Intelligent Wireless Access Gateway Configuration Guide

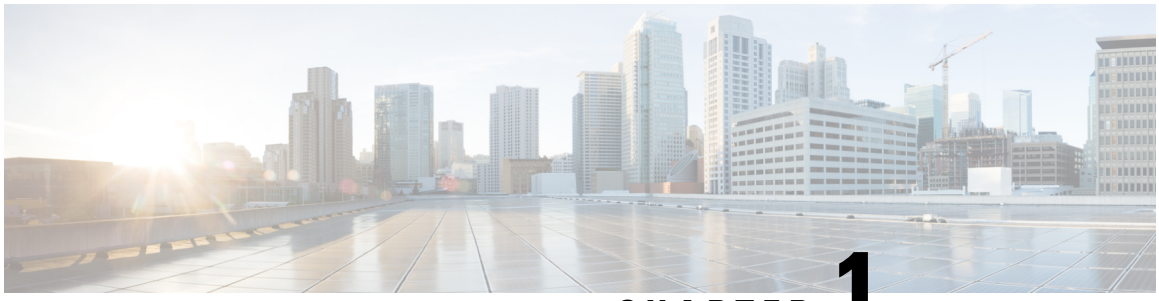
First Published: 2013-07-26

Last Modified: 2015-03-26

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

Text Part Number: OL-30226-06

CONTENTS



CHAPTER 1

Overview of the Intelligent Wireless Access Gateway

Service providers use a combination of WiFi and mobility offerings to offload their mobility networks in the area of high-concentration service usage. This led to the evolution of the Intelligent Wireless Access Gateway (iWAG).

The iWAG provides a WiFi offload option to 4G and 3G service providers by enabling a single-box solution that provides the combined functionality of Proxy Mobile IPv6 (PMIPv6) and GPRS Tunneling Protocol (GTP) on the Cisco Intelligent Services Gateway (Cisco ISG) framework. This document provides information about the iWAG and how to configure it, and contains the following sections:

Finding Feature Information

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

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

Prerequisites for the iWAG

- Enable mobile client service abstraction (MCSA).
- Enable the **ipv6 unicast-routing** command.

Restrictions for the iWAG

- Roaming from a 3G mobility network to a WLAN is not supported for the GTP and Cisco ISG sessions.
- IP subscriber-routed (L3) sessions are not supported.
- IPv6 and quality of service (QoS) are not supported in a 3G mobility network.
- Only newly established calls are offloaded to the WLAN Third-Generation Partnership Project (3GPP) IP access.
- The iWAG solution for WLAN offload is currently available only for the 3G Universal Mobile Telecommunications System (UMTS).

Information About the iWAG

The iWAG deployment includes a combination of simple IP users (traditional ISG and WiFi) and mobile IP users (PMIPv6 or GTP tunneling). The term *mobility service* is used to refer to either the GTP service or the PMIPv6 service applied to user traffic. The iWAG provides mobility services to mobile IP users, and as a result, a mobile client can seamlessly access a 3G or 4G mobility network. However, the iWAG does not provide mobility services to simple IP users. Therefore, simple IP users can access the Public Wireless LAN (PWLAN) network through the Cisco ISG. Clients are devices that access WiFi Internet (public wireless), where possible. However, if WiFi is not available, the same clients can

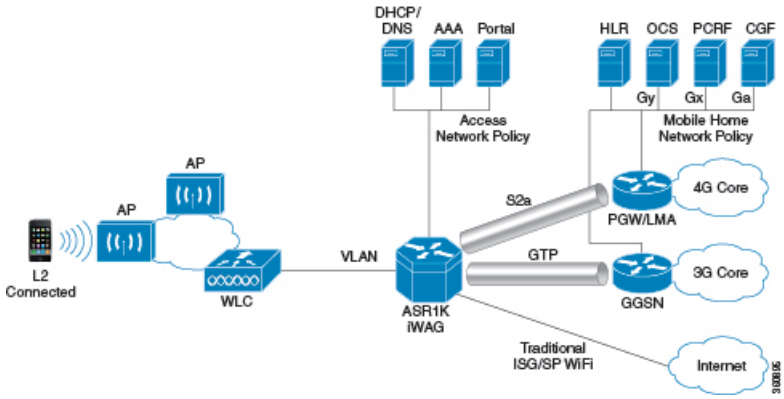
connect to the Internet service using a 3G or 4G mobility network.

The iWAG has a transport or switching element with Cisco ISG subscriber awareness. The iWAG also has RADIUS-based authentication and accounting, and policy-based subscriber routing for the WiFi wholesale model.

For more information about the iWAG, see the Overview of iWAG video.

The following figure shows a deployment model of the iWAG on a Cisco ASR 1000 Series Aggregation Services Router.

Figure 1: iWAG Deployment on a Cisco ASR 1000 Series Aggregation Services Router



Benefits of the iWAG

The iWAG offers the following benefits for mobile operators:

- Reduces network congestion by reducing OpEx and increasing network efficiency by offloading 3G and 4G traffic.
- Provides access to 3G and 4G core inspite of a lack of or weak cell signal, leading to subscriber retention.
- Lowers CapEx on per user basis or bandwidth basis in dense metro environments.

The iWAG offers the following benefits for wireline and WiFi operators:

- Provides WiFi security and subscriber control. Delivers scalable, manageable, and secure wireless connectivity.
- Enables new revenue-sharing business models, such as Mobile Virtual Network Operators (MVNO) and others.
- Delivers a WiFi platform that offers new location-based services.

The iWAG offers the following benefits for subscribers:

- Provides enhanced quality of experience to subscribers on WiFi networks.
- Provides unified billing across access networks.
- Provides mobility across radio access technologies—3G or 4G to WiFi and WiFi to WiFi.
- Provides multiple options within the WiFi platform, thereby enabling location-based services.

AAA Attributes

The following table lists the authentication, authorization, and accounting (AAA) attributes required for the iWAG configuration:

Note The following indicate the availability of the attributes:

C: Conditional

M: Mandatory

O: Optional

N: Not present

Table 1: iWAG AAA Attributes

Attribute /Subattribute	Attribute Name	Value	Description	ARq[1]	AA[2]	ARj[3]	AS[4]	CoA[5]
1	User Name	String	Network Access Identifier	M	M	M	O	C

Attribute /Subattribute	Attribute Name	Value	Description	ARq[1]	AA[2]	ARj[3]	AS[4]	CoA[5]
4	NAS-IP -Address	String	IP address of the MAG	M	N	N	M	O
31	Calling-Station-ID	String	MAC address of the mobile node	M	M	M	M	M
26/10415/1	3GPP-IMSI	String	3GPP IMSI	N	O	N	N	O
26/10415/13	3GPP -Charging -Characteristics	String	Rules for producing charging information	N	O	N	O	O
26/9/1	Cisco-Service -Selection	String	Service Identifier (APN)	N	C	N	N	C
26/9/1	Cisco -Mobile -Node -Identifier	String	Mobile Node Identifier	N	M	N	M	C
26/9/1	Cisco -WLAN -SSID	String	SSID of the Access Point	C	N	N	C	N
26/9/1	Cisco -MSISDN	String	Mobile Subscriber ISDN number	N	C	N	C	C
26/9/1	Cisco-MN -Service	ENUM • none • ipv4 • ipv6 • dual	Mobile Node Service type	N	M	N	M	O

Attribute /Subattribute	Attribute Name	Value	Description	ARq[1]	AA[2]	ARj[3]	AS[4]	CoA[5]
26/9/1	Cisco-MPC -Protocol -Interface	ENUM • none • pmipv6 • gtpv1 • pmipv4	Protocol Interface to be used for interfacing with MPC	N	M	N	O	O
26/9/1	Cisco -Multihoming -Support	Binary	True/False: Multihoming support for mobile node	N	O	N	N	O
26/9/1	Cisco -Uplink -GRE -Key	Integer	32-bit GRE Key to be used on the uplink path (4-octet hex encoding)	N	O	N	N	O
26/9/1	Cisco -Downlink -GRE -Key	Integer	32-bit GRE Key to be used on the downlink path (4-octet hex encoding)	N	O	N	N	O
26/9/1	Cisco -Home -LMA -IPv6 -Address	String	Mobile node's Home LMA IPv6 address	N	C	N	N	O
26/9/1	Cisco -Visited -LMA -IPv6 -Address	String	Mobile node's Visited LMA IPv6 address	N	C	N	N	O

Attribute /Subattribute	Attribute Name	Value	Description	ARq[1]	AA[2]	ARj[3]	AS[4]	CoA[5]
26/9/1	Cisco -Home -LMA -IPv4 -Address	IPv4 Address	Mobile node's Home LMA IPv4 address	N	C	N	N	O
26/9/1	Cisco -Visited -LMA -IPv4 -Address	IPv4 Address	Mobile node's Visited LMA IPv4 address	N	C	N	N	O
26/9/1	Cisco -Home -IPv4 -Home -Address	IPv4 Address	Mobile node's Visited LMA IPv4 address	N	O	N	N	C
26/9/1	Cisco -Visited -IPv4 -Home -Address	IPv4 Address	Mobile node's Visited IPv4 address	N	O	N	N	C
26 /10415 /5	THREEGENPP _GPRS _QOS _PROFILE	String	GRPS QoS Profile	N	O	N	N	N
26 /10415 /7	THREEGENPP _GGSN _ADDRESS	IPv4 Address	GGSN's Address	N	O	N	N	N

Attribute /Subattribute	Attribute Name	Value	Description	ARq[1]	AA[2]	ARj[3]	AS[4]	CoA[5]
26/9/1	Cisco -Access -Vrf -Id	String	Access-side VRF ID	N	O	N	N	N
26/9/1	Cisco -Apn -Vrf -Id	IPv4 Address	GGSN's IPv4 address	N	O	N	N	N

1 Access Request
2 Access Accept
3 Access Reject
4 Accounting Start
5 Change of Authorization

Supported Hardware and Software Compatibility Matrix for the iWAG

Chassis	RP Memory	ESP
Cisco ASR 1001 Router	Integrated RP with 16 GB	Integrated
Cisco ASR 1002-X Router	Integrated RP with 16 GB	Integrated
Cisco ASR 1004 Router	RP2 16 GB	ESP-40G
Cisco ASR 1006 Router and Cisco ASR 1013 Router offering duplex RP or ESP setup	RP2 16 GB	ESP-40G
Cisco ASR 1006 Router and Cisco ASR 1013 Router offering duplex RP or ESP setup	RP2 16 GB	ESP-100G

For information about the field-replaceable units (FRUs) of the Cisco ASR 1000 Series Aggregation Services Routers supported by each ROMmon release, see the "ROMmon Release Requirements" section in the Cisco ASR 1000 Series Aggregation Services Routers Release Notes.

Stateless Inter-Chassis Redundancy Support Matrix for the iWAG

Session Tunneling	Local Breakout (No Tunneling)		GTPv1		GTPv2		PMIPv6 (IWAG=MAG)	
	With HSRP	*Without HSRP*	*With HSRP*	*Without HSRP*	*With HSRP*	*Without HSRP*	*With HSRP*	*Without HSRP*
Layer 2	Yes	No	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported
Layer 3	Yes	No	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
EoGRE	Yes	No	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported

How to Configure the iWAG

Configuring the iWAG for Simple IP Users

You must configure the Cisco Intelligent Services Gateway (ISG) for the iWAG to enable simple IP users to access Internet services.

The tasks listed below enable IP sessions and indicate how these sessions are identified. For detailed steps, see the "Creating ISG Sessions for IP Subscribers" section in the Intelligent Services Gateway Configuration Guide.

- Creating ISG IP interface sessions
- Creating ISG Static Sessions
- Creating ISG IP Subnet Sessions
- Configuring IP Session Recovery for DHCP-Initiated IP Sessions
- Verifying ISG IP Subscriber Sessions
- Clearing ISG IP Subscriber Sessions
- Troubleshooting ISG IP Subscriber Sessions

You must configure DHCP support in your network before performing the tasks listed below. For detailed steps on assigning IP addresses using DHCP, see the "Assigning ISG Subscriber IP Addresses by Using DHCP" section in the Intelligent Services Gateway Configuration Guide.

- Configuring an ISG Interface for Dynamic DHCP Class Association
- Configuring DHCP Server User Authentication
- Configuring a DHCP Class in a Service Policy Map
- Configuring a DHCP Class in a Service Profile or User Profile on the AAA Server

- Configuring a DHCP Server IP Address

Configuring the iWAG for 3G Mobile IP Users

You must configure GTP for the iWAG to allow access to 3G mobile IP users. The various tasks described in the following sections are mandatory for configuring the iWAG for 3G mobile IP users.

Configuring Authentication, Authorization, and Accounting for the iWAG

This section describes how to configure authentication, authorization, and accounting (AAA) for the iWAG on the Cisco ASR 1000 Series Aggregation Services Routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
5. **server-private** *ip-address* **[auth-port** *port-number* | **acct-port** *port-number] [non-standard] [timeout seconds] [retransmit retries] [* **key** *string]*
6. **aaa authentication login {default |** *list-name}* { **[passwd-expiry]** *method1 [method2...]* }
7. **aaa authorization network** *authorization-name group server-group name*
8. **aaa authorization subscriber-service** *{default {cache* | *group* | *local}* | *list-name}* **method1 [method2...]**
9. **aaa accounting** { **auth-proxy**| *system* | *network* | *exec* | *connection* | *commands level* | *dot1x* } { { **default |** *list-name* } [**vrf** *vrf-name] {start-stop* | *stop-only* | *none}* **[broadcast]** *group group-name*
10. **action-type** *{none* | *start-stop* | *stop-only}*
11. **group** *{tacacs+ server-group}*
12. **aaa accounting** { **auth-proxy** | *system* | *network* | *exec* | *connection* | *commands level* | *dot1x* } { **default** |*list-name* } [**vrf** *vrf-name*] *{start-stop* | *stop-only* | *none}* **[broadcast] group** *group-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router# enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model.

	Command or Action	Purpose
Step 4	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius AAA_SERVER_CAR`	Groups different RADIUS server hosts into distinct lists and methods.
Step 5	**server-private** *ip-address* **[auth-port** *port-number* | **acct-port** *port-number] [non-standard] [timeout seconds] [retransmit retries] [* **key** *string]* **Example:** `Router(config-sg-radius)# server-private 5.3.1.76 auth-port 2145 acct-port 2146 key cisco`	Configures the IP address of the private RADIUS server for the group server.
Step 6	**aaa authentication login {default |** *list-name}* { **[passwd-expiry]** *method1 [method2...]* } **Example:** `Router(config-sg-radius)# aaa authentication login default none`	Sets AAA authentication at login.
Step 7	**aaa authorization network** *authorization-name group server-group name* **Example:** `Router(config)# aaa authorization network ISG_PROXY_LIST group AAA_SERVER_CAR`	Runs authorization for all network-related service requests.
Step 8	**aaa authorization subscriber-service** *{default {cache | group | local} | list-name}* **method1 [method2...]** **Example:** `Router(config)# aaa authorization subscriber-service default local group AAA_SERVER_CAR`	Specifies one or more AAA authorization methods for the Cisco ISG to provide subscriber service.
Step 9	**aaa accounting** { **auth-proxy**| *system* | *network* | *exec* | *connection* | *commands level* | *dot1x* } { { **default |** *list-name* } [**vrf** *vrf-name] {start-stop | stop-only | none}* **[broadcast]** *group group-name* **Example:** `Router(config)# aaa accounting network PROXY_TO_CAR`	Enables AAA accounting of requested services for billing and security purposes when either the RADIUS server or the TACACS+ server is used.
Step 10	**action-type** *{none | start-stop | stop-only}* **Example:** `Router(cfg-acct-mlist)# action-type start-stop`	Enables the type of actions to be performed on accounting records.
Step 11	**group** *{tacacs+ server-group}* **Example:** `Router(cfg-preauth)# group AAA_SERVER_CAR`	Specifies the AAA TACACS+ server group to use for preauthentication.

	Command or Action	Purpose
Step 12	**aaa accounting** { **auth-proxy** | *system* | *network* | *exec* | *connection* | *commands level* | *dot1x* } { **default** | *list-name* } [**vrf** *vrf-name*] *{start-stop* | *stop-only* | *none}* **[broadcast] group** *group-name* **Example:** `Router(config)# aaa accounting network ISG_PROXY_LIST start-stop group AAA_SERVER_CAR`	Enables AAA accounting of requested services for billing and security purposes when you use either the RADIUS server or the TACACS+ server.

Configuring DHCP when the iWAG Acts as a DHCP Proxy

This section describes how to configure the Dynamic Host Configuration Protocol (DHCP) for the iWAG solution when the iWAG acts as a DHCP proxy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp excluded-address** *[vrf vrf-name] ip-address*
4. **ip dhcp pool** *pool-name*
5. **network network-number** *[mask [secondary] | /prefix-length [secondary]*
6. **default-router ip-address** *[last-ip-address]*
7. **domain-name** *domain*
8. **lease** *{days [hours [minutes]] | infinite}*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**ip dhcp excluded-address** *[vrf vrf-name] ip-address* **Example:** `Router(config)# ip dhcp excluded-address 192.168.10.1`	Specifies the IP address that a DHCP server should not assign to DHCP clients.
Step 4	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool test`	Configures a DHCP address pool on a DHCP server and enters the DHCP pool configuration mode.

	Command or Action	Purpose
Step 5	**network network-number** *[mask [secondary] | /prefix-length [secondary]* **Example:** `Router(dhcp-config)# network 192.168.0.0 255.255.0.0`	Configures the network number and mask for a DHCP address pool primary subnet or DHCP address pool secondary subnet on a Cisco IOS DHCP server.
Step 6	**default-router ip-address** *[last-ip-address]* **Example:** `Router(dhcp-config)# default-router 192.168.10.1`	Specifies the default router list for a DHCP client.
Step 7	**domain-name** *domain* **Example:** `Router(dhcp-config)# domain-name example.com`	Specifies the domain name for a DHCP client.
Step 8	**lease** *{days [hours [minutes]] | infinite}* **Example:** `Router(dhcp-config)# lease 1 2 2`	Configures the duration of the lease for an IP address that is assigned from a Cisco IOS DHCP server to a DHCP client. **Note** The DHCP pool lease time is applicable only to *simple* sessions. For mobile GTP sessions, lease time from the GTP configuration will be used. Under the GTP configuration, lease duration should be configured the same way as the address hold timer in the GGSN or PGW.

Configuring the Cisco ISG Class Map and Policy Map for the iWAG

This section describes how to configure the Cisco ISG class map and policy map for the iWAG.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type traffic match-any** *class-map-name*
4. **match access-group output** *{access-group | name access-group-name}*
5. **match access-group input** *{access-group | name access-group-name}*
6. **policy-map type service** *policy-map-name*
7. **[priority] class type traffic** *{class-map-name | default {in-out | input | output } }*
8. **accounting aaa list** *aaa-method-list*
9. **[priority] class type traffic** *{ class-map-name | default {in-out | input | output}}*
10. **drop**
11. **policy-map type control** *policy-map-name*
12. **class type control** *control-class-name* | *always* } [**event** { *access-reject* | **account-logoff** | *account-logon* | **acct-notification** | *credit-exhausted* | **dummy-event** | *quota-depleted* | **radius-timeout** | *service-failed*

| **service-start |** *service-stop* | **session-default-service |** *session-restart* | **session-service-found |** *session-start* | **timed-policy-expiry** }]

13. **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* } }
14. **action-number authorize** [**aaa** {**list-name | list** *{ list-name* | *default*} } [**password** *password*]] [**upon network-service-found** *{continue* | *stop*}] [**use method authorization-type**] *identifier* **identifier-type** [*plus identifier-type*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**class-map type traffic match-any** *class-map-name* **Example:** `Router(config)# class-map type traffic match-any TC_OPENGARDEN`	Creates or modifies a traffic class map that is used for matching packets to a specified Cisco ISG traffic class.
Step 4	**match access-group output** *{access-group*	*name access-group-name}* **Example:** `Router(config-traffic-classmap)# match access-group output name ACL_OUT_OPENGARDEN`	Configures the match criteria for a Cisco ISG traffic class map on the basis of the specified access control list (ACL).
Step 5	**match access-group input** *{access-group*	*name access-group-name}* **Example:** `Router(config-traffic-classmap)# match access-group input name ACL_IN_OPENGARDEN`	Configures the match criteria for a Cisco ISG traffic class map on the basis of the specified ACL.
Step 6	**policy-map type service** *policy-map-name* **Example:** `Router(config)# policy-map type service OPENGARDEN_SERVICE`	Creates or modifies a service policy map that is used to define a Cisco ISG subscriber service.

	Command or Action	Purpose
Step 7	**[priority] class type traffic** *{class-map-name | default {in-out | input | output } }* **Example:** `Router(config-service-policymap)# 20 class type traffic TC_OPENGARDEN`	Creates or modifies a traffic class map that is used for matching packets to a specified Cisco ISG traffic class.
Step 8	**accounting aaa list** *aaa-method-list* **Example:** `Router(config-service-policymap)# accounting aaa list PROXY_TO_CAR`	Enables Cisco ISG accounting and specifies an AAA method list to which accounting updates are forwarded.
Step 9	**[priority] class type traffic** *{ class-map-name | default {in-out | input | output}}* **Example:** `Router(config-service-policymap)# class type traffic default in-out`	Creates or modifies a traffic class map that is used for matching packets to a specified Cisco ISG traffic class.
Step 10	**drop** **Example:** `Router(config-service-policymap)# drop`	Configures a Cisco ISG to discard packets belonging to the default traffic class.
Step 11	**policy-map type control** *policy-map-name* **Example:** `Router(config)# policy-map type control BB_PROFILE`	Creates or modifies a control policy map that defines a Cisco ISG control policy.
Step 12	**class type control** *control-class-name* | *always* } [**event** { *access-reject* | **account-logoff** | *account-logon* | **acct-notification** | *credit-exhausted* | **dummy-event** | *quota-depleted* | **radius-timeout** | *service-failed* | **service-start** | *service-stop* | **session-default-service** | *session-restart* | **session-service-found** | *session-start* | **timed-policy-expiry** }] **Example:** `Router (config-control-policymap)# class type control always event session-start`	Specifies a control class for which actions can be configured in a Cisco ISG control policy.
Step 13	**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:**	Activates a Cisco ISG service.

	Command or Action	Purpose
	`Router(config-control-policymap-class-control)# 10 service-policy type service name OPENGARDEN_SERVICE`	
Step 14	**action-number authorize** [**aaa** {**list-name** | **list** *{ list-name* | *default* }} [**password** *password*]] [**upon network-service-found** *{continue* | *stop* }] [**use method authorization-type**] *identifier* **identifier-type** [*plus identifier-type*] **Example:** `Router(config-control-policymap-class-control)# 20 authorize aaa list ISG_PROXY_LIST password cisco identifier mac-address`	Initiates a request for authorization based on a specified identifier in a Cisco ISG control policy.

Configuring a Session Initiator for the iWAG

This section describes how to configure a session initiator for the iWAG solution. A session can be created using different triggers, such as an unknown MAC address, an unclassified MAC address, a RADIUS message with the Cisco ASR 1000 Series Aggregation Services Router acting as RADIUS proxy or a DHCP DISCOVER message with the Cisco ASR 1000 Series Aggregation Services Router acting as DHCP proxy.

Note To enable roaming, one initiator is required for DHCP sessions and another for the unclassified MAC.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *slot/subslot/port*
4. **description** *string*
5. **ip address** *ip-address mask [secondary [vrf vrf-name]]*
6. **negotiation auto**
7. **service-policy type control** *policy-map-name*
8. **ip subscriber {l2-connected}**
9. **initiator {dhcp | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac-address}**
10. **initiator {dhcp | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac-address}**

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface GigabitEthernet** *slot/subslot/port* **Example:** `Router(config)# interface GigabitEthernet 1/3/3`	Enters the interface configuration mode for Gigabit Ethernet.
Step 4	**description** *string* **Example:** `Router(config-if)# description access interface connected to subscriber`	Adds a description to an interface configuration.
Step 5	**ip address** *ip-address mask [secondary [vrf vrf-name]]* **Example:** `Router(config-if)# ip address 192.171.10.1 255.255.0.0`	Sets a primary IP address or secondary IP address for an interface.
Step 6	**negotiation auto** **Example:** `Router(config-if)# negotiation auto`	Enables auto negotiation on a Gigabit Ethernet interface.
Step 7	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)# service-policy type control BB_Profile`	Applies a control policy to a context.
Step 8	**ip subscriber {l2-connected}** **Example:** `Router(config-if)# ip subscriber l2-connected`	Enables Cisco ISG IP subscriber support on an interface and specifies the access method that IP subscribers use for connecting to the Cisco ISG on an interface. **Note** The iWAG does not support the routed access method.
Step 9	**initiator {dhcp | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac-address}** **Example:** `Router(config-subscriber)# initiator unclassified mac-address`	Enables the Cisco ISG to create an IP subscriber session upon receipt of a specified type of packet.

	Command or Action	Purpose
Step 10	**initiator {dhcp | radius-proxy | static ip subscriber list** *listname* **| unclassified ip | unclassified mac-address}** **Example:** `Router(config-subscriber)# initiator dhcp`	Enables the Cisco ISG to create an IP subscriber session upon receipt of a specified type of packet.

Configuring a GGSN-Facing Interface for the iWAG

This section describes how to configure a GGSN-facing interface between the iWAG solution and the GGSN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface GigabitEthernet** *slot/subslot/port*
4. **description** *string*
5. **ip address** *ip-address mask [secondary [vrf vrf-name]]*
6. **negotiation auto**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface GigabitEthernet** *slot/subslot/port* **Example:** `Router(config)# interface GigabitEthernet 1/3/5`	Enters the interface configuration mode for Gigabit Ethernet interface.
Step 4	**description** *string* **Example:** `Router(config-if)#description interface connected to GGSN`	Adds a description to an interface configuration.
Step 5	**ip address** *ip-address mask [secondary [vrf vrf-name]]* **Example:** `Router(config-if)# ip address 192.170.10.1 255.255.0.0`	Sets a primary IP address or secondary IP address for an interface.

	Command or Action	Purpose
Step 6	**negotiation auto** **Example:** `Router(config-if)# negotiation auto`	Enables auto negotiation on a Gigabit Ethernet interface.

Enabling Mobile Client Service Abstraction

This section describes how to enable Mobile Client Service Abstraction (MCSA) for PMIPv6.

Note Enabling MCSA is mandatory before you enable the Mobility feature in the Cisco ASR 1000 Series Aggregation Services Routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mcsa**
4. **enable sessionmgr**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**mcsa** **Example:** `Router(config)# mcsa`	Enables MCSA on the Cisco ASR 1000 Series Aggregation Services Router.
Step 4	**enable sessionmgr** **Example:** `Router(config-mcsa)# enable sessionmgr`	Enables MCSA to receive notifications from the Cisco ISG.

Configuring the GTP of the iWAG

This section describes how to configure GTPv1 for the iWAG solution.

Before you begin

Enable MCSA.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gtp**
4. **n3-***request number of requests*
5. **interval t3-response** *number of seconds*
6. **interval echo-request** *request-number*
7. **interface local GigabitEthernet** *slot/subslot/port*
8. **apn-name** *apn-name*
9. **ip address ggsn** *ip-address*
10. **default-gw** *address* **prefix-len** *value*
11. **dns-server** *ip-address*
12. **dhcp-server** *ip-address*
13. **dhcp-lease** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**gtp** **Example:** `Router(config)# gtp`	Configures the GTP for the iWAG solution on the Cisco ASR 1000 Series Aggregation Services Router.
Step 4	**n3-***request number of requests* **Example:** `Router(config-gtp)# n3-request 3`	Specifies the number of times a control message must be retried before a failure message is sent. The default value is 5.
Step 5	**interval t3-response** *number of seconds* **Example:** `Router(config-gtp)# interval t3-response 10`	Specifies the time interval, in seconds, for which the SGSN of the iWAG waits for a response for the control message sent. The default value is 1.

	Command or Action	Purpose
Step 6	**interval echo-request** *request-number* **Example:** `Router(config-gtp)# interval echo-request 60`	Specifies the time interval, in seconds, for which the SGSN of the iWAG waits for before sending an echo request message. The range is from 60 to 65535. The default value is 60. The value of 0 disables the Echo Request feature.
Step 7	**interface local GigabitEthernet** *slot/subslot/port* **Example:** `Router(config-gtp)# interface local GigabitEthernet 0/0/3`	Configures the transport interface to communicate with the GGSN.
Step 8	**apn-name** *apn-name* **Example:** `Router(config-gtp)# apn-name example.com`	Configures an APN name string for GPRS load balancing.
Step 9	**ip address ggsn** *ip-address* **Example:** `Router(config-gtp-apn)# ip address ggsn 192.170.10.2`	Sets the IP address for the GGSN.
Step 10	**default-gw** *address* **prefix-len** *value* **Example:** `Router(config-gtp-apn)# default-gw 192.171.10.1 prefix-len 16`	Specifies the default gateway address of the subscriber. **Note** This is the default gateway address of the IP provided by the GGSN using GTP, and not the default gateway address on the physical local interface that the subscriber is connected to. They can be the same, but we recommend that they be two different subnets.
Step 11	**dns-server** *ip-address* **Example:** `Router(config-gtp-apn)# dns-server 192.165.1.1`	Specifies the Domain Name System (DNS) IP server that is available for a DHCP client.
Step 12	**dhcp-server** *ip-address* **Example:** `Router(config-gtp-apn)# dhcp-server 192.168.10.1`	Specifies the primary and backup DHCP server that is used to allocate IP addresses, the IP address can be a local iWAG interface address, to mobile station users entering a particular public data network (PDN) access point.
Step 13	**dhcp-lease** *seconds* **Example:** `Router(config-gtp-apn)# dhcp-lease 3000`	Configures the duration (in seconds) of the lease for an IP address that is assigned from a Cisco IOS DHCP Server to a DHCP client.

Configuring the iWAG for 4G Mobile IP Users

Configuring PMIPv6 for the iWAG

You must configure PMIPv6 for the iWAG to allow access to mobile IP users.

The tasks listed below describe the procedures involved in configuring the Mobile Access Gateway. For detailed steps, see the "How to Configure Proxy Mobile IPv6 Support for MAG Functionality" section in the *IP Mobility: PMIPv6 Configuration Guide, Cisco IOS XE Release 3S* .

- Configuring a Proxy Mobile IPv6 Domain by Using the Configuration from the AAA Server
- Configuring the Minimum Configuration for a MAG to Function
- Configuring a Detailed Configuration for a MAG when an AAA Server is not Available
- Configuring a Minimum Configuration for a MAG
- Configuring a Detailed Configuration for a MAG

The tasks listed below describe the procedures involved in configuring Local Mobility Anchor. For detailed steps, see the "How to Configure Proxy Mobile IPv6 Support for LMA Functionality" section in the *IP Mobility: PMIPv6 Configuration Guide, Cisco IOS XE Release 3S* .

- Configuring a Proxy Mobile IPv6 Domain by Using the Configuration from the AAA Server
- Configuring a Minimum Configuration for a Domain When an AAA Server Is Not Available
- Configuring a Detailed Configuration for a Domain When the AAA Server Is Not Available
- Configuring a Minimum Configuration for an LMA
- Configuring a Detailed Configuration for an LMA

Enabling Mobile Client Service Abstraction

This section describes how to enable Mobile Client Service Abstraction (MCSA) for PMIPv6.

