout** *seconds* **retries** *retry-count*
10. **address ipv4** *ipv4-address*
11. **address ipv6** *ipv6-address*
12. **sessionmgr**
13. **interface** *type number*
14. **binding maximum** *number*
15. **binding lifetime** *seconds*
16. **binding refresh-time** *seconds*
17. **binding init-retx-time** *milliseconds*
18. **binding max-retx-time** *milliseconds*
19. **replay-protection timestamp** [**window** *seconds*]
20. **bri delay min** *milliseconds*
21. **bri delay max** *milliseconds*
22. **bri retry** *number*
23. **lma** *lma-id domain-name*
24. **auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** | **hex**} *hex-string*
25. **ipv4-address** *ipv4-address*
26. **vrfid** *vrf-name*
27. **encap** {**gre-ipv4** | **ipv6-in-ipv6**}
28. **end**
29. **show ipv6 mobile pmipv6 mag** *mag-id* **globals**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** Device(config)# vrf definition vrf1	Configures a virtual routing and forwarding (VRF) routing table instance and enters VRF configuration mode.
Step 4	**exit** **Example:** Device(config-vrf) exit	Exits VRF configuration mode and returns to global configuration mode.
Step 5	**ipv6 mobile pmipv6-mag** *mag-id* **domain** *domain-name* **Example:** Device(config)# ipv6 mobile pmipv6-mag mag1 domain dn1	Enables the MAG service on a device, configures the PMIPv6 domain for the MAG, and enters MAG configuration mode.
Step 6	**role** {**3gpp** | **wlan**} **Example:** Device(config-ipv6-pmipv6-mag)# role 3gpp	Configures a role for the MAG. The keywords are as follows: • **3gpp**—Specifies the role as 3GPP. • **lte**—Specifies the role as LTE. • **wimax**—Specifies the role as wimax. • **wlan**—Specifies the role as wireless LAN (WLAN).
Step 7	**apn** *apn-name* **Example:** Device(config-ipv6-pmipv6-mag)# apn apn2	Specifies an access point name (APN) to the subscriber of the MAG.
Step 8	**local-routing-mag** **Example:** Device(config-ipv6-pmipv6-mag)# local-routing-mag	Enables local routing for the MAG.

	Command or Action	Purpose
Step 9	**discover-mn-detach poll interval** *seconds* **timeout** *seconds* **retries** *retry-count* **Example:** Device(config-ipv6-pmipv6-mag)# discover-mn-detach poll interval 11 timeout 3 retries 4	Enables periodic verification of the MN attachment with the MAG-enabled interface.
Step 10	**address ipv4** *ipv4-address* **Example:** Device(config-ipv6-pmipv6-mag)# address ipv4 10.1.3.1	Configures an IPv4 address for the MAG.
Step 11	**address ipv6** *ipv6-address* **Example:** Device(config-ipv6-pmipv6-mag)# address ipv6 2001:0DB8:2:4::1	Configures an IPv6 address for the MAG.
Step 12	**sessionmgr** **Example:** Device(config-ipv6-pmipv6-mag)# sessionmgr	Configures an IPv6 address for the MAG.
Step 13	**interface** *type number* **Example:** Device(config-ipv6-pmipv6-mag)# interface gigabitethernet 0/0/0	Enables an interface for the MAG.
Step 14	**binding maximum** *number* **Example:** Device(config-ipv6-pmipv6-mag)# binding maximum 200	Specifies the maximum number of Proxy Binding Update (PBU) entries allowed for the MAG.
Step 15	**binding lifetime** *seconds* **Example:** Device(config-ipv6-pmipv6-mag)# binding lifetime 5000	Specifies the maximum lifetime permitted for the PBU entry.

	Command or Action	Purpose
Step 16	**binding refresh-time** *seconds* **Example:** Device(config-ipv6-pmipv6-mag)# binding refresh-time 2000	Specifies the PBU entry refresh time.
Step 17	**binding init-retx-time** *milliseconds* **Example:** Device(config-ipv6-pmipv6-mag)# binding init-retx-time 110	Specifies the initial timeout interval between the PBU and Proxy Binding Acknowledgment (PBA) until a PBA is received.
Step 18	**binding max-retx-time** *milliseconds* **Example:** Device(config-ipv6-pmipv6-mag)# binding max-retx-time 4000	Specifies the maximum timeout interval between the PBU and the PBA until a PBA is received.
Step 19	**replay-protection timestamp** [**window** *seconds*] **Example:** Device(config-ipv6-pmipv6-mag)# replay-protection timestamp window 200	Configures the replay protection mechanism within the PMIPv6 domain.
Step 20	**bri delay min** *milliseconds* **Example:** Device(config-ipv6-pmipv6-mag)# bri delay min 500	Specifies the minimum time for which an LMA should wait before transmitting the Binding Revocation Indication (BRI) message.
Step 21	**bri delay max** *milliseconds* **Example:** Device(config-ipv6-pmipv6-mag)# bri delay max 4500	Specifies the maximum time for which an LMA should wait for the Binding Revocation Acknowledgment (BRA) message before retransmitting the BRI message.
Step 22	**bri retry** *number* **Example:** Device(config-ipv6-pmipv6-mag)# bri retry 6	Specifies the maximum number of times an LMA should retransmit a BRI message, until a BRA is received.

	Command or Action	Purpose
Step 23	**lma** *lma-id domain-name* **Example:** Device(config-ipv6-pmipv6-mag)# lma lma3 dn1	Configures the LMA for the MAG and enters MAG-LMA configuration mode.
Step 24	**auth-option spi** {*spi-hex-value* | **decimal** *spi-decimal-value*} **key** {**ascii** | **hex**} *hex-string* **Example:** Device(config-ipv6-pmipv6mag-lma)# auth-option spi decimal 258 key hex BDF	Configures authentication for the LMA within the MAG.
Step 25	**ipv4-address** *ipv4-address* **Example:** Device(config-ipv6-pmipv6mag-lma)# ipv4-address 172.16.0.1	Configures an IPv4 address for the LMA within the MAG.
Step 26	**vrfid** *vrf-name* **Example:** Device(config-ipv6-pmipv6mag-lma)# vrfid vrf1	Specifies a VRF for an LMA peer.
Step 27	**encap** {**gre-ipv4** | **ipv6-in-ipv6**} **Example:** Device(config-ipv6-pmipv6mag-lma)# encap gre-ipv4	Configures a tunnel encapsulation mode type between the MAG and the LMA.
Step 28	**end** **Example:** Device(config-ipv6-pmipv6mag-lma)# end	Exits MAG-LMA configuration mode and returns to privileged EXEC mode.
Step 29	**show ipv6 mobile pmipv6 mag** *mag-id* **globals** **Example:** Device# show ipv6 mobile pmipv6 mag mag1 globals	(Optional) Displays MAG global configuration details.

- Example, page 41
- Troubleshooting Tips, page 41

Example

The following example shows the MAG global configuration:

```
Router# show ipv6 mobile pmipv6 mag mag1 globals

------------------------------------------------------
Domain  : D1
Mag Identifier  : M1
      MN's detach discover          : disabled
      Local routing                 : disabled
      Mag is enabled on interface   : GigabitEthernet0/0/0
      Mag is enabled on interface   : GigabitEthernet0/1/0
      Max Bindings                  : 3
      AuthOption                    : disabled
      RegistrationLifeTime          : 3600 (sec)
      BRI InitDelayTime             : 1000 (msec)
      BRI MaxDelayTime              : 40000 (msec)
      BRI MaxRetries                : 6
      BRI EncapType                 : IPV6_IN_IPV6
      Fixed Link address is         : enabled
      Fixed Link address            : aaaa.aaaa.aaaa
      Fixed Link Local address is   : enabled
      Fixed Link local address      : 0xFE800000 0x0 0x0 0x2
      RefreshTime                   : 300 (sec)
      Refresh RetxInit time         : 20000 (msec)
      Refresh RetxMax time          : 50000 (msec)
      Timestamp option              : enabled
      Validity Window               : 7

Peer :  LMA1
      Max Bindings                  : 3
      AuthOption                    : disabled
      RegistrationLifeTime          : 3600 (sec)
      BRI InitDelayTime             : 1000 (msec)
      BRI MaxDelayTime              : 40000 (msec)
      BRI MaxRetries                : 6
      BRI EncapType                 : IPV6_IN_IPV6
      Fixed Link address is         : enabled
      Fixed Link address            : aaaa.aaaa.aaaa
      Fixed Link Local address is   : enabled
      Fixed Link local address      : 0xFE800000 0x0 0x0 0x2
      RefreshTime                   : 300 (sec)
      Refresh RetxInit time         : 20000 (msec)
      Refresh RetxMax time          : 50000 (msec)
      Timestamp option              : enabled
      Validity Window               : 7
Peer :  LMA2
      Max Bindings                  : 3
      AuthOption                    : disabled
```