Note Enabling MCSA is mandatory before you enable the Mobility feature in the Cisco ASR 1000 Series Aggregation Services Routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mcsa**
4. **enable sessionmgr**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables the privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**mcsa** **Example:** `Router(config)# mcsa`	Enables MCSA on the Cisco ASR 1000 Series Aggregation Services Router.
Step 4	**enable sessionmgr** **Example:** `Router(config-mcsa)# enable sessionmgr`	Enables MCSA to receive notifications from the Cisco ISG.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ISG concepts, configuration tasks, and examples	*ISG Configuration Guide*
ISG commands	Cisco IOS Intelligent Services Gateway Command Reference
iWAG commands	Cisco IOS Intelligent Wireless Access Gateway Command Reference
Mobile IP configuration concepts, tasks, and examples	*IP Mobility: PMIPv6 Configuration Guide*
IP Mobility commands	Cisco IOS IP Mobility Command Reference
GGSN configuration concepts, tasks, and examples	*Mobile Wireless GGSN 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
RFC 5845	Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6

MIBs

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

Technical Assistance

Description	Link
The Cisco Support 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

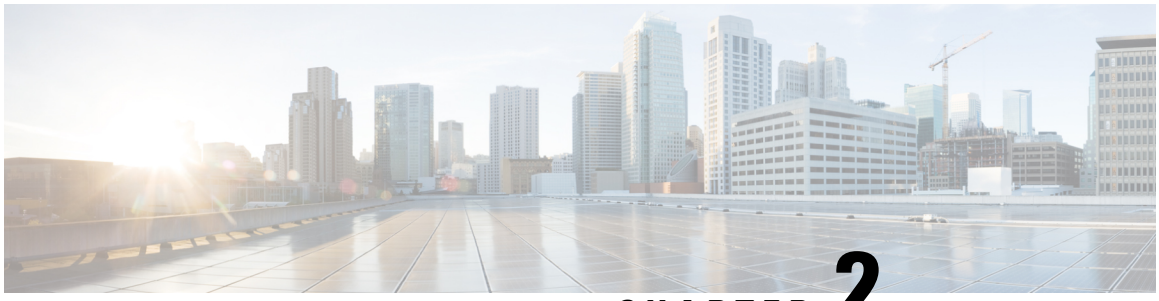
Feature Information for the Intelligent Wireless Access Gateway

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 2: Feature Information for the Intelligent Wireless Access Gateway

Feature Name	Releases	Feature Information
Intelligent Wireless Access Gateway	Cisco IOS XE Release 3.8S	The iWAG solution offers the following tunneling technologies to integrate WiFi access with the Evolved Packet Core (EPC): • GPRS Tunnel Protocol version 1 (GTPv1) allows integration of a 3G environment, where iWAG behaves in a way that is similar to a Serving GPRS Support Node (SGSN) connecting to a Gateway GPRS Support Node (GGSN). • Proxy Mobile IPv6 (PMIPv6) allows the integration of a 4G environment where iWAG behaves as a PMIPv6 Mobile Access Gateway (MAG) connecting to an Local Mobility Anchor (LMA) that is co-located with a Packet Gateway (PGW), which acts as PMIPv6 LMA. In Cisco IOS XE Release 3.8S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 2

IP Sessions Over Gigabit EtherChannel

The IP Sessions Over Gigabit EtherChannel (IPoGEC) feature enables you to add the Link Aggregation Control Protocol (LACP) functionality for IP sessions. The LACP defines a virtual interface for a port channel or a port bundle, and adds physical member links to the port channel. This section provides information about the IPoGEC 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.

Restrictions for IPoGEC

IP Sessions over Gigabit EtherChannel (IPoGEC) currently supports the 1:1 model, where only one member link is active while the second member link is passive and does not carry traffic.

Information About IP Sessions over Gigabit EtherChannel

The IP sessions over Gigabit EtherChannel (IPoGEC) feature ensures consistency between systems by adding redundancy and allows dynamic link management during local and remote system failures. LACP fast

switchover enables the standby member link to take over instantly (in milliseconds) when the active member link goes down. As a result, the port channel remains up. The **carrier-delay** {*delay-seconds* | **msec** *milliseconds*} command used in the configuration of the IPoGEC ensures fast switchover, with the delay in switchover being in milliseconds rather than seconds.

Supported Features for IPoGEC

- IPoGEC supports both simple IP sessions and mobile IP sessions.
- IPoGEC is supported over virtual local area network (VLAN) and subinterfaces.
- IPoGEC is supported on all Ethernet SPAs, including 10-Gigabit Ethernet ports and 1-Gigabit Ethernet ports.

Configuring IP Sessions over Gigabit EtherChannel

SUMMARY STEPS

1. **configure terminal**
2. **interface port-channel** *channel-number*
3. **description** *string*
4. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
5. **load-interval** *seconds*
6. **lacp fast-switchover**
7. **lacp max-bundle** *max-bundle-number*
8. **service-policy type control** *policy-map-name*
9. **ip subscriber** {**l2-connected**}
10. **initiator** {**dhcp** | **radius-proxy** | **static ip subscriber list** *listname* | **unclassified ip** | **unclassified mac-address**}
11. **initiator** {**dhcp** | **radius-proxy** | **static ip subscriber list** *listname* | **unclassified ip** | **unclassified mac-address**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 2	**interface port-channel** *channel-number* **Example:** `Router(config)#interface port-channel 1`	Creates a port-channel virtual interface.
Step 3	**description** *string* **Example:** `Router(config-if)#description GEC:1 interface towards switch`	Adds a description to an interface configuration.

	Command or Action	Purpose
Step 4	**ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] **Example:** `Router(config-if)#ip address 21.0.0.1 255.255.0.0`	Removes an IP address from an interface.
Step 5	**load-interval** *seconds* **Example:** `Router(config-if)#load-interval 30`	Changes the length of time for which data is used to compute load statistics.
Step 6	**lacp fast-switchover** **Example:** `Router(config-if)#lacp fast-switchover`	Enables the LACP 1:1 link redundancy.
Step 7	**lacp max-bundle** *max-bundle-number* **Example:** `Router(config-if)#lacp max-bundle 1`	Defines the maximum number of active, bundled LACP ports allowed in a port channel.
Step 8	**service-policy type control** *policy-map-name* **Example:** `Router(config-if)#service-policy type control BB_PMAP`	Applies a control policy to a context.
Step 9	**ip subscriber** {**l2-connected**} **Example:** `Router(config-if)#ip subscriber l2-connected`	Enables Cisco Intelligent Services Gateway (ISG) IP subscriber support on an interface, and specifies the access method that IP subscribers use for connecting to the Cisco ISG on an interface. **Note** The iWAG does not support the routed access method.
Step 10	**initiator** {**dhcp** | **radius-proxy** | **static ip subscriber list** *listname* | **unclassified ip** | **unclassified mac-address**} **Example:** `Router(config-subscriber)# initiator unclassified mac-address`	Enables the Cisco ISG to create an IP subscriber session upon receipt of a specified type of packet.
Step 11	**initiator** {**dhcp** | **radius-proxy** | **static ip subscriber list** *listname* | **unclassified ip** | **unclassified mac-address**} **Example:** `Router(config-subscriber)# initiator dhcp`	Enables the Cisco ISG to create an IP subscriber session upon receipt of a specified type of packet.

Configuring Member Links for IP Sessions over Gigabit EtherChannel

SUMMARY STEPS

1. **interface GigabitEthernet** *slot/subslot/port*
2. **no ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
3. **carrier-delay** {*delay-seconds* | **msec** *milliseconds*}
4. **lacp port-priority** *priority*
5. **channel-group** *channel-group-number* **mode** {**active** | **passive**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface GigabitEthernet** *slot/subslot/port* **Example:** `Router(config)#interface GigabitEthernet0/0/1`	Enters the interface configuration mode for Gigabit Ethernet interface.
Step 2	**no ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]] **Example:** `Router(config-if)#no ip address`	Removes an IP address from an interface.
Step 3	**carrier-delay** {*delay-seconds*	**msec** *milliseconds*} **Example:** `Router(config-if)# carrier-delay msec 50`	Sets the carrier delay on a serial interface. To achieve faster switchover from active to standby member link, the carrier delay value can be set to 0 ms.
Step 4	**lacp port-priority** *priority* **Example:** `Router(config-if)#lacp port-priority 4000`	Sets the LACP priority for a physical interface. IPoGEC currently supports 1:1 model, that is one active member link and one standby member link, which only requires choosing two different values for priority field to make sure one interface is active while the other is standby. The value set for the priority field shall match the value configured on the switch.
Step 5	**channel-group** *channel-group-number* **mode** {**active**	**passive**} **Example:** `Router(config-if)#channel-group 1 mode active`	Configures the interface in a channel group and sets the LACP mode.

Configuration Examples for IP Sessions Over Gigabit EtherChannel

Example: Configuring IPoGEC

```
interface Port-channel1
description GEC:1 interface towards switch
ip address 21.0.0.1 255.255.0.0
load-interval 30
lacp fast-switchover
lacp max-bundle 1
service-policy type control BB_PMAP
ip subscriber l2-connected
  initiator unclassified mac-address ipv4
  initiator dhcp
```

Example: Configuring Member Links for IPoGEC

```
interface GigabitEthernet0/0/1
no ip address
carrier-delay msec 50
lacp port-priority 4000
channel-group 1 mode active

interface GigabitEthernet0/0/2
no ip address
carrier-delay msec 50
lacp port-priority 3000
channel-group 1 mode active
```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

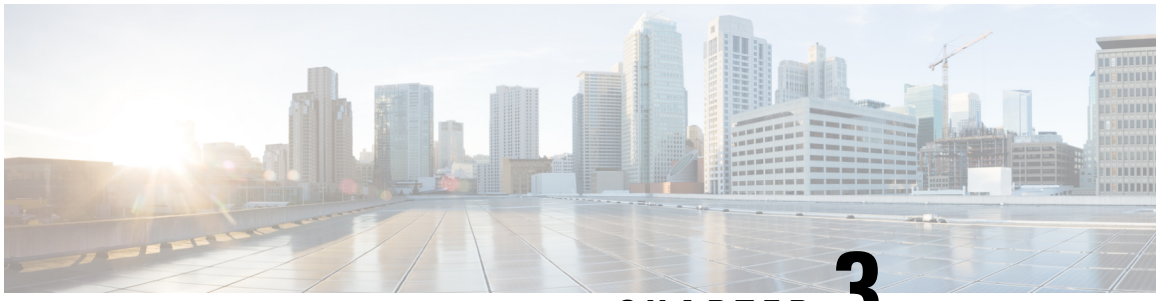
Feature Information for IP Sessions over Gigabit EtherChannel

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 3: Feature Information for IP Sessions over Gigabit EtherChannel

Feature Name	Releases	Feature Information
IP Sessions over Gigabit EtherChannel	Cisco IOS XE Release 3.9	The IP sessions over Gigabit EtherChannel (IPoGEC) feature enables you to add the Link Aggregation Control Protocol (LACP) functionality for IP sessions. In Cisco IOS XE Release 3.9S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 3

Multiple-Flow Tunnel

A tunnel facilitates bidirectional transport or acts as a conduit for forwarding subscriber traffic. In PMIPv6, subscriber traffic is transported between the MAG and the Local Mobility Anchor (LMA) through the Generic Routing Encapsulation (GRE) tunnel. In the GTP, subscriber traffic is transported between the iWAG and the GGSN through the GTP tunnel. The tunnel information structure is associated with each tunnel and specifies common tunnel attributes, such as source address, destination address, protocol, port, key, tunnel transport VRF, and tunnel mode.

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 Multiple-Flow Tunnel

Both the GTP and PMIPv6 support multiple flows per tunnel. A multiple-flow tunnel mechanism configures and manages multiple flows of traffic within the same tunnel. Each flow is identified by a flow key. A flow identifier or flow key is a 32-bit integer. The key is globally unique per system for the GTP. However, the key can be unique per tunnel for PMIPv6. The flow key for the GTP is the Tunnel Endpoint Identifier (TEID), and for PMIPv6, it is the GRE key. Each flow has parameters to describe the per-flow attributes.

PMIPv6 uses a multipoint GRE tunnel per LMA, and creates one adjacency per flow. An LMA can support scaling numbers up to 128,000 MAG. From the LMA perspective, only one multipoint GRE tunnel interface is created and 128,000 tunnel endpoints are populated. This scaling level supports the MAG functionality that is implemented on access points or hotspots, from which only one or few PMIPv6 subscribers can be attached. Cisco high-end routing platforms, such as the Cisco ASR 1000 Series Route Processor 2, the Cisco ASR 1000 Series 40-Gbps ESP, and the Cisco ASR 1000 Series 100-Gbps ESP support 128,000 scaling for the LMA.

To support 128,000 scaling, configure the following on the LMA:

```
ipv6 mobile pmipv6-lma LMA1 domain D1
   bce maximum 128000
```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

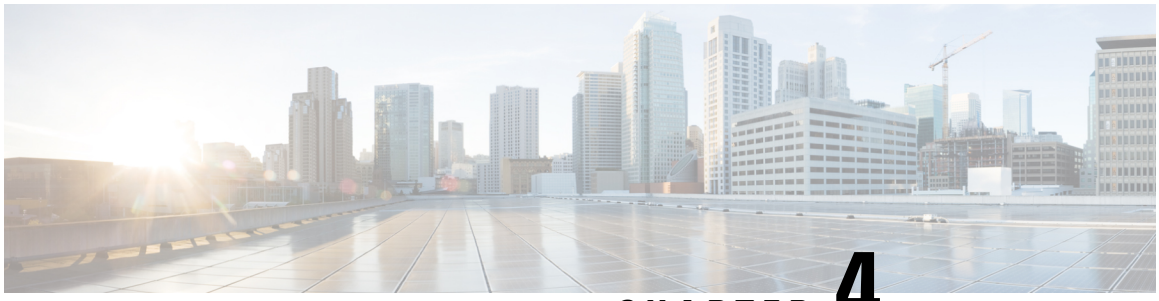
Feature Information for Multiple-Flow Tunnel

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 4: Feature Information for Multiple-Flow Tunnel

Feature Name	Releases	Feature Information
Multiple-Flow Tunnel	Cisco IOS XE Release 3.9S	In Cisco IOS XE Release 3.9S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 4

Service Provider WiFi: Support for Integrated Ethernet Over GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over a Layer 3 IPv4 or Layer 3 IPv6 access network.

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.

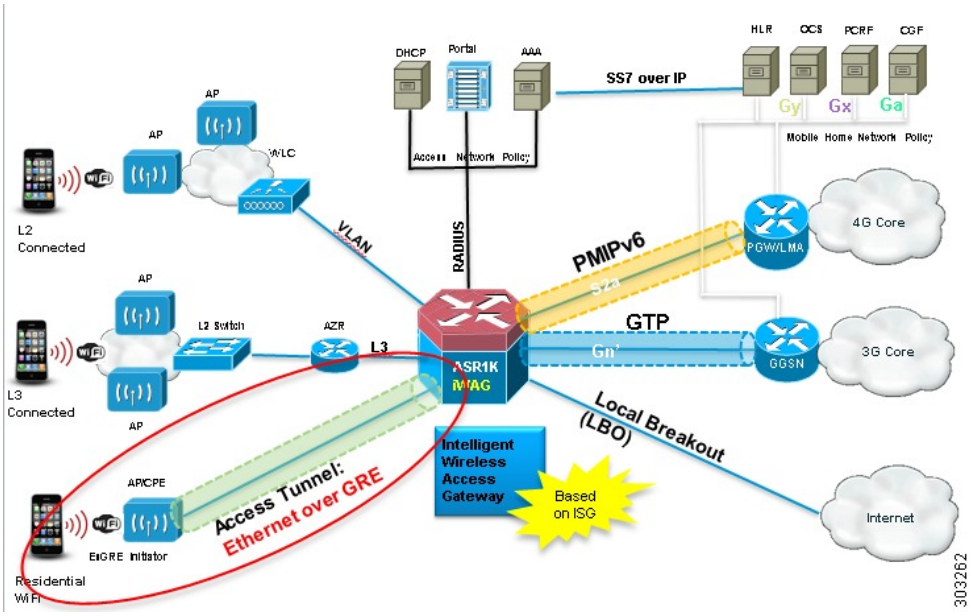
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About Ethernet Over GRE

Ethernet over GRE (EoGRE) is a new aggregation solution for aggregating WiFi 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.

The following figure shows the structure of the Ethernet over GRE.

Figure 2: Ethernet Over GRE Structure



Restrictions for Configuring Ethernet Over GRE

The following features are not supported on the Cisco ASR 1000 Series Aggregation Services Routers:

- IPsec tunnel between the Cisco ASR 1000 Series Aggregation Services Routers and the CPE devices
- Native multicast coexistence for subscribers
- Per-CPE QoS
- IPv6 subscriber
- The Cisco Intelligent Services Gateway (ISG) RADIUS proxy initiator
- QinQ tag for the inner L2 frame
- High Availability is not supported if ISG is not configured.
- If the VLAN priority tag inside the EoGRE packet is set to a nonzero value, iWAG ignores the packet

Prerequisites for Configuring Ethernet Over GRE

Before you configure the Ethernet over GRE feature on the Cisco ASR 1000 Series Aggregation Services Routers, ensure that the following prerequisites are met:

- A physical interface or dot1Q interface should be configured.
- The ISG policy should not be applied to the physical interface.

Information About Configuring Ethernet Over GRE

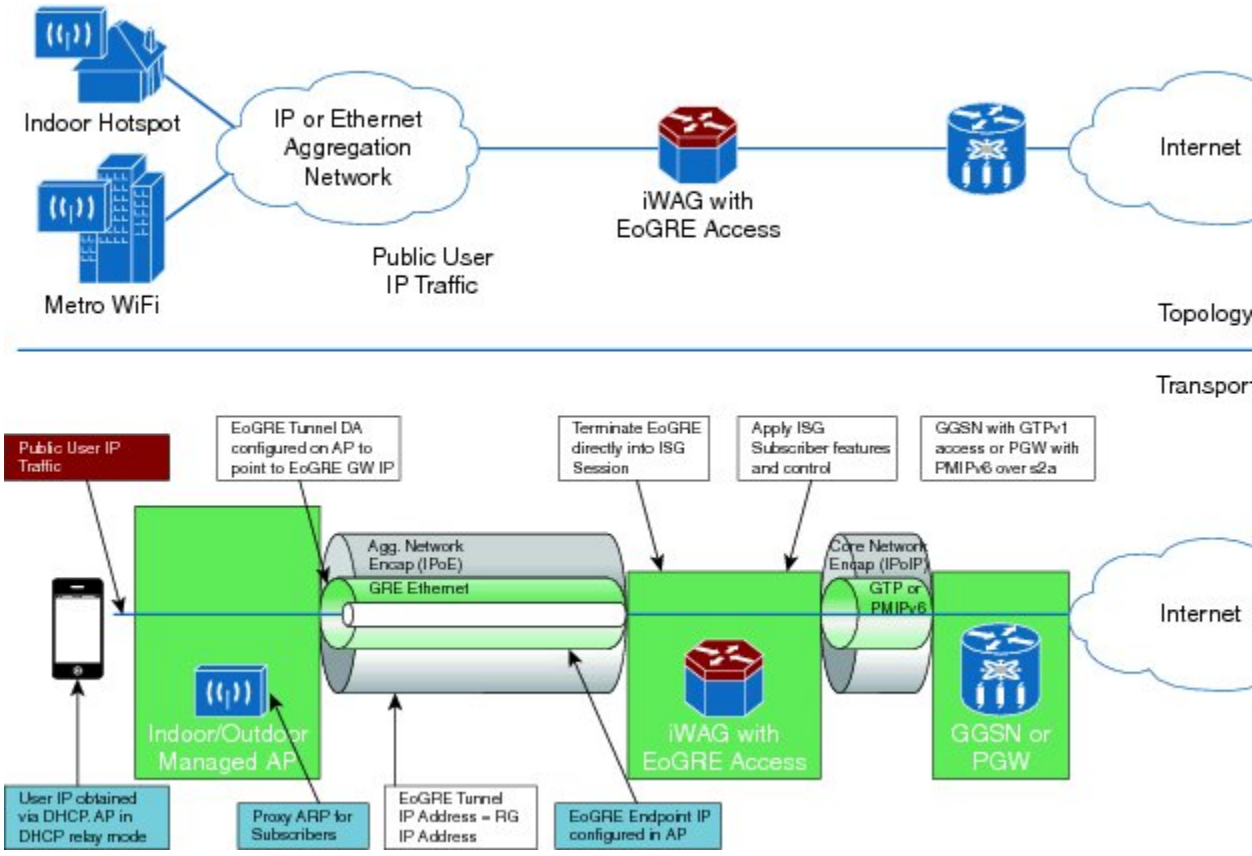
The Cisco ASR 1000 Series Aggregation Services Routers serve as a service provider broadband network gateway that:

- Terminates IPv4 or IPv6 GRE tunnels.
- Manages the subscriber session for end-host clients.

The EoGRE feature works with legacy residential gateways and CPE devices to terminate the Ethernet L2 traffic in the Cisco ASR 1000 Series Aggregation Services Routers. When configured as an intelligent Wireless Access Gateway (iWAG) with EoGRE access tunneling support, the Cisco ASR 1000 Series Aggregation Services Routers can extend mobility and the ISG services in support of these legacy devices.

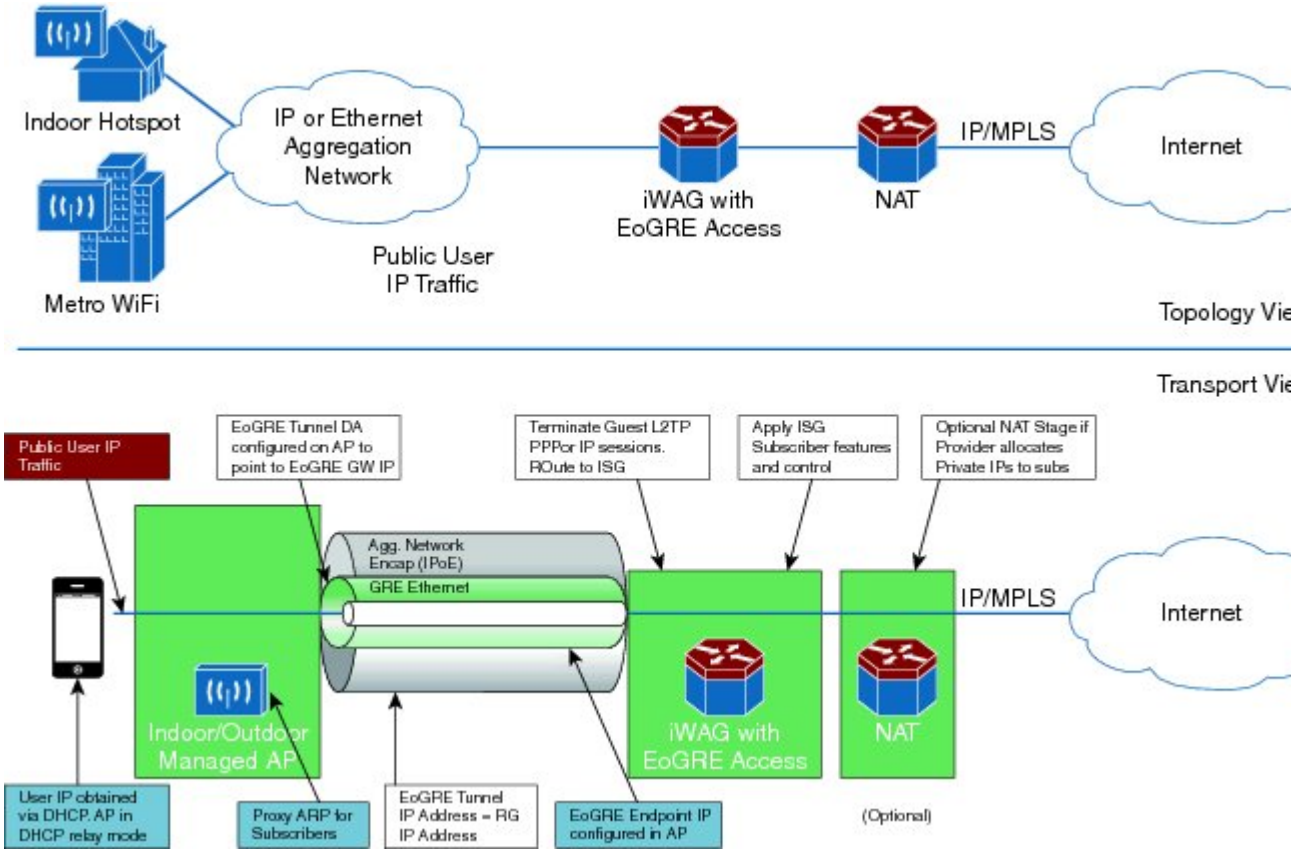
The following figure shows the structure of the EoGRE feature with PMIP/GTP integrated for mobility service.

Figure 3: Structure of the EoGRE Feature with PMIP/GTP Integrated for Mobility Service



The following figure shows the structure of the EoGRE feature for simple IP service.

Figure 4: Structure of the EoGRE Feature for Simple IP Service



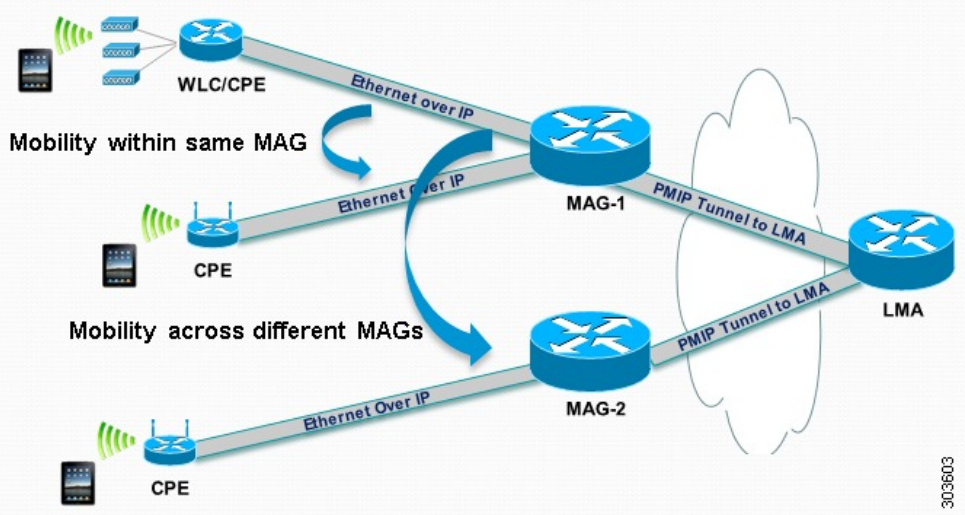
The EoGRE feature supports the following deployments:

- EoGRE Deployment with PMIPv6 Integrated for Mobility Service
- EoGRE Deployment with GTP Integrated for Mobility Service
- EoGRE Deployment with ISG Integrated for Simple IP Service

EoGRE Deployment with PMIPv6 Integrated for Mobility Service

Proxy Mobile IPv6 (PMIPv6) provides mobility service to the mobile nodes that are connected to the Mobile Access Gateway (MAG) via an EoGRE tunnel. The following figure shows the structure of the EoGRE deployment with PMIPv6 integrated for mobility service.

Figure 5: Structure of the EoGRE Deployment with PMIPv6 Integrated for Mobility Service



Mobile nodes access the mobile internet service over Wi-Fi access points. The access points are either autonomous access points or are connected to the Cisco Wireless LAN Controller (WLC). These access points and WLCs are used as residential gateways or CPE devices. CPEs are preconfigured with a point-to-multipoint GRE IP tunnel to the Cisco ASR 1000 Series Aggregation Services Routers as the MAG. The tunnel from the CPE device can be configured with a static GRE key. The CPEs are provisioned to forward the Ethernet traffic from both public and private customers to the GRE tunnel, and to add a VLAN tag on the Ethernet frame before forwarding the traffic.

As with regular PMIPv6 deployments, the Cisco ASR 1000 Series Aggregation Services Routers can create IP sessions on EoGRE access tunnels similar to the regular IP sessions on the physical Ethernet interfaces, and allocate IP addresses for mobile nodes, either locally or in the proxy mode. Mobility service is provided to the mobile nodes and the tunneled Ethernet traffic is forwarded via IP tunnels to the Local Mobility Anchor (LMA).

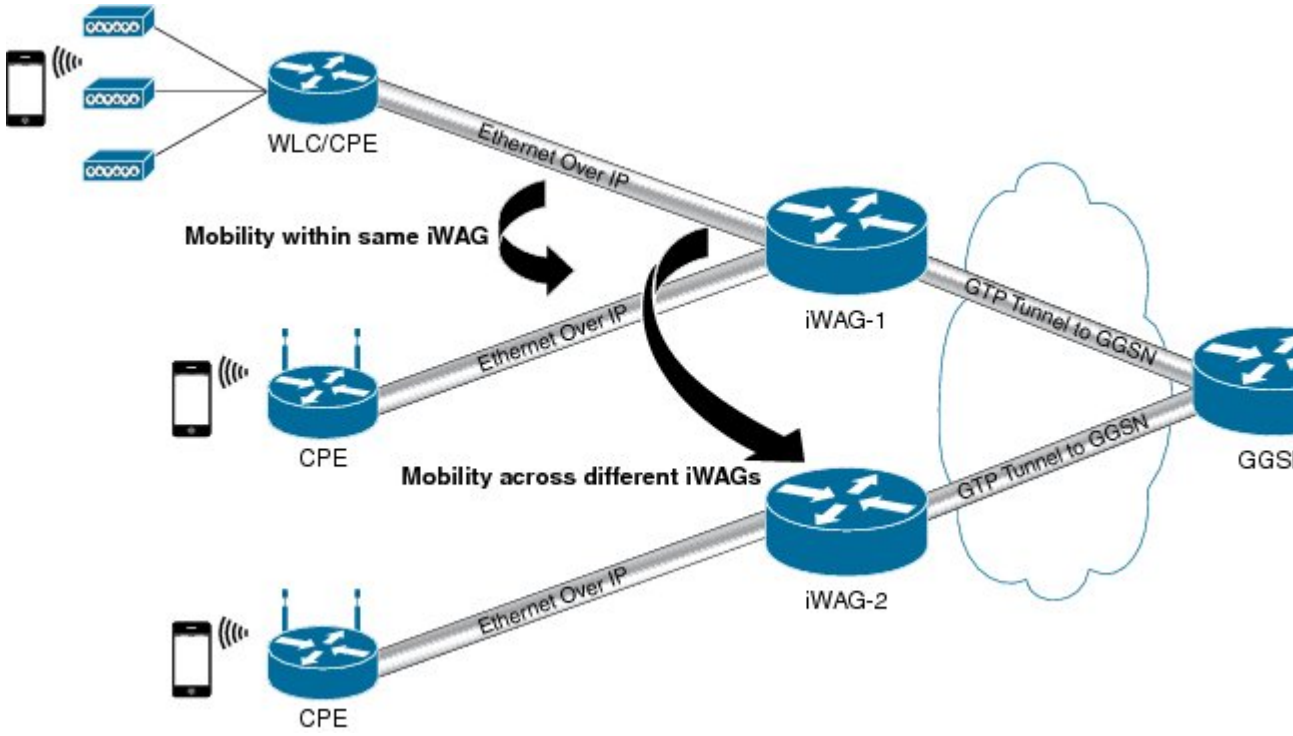
Note When you ping a mobile node from the MAG with a packet size that is larger than that of the path maximum transmission unit (PMTU) that is configured with the DF bit set, the packet will be dropped. However, you will not get the return type as M.M.M (could not fragment). This is reflected in the log messages or error messages.

For more information about PMIPv6 and the ISG configurations for the iWAG, see the *Intelligent Wireless Gateway Configuration Guide*.

EoGRE Deployment with GTP Integrated for Mobility Service

GPRS Tunneling Protocol (GTP) provides mobility service to the mobile nodes that are connected to the iWAG via an EoGRE tunnel, as shown in the following figure.

Figure 6: Structure of the EoGRE Deployment with GTP Integrated for Mobility Service

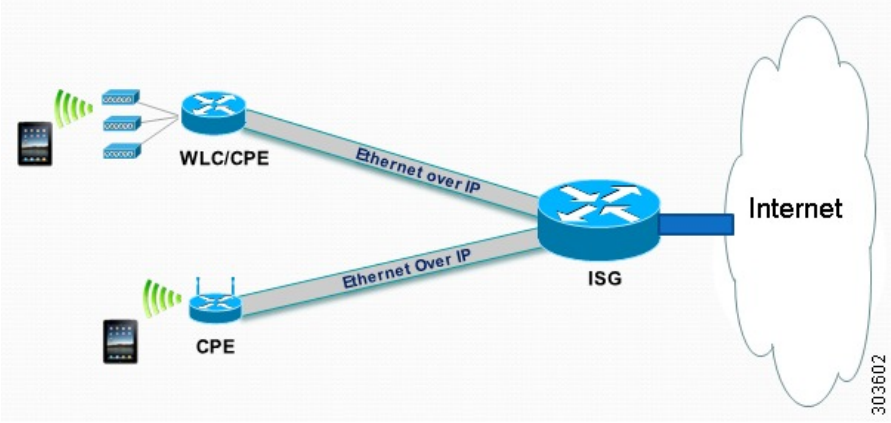


For more information about the GTP and ISG configurations for the iWAG, see the *Intelligent Wireless Gateway Configuration Guide*.