Troubleshooting Tips

You can use the following commands to troubleshoot the MAG configuration:

- **debug ipv6 mobile mag event**
- **debug ipv6 mobile mag info**
- **show ipv6 mobile pmipv6 mag bindings**
- **show ipv6 mobile pmipv6 mag globals**

Configuration Examples for Intelligent Wireless Access Gateway

Example: Creating ISG IP Interface Sessions

The following example shows how to configure an IP interface session on GigabitEthernet interface 0/0/1.401:

```
interface GigabitEthernet 0/0/1.401
 ip subscriber interface
```

Example: Creating ISG Static Sessions

The following example shows how to create an ISG static session for server 209.165.200.225 for subscribers who connect to ISG on GigabitEthernet interface 0/4 through a Layer 2-connected access network. ISG will create a static session upon receipt of valid source IP address.

```
ip subscriber list mylist
 ip source 209.165.200.225 mac 0.7.f
interface GigabitEthernet 0/4
 ip subscriber l2-connected
  initiator static ip subscriber list mylist
```

Example: Creating IP Subscriber Sessions for Layer 2-Connected ISG Subscribers

The following example shows how to configure ISG to create IP sessions for subscribers who connect to ISG on GigabitEthernet interface0/0/1.401 through a Layer 2-connected access network. ISG will create IP sessions upon receipt of any frame with a valid source MAC address.

```
interface GigabitEthernet0/0/1.401
```

```
ip subscriber l2-connected
 initiator unclassified mac-address
```

Example: Configuring IP Session Recovery for DHCP-Initiated IP Session

The following example shows how to configure an ISG policy that applies a service called “FIRST-SERVICE” upon session restart for subscribers belonging to the VRF “FIRST”:

```
class-map type control TEST
 match vrf FIRST
policy-map type control GLOBAL
 class type control TEST event session-restart
  1 service-policy type service name FIRST-SERVICE
```

Example: Configuring an ISG Interface for Dynamic DHCP Class Association

In the following example, GigabitEthernet interface 1/0/0.400 is configured with DHCP class-aware functionality, which enables ISG to influence DHCP IP address assignment. If the service SERVICE-DHCP is activated, the DHCP pool DHCP-POOL2 is used for address assignment. Otherwise, the default pool DHCP-POOL1 is used.

```
interface GigabitEthernet1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.15.1 255.255.255.0 secondary
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE_406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP-POOL1
   network 10.1.10.0 255.255.255.0
   default-router 10.1.10.1
   lease 0 0 30
   class default
!
ip dhcp class default
!
ip dhcp pool DHCP-POOL2
   network 10.1.15.0 255.255.255.0
   default-router 10.1.15.1
   lease 0 0 30
   class DHCP_CLASS2
!
ip dhcp class DHCP-CLASS2
!
policy-map type service SERVICE-DHCP
 classname DHCP-CLASS2
!
```

Example: Configuring DHCP Address Pool Classes and Relay Actions for ISG

This section contains examples of DHCP address pool configuration and relay actions for ISG.

DHCP Server Coresident with ISG Configuration

In the following configuration example, the ISPs are ISP1 and ISP2 companies. The ISP1 company has its addresses assigned from an address pool that is dynamically allocated using on-demand address pools (ODAP). The ISP2 company has its customer addresses assigned from the address pool 10.100.0.0/16. Customers not associated with any ISP will have an address allocated from the address pool 10.1.0.0/16, and the lease time is set to 10 minutes.

```
!Address pool for ISP1 customers
ip dhcp pool isp1-pool
 origin dhcp
 class isp1
!
!Address pool for ISP2 customers
!
ip dhcp pool isp2-pool
 network 10.100.0.0 255.255.0.0
 class isp2
!
!Address pool for customers without an ISP
!
ip dhcp pool temp
 network 10.1.0.0 255.255.0.0
 lease 0 0 10
 class default
```