EoGRE Deployment with ISG Integrated for Simple IP Service

The ISG provides simple IP service to mobile nodes that are connected to ISG via the EoGRE tunnel, as shown in the following figure. The Cisco ASR 1000 Series Aggregation Services Routers use the ISG framework to allocate IP sessions for authenticated subscribers. Simple IP subscribers are provided ISG services, including Internet access, but are not provided access to mobility services via GTP or PMIPv6.

Figure 7: Structure of the EoGRE Deployment with ISG Integrated for Simple IP Service



Supported Features

The following features are supported as part of the EoGRE feature on the Cisco ASR 1000 Series Aggregation Services Routers:

- Ethernet over GRE traffic termination on the routers
- Frames can have up to one dot1Q VLAN tag
- L2-connected IPv4 mobile nodes
- GRE tunnel for IPv4 or IPv6
- ISG and PMIPv6 or GTP integrated with the EoGRE tunnel
- ISG initiator-unclassified MAC, DHCP, DNAv4
- Subscriber roaming

How to Configure the EoGRE Feature

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **ip unnumbered loopback** *interface-name* or **ip address** *ip-address*
5. **tunnel source** *interface-type interface-number*
6. (For simple IP mode) **mac-address** *H.H.H*
7. **tunnel mode ethernet gre ipv4** or **tunnel mode ethernet gre ipv6**
8. (Optional) **tunnel vlan** *vlan-id*
9. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Router(config)# interface Tunnel 0`	Specifies the logical interface for the EoGRE tunnel.

	Command or Action	Purpose

Step 4	**ip unnumbered loopback** *interface-name* or **ip address** *ip-address*
	Example:
	`Router(config-if)# ip unnumbered loopback 0`
	`or`
	`Router(config-if)# ip address 20.1.1.2 255.255.255.0`
		For PMIPv6 and GTP scenarios, an unnumbered address or a specified IP address can be configured on the tunnel interface.
		For a simple IP scenario, only a specified IP address can be configured on the tunnel interface. This IP address can be used as a default gateway IP address.

Step 5	**tunnel source** *interface-type interface-number* **Example:** `Router(config-if)# tunnel source Loopback 0`	Sets the source interface for the EoGRE tunnel interface.
Step 6	(For simple IP mode) **mac-address** *H.H.H* **Example:** `Router(config-if)# mac-address 0000.5e00.5213`	Sets the source MAC address for the EoGRE tunnel interface. The MAC address is mandatory for simple IP deployment. For PMIPv6/GTP, the default MAC address associated with EoGRE Tunnel is 0000.5e00.5213.

Step 7	**tunnel mode ethernet gre ipv4** or **tunnel mode ethernet gre ipv6**
	Example:
	`Router(config-if)# tunnel mode ethernet gre ipv4`
	`or`
	`Router(config-if)# tunnel mode ethernet gre ipv6`
		Sets the EoGRE encapsulation mode for the tunnel interface for IPv4.
		or
		Sets the EoGRE encapsulation mode for the tunnel interface for IPv6.

Step 8	(Optional) **tunnel vlan** *vlan-id* **Example:** `Router(config-if)# tunnel vlan 1000`	(Optional) Sets the VLAN ID of the EoGRE tunnel.
Step 9	end **Example:** `Router(config-if)# end`	Ends the current configuration session.

Example: Configuring the EoGRE Feature

```
aaa new-model
!
aaa group server radius AAA_SERVER_CAR
server-private 5.3.1.76 auth-port 2145 acct-port 2146 key cisco
```

```
!
aaa authentication login default none
aaa authentication login ISG_PROXY_LIST group AAA_SERVER_CAR
aaa authorization network ISG_PROXY_LIST group AAA_SERVER_CAR
aaa authorization subscriber-service default local group AAA_SERVER_CAR
aaa accounting network PROXY_TO_CAR
action-type start-stop
group AAA_SERVER_CAR
!
aaa accounting network ISG_PROXY_LIST start-stop group AAA_SERVER_CAR
!
aaa server radius dynamic-author
client 5.3.1.76 server-key cisco
auth-type any
ignore server-key
!
!
ip dhcp excluded-address 172.16.254.254
!
ip dhcp pool ISG_SIMPLE_IP
 network 172.16.0.0 255.255.0.0
 default-router 172.16.254.254
 domain-name cisco.com
!
policy-map type control EOGRE_L2_ISG
 class type control always event session-start
  2 authorize aaa list ISG_PROXY_LIST password cisco identifier mac-address
  4 set-timer IP_UNAUTH_TIMER 5
 !
 class type control always event service-start
  1 service-policy type service identifier service-name
  2 collect identifier nas-port
 !
!
interface Loopback0
 ip address 9.9.9.9 255.255.255.255
interface GigabitEthernet1/0/0
ip address 192.168.0.9 255.255.255.0
negotiation auto
!
interface GigabitEthernet1/0/0.778
description "to ASR5K GGSN"
encapsulation dot1Q 778
ip address 172.16.199.9 255.255.255.0
!
interface Tunnel10
 description "EoGRE Tunnel for Simple IP subscribers"
 mac-address 0000.5e00.5213
 ip address 172.16.254.254 255.255.0.0
 no ip redirects
 tunnel source 172.16.199.9
 tunnel mode ethernet gre ipv4
 service-policy type control EOGRE_L2_ISG
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
interface Tunnel100
description "IPv4 EoGRE Tunnel for PMIP/GTP subscribers"
 ip unnumbered Loopback0
 tunnel source GigabitEthernet1/0/0
 tunnel mode ethernet gre ipv4
 tunnel vlan 100
 service-policy type control EOGRE_L2_ISG
 ip subscriber l2-connected
```

```
  initiator unclassified mac-address
  initiator dhcp
!
interface Tunnel200
description "IPv6 EoGRE Tunnel for PMIP/GTP subscribers"
 ip unnumbered Loopback0
 tunnel source 2001:161::9
 tunnel mode ethernet gre ipv6
 tunnel vlan 200
service-policy type control EOGRE_L2_ISG
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
!
mcsa
 enable sessionmgr
!
ipv6 mobile pmipv6-domain D1
 replay-protection timestamp window 255
lma LMA_5K
  ipv4-address 192.168.199.1
!
ipv6 mobile pmipv6-mag M1 domain D1
sessionmgr
 role 3GPP
 address ipv4 9.9.9.9
interface Tunnel100
 interface Tunnel200
 lma LMA_5K D1
  ipv4-address 192.168.199.1
  encap gre-ipv4
!
ntp master
!
gtp
 information-element rat-type wlan
 interface local GigabitEthernet1/0/0.778
 apn 1
  apn-name gtp.com
  ip address ggsn 172.16.199.1
  fixed link-layer address 00ab.00cd.00ef
  default-gw 20.100.254.254 prefix-len 16
  dns-server 20.100.254.254
  dhcp-server 20.100.254.254
!
end
```

You can use the following commands to check and show subscriber session information:

```
show ip dhcp sip statistics
show subscriber statistics
show subscriber session
show ipv6 mobile pmipv6 mag binding
show gtp pdp-context all
show interface tunnel-name
```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

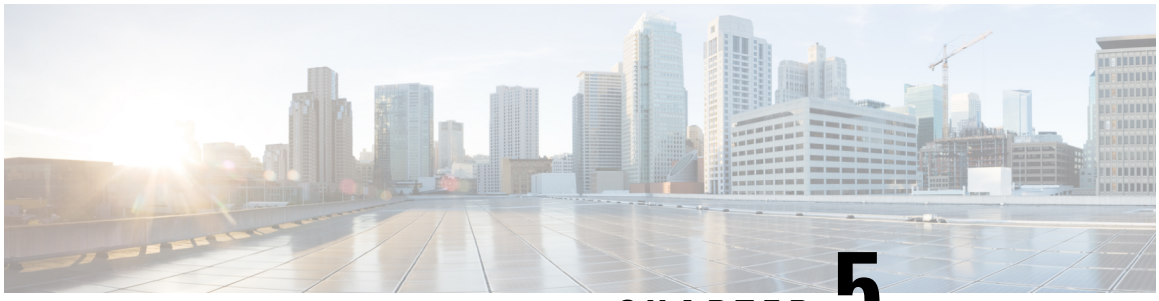
Feature Information for Configuring Ethernet Over GRE

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 5: Feature Information for Configuring the Ethernet Over GRE Feature

Feature Name	Releases	Feature Information
Service Provider WiFi: Integrated Ethernet Over GRE	3.9.1S	This feature enables the Ethernet over Generic Routing Encapsulation (EoGRE) tunnel to be used as a service provider WiFi access interface from CPE devices. A Cisco ASR 1000 Series Aggregation Services Router is used as an L2 aggregator to terminate L2 traffic at the GRE tunnel interface and provide L3 services. In Cisco IOS XE Release 3.9.1S, this feature is implemented on the Cisco ASR 1000 Series Aggregation Services Routers. The following sections provide information about this feature: • Information About Configuring Ethernet Over GRE, on page 36 • How to Configure the EoGRE Feature, on page 41



CHAPTER 5

GTPv2 Support in the iWAG

Effective from Cisco IOS XE Release 3.10S, the support for GPRS Tunneling Protocol Version 2 (GTPv2) is offered on the Cisco ASR 1000 Series Aggregation Services Routers as an enhancement to the GTPv1 offering in the iWAG solution that was introduced in Cisco IOS XE Release 3.8S. GTPv2 provides support for both the 4G and 3G mobile users, whereas GTPv1 provides support only for 3G mobile users.

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.

Restrictions for GTPv2 of the iWAG

- The same APN name cannot be configured in different APNs, for example:

Note This restriction applies to GTPv1 as well.

```
gtp
  n3-request 7
  interval t3-response 1
  interval echo-request 64
```

```
  information-element rat-type wlan
  interface local GigabitEthernet1/3/0
  apn 1
      apn-name example.com #Same donamin name as apn2356, not supported, should be
different
      ip address ggsn 98.0.7.13
      default-gw 192.168.0.1 prefix-len 16
      dns-server 192.168.255.253
      dhcp-lease 3000
  apn 2356
     apn-name example.com #Same domain name as apn1, not supported, should be different

      ip address ggsn 98.0.7.14
      default-gw 10.254.0.1 prefix-len 16
      dns-server 10.254.255.253
      dhcp-lease 3000
!
```

- The same pool cannot be associated with different APNs. The PGW or GGSN must have different IPs for pools configured on different domains, for example:

```
gtp
  n3-request 7
  interval t3-response 1
  interval echo-request 64
  information-element rat-type wlan
  interface local GigabitEthernet1/3/0
  apn 1
     apn-name example.com
     ip address ggsn 98.0.7.13
    default-gw 192.168.0.1 prefix-len 16 #different domain name but same pool ip; this
 is not supported
     dns-server 192.168.255.253
     dhcp-lease 3000
  apn 2356
     apn-name example.com #Same domain name as apn1, not supported, should be different

      ip address ggsn 98.0.7.14
      default-gw 192.168.0.1 prefix-len 16 #different domain name but same pool ip;
this is not supported
      dns-server 10.254.255.253
      dhcp-lease 3000
!
```

Information About GTPv2 in the iWAG

A GTP session with GTPv2 support uses more memory than a GTP session with GTPv1 support. GTPv2 support does not require any new AAA attributes. However, the new gtpv2 enum value for the Cisco-MPC-Protocol-Interface attribute is necessary to specify the use of GTPv2. The AAA server identifies a subscriber depending upon whether the subscriber profile is sent over GTPv1 tunnel or GTPv2 tunnel from the iWAG back to the Evolved Packet Core (EPC). The GTPv1 and GTPv2 sessions can exist simultaneously on the iWAG.

GTPv2 Configuration

All the configurations required for GTPv1 support are also needed for GTPv2 support.

RADIUS Configuration

The following configurations are required on the RADIUS server to differentiate between a GTPv1 subscriber and a GTPv2 subscriber:

```
subscriber-profile profile1 { # this is a GTPv2 profile
access-accept {
reply-msg "Default profile"
cisco-avpair { "cisco-mn-service=ipv4" }
cisco-avpair { "cisco-mpc-protocol-interface=gtpv2" }
cisco-avpair { "cisco-service-selection=example.com" }
cisco-avpair { "cisco-msisdn=4910000000" }
3gpp {
imsi 406091000000000
}
}
}
subscriber-profile profile2 { # this is a GTPv1 profile
access-accept {
reply-msg "Default profile"
cisco-avpair { "cisco-mn-service=ipv4" }
cisco-avpair { "cisco-mpc-protocol-interface=gtpv1" }
cisco-avpair { "cisco-service-selection=example.com" }
cisco-avpair { "cisco-msisdn=4900000000" }
3gpp {
imsi 406090000000000
}
}
}
sub-grp-mgr sub-grp1 {
control-by round-robin
group-profiles {
subscriber-profile profile1 profile-priority 99
subscriber-profile profile2 profile-priority 98
}
}
```

Intra-iWAG Roaming

Effective from Cisco IOS XE Release 3.10S, both GTPv1 and GTPv2 support connected subscriber roaming across different access interfaces of the iWAG. GTPv1 and GTPv2 preserve and update their existing sessions to allow their data traffic to flow through the new ingress interfaces from the access network.

Configuration for the GTPv1 and GTPv2 Roaming Scenario

The initiator unclassified mac-address command must be configured on every iWAG access interface to support subscriber roaming between these interfaces. As shown in the following configuration, all the access interfaces must be specified under the GTP configuration before bringing up the IP subscriber sessions. If the access interface is not specified under the GTP, a subscriber's roaming option is not enabled for that interface. Also, adding interfaces under the GTP after the sessions bring up fails subscriber roaming.

The following example shows the configuration for GTPv1 and GTPv2 roaming scenario:

```
interface GigabitEthernet0/0/2
description To client facing interface
ip address 192.1.1.1 255.255.0.0
```

```
negotiation auto
service-policy type control ISG_GTP_CONTROL
ip subscriber l2-connected
initiator unclassified mac-address # must for roaming config
initiator dhcp
!
interface GigabitEthernet0/0/3
description To client facing interface
ip address 192.2.1.1 255.255.0.0
negotiation auto
service-policy type control ISG_GTP_CONTROL
ip subscriber l2-connected
initiator unclassified mac-address # must for roaming config
initiator dhcp
!
gtp
  n3-request 3
  interval t3-response 10
  interval echo-request 64
  information-element rat-type wlan
  interface local GigabitEthernet1/3/0
  apn 1200
         apn-name example.com
         ip address ggsn 98.0.7.13
         default-gw 192.168.0.1 prefix-len 16
         dns-server 192.168.255.253
         dhcp-lease 3000
  interface access GigabitEthernet0/0/2
  interface access GigabitEthernet0/0/3
```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

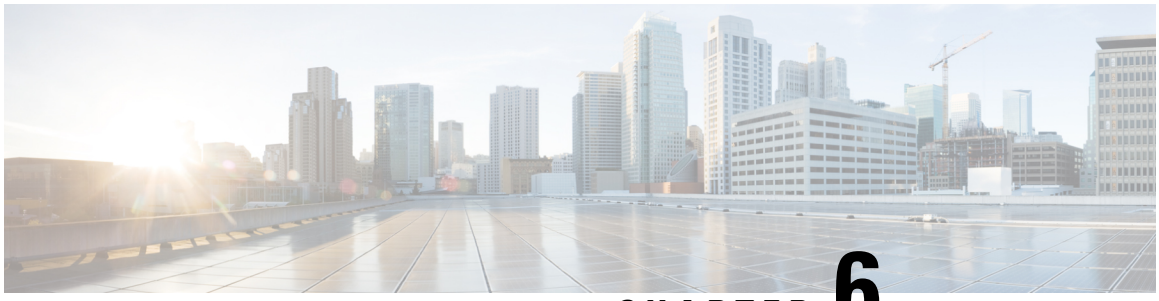
Feature Information for GTPv2 Support in the iWAG

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 6: Feature Information for GTPv2 Support in the iWAG

Feature Name	Releases	Feature Information
GTPv2 Support in the iWAG	Cisco IOS XE Release 3.10	In Cisco IOS XE Release 3.10S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 6

iWAG SSO Support for GTP

Effective from Cisco IOS XE Release 3.10S, the per-session Stateful Switchover (SSO)/In Service Software Upgrade (ISSU) feature supports iWAG mobility sessions that are tunneled to MNO using GTP. The SSO feature takes advantage of Route Processor (RP) redundancy by establishing one of the RPs as the active processor, while the other RP is designated as the standby processor, and then synchronizing the critical state information between them. When a failover occurs, the standby device seamlessly takes over, starts performing traffic-forwarding services, and maintains a dynamic routing table.

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 iWAG SSO Support for GTP

The SSO/ISSU feature supports only the Cisco ASR 1000 Series Aggregation Services Routers intrachassis (RP-to-RP) SSO, but not the interchassis (Cisco ASR1K-to-Cisco ASR1K) SSO. The First Sign Of Life (FSOL) triggers that are supported on SSO include DHCP proxy (where the iWAG acts as the DHCP proxy server) and DHCP proxy plus unclassified MAC.

For more information about ISSU, see the "Overview of ISSU on the Cisco ASR 1000 Series Routers" section of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.

The process as part of iWAG SSO handling GTP checkpoints to the standby RP the information that is necessary to create a copy of the session on the standby RP. Such an inactive copy of the session becomes active when the standby RP becomes active.

When an iWAG mobility session with GTP tunneling is enabled using the SSO/ISSU feature, the Cluster Control Manager on the active RP needs to wait for a few more components, including the GTP, to become ready before checkpoint data collection, and polls these additional components for checkpoint data during data collection. A very similar operation is performed on the standby RP as well. Although such additional CPU consumption is per session, it is not expected to be too heavy since processing in each of these components should include the time spent on a few data structure lookups and memory-copying operations.

During ISSU SIP and SPA upgrade, there is traffic interruption. To avoid session disconnect because of dropped echo messages during such traffic interruption, a user has the following options:

- Option 1 (preferred):

1. Disable the echo messages on the iWAG and GGSN for the duration of the ISSU.
2. Re-enable the echo messages after ISSU is completed on the iWAG and GGSN.

- Option 2: Extend the t3 and n3 configurations to exceed the expected traffic interruption. The traffic interruption characterized in the Cisco IOS XE Release 3.10S is 127 seconds. Hence, we recommend the following t3 and n3 settings (t3_response: 1 and n3_request: 7, resulting in 127 seconds on both the iWAG and GGSN) but the duration of the traffic interruption may depend on the types of SIPs and SPAs and how loaded the router is. If traffic interruption exceeds the configured t3 and n3 limits, the session is disconnected.

Enabling SSO Support for the GTP

This section describes how to enable SSO support for the GTP on the Cisco ASR 1000 Series Aggregation Services Routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **mode SSO**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables the privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters the global configuration mode.
Step 3	**redundancy** **Example:**	Enters the redundancy configuration mode.

	Command or Action	Purpose
	`Router(config)# redundancy`	
Step 4	**mode SSO** **Example:** `Router(config-redundan)# mode SSO`	Configures the SSO redundancy mode of operation.

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

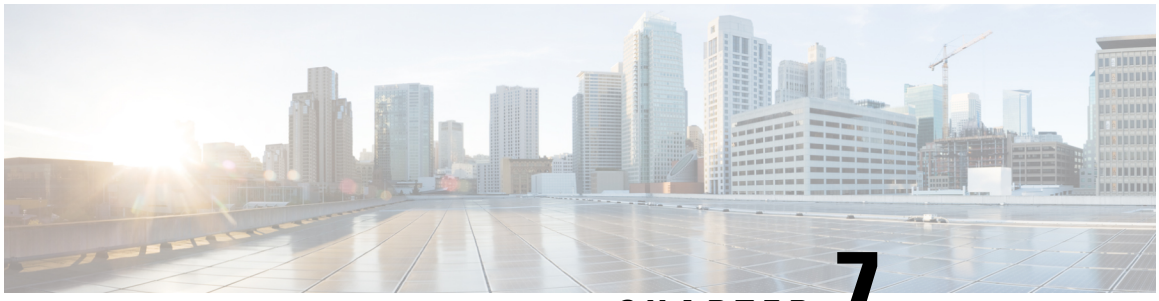
Feature Information for iWAG SSO Support for GTP

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 7: Feature Information for iWAG SSO Support for GTP

Feature Name	Releases	Feature Information
iWAG SSO Support for GTP	Cisco IOS XE Release 3.10	In Cisco IOS XE Release 3.10S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 7

Configuring ISG Policy Templates

In Cisco IOS XE Release 3.10S, the Configuring Intelligent Services Gateway (ISG) Policy Templates feature optimizes the provisioning of ISG policies on IPv4 and IPv6 subscriber sessions. It enables support of up to 128,000 IP subscriber sessions with more complex ISG policies at a higher churn rate on the Cisco ASR 1000 Series Aggregation Services Routers.

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.

Restrictions for Configuring ISG Policy Templates

Enabling policy templates in the ISG is not supported for any type of PPP sessions and IP interface sessions.

Information About Configuring ISG Policy Templates

A typical ISG configuration has very few distinct policies and many sessions that use these policies. ISG policy templates take advantage of this to optimize resource consumption and enable support for higher scale. Instead of provisioning an ISG policy with all its individual services and features on each target IP subscriber session, it provisions a template of the policy through the system only once and references the template after that to apply the policy on each target session. Enabling policy templates in the ISG does not impact session SSO.

How to Configure ISG Policy Templates

By default, the ISG policy templates are disabled. The **platform subscriber template** command enables the ISG policy templates.

Note The **platform subscriber template** command does not take effect until the router is reloaded. For example, if this command is entered at the configuration prompt, policy templating remains disabled until the router is reloaded. Similarly, if templating is enabled, the router has to be reloaded after the no subscriber template command is entered to disable ISG policy templating.

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

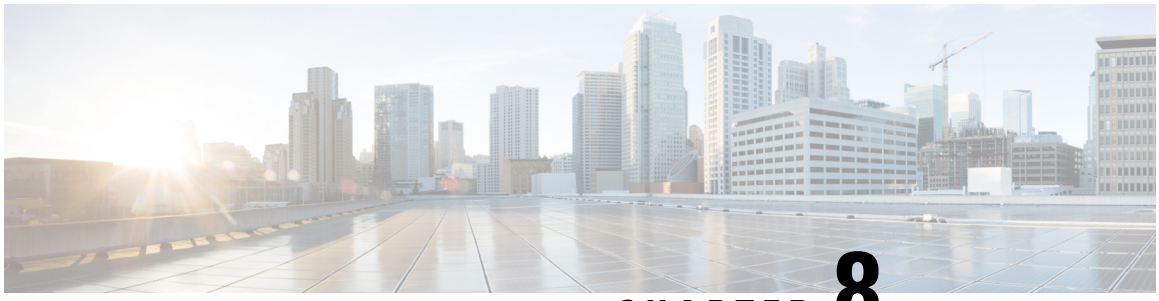
Feature Information for Configuring ISG Policy Templates

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 8: Feature Information for Configuring ISG Policy Templates

Feature Name	Releases	Feature Information
Configuring ISG Policy Templates	Cisco IOS XE Release 3.10	In Cisco IOS XE Release 3.10S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 8

Cisco ISG Accounting Accuracy for LNS Sessions

The ISG Accounting Accuracy for LNS Sessions feature improves the accuracy of reported statistics for the LNS sessions and traffic classes in the Stop Accounting messages. Because of the distributed nature of the Cisco ASR 1000 Series Aggregation Services Routers, subscriber statistics are collected periodically every 10 seconds to balance the impact to statistics accuracy, and call setup and teardown rates. Statistics reports that are generated using this collection are therefore up to 10 seconds old. When the Accounting Accuracy feature is enabled, the most recent statistics are retrieved for particular subscribers in specific conditions, such as when a session is torn down or stopped.

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 Cisco ISG Accounting Accuracy for LNS Sessions

You can enable or disable the ISG Accounting Accuracy for LNS Sessions feature using the **subscriber accounting accuracy** *timeout value* command.

When the ISG Accounting Accuracy for LNS Sessions feature is enabled, the LNS sessions that are getting disconnected are held off until the timeout value configured in the **subscriber accounting accuracy** *timeout value* command is reached. The sessions are torn down when their most recent statistics have been collected, or when the timeout period expires, whichever is sooner. The minimum timeout that can be configured is 1 second, and the maximum timeout that can be configured is 10 seconds.

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

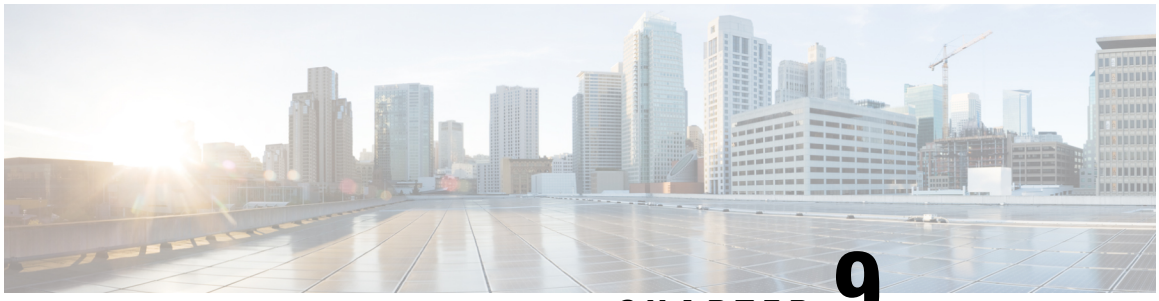
Feature Information for Cisco ISG Accounting Accuracy for LNS Sessions

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 9: Feature Information for Cisco ISG Accounting Accuracy for LNS Sessions

Feature Name	Releases	Feature Information
Cisco ISG Accounting Accuracy for LNS Sessions	Cisco IOS XE Release 3.11	The ISG Accounting Accuracy for Sessions feature improves the accuracy of reported statistics for L2TP Network Server (LNS) sessions and traffic classes in the Stop Accounting messages. In Cisco IOS XE Release 3.11S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 9

Call Admission Control

Call Admission Control (CAC) is a deterministic and informed decision that is made before a network session is established and is based on whether the required network resources are available to provide suitable quality of service (QoS) for the new session.

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.

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.

Overview of Call Admission Control for IP Sessions

In Service Provider WiFi deployments, the mobility of subscribers contributes to more dynamics when compared to wireline broadband deployments. This mobility translates into a high-average session churn rate and potential session count peaks during busy periods. For the Intelligent Wireless Access Gateway (iWAG) to function effectively under such conditions, the Call Admission Control (CAC) feature must be configured to help control IPoE session establishment.

Note In this document, a Forwarding Processor (FP) corresponds to the Embedded Services Processor (ESP) component on the ASR 1000 Series Aggregation Services Routers.

The following CAC features are implemented from Cisco IOS XE Release 3.11S onwards:

- A threshold is set for the maximum number of authenticated subscribers on the router, including the Point-to-Point Protocol over Ethernet (PPPoE) and IP over Ethernet (IPoE) sessions, but not the walk-by sessions.
- To prevent low-memory conditions, the router stops accepting a session when the committed memory from a route processor (RP) or a FP is above a specific percentage value. This also enables you to upgrade the hardware and memory with ease.
- To prevent low-memory conditions from occurring, the router stops accepting a session when the used memory from the Cisco Quatum Flow Processor (QFP) is above a specific percentage value.
- To prevent high Buffer, Queue, and Scheduler (BQS) active queue usage, the router stops accepting new sessions when the BQS active queue usage is above a specific percentage value.
- To prevent high CPU load conditions, the router stops accepting new sessions when the per-core CPU utilization per active FP or RP is above a specific percentage value.

Note After the configured session limit under CAC is attained, single-stack sessions cannot be converted into dual-stack sessions.

Call Admission Control-Supported IP Session Initiators on a Data Plane

The following IP session initiators are supported by the Call Admission Control (CAC) on a data plane:

- Unclassified MAC address IPv4 initiator
- Unclassified IPv4 initiator
- Dynamic Host Configuration Protocol v4 (DHCPv4) initiator
- Unclassified MAC address IPv6 initiator types:
  - IPv6 Neighbor Discovery (ND) packets (RS/NS/NA) that are dropped by the control plane (i.e. RP)
  - IPv6 data packets that are dropped at the data plane (i.e. FP)

Platform System Resource Monitor

A platform system resource monitor process is created when any of the CAC features listed in the following table are configured on the Cisco ASR 1000 Aggregated Services Router platform using the corresponding command:

Table 10: CAC Features and their Platform System Resource Monitor Commands

CAC Feature	Command
CPU	**platform subscriber cac cpu**

CAC Feature	Command
MEM	**platform subscriber cac mem**
BQS	**platform subscriber cac bqs**

The platform resource monitor process is disabled when all of the above CAC features are disabled on the platform.

The platform resource monitor process periodically monitors system resources such as CPU, memory, and Buffer, Queue, and Scheduler (BQS). You can set the periodic monitoring interval using the following command:

platform subscriber cac timer *interval*

The timer value specifies the frequency at which the CAC process is polled to check platform resources. The valid interval value is in the range of 1 to 10 seconds with a granularity of 1 second. The default value is 5 seconds.

Note Committed Memory is used for monitoring subscriber CAC memory resource utilization. It provides an estimate of the percentage of RAM that is needed to ensure a 99.99 percent guarantee that there is never an Out Of Memory (OOM) condition during worst-case conditions. Normally, the kernel will over commit memory by sharing the memory between several processes. A problem with the actual memory availability can be seen only when the memory is being used. While the Committed Memory is a good indicator of the memory status, the value is less dynamic. That is, if you use the **platform subscriber cac mem** command as part of CAC, a session may stay rejected for a long period of time if it reaches the memory limit. While this may be a good indicator of the decreasing memory resources, it may not be useful in production environments. We recommend that if you are using the **platform subscriber cac mem** command, ensure that the values are at least at the 95 percent threshold to enable additional troubleshooting.

Example: Configuring CAC to monitor platform specific resources, such as forwarding processor (FP) CPU, FP memory, and Quantum Flow Processor (QFP) memory.

```
platform subscriber cac timer 5      #configures the frequency at which the CAC process
polls or monitors the PD resources
platform subscriber cac bqs active-queues 95
platform subscriber cac mem rp 95
platform subscriber cac mem fp 95
platform subscriber cac mem cc 95
platform subscriber cac mem qfp 95
platform subscriber cac cpu rp 95
```

Example: Configuring CAC to monitor IOS CPU load, maximum number of sessions, and session charges (or calls per second).

```
call admission new-model
call admission limit 1580
call admission cpu-limit 90
call admission session-limit 128000
call admission ip 10 1
```

CAC is applicable to any initiator for IP sessions such as unclassified MAC or DHCP-initiated sessions. To enable CAC, the **call admission new-model** command must always be configured.

The **call admission limit** command specifies the total session charge the system will accept before it starts rejecting incoming calls. In the above example, the cpu-limit of 90 means incoming calls will be dropped when the measured 5-second CPU utilization is 90% or higher.

Depending on which condition occurs first, cpu-limit or call admission limit (charge limit), the IP sessions will be rejected. The **call admission ip** command specifies the charge for a single IP session. In the example given above, the charge for a single session is 10 is and lifetime of the fixed charge (2s) is 1.

In the example above, CAC will accept 79 CPS based on the following calculation:

```
Approximate CPS = (Call admission limit)/(Single session charge * Charge lifetime)
                = 1580/(10 * (1*2))
                = 79 CPS
```

Examples

The following examples show how to enable the Call Admission Control (CAC) feature, and how to display the CAC statistics.

Enabling the Call Admission Control Feature

The **platform subscriber cac cpu rp** *value* command enables the CAC feature based on the per-core average CPU load on the active RP:

```
Router# config t
Router#(config)# platform subscriber cac cpu rp 95
Router#(config)# end
```

No new IP session will be allowed in the system if the CPU on the active RP is greater than 95 percent; also, the FSOL packet is immediately dropped at the data plane layer.

Displaying the Call Admission Control Feature Statistics in Detail

The **show call admission statistics detailed** command displays the CAC statistics in detail. It also provides packet drop statistics for each CAC type.