DHCP Relay Agent Coresident with ISG Configuration

In the following configuration example, there are two ISPs, “poolA” and “poolB”. The “poolA” ISP and its customers are allowed to have addresses in the ranges 10.1.0.0/16 and 10.3.0.0/16 and are relayed to the DHCP server at 10.55.10.1. The “poolB” ISP and its customers are allowed to have addresses in the range 10.2.0.0/16 and 10.4.0.0/16, and are relayed to the DHCP server at 10.10.2.1.

```
!Address ranges:
interface gigabitethernet1/0/0
 ip address 10.1.0.0 255.255.0.0
 ip address 10.2.0.0 255.255.0.0 secondary
interface gigabitethernet2/0/0
 ip address 10.3.0.2 255.255.0.0
 ip address 10.4.0.2 255.255.0.0
!Address pools for poolA1 and poolB2:
 ip dhcp pool poolA1
 relay source 10.1.0.2 255.255.0.0
 class poolA1
 relay target 10.55.10.1
!Address pool for poolA2:
ip dhcp pool poolA2
 relay source 10.3.0.2 255.255.0.0
 class poolA2
 relay target 10.55.10.1
!Address pools for poolB1 and poolB2:
ip dhcp pool poolB1
 relay source 10.2.0.2 255.255.0.0
 class poolB1
 relay target 10.10.2.1
ip dhcp pool poolB2
 relay source 10.4.0.0 255.255.0.0
 class poolB2
  relay target 10.10.2.1
```

Configuration of secure ARP for the relay uses the same configuration command as secure ARP uses on a DHCP server. It uses the **update arp** command in address-pool configuration mode. If the system allocates an address from this address pool, secure ARP is added to it. If the system relays a packet using this address pool, secure ARP is also added to it.

Example: Configuring ISG Dynamic VPN Selection

The following example shows a configuration in which subscribers are initially assigned an IP address from the DHCP global pool DHCP-POOL1. After a subscriber accesses the web portal and selects the Corporate VPN service, ISG performs a VRF transfer and the subscriber is assigned a new IP address from the DHCP pool, VPN-POOL1. In this case, a single multiservice interface is required.

```
!
ip vrf VPN_406_1001
rd 406:1001
route-target export 406:1001
route-target import 406:1001
!
interface GigabitEthernet 1/0/0.400
 encapsulation dot1Q 400
 ip address 10.1.10.1 255.255.255.0
 no snmp trap link-status
 service-policy type control RULE-406a
 ip subscriber l2-connected
  initiator dhcp class-aware
!
ip dhcp relay information trust-all
ip dhcp use vrf connected
!
!!!! Default Global DHCP Pool
!
ip dhcp excluded-address 10.1.10.1
!
ip dhcp pool DHCP-POOL1
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 lease 0 0 30
 class default
!
ip dhcp class default
!
!
!!! DHCP Pool for CorporateVPN
!
ip dhcp excluded-address 10.1.11.1
!
ip dhcp pool VPN-POOL1
 vrf VPN-406-1001
 network 10.1.11.0 255.255.255.0
 default-router 10.1.11.1
 lease 0 0 30
class DHCP-CLASS-VPN-406-1001
!
interface multiservice 1
 ip vrf forwarding VPN_406_1001
 ip address 10.1.11.1 255.255.255.0
 no keepalive
```

Example: Troubleshooting DHCP Server User Authentication

You can determine the DHCP authentication by using the **debug ip dhcp server events**, **debug ip dhcp server packets**, and **debug subscriber policy dpm event** commands. The following is sample output from the **debug subscriber policy dpm event** command:

```
*Apr 20 20:20:03.510: SG-DPM: DHCP Discover notification from client, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Could not find a dhcp_context for 001a.7014.c03e:
*Apr 20 20:20:03.510: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.510: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.510: SG-DPM: Session Initiation notification on Active
*Apr 20 20:20:03.510: SG-DPM: Allocated SHDB Handle (0xB6000252) for Mac address 001a.7014.c03e
```

```
*Apr 20 20:20:03.510: SG-DPM: Client is able to perform DHCP Authentication.Setting the SSS_INFOTYPE_DHCP_AUTH_KEY
*Apr 20 20:20:03.510: SG-DPM: Sending Session start to PM, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Request for Classname from client, mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: getting the context for mac_address = 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Sending an ID manager request with key as 001a.7014.c03e
*Apr 20 20:20:03.514: SG-DPM: Received reply from Id manager
*Apr 20 20:20:03.514: SG-DPM: No session found in ID manager
*Apr 20 20:20:03.514: SG-DPM: Processing sg_dpm_get_more_keys from SSS hdl 56000E52
*Apr 20 20:20:03.514: SG-DPM: DPM is providing Auth-User
```