Note The **show call admission statistics detailed** command only displays the details of platform resources, which are already configured. For example, the detail for the MEM_RP field is displayed in the output, only if it has been configured. Otherwise, it is not displayed in the output.

```
Router# show call admission statistics detailed

CAC New Model (SRSM) is ACTIVE
CAC statistics duration:  1873(seconds)
Total calls rejected 29, accepted 1749
Current hardware CAC status is: Not Dropping
Total call Session charges: 0, limit 0

CPU utilization: Five Sec Average CPU Load, Current actual CPU: 1%, Limit: 2%
Total count of session 1659, Limit: 128000

CAC Events:
```

```
        Reject reason          Times of activation   Duration of activation(secs)
Rejected calls
        CPU-limit:                      9                     42
 9
        SessionCharges:                 18                    42
 18
        LowPlatformResource:            8                     832
 1
        Session Limit:                  1                     47
 1

Total dropped FSOL packets at data plane: 4581  # total packets dropped at PD is 4581
  IOSD_CPU_OVERLIMIT_DROPS:     2381    # 2381 packets dropped due to IOS CPU overload
  CPS_OVERLIMIT_DROPS:          1892    # 1892 packets dropped due to CPS over limit
  TOTAL_SESSION_OVERLIMIT_DROPS:189     # 189 packets dropped due to total session limit
  CPU_RP_OVERLIMIT_DROPS:       20      # 20 packets dropped due to RP CPU overload
  CPU_FP_OVERLIMIT_DROPS:       20      # 20 packets dropped due to FP CPU overload
  MEM_RP_OVERLIMIT_DROPS:       20      # 20 packets dropped due to RP memory over limit
  MEM_FP_OVERLIMIT_DROPS:       20      # 20 packets dropped due to FP memory over limit

  MEM_QFP_OVERLIMIT_DROPS:      20      # 20 packets dropped due to QFP memory over limit
  MEM_CC_OVERLIMIT_DROPS:       19      # 19 packets dropped due to CC memory over limit

platform resource low: FALSE
platform resource polling interval: 5 seconds
    BQS_QUEUE       : current:  0%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 0
    MEM_RP          : current: 67%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 251
    MEM_FP          : current:  8%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 494
    MEM_CC          : current: 52%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 829
    MEM_QFP         : current: 11%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 778
    CPU_RP          : current:  7%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 383
    CPU_FP          : current: 11%,  limit: 95%,  overlimit: FALSE, overlimit_seconds: 697
```

Reference

Related Documents

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

MIBs

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

Technical Assistance

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

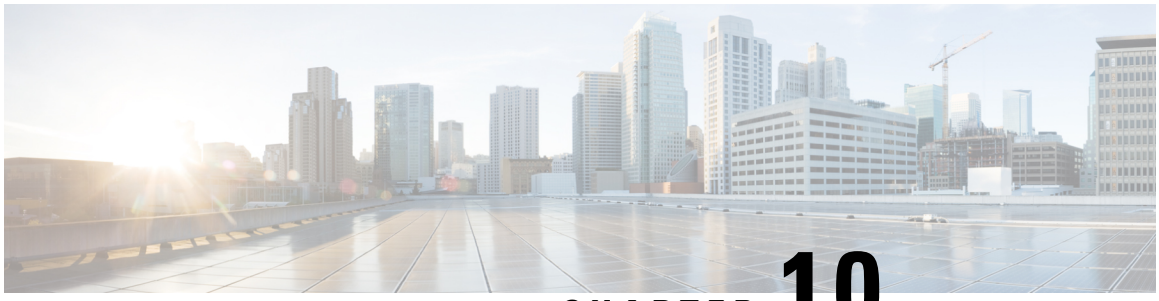
Feature Information for Call Admission Control

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 11: Feature Information for Call Admission Control

Feature Name	Releases	Feature Information
Call Admission Control	Cisco IOS XE Release 3.11	Call Admission Control (CAC) is a deterministic and informed decision that is made before a network session is established and is based on whether the required network resources are available to provide suitable quality of service (QoS) for the new session.



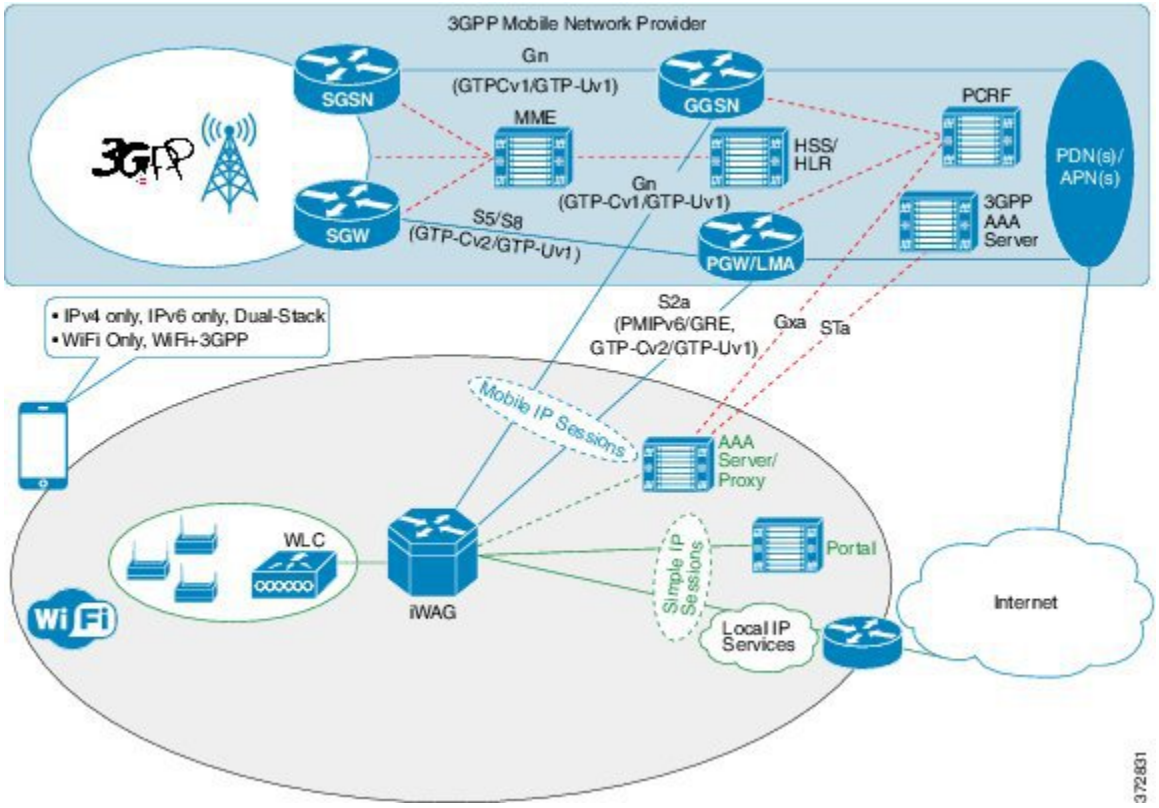
CHAPTER 10

iWAG Dual-Stack IPoE Session

Effective from Cisco IOS XE Release 3.11S, the Intelligent Wireless Access Gateway (iWAG) supports dual-stack session for Proxy Mobile IPv6 (PMIPv6), GPRS Tunneling Protocol (GTP) and Intelligent Services Gateway (ISG). With dual-stack, both IPv4 and IPv6 are simultaneously supported within a single IPoE session. For a dual-stack client device connecting to the iWAG over layer 2 network, a MAC-based session is established on receiving any FSOL. Based on the subscriber profile, IPv4 and IPv6 services are provisioned and activated when respective FSOL is received.

The following figure shows a deployment model of the iWAG Dual-Stack on a Cisco ASR 1000 Series Aggregation Services Router.

Figure 8: iWAG Dual-Stack Deployment on a Cisco ASR 1000 Series Aggregation Services Router



A session can be simple IPoE or mobile IPoE but the iWAG is the first-hop gateway/router for both IPv4 and IPv6.

For simple IPoE session, the iWAG provides the network connectivity and traffic is routed directly. IPv4 address and IPv6 /64 prefix are allocated locally by the iWAG and assigned to the client through DHCPv4 and IPv6 SLAAC. All the IPv4 and IPv6 features and services for simple IPoE session are handled by the iWAG.

For mobile IPoE session, mobile packet core provides the network connectivity over a tunnel established between the iWAG and the respective mobile packet core gateway. The tunnel is established between the iWAG and the packet core gateway when the session is established, and both IPv4 and IPv6 traffic is routed through the tunnel.

Mobility protocol used for establishing the tunnel and the tunnel type depends on the packet core gateway. The following mobility protocols and tunnel types are available:

- PMIPv6 for GRE tunnel between iWAG and LMA
- GTPv1 for GTP-U tunnel between iWAG and GGSN
- GTPv2 for GTP-U tunnel between iWAG and PGW

The IPv4 address and IPv6/64 prefix for the session are allocated by mobile packet core and passed to the iWAG through mobility protocol, which in turn assigns to client through DHCPv4 and IPv6 Stateless Address Auto Configuration (SLAAC). Only applicable IPv4 and IPv6 features and services for mobile IPoE session are handled by iWAG and the rest by mobile packet core gateway.

This chapter contains the following sections:

Finding Feature Information

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

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

Restrictions for the iWAG Dual-Stack IPoE Session

Dual Stack is not supported on EoGRE and L3 initiated sessions.

IPoE Dual-Stack Features

The following table provides the IPoE Dual-Stack features that are supported for Simple IP and Mobile IP sessions.

Features	Simple IP	Mobile IP (PMIPv6)	Mobile IP (GTP)	Notes
Authentication and Authorization	MAC TAL • Web Logon	MAC TAL	MAC TAL	Web logon can happen through IPv4 or IPv6 and Web Server and Portal Server should be dual stack.
Session Initiators (FSOLs)	DHCPv4, IPv6 ND (RS/NS/ NA), and Unclassified MAC Packet	DHCPv4, IPv6 ND (RS/NS/NA), Unclassified MAC Packet	DHCPv4, IPv6 ND (RS/NS/NA), Unclassified MAC Packet	First Sign of Life (FSOL) can be IPv4 or IPv6, for initiating a session and IPv4 address assignment (through DHCPv4) or IPv6 (/64) prefix assignment (through SLAAC with unicast RA) can happen first. In case of mobile IP, address and prefix allocation happens from LMA or GGSN or PGW.
Address Allocation	DHCPv4, IPv6 SLAAC	DHCPv4, IPv6 SLAAC	DHCPv4, IPv6 SLAAC	
Layer 4 Redirect (L4R)	Supported	Not Applicable	Not Applicable	L4R is a TC feature and separate TCs are required for IPv4 and IPv6.
Flow Based Redirect	Supported	Not Supported	Not Supported	Flow Based Redirect is a TC feature and separate TCs are required for IPv4 and IPv6.
Flow Based Redirect-SIPTO	Not Supported	Not Supported	Supported	
VRF Mapping	Supported	Not Applicable		Both IPv4 and IPv6 traffic are mapped to the same VRF.
PBHK	IPv4 only	Not Supported	Not Supported	PBHK is not supported for IPv6.
Session LI (SNMP /RADIUS)	Supported	Supported		

Features	Simple IP	Mobile IP (PMIPv6)	Mobile IP (GTP)	Notes
Mobility Protocols	Not Applicable	PMIPv6 (MAG - S2a)	GTP v1 (Gn) GTPv2 (S2a)	Partial compliance to 3GPP standards with basic features/functionality and mandatory IEs.
RADIUS CoA				
Account logon and logoff	Supported	Not Applicable	Not Applicable	Session identifier in CoA can be any of following: • Accounting-Session-ID • Session IPv4 address • iWAG IPv4 address and port in case of PBHK • Session IPv6 address
Service activation and deactivation	Supported	Supported		
Timeout Features				
Absolute	Supported	Supported	Supported	Absolute and Idle timeout features are supported at session level as well as Traffic Class - Service and Flow level.
Idle	Supported	Supported	Supported	
QoS				
Data Rate Limiting (DRL)	Supported	Supported	Supported	DRL feature is supported at session level as well as TC level.
Shaping	Supported	Supported	Supported	Shaping feature is supported only at session level.
Accounting				
Post Paid	Supported	Supported	Supported	Post-paid accounting feature is supported at session level as well as TC level.

Features	Simple IP	Mobile IP (PMIPv6)	Mobile IP (GTP)	Notes
Prepaid	Supported	Not Applicable	Not Applicable	Prepaid is a service and applicable only for TCs. Separate TCs are required for IPv4 and IPv6. iWAG prepaid authorization and re-authorization is separate for IPv4 and IPv6. The back-end system (prepaid server) can manage quota either separately for IPv4 and IPv6 TCs, or combined. Prepaid for mobile IP is done at MPC/EPC (GGSN/PGW, LMA) side.

Information About Dual Stack Support for Simple IP Subscriber Sessions

Dual-Stack Support for Simple IP Subscriber Sessions

The Dual-Stack Support for Simple IP Subscriber Sessions feature enables L2-connected, dual-stack IP over Ethernet (IPoE) sessions to be provisioned on the Cisco Intelligent Services Gateway (ISG). This module describes how to configure ISG to support IPv6 L2-connected sessions and dual-stack IP sessions.

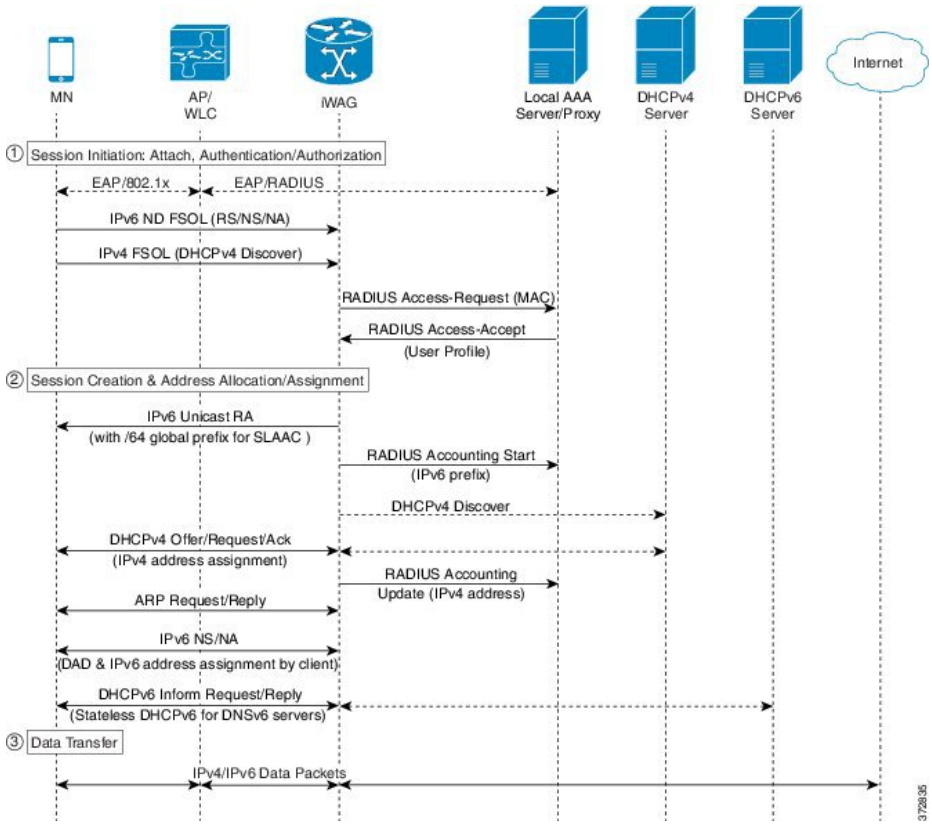
Prerequisites for Dual-Stack Support for Simple IP Subscriber Sessions

- The subscriber must be Layer 2-connected.
- The web or portal server should be a dual-stack host.
- The **ipv6 unicast-routing** command needs to be enabled on the ISG to enable dual-stack sessions.
- Either the IPv6 pool has to be configured in the ISG or the framed IPv6 prefix needs to be downloaded from RADIUS.
- The ISG has to be configured with the respective TCs or services to ensure proper web or portal access.
- You should be familiar with the concepts and tasks described in the “Configuring ISG Control Policies” module.

Dual-Stack Simple IPoE Session with MAC TAL Call Flow

The following figure illustrates the call flow for a dual-stack simple IPoE session with MAC TAL.

Figure 9: Dual-Stack Simple IPoE Session with MAC TAL call flow



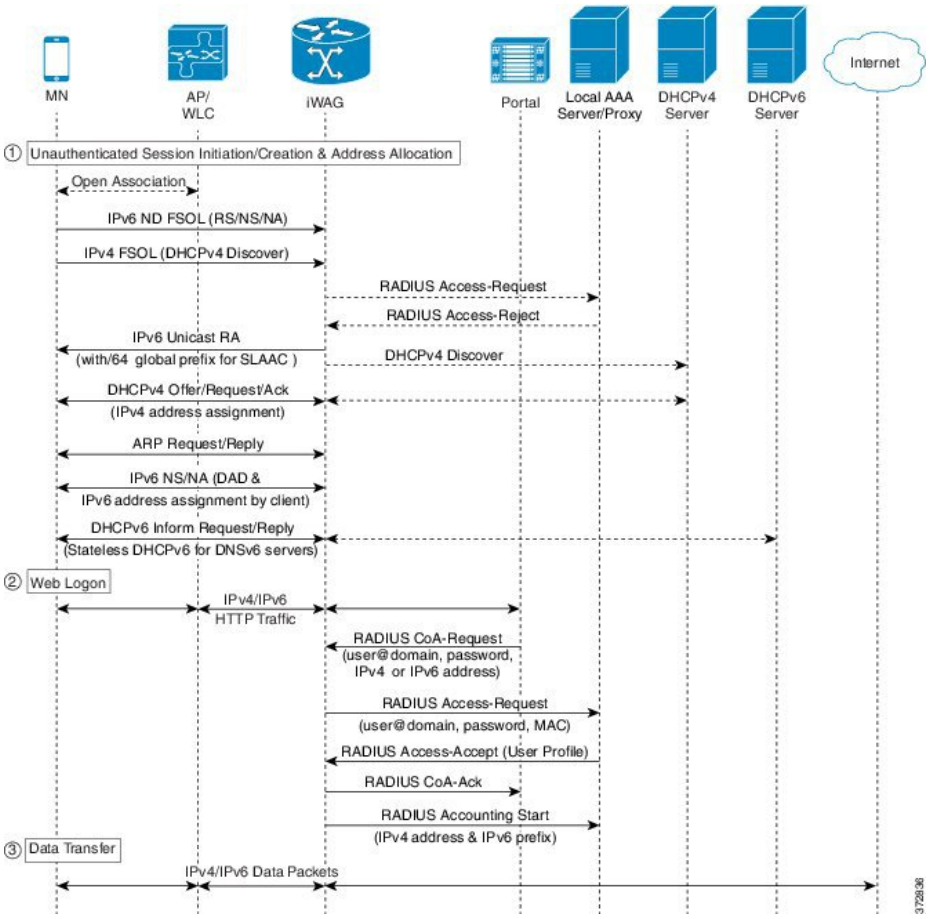
1. A mobile device is automatically associated to the service set identifier (SSID) broadcast by the access points to establish and maintain wireless connectivity.
2. The access point (AP) or Wireless LAN controller (WLC) starts the authentication process using Extensible Authentication Protocol (EAP) by sending an EAP Request ID to the mobile device.
3. The mobile device sends a response for the EAP Request ID back to the AP or WLC.
4. Upon successful authentication, the mobile device sends a DHCPv4 Discover message to the iWAG.
5. The iWAG sends a RADIUS Access Request to the AAA server asking it to authenticate the subscriber.
6. The iWAG creates a MAC-based ISG session, initiates MAC TAL and pulls the subscriber profile from the AAA server. If the profile has the AAA attribute value as "Cisco-AVPair=mn-service=dual", then the subscriber is authorized for both IPv4 and IPv6 data transfer. Similarly, the AAA attribute value of "Cisco-AVPair=mn-service=ipv4" or "Cisco-AVPair=mn-service=ipv6" represents the IPv4 or IPv6 protocol, using which the subscriber is authorized to send data.
7. The mobile device sends an IPv6 FSOL that could be router solicit, neighbor solicit, or neighbor advertisement, to the iWAG.
8. The iWAG checks whether the ISG session for the MAC address is initiated or created. IWAG waits for verifying the subscriber profile from AAA server.
9. The AAA server sends the RADIUS Access Accept message to the iWAG.

10. In response to the IPv6 (RS) FSOL sent, the iWAG sends a router advertisement (RA) packet using SLAAC that includes the IPv6 prefix, to the mobile device. The mobile device appends the IPv6 prefix to it's 64-bit (EUI or MAC address appended with FFFE) to form a unique 128 bit address.
11. The iWAG sends the IPv4 address through a DHCP Offer message to the mobile device. The iWAG provisions the IPv4 stack.
12. An Accounting Start message is sent to the application provider to indicate the start of the subscriber's service. Now, the subscriber is connected to the Internet.

Dual-Stack Simple IPoE Session with Web Logon Call Flow

The following figure illustrates the call flow for a dual-stack simple IPoE session with Web Logon.

Figure 10: Dual-Stack Simple IPoE Session with Web Logon call flow



1. A mobile device is automatically associated to the service set identifier (SSID) broadcast by the access points to establish and maintain wireless connectivity.
2. The access point (AP) or Wireless LAN controller (WLC) starts the authentication process using Extensible Authentication Protocol (EAP) by sending an EAP Request ID to the mobile device.
3. The mobile device sends a response for the EAP Request ID back to the AP or WLC.

4. Upon successful authentication, the mobile device sends an IPv6 FSOL that could be router solicit, neighbor solicit, or neighbor advertisement, to the iWAG.
5. The iWAG creates a MAC-based ISG session and pulls the subscriber profile from the AAA server. If the profile has the AAA attribute value as "Cisco-AVPair=mn-service=dual", then the subscriber is authorized for both IPv4 and IPv6 data transfer. Similarly, the AAA attribute value of "Cisco-AVPair=mn-service=ipv4" or "Cisco-AVPair=mn-service=ipv6" represents the IPv4 or IPv6 protocol, using which the subscriber is authorized to send data.
6. The iWAG sends a RADIUS Access Request to the AAA server asking it to authenticate the subscriber.
7. The mobile device sends a DHCPv4 Discover message to the iWAG.
8. The iWAG checks whether the ISG session for the MAC address is initiated or created.
9. The AAA server sends the RADIUS Access Accept message to the iWAG.
10. In response to the IPv6 (RS) FSOL sent, the iWAG sends a router advertisement (RA) packet using SLAAC that includes the IPv6 prefix, to the mobile device. The mobile device appends the IPv6 prefix to it's 64-bit (EUI or MAC address appended with FFFE) to form a unique 128 bit address.
11. The iWAG sends the IPv4 address through a DHCP Offer message to the mobile device. The iWAG provisions the IPv4 stack.
12. An Accounting Start message is sent to the application provider to indicate the start of the subscriber's service. Now, the subscriber is connected to the Internet.

How to Configure Dual-Stack Support for Simple IP Subscriber Sessions

Configuring Dual Stack Support on ISG

Dual stack can be configured in ISG for both MAC TAL and WebAuth subscribers.

To configure dual stack for MAC TAL users, perform the following actions:

- Configure the class map
- Define the services
- Associate the service to the control policy

To configure dual stack for WebAuth users, perform the following actions:

- Configure the ACL
- Configure the class map
- Define the services
- Associate the service to the control policy

Verifying Dual Stack Support on ISG

To verify the dual stack configuration on an ISG device, use any of the following show commands, in any order, in privileged EXEC mode.

SUMMARY STEPS

1. show subscriber session detail
2. show ip subscriber detail

DETAILED STEPS

Step 1 show subscriber session detail

Example:

```
#---------------------------
#  IPV4/IPv6 Session
#---------------------------

ISG#show subscriber session detail
Current Subscriber Information: Total sessions 1
-------------------------------------------------
Type: IPv4/IPv6, UID: 256, State: authen, Identity: aaaa.bbbb.cccc
IPv4 Address: 11.11.11.2
IPv6 Address: 5001::
Session Up-time: 00:00:26, Last Changed: 00:00:09
Switch-ID: 5015

Policy information:
  Context 7F0D2045B278: Handle 4A0001BB
  AAA_id 0000010C: Flow_handle 0
  Authentication status: authen
  Downloaded User profile, excluding services:
    service-type         0   2 [Framed]
  Downloaded User profile, including services:
    service-type         0   2 [Framed]
  Config history for session (recent to oldest):
    Access-type: IP Client: SM
     Policy event: Service Selection Request
      Profile name: aaaa.bbbb.cccc, 2 references
        service-type         0   2 [Framed]
  Rules, actions and conditions executed:
    subscriber rule-map TAL
      condition always event session-start
        10 authorize identifier mac-address

Classifiers:
Class-id    Dir   Packets    Bytes                 Pri.  Definition
0           In    10         1112                  0    Match Any
1           Out   9          1026                  0    Match Any

Configuration Sources:
Type  Active Time  AAA Service ID  Name
USR   00:00:26     -               Peruser
INT   00:00:26     -               FastEthernet0/0/2

#---------------------------
#  DHCPV4/IPv6 Session
#---------------------------

ISG#show subscriber session detail
Current Subscriber Information: Total sessions 1
-------------------------------------------------
Type: DHCPv4/IPv6, UID: 256, State: authen, Identity: aaaa.bbbb.cccc
IPv4 Address: 11.11.11.2
```

```
IPv6 Address: 5001::
Session Up-time: 00:00:26, Last Changed: 00:00:09
Switch-ID: 5015

Policy information:
  Context 7F0D2045B278: Handle 4A0001BB
  AAA_id 0000010C: Flow_handle 0
  Authentication status: authen
  Downloaded User profile, excluding services:
    service-type         0   2 [Framed]
  Downloaded User profile, including services:
    service-type         0   2 [Framed]
  Config history for session (recent to oldest):
    Access-type: IP Client: SM
     Policy event: Service Selection Request
      Profile name: aaaa.bbbb.cccc, 2 references
        service-type         0   2 [Framed]
  Rules, actions and conditions executed:
    subscriber rule-map TAL
      condition always event session-start
        10 authorize identifier mac-address

Classifiers:
Class-id    Dir   Packets    Bytes                 Pri.  Definition
0           In    10         1112                  0    Match Any
1           Out   9          1026                  0    Match Any

Configuration Sources:
Type  Active Time  AAA Service ID  Name
USR   00:00:26     -               Peruser
INT   00:00:26     -               FastEthernet0/0/2
```

Step 2 **show ip subscriber detail**

Example:

```
ISG#show ip subscriber detail
IP subscriber: 0019.aa9f.6619, type connected, status up
  display uid: 196, aaa uid: 1229
  segment id: 38589, session hdl: 0x71000296, shdb: 0x8000162
  session initiator: unclassified traffic dhcp discovery
  access interface: GigabitEthernet0/2/0
  access address: 2001::
  service address: 2001::
  access address: 12.1.1.27
  service address: 12.1.1.27
  status: IPv4 - Up  IPv6 - Up
  conditional debug flag: 0x0
  control plane state: connected, start time: 00:03:01
  data plane state: connected, start time: 00:03:01
  arp entry: 12.1.1.27, GigabitEthernet0/2/0
  route: 2001::/64 -> GigabitEthernet0/2/0
  forwarding statistics:
    packets total: received 0, sent 0
    bytes total: received 0, sent 0
    packets dropped: 0, bytes dropped: 0
  hardware forwarding statistics:
    packets total: received 2, sent 0
    bytes total: received 164, sent 0
```

Configuration Examples for Dual-Stack Support for Simple IP Subscriber Sessions

Example: Configuring Simple IP Dual Stack with MAC TAL

```
#-----------------------------
# Configure the IPv6 pool
#-----------------------------
!
access-list 101 permit ip host 22.22.22.1 any
access-list 101 permit icmp host 22.22.22.1 any
ipv6 route 2001:420:54FF:4::400:0/119 2001:420:54FF:4::400:1
ipv6 local pool FIRST 9999::/48 64   ---> To support ipv6 on the existing v4 box
ipv6 local pool RED 6868::/48 64
!
!
!
#-----------------------------
# Enable IPv6 on the interface
#-----------------------------
!
interface GigabitEthernet0/0/0                #Configuring the core interface
 ip address 9.27.52.4 255.255.0.0
 ip portbundle outside
 negotiation auto
 ipv6 enable
!
interface GigabitEthernet0/0/1                #Configuring the access interface
 ip unnumbered Loopback68
 negotiation auto
 ipv6 enable
 service-policy type control START_WEB
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
!
```

Example: Configuring Simple IP Dual Stack with Web Auth

```
#-----------------------------
# Configure the IPv6 pool
#-----------------------------
!
access-list 101 permit ip host 22.22.22.1 any
access-list 101 permit icmp host 22.22.22.1 any
ipv6 route 2001:420:54FF:4::400:0/119 2001:420:54FF:4::400:1
ipv6 local pool FIRST 9999::/48 64   ---> To support ipv6 on the existing v4 box
ipv6 local pool RED 6868::/48 64
!
!
!
#-----------------------------
# Enable IPv6 on the interface
#-----------------------------
!
interface GigabitEthernet0/0/0                #Configuring the core interface
 ip address 9.27.52.4 255.255.0.0
```

```
 ip portbundle outside
 negotiation auto
 ipv6 enable
!
interface GigabitEthernet0/0/1                 #Configuring the access interface
 ip unnumbered Loopback68
 negotiation auto
 ipv6 enable
 service-policy type control START_WEB
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
!
#-----------------------------
# Configure policy
#-----------------------------
!
ipv6 access-list TCPv6                         #Configuring IPv6 ACL
 permit tcp any any
!
ipv6 access-list TCPv6_ALL
 permit tcp any any
!
class-map type traffic match-any TCPv6         #Configuring the class map for IPv6 traffic
 match access-group input name TCPv6
 match access-group output name TCPv6
!
class-map type traffic match-any TCPv4
 match access-group input name TCPv4
 match access-group output name TCPv4
!
policy-map type service L4Rv4
 class type traffic TCPv4
  redirect to ip 18.18.18.18 port 8080
 !
!
policy-map type service L4Rv6                  #Service definition for IPv6
 class type traffic TCPv6
  redirect to ip 1818::1818 port 80
 !
!
policy-map type control START_WEB
 class type control UNAUTH_COND event timed-policy-expiry
  10 service disconnect
 !
 class type control always event session-start
  8 service-policy type service name PBHK
  9 authorize identifier mac-address
  11 service-policy type service name L4Rv6    #Associating the service to the control
policy
  12 service-policy type service name L4Rv4
  15 set-timer UNAUTH_TIMER 10
 !
 class type control always event session-restart
  8 service-policy type service name PBHK
  9 authorize identifier mac-address
  11 service-policy type service name L4Rv6
  12 service-policy type service name L4Rv4
  15 set-timer UNAUTH_TIMER 10
 !
 class type control always event account-logon
  2 authenticate aaa list List1
  14 service-policy type service unapply name L4Rv6
  15 service-policy type service unapply name L4Rv4
```

!
!