You can also use the **show subscriber session detailed** and **show ip dhcp binding** commands to display subscriber information and DHCP pool information. The following is sample output from the **show ip dhcp binding** command:

```
Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
10.0.0.1            0100.1a70.1530.38       Nov 18 2008 03:43 PM    Automatic
```

Example: Configuring a Proxy Mobile IPv6 Domain by Using the Configuration from the AAA Server

The following example shows how to configure the PMIPv6 domain by using the AAA server configuration:

```
Device# configure terminal
Device(config)# ipv6 mobile pmipv6-domain D1 load-aaa
```

The following example shows how to configure the PMIPv6 domain by using the configuration from the AAA server and how to override the configuration for specific PMIPv6 domain parameters:

```
Device# configure terminal
Device(config)# ipv6 mobile pmipv6-domain D11 load-aaa
Device(config)# ipv6 mobile pmipv6-domain D11
Device(config-ipv6-pmipv6-domain)# gre-ipv4
Device(config-ipv6-pmipv6-domain)# auth-option spi 67 key ascii key1
```

Example: Configuring a Proxy Mobile IPv6 Domain When the Configuration from an AAA Server Is Not Available

The following example shows how to configure the PMIPv6 domain when an AAA server configuration is not available:

```
Device# configure terminal
Device(config)# ipv6 mobile pmipv6-domain D2
Device(config-ipv6-pmipv6-domain)# replay-protection timestamp window 200
Device(config-ipv6-pmipv6-domain)# auth-option spi 100 key ascii hi
Device(config-ipv6-pmipv6-domain)# encap ipv6-in-ipv6
!
Device(config-ipv6-pmipv6-domain)# lma lma1
Device(config-ipv6-pmipv6-domain-lma)# ipv4-address 10.1.1.1
Device(config-ipv6-pmipv6-domain-lma)# ipv6-address 2001:0DB8:2:3::1
Device(config-ipv6-pmipv6-domain-lma)# exit
!
Device(config-ipv6-pmipv6-domain)# mag mag1
Device(config-ipv6-pmipv6-domain-mag)# ipv4-address 10.1.3.1
Device(config-ipv6-pmipv6-domain-mag)# ipv6-address 2001:0DB8:2:5::1
Device(config-ipv6-pmipv6-domain-mag)# exit
!
```

```
Device(config-ipv6-pmipv6-domain)# nai example1@example.com
Device(config-ipv6-pmipv6-domain-mn)# lma lma1
Device(config-ipv6-pmipv6-domain-mn)# int att gigabitethernet l2-addr 02c7.f800.0422
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key up 1234
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key down 5678
Device(config-ipv6-pmipv6-domain-mn)# service ipv4
Device(config-ipv6-pmipv6-domain-mn)# end
```

Example: Configuring a Minimum Configuration for a Domain When the Configuration from the AAA Server Is Not Available

The following example shows how to configure a minimum configuration for a domain when the AAA server configuration is not available:

```
Device# configure terminal
Device(config)# ipv6 mobile pmipv6-domain D2
Device(config-ipv6-pmipv6-domain)# replay-protection timestamp window 200
Device(config-ipv6-pmipv6-domain)# auth-option spi 100 key ascii hi
Device(config-ipv6-pmipv6-domain)# encap ipv6-in-ipv6
!
Device(config-ipv6-pmipv6-domain)# lma lma1
Device(config-ipv6-pmipv6-domain-lma)# ipv4-address 10.1.1.1
Device(config-ipv6-pmipv6-domain-lma)# ipv6-address 2001:0DB8:2:3::1
Device(config-ipv6-pmipv6-domain-lma)# exit
!
Device(config-ipv6-pmipv6-domain)# mag mag1
Device(config-ipv6-pmipv6-domain-mag)# ipv4-address 10.1.3.1
Device(config-ipv6-pmipv6-domain-mag)# ipv6-address 2001:0DB8:2:5::1
Device(config-ipv6-pmipv6-domain-mag)# exit
!
Device(config-ipv6-pmipv6-domain)# nai example@example.com
Device(config-ipv6-pmipv6-domain-mn)# lma lma1
Device(config-ipv6-pmipv6-domain-mn)# int att GigabitETHERNET l2-addr 02c7.f800.0422
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key up 1234
Device(config-ipv6-pmipv6-domain-mn)# gre-encap-key down 5678
Device(config-ipv6-pmipv6-domain-mn)# service ipv4
Device(config-ipv6-pmipv6-domain-mn)# network-name example1
Device(config-ipv6-pmipv6-domain-mn)# end
```