Information About Dual-Stack Support for PMIPv6

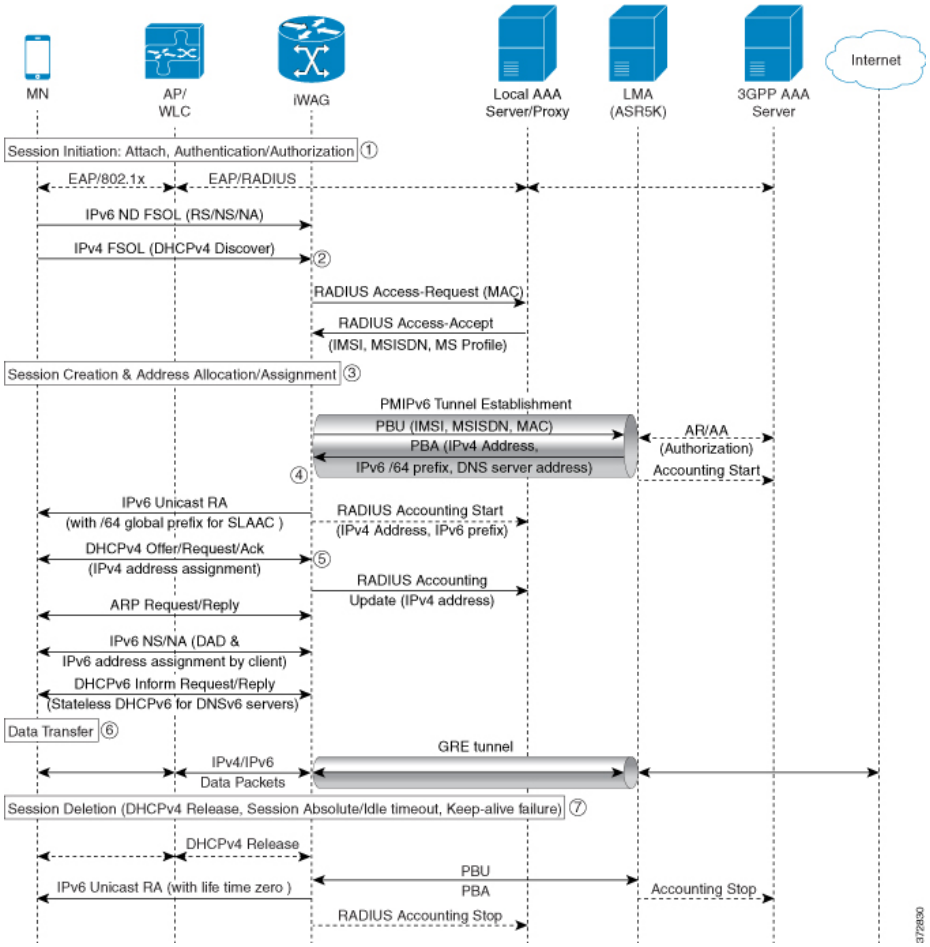
The Dual Stack Support for PMIPv6 feature allows both IPv4 and IPv6 traffic streams to flow through a single PMIPv6 session. The IPv4 and IPv6 traffic streams from a subscriber are identified using the Subscriber MAC address. The iWAG supports following functionalities:

- IPv6 L2-connected subscriber sessions
- Dual-stack L2-connected Internet Protocol Over Ethernet (IPoE) subscriber sessions

Dual-Stack Mobile IPoE Session PMIPv6 Call Flow

The following figure and steps describe the call flow pertaining to a Dual-Stack Mobile IP over Ethernet (IPoE) session as first sign of life (FSOL) for PMIPv6.

Figure 11: Dual-Stack Mobile IPoE Session for PMIPv6



1. iWAG initiates the session with the subscriber by enabling AAA.
2. The first FSOL packet from the mobile subscriber is either IPv6 ND packet or DHCP Discover. When iWAG receives any FSOL, MAC TAL is initiated for authorization. The mobile subscriber profile obtained from AAA server contains both IPv4 and IPv6 features and services.
3. Upon successful subscriber authorization, the session is created and the address is allocated and assigned.
4. The IPv6 prefix received from the LMA is assigned to the subscriber through stateless address auto-configuration (SLAAC) (unicast RA). Based on the received mobile subscriber Profile and the local configuration, IPv6 features and services for the session are activated.
5. The IPv4 address received from the LMA is assigned to the mobile subscriber through DHCPv4. Based on the received mobile subscriber profile and local configuration, the IPv4 features and services for the session are activated.
6. After the tunnel has been established, the data flows bidirectionally.

Configuration Examples for Dual-Stack PMIPv6

Example: Dual Stack Mobile IPoE Session for PMIPv6

```
#-----------------------------------------------
# Configuring AAA and RADIUS
#-----------------------------------------------
aaa new-model
!
aaa server radius dynamic-author
 client 10.5.5.1 server-key cisco1
!
aaa group server radius SERVER_GROUP1
server name RAD1
!
aaa authentication login AUTHEN_LIST group SERVER_GROUP1
aaa authorization network default group SERVER_GROUP1 local
aaa authorization network AUTHOR_LIST group SERVER_GROUP1 local
aaa authorization subscriber-service default local group SERVER_GROUP1
aaa accounting network List1 start-stop group SERVER_GROUP1
aaa accounting system default start-stop group radius
!
radius-server key cisco1
!
radius server RAD1
address ipv4 192.0.2.1 auth-port 1645 acct-port 1646


#-------------------------------------------------
#Configuring an Access Interface for Dual-Stack PMIPv6
#-------------------------------------------------
interface GigabitEthernet0/0/2
 description user1 connected to MN1
 ip address 192.0.2.20 255.255.255.0
 negotiation auto
 ipv6 address FE80::260:3EFF:FE11:6770 link-local
 service-policy type control PMIP_DUAL_STACK    #subscriber services are applied based on

                                                the control policy definition
 ip subscriber l2-connected                     #invokes iWAG functionality

 initiator unclassified mac-address             #unclassified MAC address with IPv4
```

```
                                                    and IPv6 packets,are treated
                                                    as FSOL to create a dual stack session
initiator dhcp                                     #DHCP control packets are used as FSOL
                                                   to create DHCPv4 only session
end


#-------------------------------------------------------
#Configuring Mobile Access Gateways for Dual-Stack PMIPv6
#-------------------------------------------------------
ipv6 mobile pmipv6-domain D1            #domain with name D1 configuration
 replay-protection timestamp window 255
 mn-profile-load-aaa              #subscriber service profile downloaded from AAA server
 lma lma1                         #associating LMA with name lma1 to domain D1
  ipv6-address 2001:DB8::1
  ipv4-address 10.1.1.2
 mag M1                           #associating MAG with name M1 to domain D1
  ipv6-address 2001:DB8:0:ABCD::1
  ipv4-address 10.1.1.1
 nai MN1@example.com               #local subscriber NAI definition for authotrization,
                                    where service for this particular NAI is defined
  apn example.com
  lma lma1
  service dual                     #dual stack is enabled for MN1@example.com client
  int att ETHERNET l2-addr 0000.1111.2222
!
ipv6 mobile pmipv6-mag M1 domain D1
 no discover-mn-detach
 sessionmgr
 apn example.com
 address ipv6 2001:DB8:0:ABCD::1
 address ipv4 10.1.1.1
 binding maximum 40000
 replay-protection timestamp window 255
 interface GigabitEthernet0/0/2
  enable pmipv6 default MN1@example.com
 lma lma1 D1
  ipv6-address 2001:DB8::1
  ipv4-address 10.1.1.2
  encap gre-ipv4

#-------------------------------------------------------------------------------
#Configuring an Access List Traffic Classmap for Dual-Stack PMIPv6
#-------------------------------------------------------------------------------
 ip access-list extended ACL_OUT_INTERNET
 permit ip any any
ip access-list extended ACL_OUT_INTERNET2
 permit ip any any
ip access-list extended ACL_OUT_OPENGARDEN
 permit ip any any
 permit udp any any
ip access-list extended ACL_IN_INTERNET
 permit ip any any
ip access-list extended ACL_IN_INTERNET2
 permit ip any any
ip access-list extended ACL_IN_OPENGARDEN
 permit ip any any
 permit udp any any

ipv6 access-list IPV6_ACL_INTERNET
 permit ipv6 any any
ipv6 access-list IPV6_ACL_INTERNET2
 permit ipv6 any any
```

```
ipv6 access-list IPV6_ACL_OPENGARDEN
 permit ipv6 any any

#-------------------------------------------------------------
#Configuring a Classmap for Dual-Stack PMIPv6
#-------------------------------------------------------------
class-map type traffic match-any TC_OPENGARDEN     #defines the traffic rule used
                                                   in the service using ACL.
 match access-group output name ACL_OUT_OPENGARDEN
 match access-group input name ACL_IN_OPENGARDEN
!
class-map type traffic match-any TC_INTERNET2
 match access-group output name ACL_OUT_INTERNET2
 match access-group input name ACL_IN_INTERNET2
!
class-map type traffic match-any TC_INTERNET
 match access-group output name ACL_OUT_INTERNET
 match access-group input name ACL_IN_INTERNET

class-map type traffic match-any TC_INTERNET_IPV6
 match access-group output name IPV6_ACL_INTERNET
 match access-group input name IPV6_ACL_INTERNET

class-map type traffic match-any TC_INTERNET_IPV6_2
 match access-group output name IPV6_ACL_INTERNET2
 match access-group input name IPV6_ACL_INTERNET2

class-map type traffic match-any TC_OPENGARDEN_IPV6
 match access-group output name IPV6_ACL_OPENGARDEN
 match access-group input name IPV6_ACL_OPENGARDEN

#-------------------------------------------------------------
# Configuring a Policymap for Dual-Stack PMIPv6
#-------------------------------------------------------------
policy-map type service DRL_V4        #provides service definition for services
                                       applied during session start and restart
 20 class type traffic TC_INTERNET
  police input 512000 512000 10000
  police output 1280000 560000 20000
 !
policy-map type service ACC_V4
 20 class type traffic TC_INTERNET2
  accounting aaa list default
!
policy-map type service TO_V4
 20 class type traffic TC_OPENGARDEN
  timeout idle 60
 !
policy-map type service DRL_V6
 20 class type traffic TC_INTERNET_IPV6
  police input 512000 512000 10000
  police output 1280000 560000 20000
 !
policy-map type service ACC_V6
 20 class type traffic TC_INTERNET_IPV6_2
  accounting aaa list default
  !
policy-map type service TO_V6
 20 class type traffic TC_OPENGARDEN_IPV6
timeout idle 60
 !

#-------------------------------------------------------------
#Configuring a Control Policy for Dual-Stack PMIPv6
```

```
#------------------------------------------------------------
policy-map type control PMIP_DUAL_STACK
 class type control always event session-start
  10 service-policy type service name DRL_V4       #applying services during dual stack
  11 service-policy type service name DRL_V6       #applying services during dual stack
  15 service-policy type service name ACC_V4       #applying services during dual stack
  16 service-policy type service name ACC_V6       #applying services during dual stack
  20 service-policy type service name TO_V4        #applying services during dual stack
  21 service-policy type service name TO_V6        #applying services during dual stack
  25 service-policy type service name SESSION_TIMEOUT_SERVICE  #applying services
                                                                during dual stack
  30 authorize aaa list default identifier mac-address   #performs MAC TAL authorization


 class type control always event session-restart
  10 service-policy type service name DRL_V4       #applying services during dual stack
  11 service-policy type service name DRL_V6       #applying services during dual stack
  15 service-policy type service name ACC_V4       #applying services during dual stack
  16 service-policy type service name ACC_V6       #applying services during dual stack
  20 service-policy type service name TO_V4        #applying services during dual stack
  21 service-policy type service name TO_V6        #applying services during dual stack
  25 service-policy type service name SESSION_TIMEOUT_SERVICE  #applying services during
                                                                dual stack
  30 authorize aaa list default identifier mac-address        #performs MAC TAL authorization


#-------------------------------------------------------------------------------------
#Configuring the Local Mobility Anchor for Cisco ASR 5000 Routers
#-------------------------------------------------------------------------------------
 context pgw
    ip pool PMIP_POOL 192.168.1.0 255.255.0.0 public 0 subscriber-gw-address 192.168.2.0
    ip pool v4_staticpool 192.168.255.255 255.255.0.0 static
    ipv6 pool v6_pool prefix eeee::1/48 public 0 policy allow-static-allocation
    router rip
      network ip 192.168.1.0/16
      network name lma2
      redistribute connected
      version 2
    exit
    interface lma2
      ipv6 address 2001:DB8:2222:7272::72/64
      ip address 192.0.2.201 255.255.255.0 secondary
    exit
    subscriber default
    exit
    apn example.com
      pdp-type ipv4 ipv6      #enables dual-stack address assignment under ASR 5K LMA
      selection-mode sent-by-ms
      accounting-mode none
      ip context-name pgw
    exit
    aaa group default
    exit
    gtpp group default
    exit
    lma-service lma2
      no aaa accounting
      reg-lifetime 40000
      timestamp-replay-protection tolerance 0
      mobility-option-type-value standard
      revocation enable
      bind address 2001:DB8:2222:7272::72
    exit
    pgw-service pgw1
```

```
      plmn id mcc 100 mnc 200
      associate lma-service lma2
    exit
    ipv6 route 2001:DB8::/64 next-hop 2001:DB8:0:0:E000::F interface lma2
    ip igmp profile default
    exit
  exit
  port ethernet 17/1
    boxertap ethernet 4
    no shutdown
    bind interface lma2 pgw
  exit
  port ethernet 17/3
    vlan 200
      no shutdown
    exit
  exit
  port ethernet 17/4
    no shutdown
  exit
end
```

Information About Dual-Stack Support for GTP

The Dual Stack Support for GTP feature allows both IPv4 and IPv6 traffic streams to flow through a single GTP session. The IPv4 and IPv6 traffic streams from a subscriber are identified using the Subscriber MAC address. This feature enables the assignment of both an IPv4 address and an IPv6 address to a client. Therefore, the overall number of supported subscribers on the Cisco ASR 1000 Series Aggregation Services Routers are not affected by a mix of IPv4 and IPv6 traffic.

Note Prior to the introduction of the Dual-Stack feature, GTP supported only IPv4 sessions.

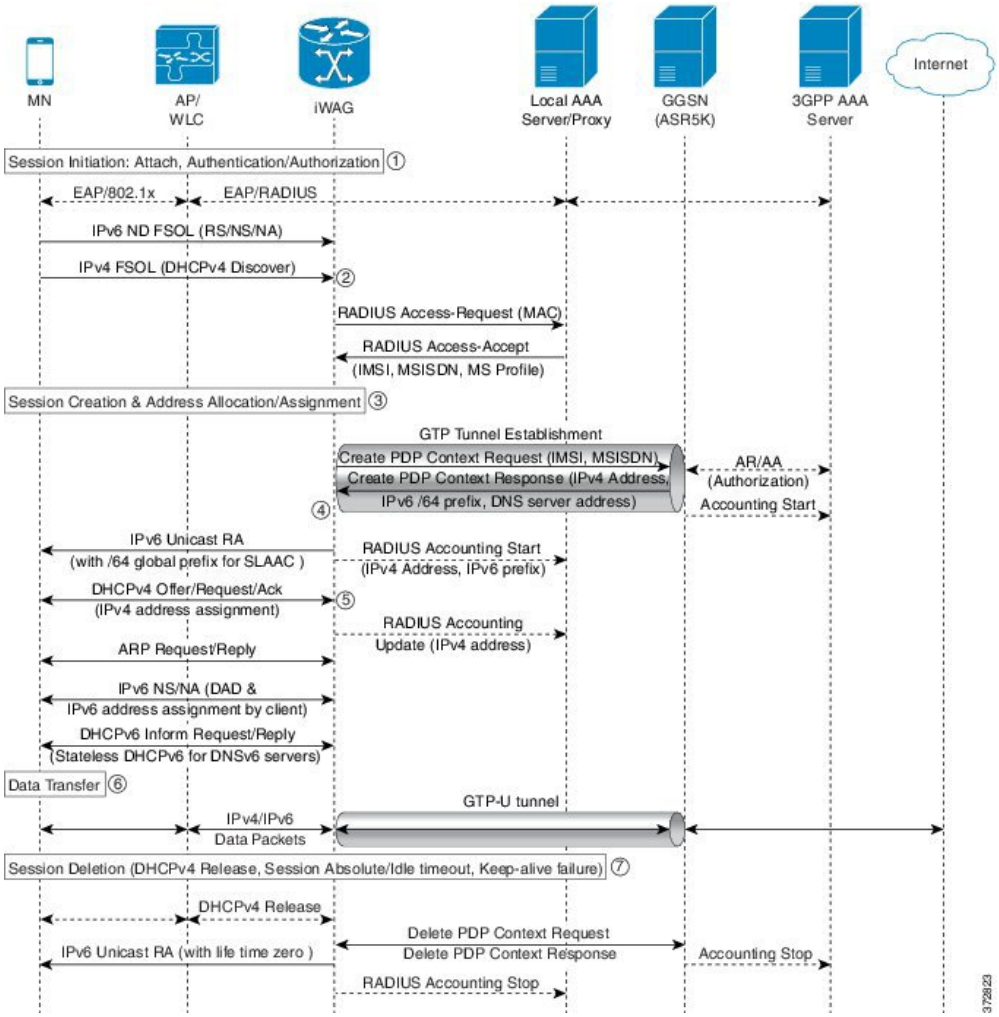
Dual-Stack GTP sessions support the following session initiators:

- Unclassified MAC
- IPv6 Neighbor Discovery
- DHCPv4

Dual-Stack Mobile IPoE Session for GTPv1 Call Flow

The following figure and steps describe the call flow pertaining to a Dual-Stack Mobile IP over Ethernet (IPoE) session for GTPv1.

Figure 12: Dual-Stack Mobile IPoE Session for GTPv1 Call Flow



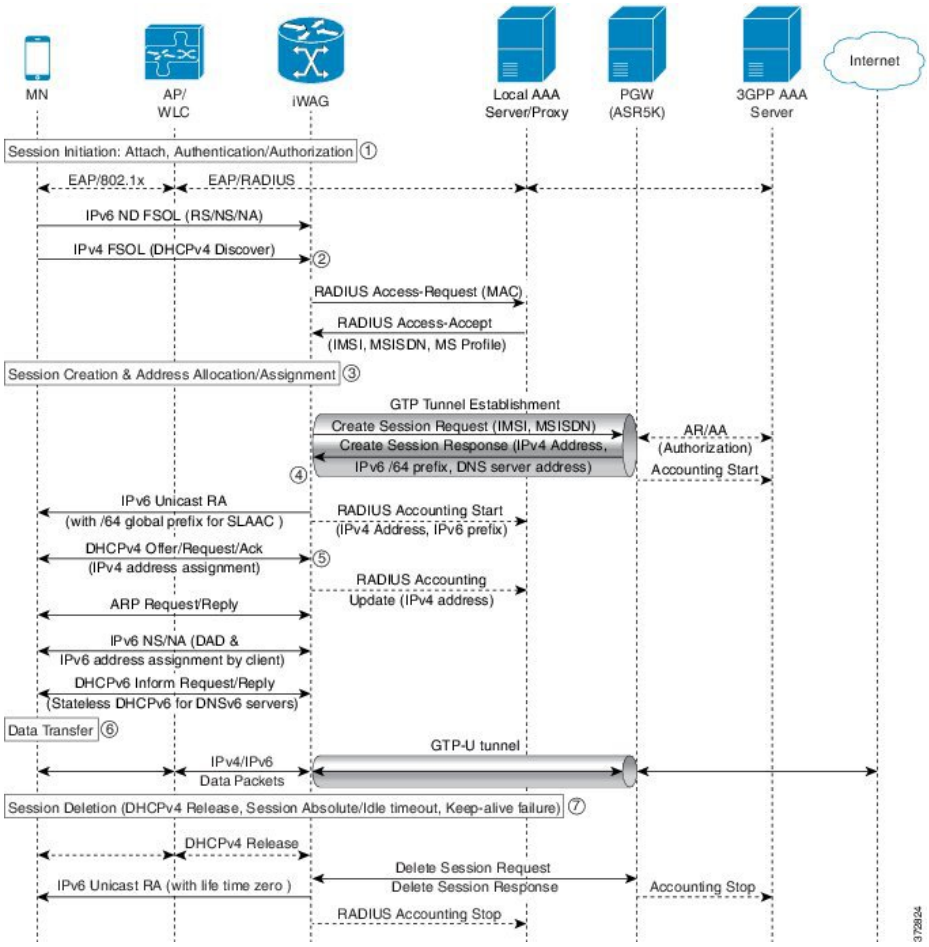
1. The iWAG initiates the session with the subscriber by enabling AAA.
2. The first FSOL packet from the mobile subscriber is either IPv6 ND packet or DHCP Discover. When iWAG receives any FSOL, MAC TAL is initiated for authorization.

   The mobile subscriber profile obtained from AAA server contains both IPv4 and IPv6 features and services.
3. Upon successful subscriber authorization, the session is created and the address is allocated and assigned.
4. The IPv6 prefix received from the GGSN is assigned to the mobile subscriber through stateless address auto configuration (SLAAC) (unicast RA). Based on the received mobile subscriber profile and the local configuration, IPv6 features and services for the session are activated.
5. The IPv4 address received from the GGSN is assigned to the mobile subscriber through DHCPv4. Based on the received mobile subscriber profile and local configuration, IPv4 features and services for the session are activated.
6. After the tunnel has been established, the data can flow bi-directionally.

Dual-Stack Mobile IPoE Session for GTPv2 Call Flow

The following figure and steps describe the call flow pertaining to a Dual-Stack Mobile IP over Ethernet (IPoE) session for GTPv2.

Figure 13: Dual-Stack Mobile IPoE Session for GTPv2 Call Flow



1. The iWAG initiates the session with the subscriber by enabling AAA.
2. The first FSOL packet from the mobile subscriber is either IPv6 ND packet or DHCP Discover. When iWAG receives any FSOL, MAC TAL is initiated for authorization.

   The mobile subscriber profile obtained from AAA server contains both IPv4 and IPv6 features and services.
3. Upon successful subscriber authorization, the session is created and the address is allocated and assigned.
4. The IPv6 prefix received from the PGW is assigned to the mobile subscriber through stateless address auto configuration (SLAAC) (unicast RA). Based on the received mobile subscriber profile and the local configuration, IPv6 features and services for the session are activated.
5. The IPv4 address received from the PGW is assigned to the mobile subscriber through DHCPv4. Based on the received mobile subscriber profile and local configuration, IPv4 features and services for the session are activated.

6. After the tunnel has been established, the data can flow bi-directionally.

Configuration Examples for Dual-Stack GTP

Example: Configuring Dual-Stack Sessions for GTP

```
gtp
information-element rat-type wlan
interface local GigabitEthernet0/1/3
apn 1
  apn-name example1.com
  ip address ggsn 10.201.31.2
  default-gw 30.1.0.1 prefix-len 16
  dns-server 192.165.1.1
  dhcp-lease 1801
apn 2
  apn-name example2.com
  ip address ggsn 10.201.31.4
  default-gw 30.2.0.1 prefix-len 16
  dns-server 192.165.1.1
  dhcp-lease 1801
```

Example: Configuring an Interface to PGW or GGSN

```
interface GigabitEthernet0/1/3
description SGSN to GGSN port
ip address 10.201.31.1 255.255.255.0
negotiation auto
ipv6 address 2007::2/64
end
```

Example: Configuring a Control Policy for Dual-Stack GTP

```
policy-map type control BB_PMAP
class type control always event session-start
10 authorize aaa list BB_1 password cisco identifier mac-address
```

Example: Configuring an Access Interface for Dual-Stack GTP

```
interface GigabitEthernet0/0/3
ip address 21.0.0.1 255.255.0.0
ipv6 address 8001::1/16
ipv6 enable
ipv6 nd ra interval 600
service-policy type control BB_PMAP
ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
end
```

Example: Enabling IPv6 Routing

```
ipv6 unicast-routing
```

AAA Attributes for Dual Stack

After the AAA server authenticates a subscriber, an AAA attribute is returned in the Access Accept message sent to the iWAG to indicate the session type.

The AAA attribute for the Dual Stack configuration can have the following value:

"cisco-AVPair=mn-service=dual"

(The iWAG retrieves both the IPv4 and IPv6 addresses, but will assign the IPv4 or IPv6 address to the subscriber based on the FSOL.)

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

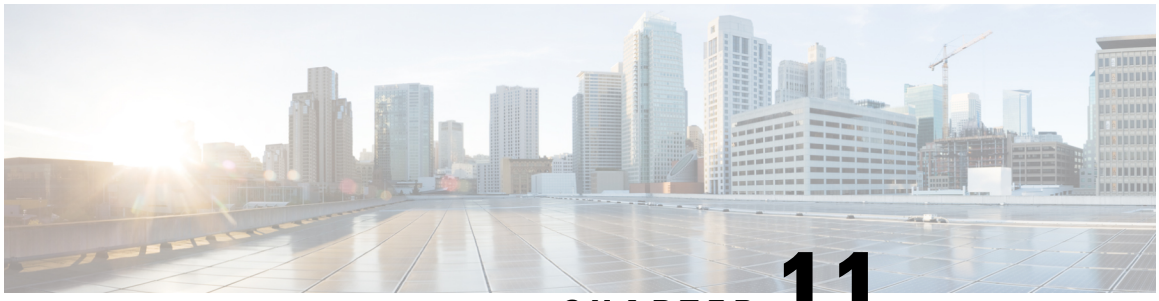
Feature Information for iWAG Dual-Stack IPoE Session

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 12: Feature Information for iWAG Dual-Stack IPoE Session

Feature Name	Releases	Feature Information
iWAG Dual-Stack IPoE Session	Cisco IOS XE Release 3.11	The iWAG Dual-Stack IPoE Session feature allows both IPv4 and IPv6 traffic streams to flow through a single PMIPv6 or GTP or ISG session. In Cisco IOS XE Release 3.11S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 11

Flow-Based Redirect

The traffic from an IP session is redirected based on the destination address (for a simple IP session), and to a tunnel (for a mobile IP session). However, in some application scenarios, some of the traffic is routed to a specific system or a specific interface for additional service or processing. Through the Adult Content Filtering (ACF) capability, web traffic of some sessions can be routed to an ACF appliance that filters the traffic based on the URL or content. The Flow-Based Redirect (FBR) feature enables applications such as the ACF to route matching traffic to a specified next hop device.

The FBR feature is Virtual Routing and Forwarding (VRF)-aware. You can map an interface to a VRF or transfer a VRF as long as the session and the interface connecting the next hop device are within the same VRF network.

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.

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.

Flow-Based Redirect for Adult Content Filtering

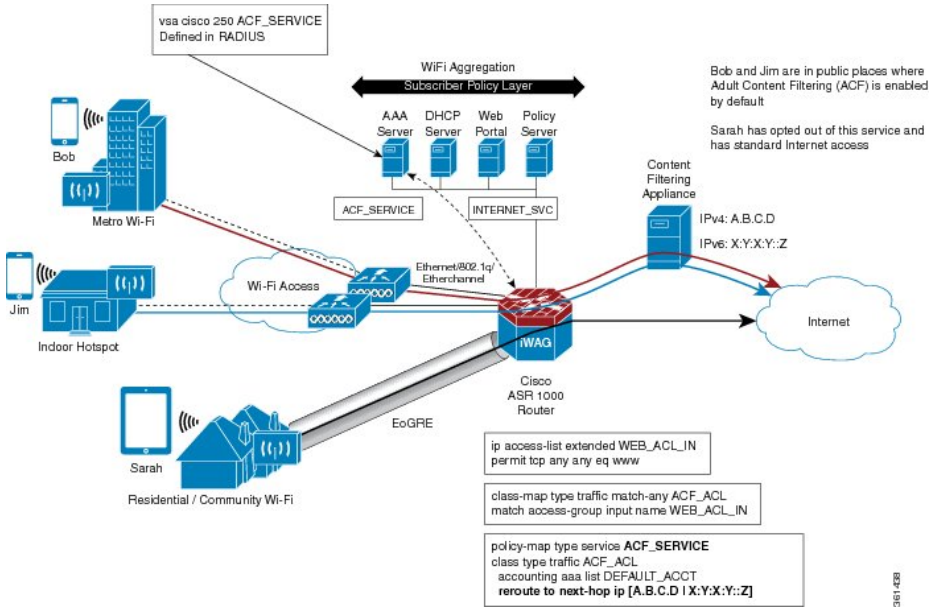
In a typical WiFi hotspot deployment, all subscriber traffic goes through Cisco ISG (Intelligent Service Gateway) after successful authentication. For unauthenticated traffic, L4R feature offers a logic to redirect traffic based on a pre-defined access-list (ACL). This L4R feature acts as a way to redirect some traffic to a web portal or opengarden environment using a translation logic. In order to implement a similar redirection logic after successful authentication without the need for translating the traffic, the flow based redirect has been implemented in ISG to allow traffic to be redirected/rerouted. A typical use case is Adult Content Filtering (ACF) where web traffic needs to be redirected to a Web Filtering Appliance.

You can apply the ACF policy to subscriber traffic in the following ways:

- If the Wi-Fi hotspot provider allows individual subscribers to opt out of the ACF, the ACF policy is not applied on their personal profile. For those subscribers who do not opt out of the ACF, the ACF policy is applied on their personal profile through the RADIUS vendor-specific attribute (VSA) when they log in to their account. For more information about RADIUS VSA attributes, see Activating and Deactivating the Flow-Based Redirect Feature Through Vendor-Specific Attributes .
- If the Wi-Fi hotspot provider enforces ACF on all the subscribers accessing the internet from their site, the ACF policy is configured in the local policy of the Cisco ISG.

The following figure shows a typical scenario where ACF is applied on Wi-Fi hotspots.

Figure 14: Adult Content Filtering on Wi-Fi Hotspots



Flow-Based Redirect for Selective IP Traffic Offload

Mobile IP sessions are provisioned with a traffic class service in the Cisco Intelligent Wireless Access Gateway (iWAG) for routing web traffic to a next hop device, depending on the local policies or the policies that are downloaded from the Cisco IOS authentication, authorization, and accounting (AAA) network security services.

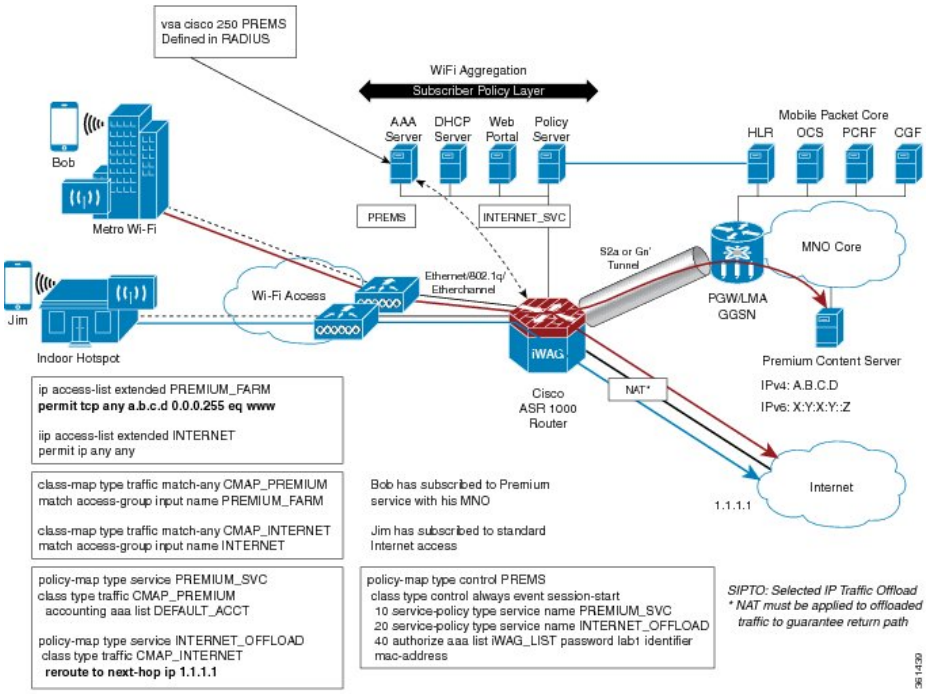
The traffic class service can be configured for routing traffic to the next hop along with the other supported features such as policing and Dynamic Rate Limit (DRL) accounting. You can configure multiple TC services with different next hop addresses with the Flow-Based Redirect feature. However, only 16 traffic class services can be applied to a session.

Network Address Translation (NAT) with Selective IP Traffic Offload (SIPTO) is required only for IPv4 and Dual Stack IPv4 traffic sessions. NAT is enabled at the outgoing interface level so NAT does not need to be IPoE session aware when used with Flow Based Redirect for Selective IP Traffic Offload.

Note In existing deployment, a NAT or Carrier Grade Network Address Translation (CGN) device may exist upstream of the Intelligent Wireless Access Gateway (iWAG) device. In such a scenario, it is possible to keep the architecture in place without enabling NAT on the Cisco ASR 1000 Series Aggregation Services Router acting as iWAG, if and only if, there is a simple way for the return traffic to go from the NAT or CGN device back to the iWAG. This needs to be verified prior to deployment to guarantee return paths.

The following figure shows a typical deployment scenario where internet traffic is offloaded from the access network, and is routed directly through the nearest IP gateway.