Example: Configuring MCSA

```
Device> enable
Device# configure terminal
Device(config) mcsa
Device(config-mcsa) enable sessionmgr
Device(config-mcsa) end
Device# show mcsa statistics
```

Example: Configuring a Mobile Access Gateway

The following example shows the minimum configuration required to enable MAG:

```
Device# configure terminal
Device(config)# ipv6 mobile pmipv6-domain D2
Device(config-ipv6-pmipv6-domain)# lma lma1
Device(config-ipv6-pmipv6-domain-lma)# ipv4-address 10.1.1.1
Device(config-ipv6-pmipv6-domain-lma)# ipv6-address 2001:0DB8:2:3::1
Device(config-ipv6-pmipv6-domain-lma)# exit
Device(config-ipv6-pmipv6-domain)# lma lma2
Device(config-ipv6-pmipv6-domain-lma)# ipv4-address 10.2.1.1
Device(config-ipv6-pmipv6-domain-lma)# ipv6-address 2001:0DB8:2:4::1
Device(config-ipv6-pmipv6-domain-lma)# exit
Device(config-ipv6-pmipv6-domain)# nai example1@example.com
Device(config-ipv6-pmipv6-domain-mn)# lma lma1
```

```
Device(config-ipv6-pmipv6-domain-mn)# exit
Device(config-ipv6-pmipv6-domain)# nai example2@example.com
Device(config-ipv6-pmipv6-domain-mn)# lma lma2
Device(config-ipv6-pmipv6-domain-mn)# exit
Device(config)# ipv6 mobile pmipv6-mag mag1 domain D2
Device(config-ipv6-pmipv6-mag)# address ipv6 2001:DB8:0:0:E000::F
Device(config-ipv6-pmipv6-mag)# address ipv4 10.2.1.1
Device(ipv6-mag-config)# interface gigabitethernet 0/0/0
Device(ipv6-mag-config)# role 3gpp
Device(ipv6-mag-config)# apn a
Device(ipv6-mag-config)# exit
```

Where to Go Next

For more information about configuring services on the iWAG, see the following:

- To configure PMIPv6 support for MAG, see the *Cisco IOS IP Mobility: Mobile IP Configuration Guide*.
- To configure GTP services on the GGSN, see the *GGSN Configuration Guide*.
- To configure ISG access for IP subscriber sessions, see the *ISG Configuration Guide*.

Additional References for Implementing iWAG

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Master Command List, All Releases*
ISG concepts, configuration tasks, and examples	*ISG Configuration Guide*
ISG commands	*ISG Command Reference*
Mobile IP configuration concepts, tasks, and examples	*IP Mobility: Mobile IP Configuration Guide*
IP Mobility commands	*IP Mobility Command Reference*
GGSN configuration concepts, tasks, and examples	*Mobile Wireless GGSN Configuration Guide*
GTP configuration concepts, tasks, and examples	*GTP on iWAG Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 3775	Mobility Support in IPv6
RFC 5213	Proxy Mobile IPv6

Standard/RFC	Title
RFC 5844	IPv4 Support for Proxy Mobile IPv6

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Implementing iWAG

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 Intelligent Wireless Access Gateway

Feature Name	Releases	Feature Information
Intelligent Wireless Access Gateway	Cisco IOS XE Release 3.8S	Intelligent Wireless Access Gateway (iWAG) is a Cisco IOS XE software feature set that supports clientless integration into the existing Gateway General Packet Radio Service (GPRS) Support Node (GGSN). iWAG provides a WiFi offload option to 3G service providers by enabling a single-box solution of providing the combined functionality of Proxy Mobile IPv6 (PMIPv6), and GPRS Tunneling Protocol (GTP) on the Intelligent Services Gateway (ISG) framework. The following commands were introduced or modified: **clear mcsa statistics**, **dynamic mag learning**, **enable sessionmgr**, **generate grekey**, **mcsa**, **sessionmgr**, **show mcsa statistics**, and **vrfid** (proxy mobile IPv6).