Figure 15: Flow-Based Redirect for Selective IP Traffic Offload



Activating and Deactivating the Flow-Based Redirect Feature Through Vendor-Specific Attributes

You can provision or activate a traffic class service with the Flow-Based Redirect feature by adding the following vendor-specific attribute (VSA) in the user profile of the RADIUS server:

```
vsa cisco 250 ACF_SERVICE
```

You can activate a traffic class service with the Flow-Based Redirect feature for an established session through the RADIUS Change of Authorization (CoA) feature, using the following VSAs:

```
vsa cisco 250 S<sessionID>
vsa cisco generic 1 string "subscriber:command=activate-service"
vsa cisco generic 1 string "subscriber:service-name=ACF_SERVICE”
```

You can deactivate a traffic class service with the Flow-Based Redirect feature for an established session through the RADIUS CoA feature, using the following VSAs:

```
vsa cisco 250 S<sessionID>
vsa cisco generic 1 string "subscriber:command=deactivate-service"
vsa cisco generic 1 string "subscriber:service-name=ACF_SERVICE”
```

Configuring Flow-Based Redirect for a Traffic Class Service

The following steps show how to configure the Flow-Based Redirect feature for a traffic class service.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *traffic class*
4. **permit tcp** *source_IP destination_IP* **eq** *port*
5. **class-map type traffic match-any** *traffic class map*
6. **match access-group input name** *traffic class*
7. **policy-map type service** *policy-map name*
8. **class type traffic** *traffic class map*
9. **reroute to next-hop ip** *IP address*
10. **policy-map type control** *policy-map name*
11. **class type control always event account-logon**
12. **20 service-policy type service name** *service-policy name*
13. **class type control always event service-stop**
14. **1 service-policy type service unapply identifier service-name**
15. **class type control always event service-start**
16. **10 service-policy type service identifier service-name**
17. **class type control always event account-logoff**
18. **10 service disconnect delay 5**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip access-list extended** *traffic class* **Example:** `Router (config)# ip access-list extended WEB_ACL_IN`	Defines the traffic class WEB_ACL_IN
Step 4	**permit tcp** *source_IP destination_IP* **eq** *port* **Example:** `Router (config-ext-nacl)# permit tcp any any eq www`	Permits TCP traffic with destination port values that match WWW (port 80).
Step 5	**class-map type traffic match-any** *traffic class map* **Example:** `Router (config)# class-map type traffic match-any ACF_ACL`	Creates the traffic class map ACF_ACL.
Step 6	**match access-group input name** *traffic class* **Example:** `Router (config-traffic-classmap)# match access-group input name WEB_ACL_IN`	Configures the match criteria for the ACF_ACL traffic class map on the basis of the specified host traffic class.
Step 7	**policy-map type service** *policy-map name* **Example:** `Router (config)# policy-map type service ACF_SERVICE`	Creates the ACF_SERVICE policy map, which is used to define an ISG service.
Step 8	**class type traffic** *traffic class map* **Example:** `Router (config-service-policymap)# class type traffic ACF_ACL`	Associates the ACF_ACL traffic class map with the service policy map.
Step 9	**reroute to next-hop ip** *IP address* **Example:** `Router (config-service-policymap-class-traffic)# reroute to next-hop ip 44.0.0.22`	Redirects traffic to the specified IP address.
Step 10	**policy-map type control** *policy-map name* **Example:** `Router (config)# policy-map type control INTERNET_SERVICE_RULE`	Creates the INTERNET_SERVICE_RULE policy map, which is used to define a control policy.
Step 11	**class type control always event account-logon** **Example:**	Specifies a control class for an account-logon event.

	Command or Action	Purpose
	`Router (config-control-policymap)# class type control always event account-logon`	
Step 12	**20 service-policy type service name** *service-policy name* **Example:** `Router (config-control-policymap-class-control)# 20 service-policy type service name ACF_SERVICE`	Applies the ACF_SERVICE policy.
Step 13	**class type control always event service-stop** **Example:** `Router (config-control-policymap)# class type control always event service-stop`	Specifies a control class for a service-stop event.
Step 14	**1 service-policy type service unapply identifier service-name** **Example:** `Router (config-control-policymap-class-control)# 1 service-policy type service unapply identifier service-name`	Specifies the service name that is currently associated with the user.
Step 15	**class type control always event service-start** **Example:** `Router (config-control-policymap)# class type control always event service-start`	Specifies a control class for the service-start event.
Step 16	**10 service-policy type service identifier service-name** **Example:** `Router (config-control-policymap-class-control)# 10 service-policy type service identifier service-name`	Applies the defined service upon a service-start event.
Step 17	**class type control always event account-logoff** **Example:** `Router (config-control-policymap)# class type control always event account-logoff`	Specifies a control class for an account-logoff event.
Step 18	**10 service disconnect delay 5** **Example:** `Router (config-control-policymap-class-control)# 10 service disconnect delay 5`	Disconnects upon an account-logoff event, after a 5 second delay.

Examples

Configuring Flow-Based Redirect for a Traffic Class Service

The following sample output shows how a traffic class service with the Flow-Based Redirect feature is configured to redirect all HTTP traffic to a different next hop device upon logging in to the account:

```
Router# configure terminal
Router (config)# ip access-list extended WEB_ACL_IN
Router (config-ext-nacl)# permit tcp any any eq www
Router (config-ext-nacl)# permit tcp any any eq www
Router (config-ext-nacl)# class-map type traffic match-any ACF_ACL
Router (config-traffic-classmap)# match access-group input name WEB_ACL_IN
Router (config-traffic-classmap)# policy-map type service ACF_SERVICE
Router (config-service-policymap)# class type traffic ACF_ACL
Router (config-service-policymap-class-traffic)# reroute to next-hop ip 44.0.0.22
Router (config-control-policymap-class-control)# policy-map type control INTERNET_SERVICE_RULE
Router (config-control-policymap)# class type control always event account-logon
Router (config-control-policymap-class-control)# 20 service-policy type service name
ACF_SERVICE
Router (config-control-policymap-class-control)# class type control always event service-stop
Router (config-control-policymap-class-control)# 1 service-policy type service unapply
identifier service-name
Router (config-control-policymap)# class type control always event service-start
Router (config-control-policymap-class-control)# 10 service-policy type service identifier
 service-name
Router (config-control-policymap)# class type control always event account-logoff
Router (config-control-policymap-class-control)# 10 service disconnect delay 5
```

Viewing the FBR Policy that is Attached to a Session

To view the FBR policy that is attached to a session at session start, use the **show subscriber session uid** *uid* command:

```
Router# show subscriber session uid 249
Type: IPv4, UID: 249, State: authen, Identity: 33.0.0.4
IPv4 Address: 33.0.0.4
Session Up-time: 00:01:43, Last Changed: 00:01:43
Switch-ID: 16972

Policy information:
  Authentication status: authen
  Active services associated with session:
  name "ACF_SERVICE", applied before account logon
  Rules, actions and conditions executed:
    subscriber rule-map INTERNET_SERVICE_RULE
      condition always event session-start
        80 authorize identifier source-ip-address
    subscriber rule-map default-internal-rule
      condition always event service-start
        1 service-policy type service identifier service-name


  Classifiers:
Class-id    Dir   Packets    Bytes                Pri.  Definition
0           In    499        31936                0    Match Any
1           Out   0          0                    0    Match Any
56          In    499        31936                0    Match ACL WEB_ACL_IN
57          Out   0          0                    0    Match ACL WEB_ACL_OUT
```

```
Template Id : 1

Features:

Absolute Timeout:
Class-id   Timeout Value    Time Remaining       Source
0          3000             00:48:16             Peruser

Forced Flow Routing:
Class-id   FFR Tunnel Details Source
56
Next-hop IP: 44.0.0.2
 ACF_SERVICE

Configuration Sources:
Type  Active Time  AAA Service ID  Name
SVC   00:01:43     -               ACF_SERVICE
USR   00:01:43     -               Peruser
INT   00:01:43     -               GigabitEthernet0/0/4
```

Verifying the Packet Count Status

To verify whether the packet count on the interface that is connected to the next hop device is increasing, use the **show interface** *interface connected to the next hop device* command:

```
Router(config)# show interface GigabitEthernet0/0/5

GigabitEthernet0/0/5 is up, line protocol is up
  Hardware is SPA-8X1GE-V2, address is 0021.d81a.d305 (bia 0021.d81a.d305)
  Description: IXIA_Client_Facing
  Internet address is 44.0.0.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is SX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:05:03, output 00:05:03, output hang never
  Last clearing of "show interface" counters 00:06:48
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 12000 bits/sec, 20 packets/sec
     7 packets input, 690 bytes, 0 no buffer
     Received 2 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     4897 packets output, 382284 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

Viewing Statistics of Dropped Packets

To display the statistics of all the dropped packets on the Embedded Services Processor (ESP), use the **show platform hardware qfp active statistics drop** command.

Note As per FBR behavior, the ISG drops packets if *next hop* is unreachable. The **show platform hardware qfp active statistics drop** command output shows counters for the dropped packets.

```
Router# Show platform hardware qfp active statistics drop
-------------------------------------------------------------------------
Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------
Disabled                                        13                   1166
essipsubfsoldrop                                2327                 216495
UnconfiguredIpv6Fia                             90                   9492
```

Configuring NAT Access Interface for Ingress Traffic

```
interface GigabitEthernet0/0/4
 ip address 36.0.0.1 255.255.255.0
 ip nat inside
 negotiation auto
 ipv6 address FE80::200:5EFF:FE00:5213 link-local
 service-policy type control PREMS
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp
!
```

Configuring NAT Network Interface for Egress Traffic

```
interface GigabitEthernet1/2/4
 description IXIA_port_for_offload
 ip address 44.0.0.1 255.255.255.0
 ip nat outside
 load-interval 30
 negotiation auto
 ipv6 address 44::1/60
!
```

Enabling Carrier Grade NAT

```
ip nat settings mode cgn
no ip nat settings support mapping outside
ip nat pool natpool 55.0.0.3 55.0.255.250 netmask 255.255.0.0
ip nat inside source list 100 pool natpool overload
```

Best Practices for Configuring the NAT on the Cisco ASR 1000 Series Routers

The following are the recommended best practices to configure the NAT on the Cisco ASR 1000 Series Aggregation Services Routers:

- Restriction on the total QFP DRAM usage

At 97 percent DRAM utilization, depletion messages are displayed in the syslog as a warning message to make the operator aware of low QFP DRAM availability. We recommend that you configure QFP DRAM CAC in the system to avoid any unexpected behavior. The Call Admission Control (CAC) functionality ensures that new subscriber sessions cannot be established when QFP DRAM utilization exceeds the configured threshold.

The configuration example below demonstrates configuration of a QFP DRAM threshold set to 95 percent:

platform subscriber cac mem qfp *95*.

- Set the maximum limit for total number of NAT translations:
  - ESP40: **ip nat translation max-entries** *1000000*
  - ESP100: **ip nat translation max-entries** *4000000*
- The **ip nat translation max-entries all-host** command can be used in scenarios where the Cisco ASR 1000 Series Router acting as ISG, performs NAT on all or most of the subscriber traffic. This helps the operator to prevent a single host from occupying the entire translation table, while allowing a reasonable upper limit to each host.
- The maximum number of translations per host can be configured using either of these ways:
  - Configuring the same number of maximum translation entries for all the subscribers using the following command:

    ip nat translation max-entries all-host *maximum number of NAT entries for each host*
  - Configuring the maximum translation entries for a given subscriber using the following command:

    ip nat translation max-entries host *ip-address* [*per-host NAT entry limit*]
- Ensure that you keep the translations timeout low, around 2 minutes for TCP, and 1 minute for UDP translations:
  - **ip nat translation timeout** *120*
  - **ip nat translation tcp-timeout** *120*
  - **ip nat translation udp-timeout** *60*

NAT Overloading and Port Parity

You can preserve the addresses in the global address pool by allowing a device to use one global address for many local addresses. This type of NAT configuration is called overloading.

When an Interface IP is overloaded for the translations and a single IP address is used for all the expected translations, a maximum of 60,000 translations can be achieved with this configuration depending on the traffic ports and the port parity involved. You can use the NAT Pool Overload configuration to achieve maximum translations.

There is a concept of port parity (even/odd) in NAT and NAT64. If a source port is in the port range of 0 to 1023, it is translated between ports 512 to 1023. If a source port range is more than 1023, it takes ports from 1024 onwards.

NAT Interface Overloading with VRF

The NAT Interface Overloading with VRF scenario assumes that the service provider is only interested in performing application-specific NAT, for example, the service provider perform NAT only on the DNS requests from clients and the rest of the traffic will proceed as it is. Therefore, we can use Interface Overloading instead of a pool. With this, we can have a maximum of 60000 translations per interface, which is deemed good for the application-specific NAT. Also, the IP sessions and NAT are in a VRF (named PROVIDER_WIFI_01, in the example below).

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

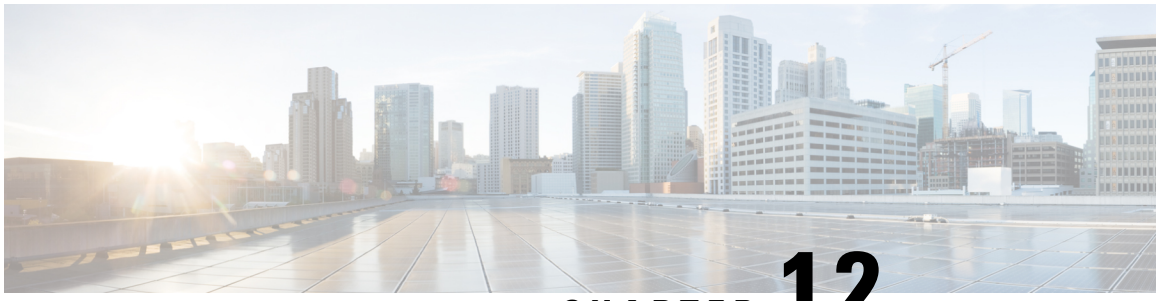
Feature Information for Flow-Based Redirect

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 13: Feature Information for Flow-Based Redirect

Feature Name	Releases	Feature Information
Flow-Based Redirect	Cisco IOS XE Release 3.11	Flow-Based Redirect (FBR) feature enables Adult Content Filtering (ACF) to route matching traffic to a specified next hop device.
Flow-Based Redirect for Selective IP Traffic Offload	Cisco IOS XE Release 3.12	Flow-Based Redirect (FBR) feature enables Selective IP Traffic Offload (SIPTO) to route matching traffic to a specified next hop device.



CHAPTER 12

Web Authentication Support for iWAG-GTP

Service Provider Wi-Fi is gaining popularity as the non-Third Generation Partnership Project (3GPP) high-speed access mechanism for mobile operators. Mobile data offload is straightforward for the Extensible Authentication Protocol-Subscriber Identity Module-based handsets that send their identity for authentication using EAP mechanism. However, non-EAP-capable handsets and users wishing to use Wi-Fi service on laptops are unable to authenticate themselves using their SIM, Mobile Station International Subscriber Directory Number (MSISDN), and International Mobile Station Identity (IMSI), and have to use Wi-Fi as a walk-in subscriber.

With the Web Authentication Support for iWAG-GTP feature, Intelligent Wireless Access Gateway (iWAG) supports non-EAP-SIM-capable users for mobile packet core integration using GPRS Tunneling Protocol (GTP).

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.

Restrictions for Web Authentication Support for iWAG-GTP

- This feature is applicable for IPv4 sessions, but not for IPv6 and dual-stack sessions.
- Only one local Dynamic Host Configuration Protocol (DHCP) pool can be used for simple IP sessions to perform web authentication.

- Only one access point name (APN) (corresponding to one Gateway GPRS Support Node [GGSN] IP address pool) is supported for web-authenticated sessions.

Information About Web Authentication Support for iWAG-GTP

Overview of Web Authentication Support for iWAG-GTP

A simple IP session exists even before web authentication. During the transition from an unauthenticated session to an authenticated session, the session transits from a simple IP session to a mobile IP session. To redirect a user to a portal for web authentication (for the first time) without experiencing a service disruption or disconnection, the simple IP session address and mobile IP session address must remain the same.

The Web Authentication Support for iWAG-GTP feature reuses simple IP session addresses for mobile IP sessions in a web authentication scenario by introducing a default gateway-sharing mechanism in iWAG-GTP. The GTP provides web authentication using the access interface as default gateway besides the existing IP address and subnet configuration (virtual interface). This improves user experience because subscribers do not have service disruption or disconnection after the web authentication, and can continue to use the assigned addresses. Without IP address reuse, mobile subscribers have to dissociate and reattach to get a new mobile IP address. However the Web Authentication Support for iWAG-GTP feature provides a seamless way to migrate a simple IP session to a mobile IP session.

This feature is supported in both GTPv1 and GTPv2.

GTP Default Gateway

An access interface or a loopback interface can be used as the GPRS Tunneling Protocol (GTP) default gateway.

Using Access Interface as GTP Default Gateway

For a user equipment's (UE) initial attach, an unauthenticated simple IP session is created. The UE is assigned an IP address from a local DHCP pool that is identified using the access interface's subnet mask.

After the UE is authenticated through web portal, the simple IP session is transformed to a mobile IP session, and the access interface is used as the mobile IP session's default gateway instead of creating a new virtual interface.

The following example shows how to configure an access interface as the GTP default gateway on iWAG:

```
ip dhcp excluded-address 10.202.255.254
ip dhcp pool test
 network 10.202.0.0 255.255.0.0

interface Ethernet0/3
 ip address 10.202.255.254 255.255.0.0
 service-policy type control GTP_DHCP
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp class-aware
end

gtp
```

```
 n3-request 3
 information-element rat-type wlan
 interface local Ethernet0/0
apn 1
  apn-name apn1.starent.com
  ip address ggsn 10.10.1.2
  default-gw Ethernet0/3
```

Using Loopback Interface as GTP Default Gateway

If multiple access interfaces are used for web-authenticated sessions, these access interfaces have to share the same local DHCP pool. You can configure these access interfaces as unnumbered interfaces and use a loopback interface as their default gateway.

After the UE is authenticated through web portal, the loopback interface is used as the mobile IP session's default gateway instead of creating a new virtual interface.

The following example shows how to configure a loopback interface as the GTP default gateway on iWAG:

```
ip dhcp excluded-address 10.202.255.254
ip dhcp pool test
 network 10.202.0.0 255.255.0.0

interface Ethernet0/2
 ip unnumbered Loopback1
 service-policy type control GTP_DHCP
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp class-aware
end

interface Ethernet0/3
 ip unnumbered Loopback1
 service-policy type control GTP_DHCP
 ip subscriber l2-connected
  initiator unclassified mac-address
  initiator dhcp class-aware
end

interface Loopback1
 ip address 10.202.255.254 255.255.0.0
end

gtp
 n3-request 3
 information-element rat-type wlan
 interface local Ethernet0/0
apn 1
  apn-name apn1.starent.com
  ip address ggsn 10.10.1.2
  default-gw Loopback1
```

Reusing a Locally Allocated IP Address for a Mobile Session

To reuse a simple IP session address for a mobile IP session in a web authentication scenario, the following options are available:

- Using the authentication, authorization, and accounting (AAA) server

For more information on this, see the procedure described in the Web Authentication Support for iWAG-GTP Call Flow, on page 110 section.

- Using mobile client service abstraction (MCSA)

  The web authentication accepts an IPv4 address that is being passed from an unauthenticated subscriber session, and sends it to either the GPRS Gateway Support Node (GGSN) or Packet Gateway (PGW).

  The **allow-static-ip** command specifies whether the static IP address provided by the unauthenticated session is allowed by iWAG-GTP or not. This is applicable only to the IPv4 addresses and not the IPv6 addresses.

Interface Change Considerations

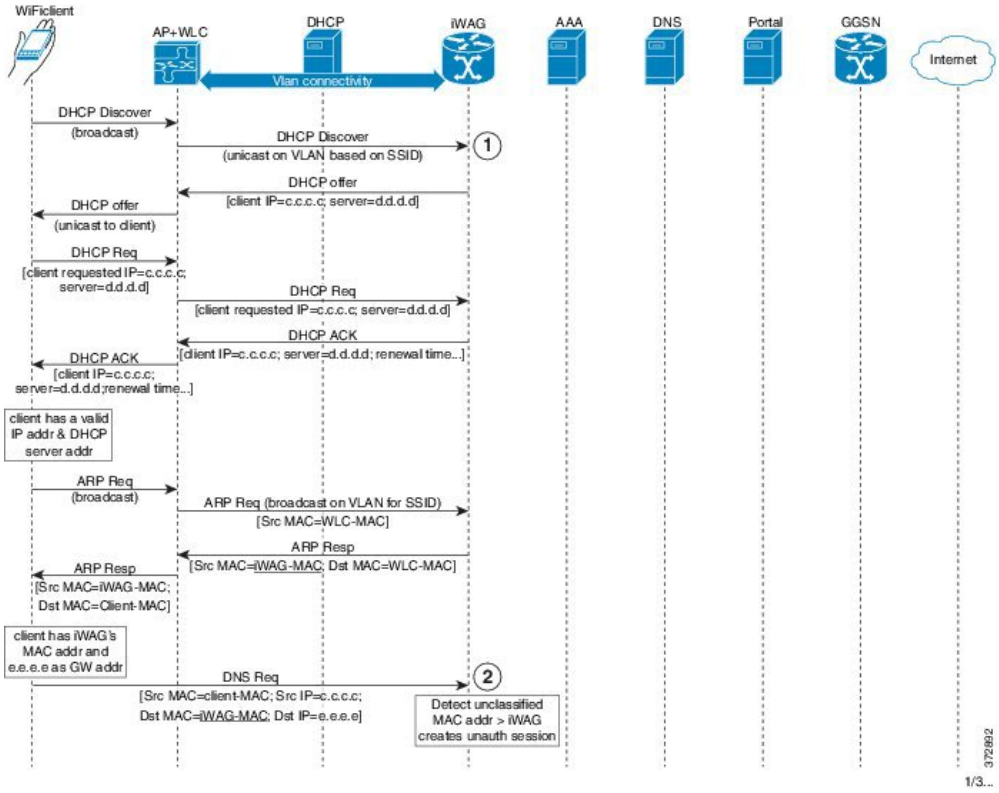
If an interface is configured as default gateway, the following events may occur on the configured interface:

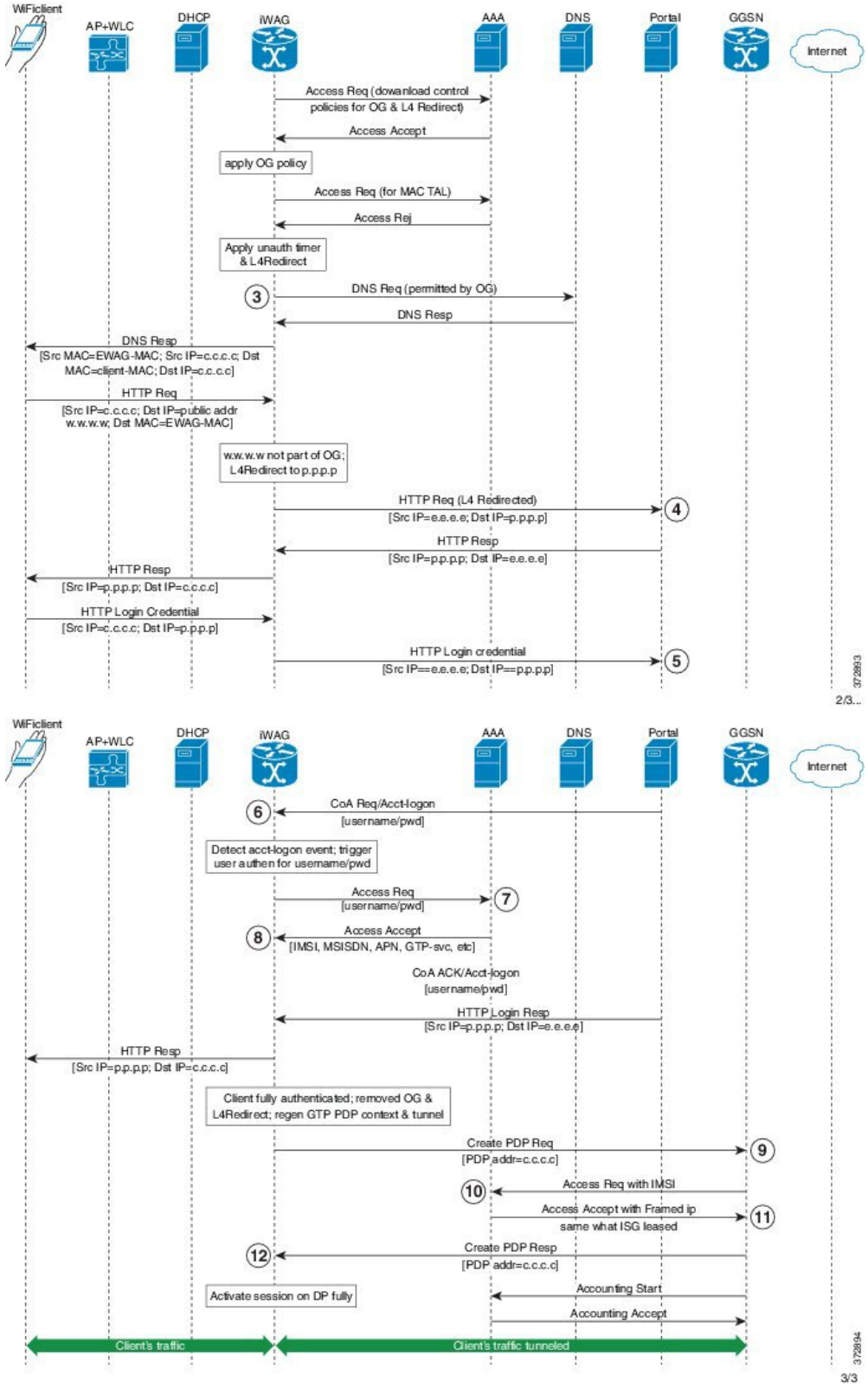
- If an IP address or a network mask on a configured interface is changed, the traffic may still continue, but the sessions may not be torn down by the DHCP clients depending on the idle timeout. New session setup requests may either continue through the default gateway if the subnet of the GTP Packet Data Protocol (PDP) assigned from GGSN or PGW matches the subnet of the default gateway, or may be rejected if the subnet does not match.
- If the configured interface is shut down, the interface is removed from the active default gateway list. The traffic may still continue, but the sessions may not be torn down by the DHCP client depending on the idle timeout. New session setup requests are rejected due to lack of proper default gateway.
- If the configured interface is removed from the system (unconfiguring a subinterface or a loopback interface), the interface is removed from the active default gateway list. The traffic may still continue, but the sessions may not be torn down by the DHCP client depending on the idle timeout. New session setup requests are rejected due to lack of proper default gateway.

Web Authentication Support for iWAG-GTP Call Flow

The following figure and steps describe the call flow pertaining to web authentication for a subscriber using GTP:

Figure 16: Web Authentication Using GTP Call Flow




WiFiclient
AP+WLC
DHCP
iWAG
AAA
DNS
Portal
GGSN
Internet
Access Req (dowanload control policies for OG & L4 Redirect)
Access Accept
apply OG policy
Access Req (for MAC TAL)
Access Rej
Apply unauth timer & L4Redirect
3
DNS Req (permitted by OG)
DNS Resp
DNS Resp
[Src MAC=EWAG-MAC; Src IP=c.c.c.c; Dst MAC=client-MAC; Dst IP=c.c.c.c]
HTTP Req
[Src IP=c.c.c.c; Dst IP=public addr w.w.w.w; Dst MAC=EWAG-MAC]
w.w.w.w not part of OG; L4Redirect to p.p.p.p
HTTP Req (L4 Redirected)
[Src IP=e.e.e.e; Dst IP=p.p.p.p]
4
HTTP Resp
[Src IP=p.p.p.p; Dst IP=e.e.e.e]
HTTP Resp
[Src IP=p.p.p.p; Dst IP=c.c.c.c]
HTTP Login Credential
[Src IP=c.c.c.c; Dst IP=p.p.p.p]
HTTP Login credential
[Src IP==e.e.e.e; Dst IP==p.p.p.p]
5
372893
2/3...
WiFiclient
AP+WLC
DHCP
iWAG
AAA
DNS
Portal
GGSN
Internet
6
CoA Req/Acct-logon
[username/pwd]
Detect acct-logon event; trigger user authen for username/pwd
Access Req
[username/pwd]
7
8
Access Accept
[IMSI, MSISDN, APN, GTP-svc, etc]
CoA ACK/Acct-logon
[username/pwd]
HTTP Login Resp
[Src IP=p.p.p.p; Dst IP=e.e.e.e]
HTTP Resp
[Src IP=p.p.p.p; Dst IP=c.c.c.c]
Client fully authenticated; removed OG & L4Redirect; regen GTP PDP context & tunnel
Create PDP Req
[PDP addr=c.c.c.c]
9
10
Access Req with IMSI
Access Accept with Framed ip same what ISG leased
11
12
Create PDP Resp
[PDP addr=c.c.c.c]
Activate session on DP fully
Accounting Start
Accounting Accept
Client's traffic
Client's traffic tunneled
372894
3/3

1. Subscriber connects to an open wireless local area network (WLAN) and gets an IP address from DHCP or the iWAG.
2. The iWAG creates a session on unclassified MAC.
3. L4 redirection and open garden is applied to the session.
4. Subscriber's HTTP request is redirected to the portal.
5. Mobility subscriber enters MSISDN in the portal, or a voucher in the case of walk-by user.
6. Portal sends change of authorization (CoA) to the iWAG with MSISDN as username.
7. iWAG sends an Access Request to the AAA server with MSISDN.
8. The AAA server receives the 3GPP parameters from the Home Location Register (HLR) and replies with an Access Accept message containing 3GPP information in AV pairs.

   The AAA server creates a tuple with IMSI and IP address for this session.
9. The iWAG sends Create PDP request to the GGSN.
10. The GGSN performs an AAA IMSI authentication with the same AAA server.
11. The AAA server provides the same as IP address in Framed-IP-address to the GGSN.
12. The GGSN provides the IP address provided by the iWAG to the session.

    Thus the simple IP and mobile IP sessions reuse the same IP address, providing a seamless migration.

Configuration Examples for Web Authentication Support for iWAG-GTP

Example: Configuring GTP Default Gateway

The following example shows how to configure the GTP Default Gateway for the iWAG on the Cisco ASR 1000 Series Aggregation Services Routers:

```
Router(config)#gtp
Router(config-gtp)#apn 0001
Router(config-gtp-apn)#apn-name starent.com
Router(config-gtp-apn)#ip address ggsn 98.0.123.16
Router(config-gtp-apn)#default-gw loopback1
Router(config-gtp-apn)#dhcp-lease 3000
Router(config-gtp-apn)#dns-server 192.168.255.253
Router(config-gtp-apn)#end
```

Note To reuse an access interface as GTP default gateway, configure the access interface under a specific GTP APN. If the access interface is an unnumbered interface, use the associated loopback interface.

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

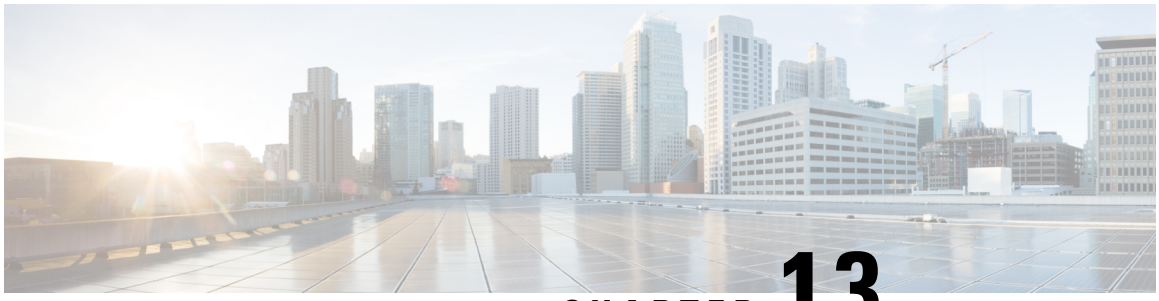
Feature Information for Web Authentication Support for iWAG-GTP

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 14: Feature Information for Web Authentication Support for iWAG-GTP

Feature Name	Releases	Feature Information
Web Authentication Support for iWAG-GTP	Cisco IOS XE Release 3.13S	The Web Authentication Support for iWAG-GTP feature provides a seamless way to migrate a simple IP session to a mobile IP session by reusing the simple IP session addresses for mobile IP sessions. In Cisco IOS XE Release 3.13S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 13

QoS on Ethernet over GRE Tunnels

The QoS on Ethernet over GRE (EoGRE) Tunnels feature enables service providers to configure one common Quality of Service (QoS) policy for all endpoints, where an end-point can be a customer premise equipment (CPE) or a VLAN on a CPE. This feature supports high availability on a route processor.

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.

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.

Restrictions for QoS on Ethernet over GRE Tunnels

- Per-session QoS policies are not supported in conjunction with the tunnel QoS (class-default policer).
- The QoS policy can be applied for an entire tunnel, but not per-virtual local area network (VLAN) and per-customer premises equipment (CPE).
- Upstream QoS for EoGRE tunnel is not supported.
- Hierarchical QoS, bandwidth guarantees, priority, and shaping are not supported.
- Dynamic per-endpoint QoS policies downloaded from the authentication, authorization, and accounting (AAA) server are not supported.

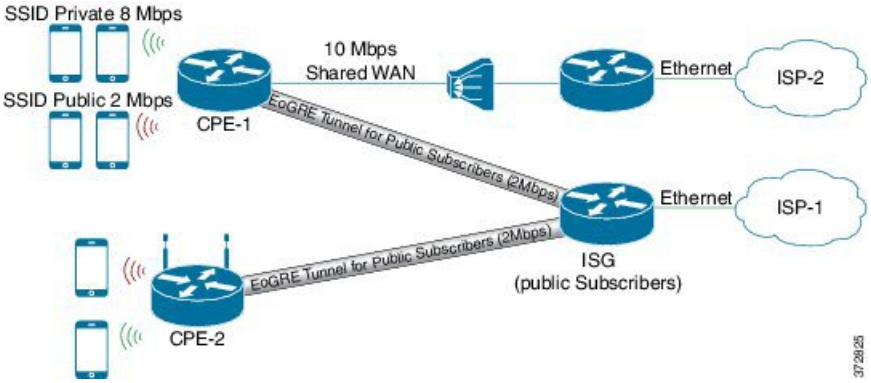
Information About QoS on Ethernet over GRE Tunnels

EoGRE Downstream QoS

The Quality of Service (QoS) on Ethernet over GRE (EoGRE) Tunnels feature enables service providers to apply a unified QoS policy on all endpoints of a tunnel. This controls the bandwidth that public subscribers can download and ensures maximum bandwidth for private customers.

In the deployment scenario given in the figure below, the total available WAN bandwidth at the customer premise equipment (CPE) is 10 Mbps, of which public users are allowed 2 Mbps and the remaining bandwidth is available for private users.

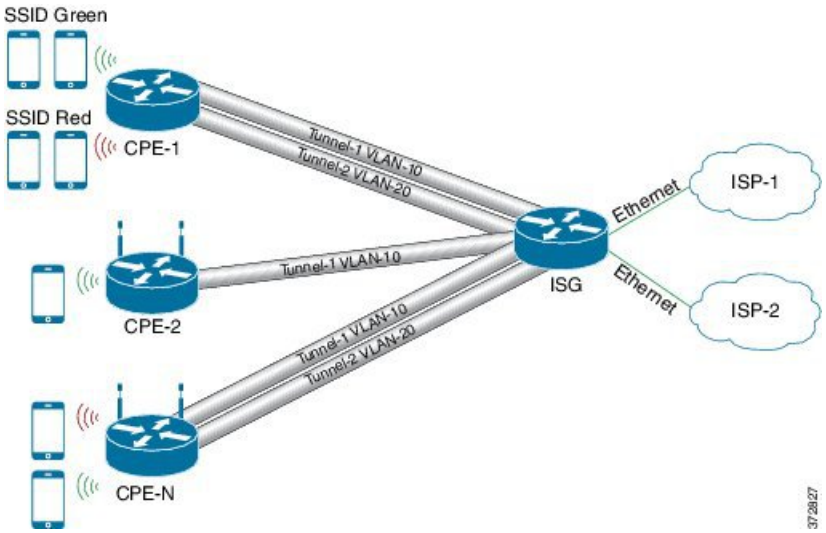
Figure 17: EoGRE Downstream QoS Use Case



Single SSID

Mobile nodes connect to wireless access points (APs). These APs have Service Set Identifiers (SSIDs) provided by the service provider. The SSID of a customer premise equipment (CPE) is the VLAN identifier. Service providers can provide more than one public SSID at a CPE. If a CPE has more than one SSID, then additional mGRE tunnels are configured with a corresponding VLAN tag. The configured multipoint generic routing encapsulation (mGRE) tunnels learn about remote subscribers and the corresponding CPEs independently. This ensures that VLANs, their subnets, default gateways, and VRFs are kept separate and independent of each other, and any QoS policy that is configured on each endpoint of these tunnels also applies to the traffic from the VLAN on the CPE.

Figure 18: Separate Tunnels for Each SSID



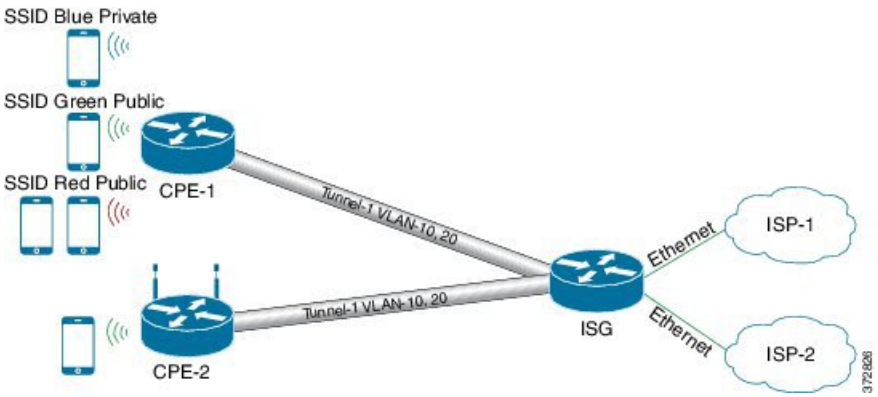
Multiple SSIDs

In a single tunnel for a multiple Service Set Identifiers (SSID), service providers can configure a VLAN range on the multipoint generic routing encapsulation (mGRE) tunnel. When a subscriber traffic is received, the traffic is matched according to the tunnel source and the VLAN range. The Ethernet over GRE (EoGRE) control process also learns the MAC address of subscribers and the VLAN tag of the CPE from which the traffic is originating.

Note You cannot change a VLAN configuration if any subscriber session or MAC address is already learned in the EoGRE control process. To change the VLAN configurations, you must clear all subscriber sessions.

In the figure below, all endpoints learned on Tunnel-1 represent a CPE and a Quality of Service (QoS) policy applied on this tunnel endpoint applies to all traffic going towards the CPE irrespective of the VLAN.

Figure 19: Single Tunnel for Multiple SSIDs



Scaling Considerations for QoS on Ethernet over GRE Tunnels

QoS on EoGRE tunnels support the following scaling features for ESP40, ESP100 and ESP200:

- 64 k EoGREv4 Transport Tunnels, 1 VLAN, 1 Subscriber per Tunnel
- 32 k EoGREv4 Transport Tunnels, 2 VLANs, 2 Subscribers per Tunnel
- 64 k EoGREv4 Transport Tunnels, 1 VLAN, 1 Subscriber per Tunnel, ISG as DHCP relay

How to Configure QoS on Ethernet over GRE Tunnels

Configuring Downstream QoS Policy on Ethernet over GRE Tunnels

Before you begin

Create a Quality of Service (QoS) policy map to attach to the Ethernet over GRE (EoGRE) tunnel.

Note How to create a QoS policy map is not described in the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **interface source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
5. **tunnel vlan** *vlan-id*
6. **ip address** *ip-address mask*
7. **tunnel mode ethernet gre** {**ipv4** | **ipv6**}
8. **tunnel endpoint service-policy output** *policy-map-name*
9. **ip subscriber l2-connected**
10. **initiator unclassified mac-address**
11. **initiator dhcp**
12. **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 tunnel** *tunnel-number* **Example:** `Device(config)# interface tunnel 1`	Specifies a tunnel interface and number and enters interface configuration mode.
Step 4	**interface source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} **Example:** `Device(config-if)# tunnel source loopback 2`	Sets the source address of a tunnel interface.
Step 5	**tunnel vlan** *vlan-id* **Example:** `Device(config-if)# tunnel vlan 10, 20`	Associates a VLAN identifier with the Ethernet over GRE tunnel.
Step 6	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 192.168.4.3 255.255.255.0`	Specifies the IP address and mask of the mobile node.
Step 7	**tunnel mode ethernet gre** {**ipv4** | **ipv6**} **Example:** `Device(config-if)# tunnel mode ethernet gre ipv4`	Sets the encapsulation mode of the tunnel to Ethernet over GRE IPv4 or GRE IPv6.
Step 8	**tunnel endpoint service-policy output** *policy-map-name* **Example:** `Device(config-if)# tunnel endpoint service-policy output tunnel-qos-policy`	Configures the QoS policy for tunnel endpoints.
Step 9	**ip subscriber l2-connected** **Example:** `Device(config-if)# ip subscriber l2-connected`	Enters IP subscriber configuration mode.
Step 10	**initiator unclassified mac-address** **Example:** `Device(config-subscriber)# initiator unclassified mac-address`	Initiates IP sessions from unclassified MAC address.
Step 11	**initiator dhcp** **Example:** `Device(config-subscriber)# initiator dhcp`	Enables IP sessions initiated by DHCP.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config-subscriber)# end`	Exits to global configuration mode.

Verifying QoS on Ethernet over GRE Tunnels

The **show** commands can be entered in any order.

Before you begin

Configure QoS on Ethernet over GRE (EoGRE) tunnel.

SUMMARY STEPS

1. **show interface tunnel** *tunnel-interface*
2. **show tunnel endpoints tunnel** *tunnel-interface*
3. **show tunnel mac-table tunnel** *tunnel-interface*
4. **show policy-map multipoint tunnel** *tunnel-interface*

DETAILED STEPS

Step 1 **show interface tunnel** *tunnel-interface*

This command displays information about the tunnel.

Example:

```
Device# show interface tunnel 1

Tunnel1 is up, line protocol is up
Hardware is Tunnel
Internet address is 11.1.1.1/24
MTU 17846 bytes, BW 100 Kbit/sec, DLY 50000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10.0.0.1
Tunnel MAC address 0000.5e00.5213
Tunnel Vlan-id 1
Tunnel protocol/transport Ethernet-GRE/IP Key 0x1, sequencing disabled Checksumming of packets disabled
Tunnel TTL 255
Tunnel transport MTU 1454 bytes
Tunnel transmit bandwidth 8000 (kbps) Tunnel receive bandwidth 8000 (kbps)
Last input 00:48:08, output never, output hang never
Last clearing of "show interface" counters 00:48:26
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 107
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1867 packets input, 161070 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
43 packets output, 4386 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out ind-uut#
--- 22:03:51 ---
44: 2013-01-30T22:03:51: %SCRIPT-6-INFO: {_haExecCmd: Executing cmd exec with ind-uut-a}


Device# show interface tunnel 2

Tunnel2 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.1.1.1/24
MTU 1434 bytes, BW 100 Kbit/sec, DLY 50000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10::1
Tunnel MAC address 0000.5e00.5213
Tunnel Vlan-id 2
Tunnel protocol/transport Ethernet-GRE/IPv6
Key 0x2, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255
Path MTU Discovery, ager 10 mins, min MTU 1280
Tunnel transport MTU 1434 bytes
Tunnel transmit bandwidth 8000 (kbps) Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:48:28
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 106
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
```

Step 2 **show tunnel endpoints tunnel** *tunnel-interface*

This command displays tunnel interface endpoints and verifies if the tunnel is created correctly.

Example:

```
Device# show tunnel endpoints tunnel

Tunnel0 running in Ethernet-GRE/IP mode

Endpoint transport 10.1.1.1 Refcount 3 Base 0x2A98DD03C0 Create Time 3d02h
   overlay 10.1.1.1 Refcount 2 Parent 0x2A98DD03C0 Create Time 3d02h
 Endpoint transport 3.3.3.3 Refcount 3 Base 0x2A98DD0300 Create Time 3d02h
   overlay 10.1.1.3 Refcount 2 Parent 0x2A98DD0300 Create Time 3d02h
```

Step 3 **show tunnel mac-table tunnel** *tunnel-interface*

This command displays MAC table entries that are associated with a tunnel.

Example:

```
Device# show tunnel mac-table tunnel0
```

```
overlay-address 30.0.0.21, transport-address 192.168.0.50
mac-address 0000.1200.0001, vlan 400 Mac Age 3d06h

overlay-address 60.0.0.8, transport-address 120.0.40.2
mac-address 3010.e495.b058, vlan 10 Mac Age 00:01:00
```

Step 4 **show policy-map multipoint tunnel** *tunnel-interface*

This command displays the policy-map that is associated with a tunnel.

Example:

```
Device> show policy-map multipoint tunnel 1

Interface Tunnel 1 <--> 1.1.1.1
  Service-policy output: test
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
      police:rate 300000 bps, burst 17898 bytes
      conformed 0 packets, 0 bytes;actions:transmit
      exceeded 0 packets, 0 bytes; actions:drop
        conformed 0000 bps, exceeded 0000 bps
```

Configuration Examples for QoS on Ethernet over GRE Tunnels

Example: QoS on Ethernet over GRE Tunnels

Configuring Ethernet over GRE (EoGRE) on the mobile node.

```
! configure the topology
mobile-node1(config-if)# interface GigabitEthernet0/1
mobile-node1(config-if)# ip address 10.21.1.1 255.255.255.0
mobile-node1(config-if)# no shutdown
mobile-node1(config-if)# exit
mobile-node1(config)# ip route 10.0.0.1 255.255.255.255 10.21.1.2

! Configure the interface used as the source of the tunnel
mobile-node1(config)# interface Loopback0
mobile-node1(config-if)# ip address 10.40.0.1 255.255.255.0
mobile-node1(config-if)# ipv6 address 2001:db8:2:40::1/64
mobile-node1(config-if)# no shutdown

! Configure the Ethernet over GRE IPv4 Tunnel
mobile-node1(config-if)# interface Tunnel1
mobile-node1(config-if)# mac-address 0000.0000.0001
mobile-node1(config-if)# ip dhcp client client-id ascii MN1@cisco.com
mobile-node1(config-if)# ip address dhcp
mobile-node1(config-if)# no ip redirects
mobile-node1(config-if)# no ip route-cache
mobile-node1(config-if)# tunnel source Loopback0
mobile-node1(config-if)# tunnel mode ethernet gre ipv4
mobile-node1(config-if)# tunnel key 1
mobile-node1(config-if)# tunnel vlan 10, 20
```

```
mobile-node1(config-if)# no shutdown
mobile-node1(config-if)# exit

Configuring Ethernet over GRE tunnel on the MAG

! Configure the topology
MAG(config)# interface FastEthernet1/1/5
MAG(config-if)# ip address 10.21.1.2 255.255.255.0
MAG(config-if)# ipv6 address 2001:db8:2:21::2/64
MAG(config-if)# no shutdown
MAG(config)# ip route 10.40.0.1 255.255.255.255 10.21.1.1

! Configure the interface used as source of the tunnel
MAG(config-if)# interface Loopback0
MAG(config-if)# ip address 10.0.0.1 255.255.255.0
MAG(config-if)# no shutdown

! configure the policy map
MAG(config)# policy-map tunnel-qos-policy
MAG(config-pmap)# class class-default
MAG(config-pmap-c)# police rate 200000 bps
MAG(config-pmap-c)# exit

! Configure the Ethernet over GRE IPv4 Tunnel
MAG(config)# interface Tunnel1
MAG(config-if)# ip address 10.11.1.1 255.255.255.0
MAG(config-if)# tunnel mode ethernet gre ipv4
MAG(config-if)# tunnel source Loopback0

! Configure a static GRE and VLAN ID for the tunnel
MAG(config-if)# tunnel key 1
MAG(config-if)# tunnel vlan 10, 20

!Associate the QoS policy to the tunnel interface
MAG(config-if)# tunnel endpoint service-policy output tunnel-qos-policy

! Enable ISG on the tunnel
MAG(config-if)# ip subscriber l2-connected
MAG(config-subscriber)# initiator unclassified mac-address
MAG(config-subscriber)# initiator dhcp
MAG(config-subscriber)# exit
```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

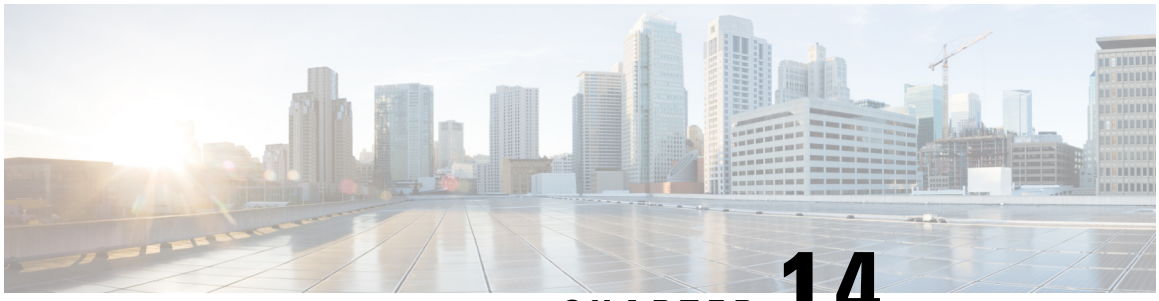
Feature Information for QoS on Ethernet over GRE Tunnels

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 15: Feature Information for QoS on Ethernet over GRE Tunnels

Feature Name	Releases	Feature Information
QoS on Ethernet over GRE Tunnels	Cisco IOS XE 3.13S	The QoS on Ethernet over GRE (EoGRE) Tunnels feature enables service providers to configure a common QoS policy for all endpoints. This feature supports dual high availability for a route processor. The following command was introduced by this feature: **tunnel endpoint service-policy output**.



CHAPTER 14

PMIP MAG SSO

Effective from Cisco IOS XE Release 3.13S, PMIP MAG SSO feature supports iWAG mobility sessions that are tunneled to the Mobile Network Operator (MNO) using Proxy Mobile IPv6 (PMIPv6). The Stateful Switchover (SSO) feature takes advantage of Route Processor (RP) redundancy by establishing one of the RPs as the active processor, while the other RP is designated as the standby processor, and then synchronizing the critical state information between them. When a failover occurs, the standby device seamlessly takes over, starts performing traffic-forwarding services, and maintains a dynamic routing table.

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.

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 PMIP MAG SSO

The PMIP MAG SSO feature supports only the Cisco ASR 1000 Series Aggregation Services Routers intrachassis (RP-to-RP) SSO, but not the interchassis (Cisco ASR1K-to-Cisco ASR1K) SSO. The First Sign Of Life (FSOL) triggers that are supported on SSO include DHCP proxy (where the iWAG acts as the DHCP proxy server) and DHCP proxy plus unclassified MAC.

For more information about ISSU, see the "Overview of ISSU on the Cisco ASR 1000 Series Routers" section of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*.

The process as part of iWAG SSO handling PMIPv6 checkpoints to the standby RP the information that is necessary to create a copy of the session on the standby RP. Such an inactive copy of the session becomes active when the standby RP becomes active.

When an iWAG mobility session with PMIPv6 tunneling is enabled using the SSO/ISSU feature, the Cluster Control Manager on the active RP needs to wait for a few more components, including the Policy, SSS, DHCP-SIP etc, to become ready before checkpoint data collection, and polls these additional components for checkpoint data during data collection. A very similar operation is performed on the standby RP as well. Although such additional CPU consumption is per session, it is not expected to be too heavy since processing in each of these components should include the time spent on a few data structure lookups and memory-copying operations.

Default IWAG configuration enables IWAG SSO. No specific command is required for configuring this feature.

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

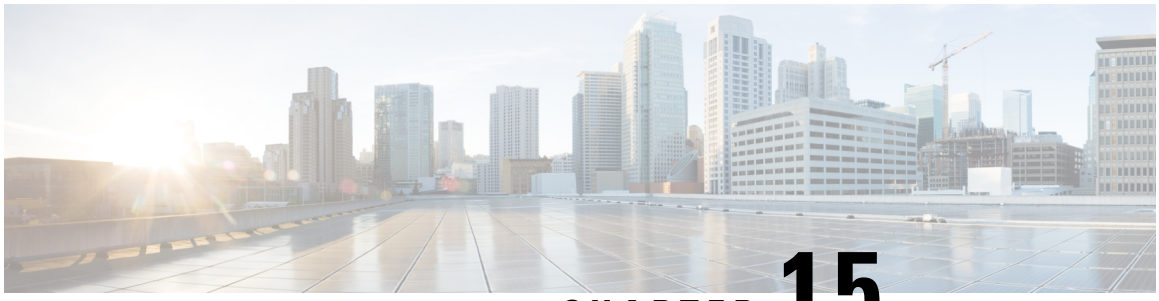
Feature Information for PMIP MAG SSO

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 16: Feature Information for PMIP MAG SSO

Feature Name	Releases	Feature Information
PMIP MAG SSO	Cisco IOS XE Release 3.13S	In Cisco IOS XE Release 3.13S, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 15

iWAG-GTP: S2a Interface Support and High Availability Enhancements

This chapter describes the enhancements for Intelligent Wireless Access Gateway-General Packet Radio Service Tunneling Protocol (iWAG-GTP) to support S2a interface type and related features for the trusted Wireless LAN (WLAN) Access Network deployment.

This chapter also covers iWAG-GTP high availability and In-Service Software Upgrade (ISSU) enhancements to support different GTP-C and GTP-U addresses from Cisco Packet Data Network Gateway (PGW) and Gateway GPRS Support Node (GGSN).

This chapter contains the following topics:

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 S2a Interface Support for GTPv2

iWAG-GTP supports the S2a interface for trusted networks. Earlier, the implementation of GPRS Tunneling Protocol Version 2 (GTPv2) on iWAG-GTP supported only the S5 interface and S8 interface that connect a

serving gateway (SGW) and a packet data network gateway (PGW). Effective from Cisco IOS XE Release 3.14, by default, GTPv2 supports the S2a interface on the iWAG side for trusted WLAN Access Network deployment, according to the specifications provided in 3GPP TS 29.274 V11.5.0.

In the new S2a interface, GTPv2 supports some new information elements like Additional Protocol Configuration Options (APCO) for Domain Name System (DNS) provisioning, and IPv4 Configuration Parameters (IP4CP) for dynamic default gateway provisioning.

The interface that connects the iWAG to PGW is configurable for backwards compatibility, and S2a interface is used by default.

ISSU and High Availability Support for GTPv2

Because GTPv2 supports both S5/S8 interface and S2a interface, the interface type should be stored on a per-PDP basis, so that the same interface type is used when deleting the PDP.

In a high availability (HA) scenario, the interface type should be checkpointed to the standby RP so that after switchover, a PDP on the newly active RP has the interface type information.

Table 17: ISSU and High Availability Support for GTPv2

	S5/S8	**S2a**
ISSU Upgrade	Supported	ISSU upgrade is not applicable for S2a interface. In releases prior to Cisco IOS XE 3.14, S2a interface type was not supported.
ISSU Downgrade	Supported	Not supported. After downgrade, only the S5/S8 interface type is supported, it may not be possible to delete sessions.
SSO Checkpoint	Supported	Supported from Cisco IOS XE Release 3.14 onwards.

Example: Configuring the S2a Interface for GTPv2

The following example shows how to configure the S2a interface for GTPv2:

```
Router(config)#gtp
Router(config-gtp)#apn 1
Router(config-gtp-apn)#gtpv2 interface-type ?
  s2a   Interface between TWAG and PGW (default value for backwards compatibility)
  s5s8  Interface between SGW and PGW
```

GTP Control and GTP User Tunnel Address Separation for GTPv1 and GTPv2

In Cisco IOS XE Release 3.11 and earlier, iWAG-GTP did not support separate GTP-C and GTP-U paths to GGSN and PGW.

Effective from Cisco IOS XE Release 3.12, iWAG-GTP partially supports GTP-C and GTP-U address separation. The separation works only on non-high availability boxes because there is no checkpointing of the GGSN and PGW data path (GTP-C) address to standby RPs.

Effective from Cisco IOS XE Release 3.14, iWAG-GTP supports different GTP-C and GTP-U addresses in an HA setup for both GTPv1 and GTPv2.

Note GTP path version is not checkpointed to standby RPs. Therefore, GTPv1 and GTPv2 sessions are not supported on the same path.

Additional PCO Support on S2a Interface for DNS Provisioning

Effective from Cisco IOS XE Release 3.14, GTPv2 supports a new information element type called additional PCO to support DNS provisioning over the S2a interface.

Additional PCO applies only to transparent single-connection mode. You can use PCO or additional PCO options for DNS provisioning, but the default option is additional PCO.

Example: Configuring Additional PCO for GTPv2

The following example shows how to configure additional PCO for GTPv2:

```
Router(config)#gtp
Router(config-gtp)#apn 1
Router(config-gtp-apn)#gtpv2 pco-type ?
  apco  Using APCO for DNS provisioning (default value for backwards compatibility)
  pco   Using PCO for DNS provisioning
```

IP4CP Support on S2a Interface for Dynamic Provisioning of Default Gateway

The S2a interface supports IPv4 Configuration Parameters (IP4CP) information element type. IP4CP information element enables the PGW to dynamically provision the default gateways instead of tedious local configuration on the iWAG. IP4CP is applicable only to transparent single-connection mode.

In order to be backward compatible, local configuration of default gateways is supported.

- If the default gateway address and subnet prefix length provisioned from PGW are the same as for the locally configured default gateway, the default gateway is created as a static default gateway.

- If local configuration does not exist, the dynamically provisioned default gateway is used.
- If there is no IP4CP to provision the dynamic default gateway and there is no local configuration, session creation fails due to the absence of a default gateway.

APN-AMBR Support for GTPv2

APN aggregate maximum bit rate (AMBR) is the maximum allowed total nonguaranteed bit rate (GBR) throughput to a specific APN. It is specified interdependently for uplink and downlink. The APN-AMBR IE type is used to define the per-APN uplink and downlink aggregate maximum bit rate for a specific UE.

Effective from Cisco IOS XE Release 3.14, GTPv2 supports the APN-AMBR IE type for uplink and downlink.

Example: Configuring APN-AMBR Uplink and Downlink for GTPv2

The following example shows how to configure APN-AMBR uplink and downlink for GTPv2:

```
Router(config)#gtp
Router(config-gtp)#apn 1
Router(config-gtp-apn)#gtpv2 apn-ambr ?
  uplink  Configure uplink ambr
Router(config-gtp-apn)#gtpv2 apn-ambr uplink ?
  <0-2147483647>  Uplink Aggregate Maximum Bit Rate (kbps)
Router(config-gtp-apn)#gtpv2 apn-ambr uplink 128 ?
  downlink  Configure downlink ambr
Router(config-gtp-apn)#gtpv2 apn-ambr uplink 128 downlink ?
  <0-2147483647>  Downlink Aggregate Maximum Bit Rate (kbps)
```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

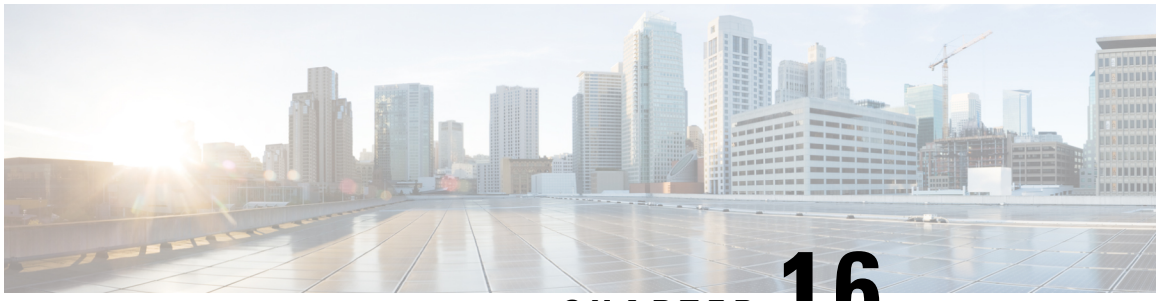
Feature Information for iWAG-GTP: S2a Interface Support and High-Availability Enhancements

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 18: Feature Information for iWAG-GTP: S2a Interface Support and High-Availability Enhancements

Feature Name	Releases	Feature Information
iWAG-GTP: S2a Interface Support and High-Availability Enhancements	Cisco IOS XE Release 3.14	In Cisco IOS XE Release 3.14, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 16

DHCP Option 82 Remote ID Format

Remote identifier is the sub-option 2 of DHCP Option 82 field. Service Providers use remote identifier for troubleshooting, authentication, and accounting.

The DHCP Option 82 Remote ID Format feature adds support for the interpretation of remote-IDs that are inserted by customer premises equipment (CPE).

This chapter contains the following topics:

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.

Restrictions for DHCP Option 82 Remote ID Format

The **subscriber session set cuid remote-id** command cannot be used simultaneously with either the **1 authorize identifier nas-port include-cui** command or the **1 authenticate aaa list AAA_AUTH include-cui** command because both the remote ID and Chargeable User Identity (CUID) use the same Cisco AV pair.

If the CUID has to be retrieved from AAA server and used, then configure the include-cui keyword in the **1 authorize identifier nas-port include-cui** command or the **1 authenticate aaa list AAA_AUTH include-cui** command.

If an unformatted remote-id needs to be sent in CUID, then use the **subscriber session set cuid remote-id** command.

The following example shows how to configure the CUID attribute.

```
policy-map type control TAL
 class type control always event session-start
  1 authorize identifier nas-port include-cui
!
 class type control always event account-logon
  1 authenticate aaa list AAA_AUTH include-cui
 !
```

Information About DHCP Option 82 Remote ID Format

The remote ID is passed to AAA server through RADIUS Access Request and Accounting messages, as a printable ASCII string in Cisco remote-id-tag vendor specific attribute (VSA). For example, ‰"remote-id-tag=XYZ" where XYZ is the value received in DHCP option 82 remote-id field. If the character is non-printable ASCII such as control, NULL, and non-ASCII, then the whole string is converted to hexadecimal, and each hexadecimal is sent as printable character (0-9 and A-F) in the Cisco remote-id-tag VSA.

With the introduction of DHCP Option 82 Remote ID Format feature, the remote ID can be an octet string with any of the following formats:

- Printable ASCII characters
- Non-printable ASCII characters
- Non-ASCII characters

The remote ID is transparently passed to AAA server without any modification or conversion in Chargeable User Identifier (CUID) attribute as specified in GSMA specification IR.61.

Enabling DHCP Option 82 Remote ID Format

Perform this task to enable the DHCP Option 82 Remote ID Format feature.

SUMMARY STEPS

1. enable
2. configure terminal
3. subscriber session set cuid remote-id
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables privileged EXEC mode. Enter password when prompted.
Step 2	configure terminal	Enters global configuration mode.

	Command or Action	Purpose
	Example: `Router# configure terminal`	
Step 3	subscriber session set cuid remote-id **Example:** `Router(config)# subscriber session set cuid remote-id`	Enables the DHCP Option 82 Remote ID Format feature. This command sets the CUID attribute in the RADIUS Access Request and Accounting Request messages with the unmodified value of the remote ID, which is received in the DHCP request. **Note** The **no** form of this command disables the DHCP Option 82 Remote ID Format feature.
Step 4	end **Example:** `Router(config)# end`	Returns the device to privileged EXEC mode.

Example

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

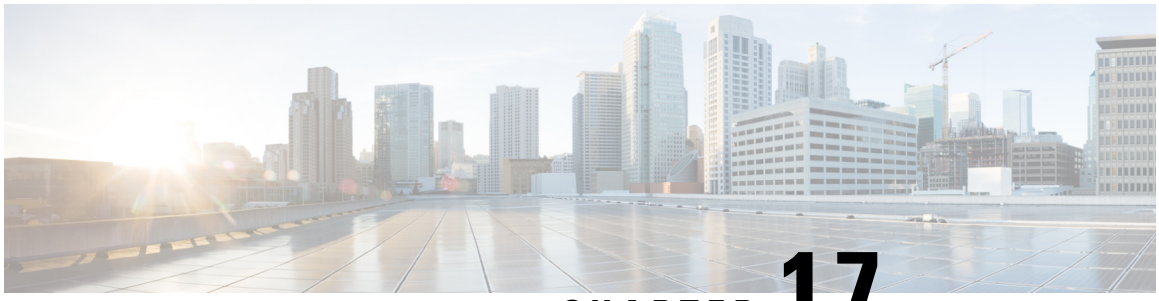
Feature Information for DHCP Option 82 Remote ID Format

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 19: Feature Information for DHCP Option 82 Remote ID Format

Feature Name	Releases	Feature Information
DHCP Option 82 Remote ID Format	Cisco IOS XE Release 3.15	In Cisco IOS XE Release 3.15, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 17

VLAN ID Based Policy Control

The VLAN ID based policy control feature is used to segregate subscribers based on VLAN IDs. Service Set Identifier (SSID) is mapped to virtual local area network (VLAN), and hence VLAN-based segregation allows Intelligent Services Gateway(ISG) and Intelligent Wireless Access Gateway (iWAG) to detect subscribers connecting to open and secure SSID efficiently. In case of sessions where a NAS port ID is not available for segregation of the subscribers, (e.g. - Walk-By users), the VLAN ID can be used to segregate subscribers. This feature is specifically designed for Ethernet over Generic Routing Encapsulation (EoGRE) access where multiple VLANs get terminated on the same Tunnel Interface.

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.

Restrictions for VLAN ID Based Policy Control

The VLAN ID Based Policy Control feature is applicable only to session-start and session-restart events in the control policy.

Information About VLAN ID Based Policy Control

With VLAN-based control policies, subscribers connecting through specific SSIDs can be identified with any packet (DHCP, ARP, Data Packet) based on VLANs, and respective policies or features can be applied during session start and restart. Multiple VLANs can be mapped to the same SSID with specific IP pools and subnets. IP address is allocated to WiFi subscriber device connecting through specific SSID/VLAN from respective subnet.

Multipoint Generic Routing Encapsulation (mGRE) Tunnels can map to multiple VLANs and all the VLAN may be terminated in the single EoGRE Tunnel. As a result, subscribers connecting to VLAN1 and VLAN2 will reach iWAG on the same access interface. It is necessary to identify such subscribers and apply a different control policy based on the VLAN IDs.

Configuring VLAN ID Based Policy Control

Perform this task to configure VLAN ID Based Policy Control feature.

SUMMARY STEPS

1. enable
2. configure terminal
3. match vlan *vlan_id*
4. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password when prompted.
Step 2	configure terminal **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	match vlan *vlan_id* **Example:** `Router(config)# match vlan 200`	Segregates subscribers based on VLAN IDs. When the VLAN ID-based control policy is applied under condition class map, different control policies are applied for different subscribers. **Note** The **no** form of this command unconfigures the VLAN ID based control policy feature.
Step 4	end **Example:** `Router(config)# end`	Returns the device to privileged EXEC mode.

Example

Configuration Examples for VLAN ID Based Policy Control

Example: Defining a Default Control Policy

```
policy-map type control EOGRE_WALKBY_RULE
 class type control SECURE_SSID_VLAN event session-start
  10 default-exit
 !
 class type control always event session-start
  .......
 !
 class type control always event timed-policy-expiry
  1 service disconnect
 !
!
```

Example: Defining a Regular Control Policy

```
policy-map type control EOGRE_POLICY_RULE
 class type control IP_UNAUTH_COND event timed-policy-
expiry
  10 service disconnect
 !
class type control SECURE_SSID_VLAN event session-start
  ......
 !
 class type control SECURE_SSID_VLAN event session-restart
...... !

 class type control always event session-start
  ....
 !
 class type control always event session-restart
...... !
```

Example: Defining a Condition Map

```
class-map type control match-any SECURE_SSID_VLAN
 match vlan 200
 match vlan 201
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*

Related Topic	Document Title
iWAG commands	Cisco IOS Intelligent Wireless Access Gateway Command Reference

MIBs

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

Technical Assistance

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

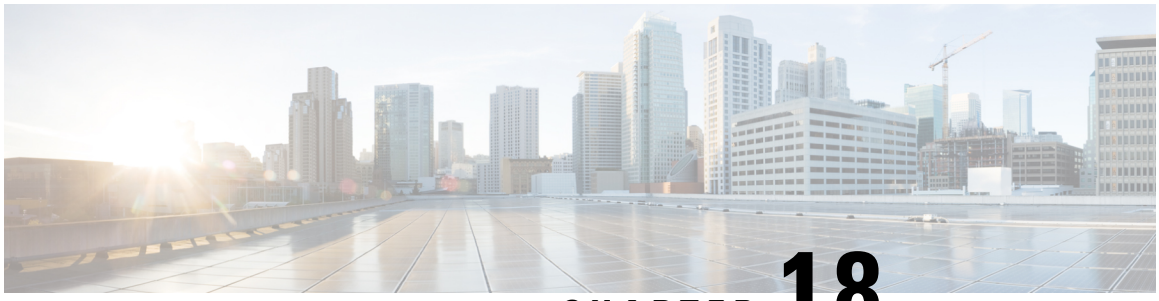
Feature Information for VLAN ID Based Policy Control

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 20: Feature Information for VLAN ID Based Policy Control

Feature Name	Releases	Feature Information
VLAN ID Based Policy Control	Cisco IOS XE Release 3.15	In Cisco IOS XE Release 3.15, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 18

EoGRE iWAG Subscriber Roaming

When a Wi-Fi subscriber device roams or reconnects with the same or a different SSID, it may send a DHCP Discover, a DHCP Request (Init-Reboot, unicast/broadcast renew), an Address Resolution Protocol (ARP) and Data Packet messages. Some devices, for example, Apple/iOS, sends a DHCP Release message followed by a DHCP Discover message when they reconnect.

This chapter covers different scenarios in which a Wi-Fi subscriber can roam and reconnect.

Finding Feature Information

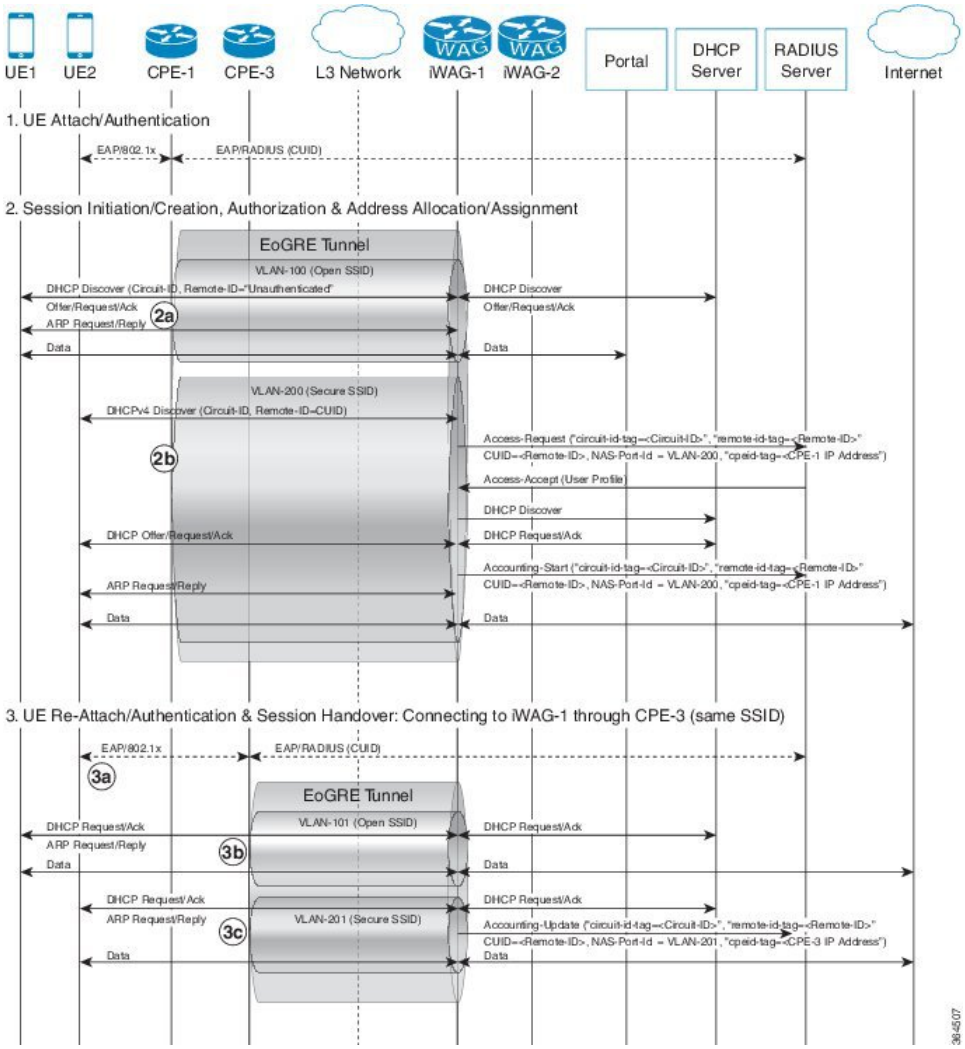
Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the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

EoGRE Intra-iWAG Roaming and Handover With Same SSID Call Flow

The following figure and steps describe the call flow pertaining to a EoGRE intra-iWAG roaming and handover with the same SSID.

Figure 20: EoGRE Intra-iWAG Roaming and Handover With Same SSID Call Flow



1. Extensible Authentication Protocol (EAP) authentication for the subscriber connecting through Secure SSID.
2. DHCP session is established when a subscriber device connects to the network through an open or secure SSID.

   2a. Session establishment through Open SSID

   2b. Session establishment through Secure SSID
3. When the subscriber device roams across CPEs connected to the same iWAG and SSID, the subscriber continues with the existing session.

   3a. EAP Authentication for the subscriber connecting through Secure SSID.

   3b. DHCP Request on Open SSID is honored and DHCP ACK is sent, and in case of ARP, ARP reply is sent. Session continues with new CPE (to which the client roamed) and Accounting-Update is sent to AAA with latest circuit and remote IDs (received in DHCP Request), CPE ID, and NAS Port/VLAN.

3c. DHCP Request on Secure SSID is honored and DHCP ACK is sent, and in case of ARP, ARP reply is sent. Session continues with new CPE (to which the client roamed) and Accounting-Update is sent to AAA with latest circuit and remote IDs (received in DHCP Request), CPE ID, and NAS Port/VLAN.

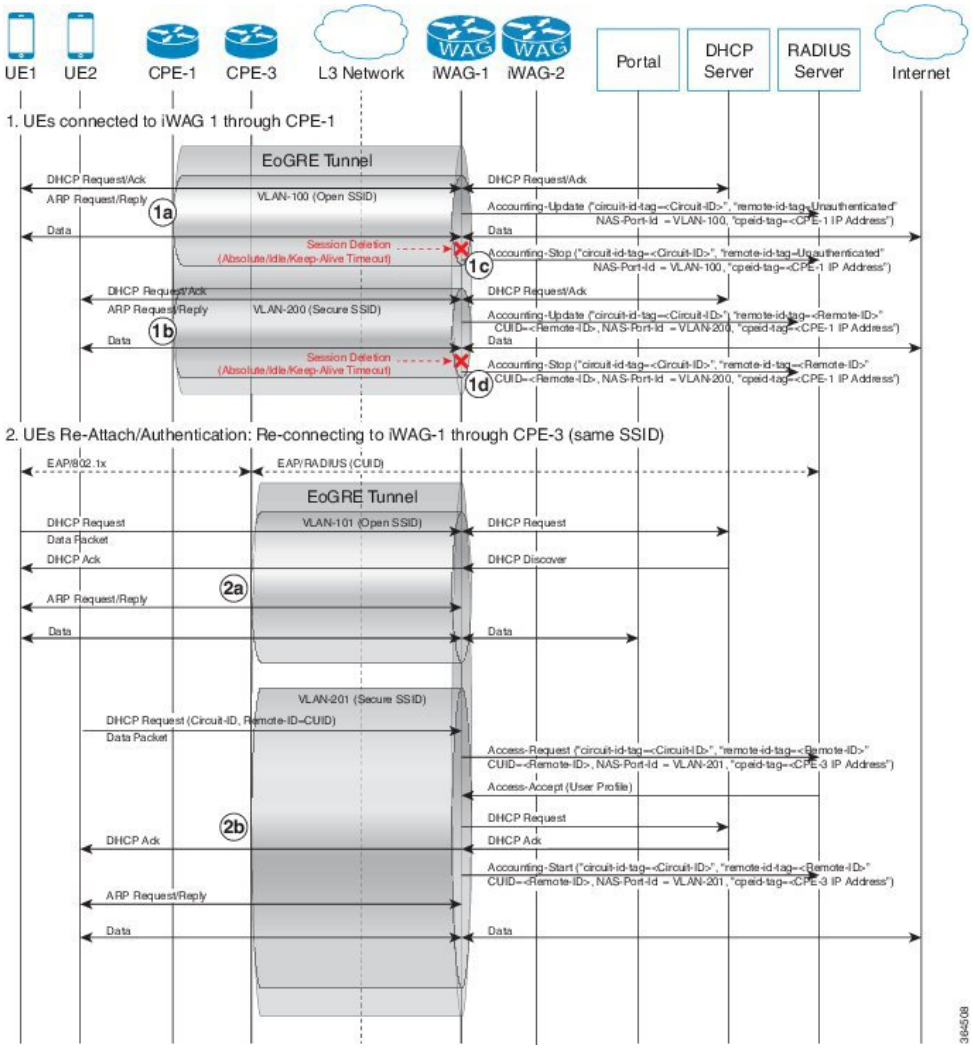
Note

- In case of DHCP Discover, existing session is cleared and Accounting-Stop message is sent with latest circuit and remote IDs (received in DHCP Discover), CPE ID, and NAS Port/VLAN. For a subsequent DHCP Discover, a new session is established with respective policies or features (including L4R in case of open SSID) and IP address allocated from respective subnet.
- In case of DHCP Release followed by DHCP Discover, existing session is cleared for DHCP Release and Accounting-Stop message is sent with latest circuit and remote IDs (received in DHCP Discover), CPE ID, and NAS Port/VLAN. For a subsequent DHCP Discover, a new session is established with respective policies or features (including L4R in case of open SSID) and IP address allocated from respective subnet. If the DHCP Discover is received while the session is cleared, it may be discarded but the session is established with subsequent DHCP Discover.
- Data packet-triggered roaming is not supported; so, the existing session is not updated. Up Link data packets may still be forwarded but Down Link packets are sent to old CPE.

EoGRE Intra-iWAG Roaming and Restart With Same SSID Call Flow

The following figure and steps describe the call flow pertaining to a EoGRE intra-iWAG roaming and restart with the same SSID.

Figure 21: EoGRE Intra-iWAG Roaming and Restart With Same SSID Call Flow



1. DHCP session is established when a subscriber device connects to the network through an open or secure SSID.

   1a. Session establishment through Open SSID

   1b. Session establishment through Secure SSID

   1c. Subscriber session gets removed due to keep-alive timeout or session timeout.

2. When subscriber device roams across CPEs connected to the same iWAG and SSID, the subscriber may choose to send the DHCP packet or Data packet as the lease remains valid.

   2a. In case of DHCP Request on Open SSID, subscriber session is re-established with the same IPv4 address that the device is using, and respective policies or features (including L4R in case of open SSID), and the subscriber continues with the same session. Accounting-Start is sent with latest circuit and remote IDs (received in DHCP Request), CPE ID, and NAS Port/VLAN.

   2b. In case of DHCP Request on Secure SSID, subscriber session is re-established with the same IPv4 address that the device is using, and respective policies or features, and the subscriber continues with the

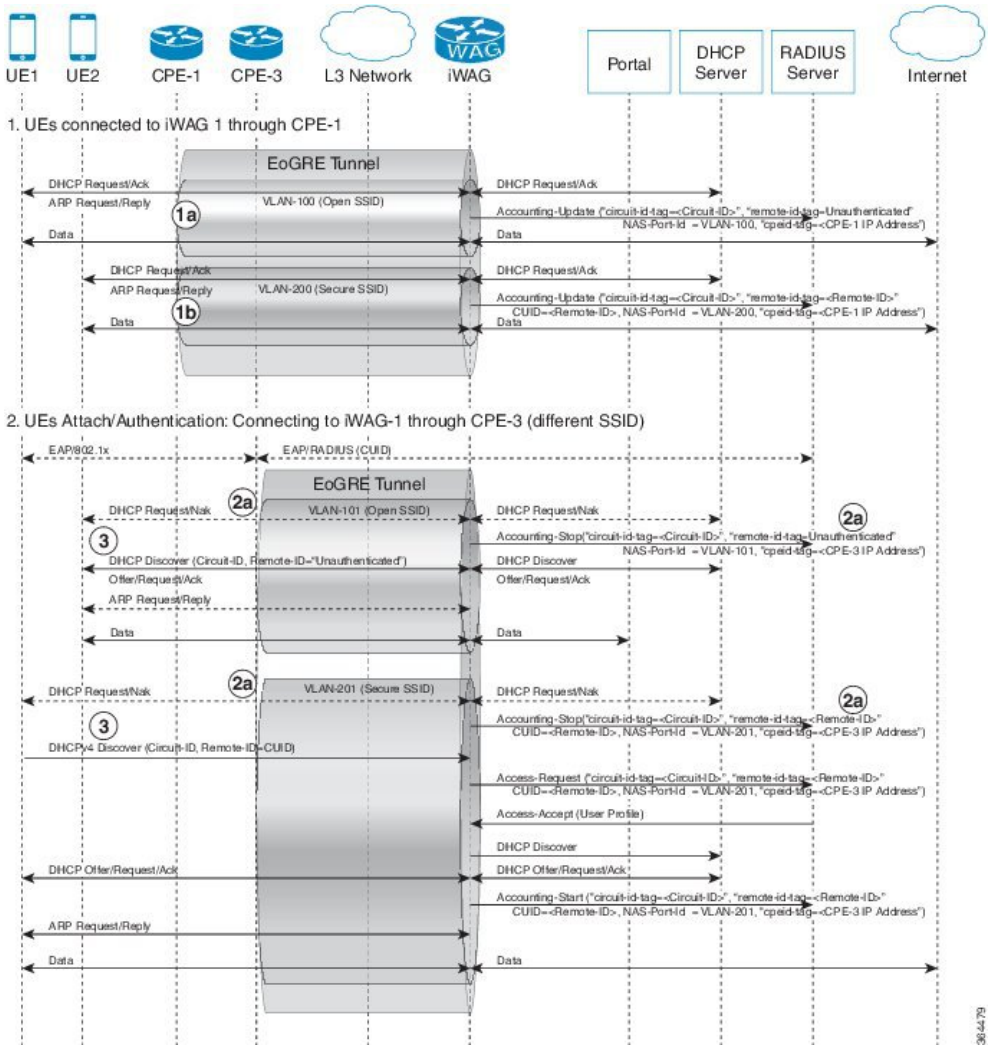
same session. Accounting-Start is sent with latest circuit and remote IDs (received in DHCP Request), CPE ID, and NAS Port/VLAN.

Note ARP-triggered session is not supported; so, the session initiation or restart on ARP packet is not supported.

EoGRE Intra-iWAG Roaming and Reconnect With Different SSIDs Call Flow

The following figure and steps describe the call flow pertaining to EoGRE intra-iWAG roaming and reconnect with different SSIDs.

Figure 22: EoGRE Intra-iWAG Roaming and Reconnect With Different SSIDs Call Flow



1. An IPoE session is established when a subscriber device connects to the network through an open or secure SSID.

   1a. Session establishment using Open SSID

   1b. Session establishment using Secure SSID

2. When subscriber device reconnects to different SSID, the following happens:

   2a. DHCP Request on different SSID

   - Existing session is cleared and Accounting-Stop message is sent with latest circuit and remote IDs (received in DHCP packet), CPE ID, and NAS Port ID or VLAN ID.
   - In case of DHCP Request (Init-Reboot), requested IP address is checked with respective subnet of VLAN/SSID
     - If the requested IP address matches with the respective subnet, DHCP ACK is sent and new session is established. Accounting-Start is sent with latest circuit and remote IDs (received in DHCP Request), CPE ID, and NAS Port ID or VLAN ID.
     - If the requested IP address does not match with the respective subnet, DHCP NAK is sent.

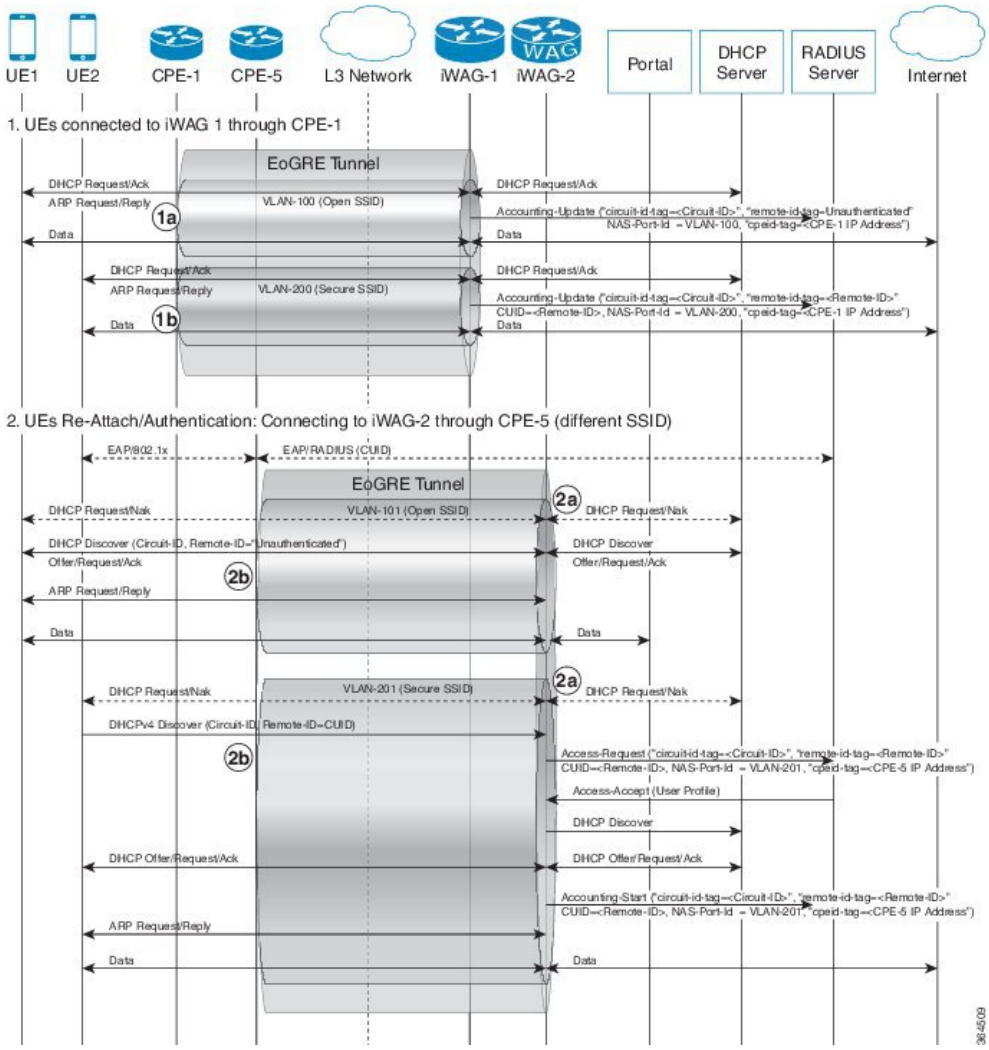
3. For subsequent DHCP Discover, new session is established with respective policies/features (including L4R in case of open SSID) and an IP address is allocated from respective subnet. Accounting-Start is sent with latest circuit and remote IDs (received in DHCP packet), CPE ID, and NAS Port ID or VLAN ID.

Note: If DHCP Discover is received while the session is cleared, it may be discarded.

EoGRE Inter-iWAG Roaming and Reconnect Call Flow

The following figure and steps describe the call flow pertaining to a EoGRE inter-iWAG roaming and reconnect.

Figure 23: EoGRE Inter-iWAG Roaming and Reconnect Call Flow



1. DHCP session is established when a subscriber device connects to the network through an open or secure SSID.

   1a. Session establishment through Open SSID

   1b. Session establishment through Secure SSID

2. When subscriber device roams across CPEs connected to different iWAGs and the same SSID, the subscriber may choose to send DHCP renew packet or Init-reboot packet as the lease remains valid.

   2a. DHCP packets are NAK'ed by DHCP server resulting in the following:

   - Existing session is cleared and Accounting-Stop is sent with latest circuit and remote IDs (received in DHCP packet), CPE ID and NAS Port/VLAN.
   - If case of DHCP Request (Init-Reboot), the requested IP address is checked with the respective subnet of VLAN/SSID.

- If the requested IP address matches with the respective subnet, DHCP Acknowledgement is sent and a new session is established. Accounting-Start is sent with latest circuit and remote IDs (received in DHCP Request), CPE ID and NAS Port/VLAN.
- If the requested IP address does not match with the respective subnet, DHCP NAK is sent.

2b. For subsequent DHCP Discover, a new session is established with respective policies or features (including L4R in case of open SSID) and an IP address allocated from respective subnet. Accounting-Start is sent with latest circuit and remote IDs (received in DHCP Request), CPE ID and NAS Port/VLAN.

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

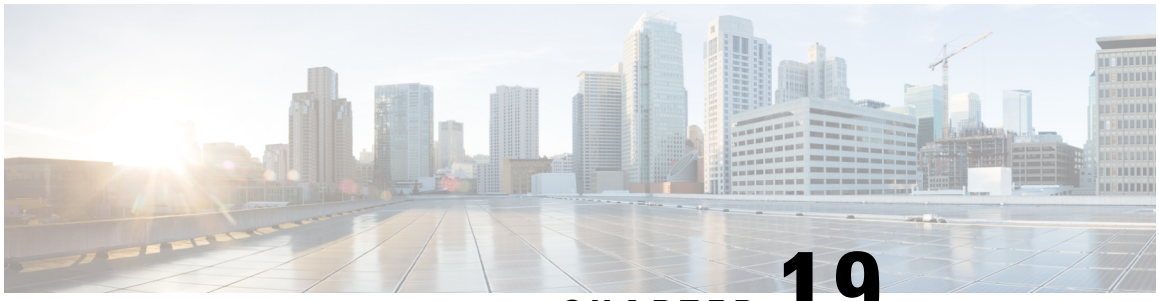
Feature Information for EoGRE iWAG Subscriber Roaming

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 21: Feature Information for EoGRE iWAG Subscriber Roaming

Feature Name	Releases	Feature Information
EoGRE iWAG Subscriber Roaming	Cisco IOS XE Release 3.15	In Cisco IOS XE Release 3.15, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.



CHAPTER 19

EoGRE: Inter-chassis HA

The EoGRE: Inter-chassis HA feature converts the existing IP session to Dynamic Host Configuration Protocol (DHCP) session upon receiving DHCP control packets requested by the subscriber.

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.

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 EoGRE: Inter-Chassis HA

Overview of EoGRE: Inter-Chassis HA

The support for interchassis stateless High Availability (HA) results in an existing DHCP session to appear as unclassified IP session. The subscriber is unaware about the reboot of iWAG on the device and continues to send data packets thereby creating an unclassified IP session. After half lease time, the subscriber may send a unicast renew which removes the existing session and creates a new DHCP session. Therefore it is mandatory to keep the existing session and continue the service to the subscriber unless the subscriber reappears on different service set identifier (SSID) or reboot and send discover packet.

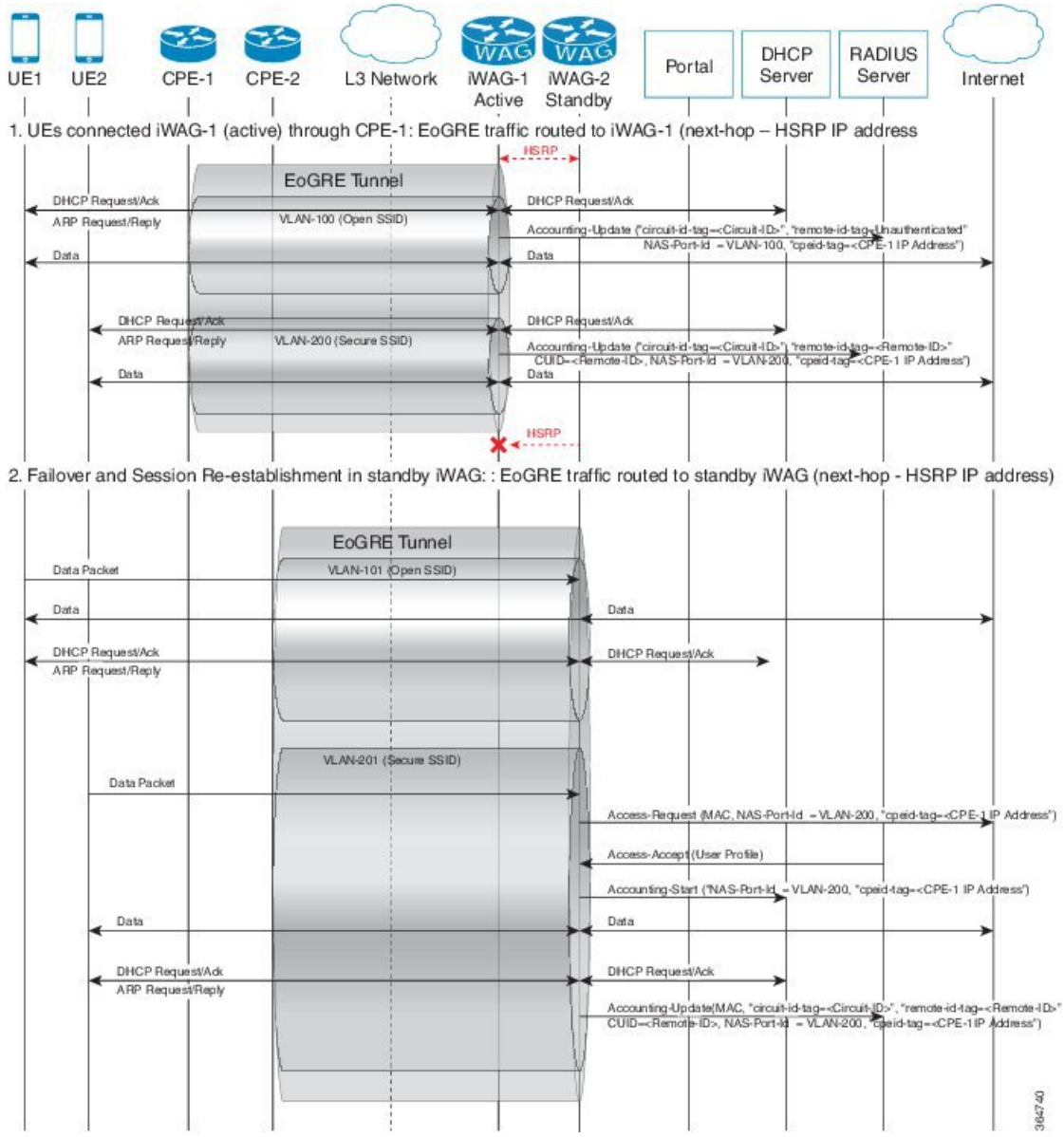
On receiving the DHCP control packets, iWAG validates the packets against any existing unclassified session. If an unclassified session is found, iWAG validates the subnet of both the existing session and the DHCP control packet. If the subnets match, iWAG will update the existing session from unclassified MAC to DHCP session creating a DHCP binding.

Note In case of any discrepancy, iWAG will bring down the existing unclassified session, discarding the DHCP control packet as well.

EoGRE: Inter-Chassis Stateless HA Call Flow

The following figure and the subsequent steps describes a call flow pertaining to a Ethernet over GRE (EoGRE): intra-chassis stateless HA.

Figure 24: E0GRE: Inter-Chassis Stateless HA Call Flow



1. IP session is established on iWAG when a subscriber device connects to network through open or secure SSID.

   1a. Session establishment through Open SSID

   1b. Session establishment through Secure SSID

2. In case of a fail over, session is re-established on the standby iWAG.

   2a. Coverts subscriber from existing IP session to DHCP session.

Additional References for EoGRE: Inter-Chassis HA

Related Documents

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

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

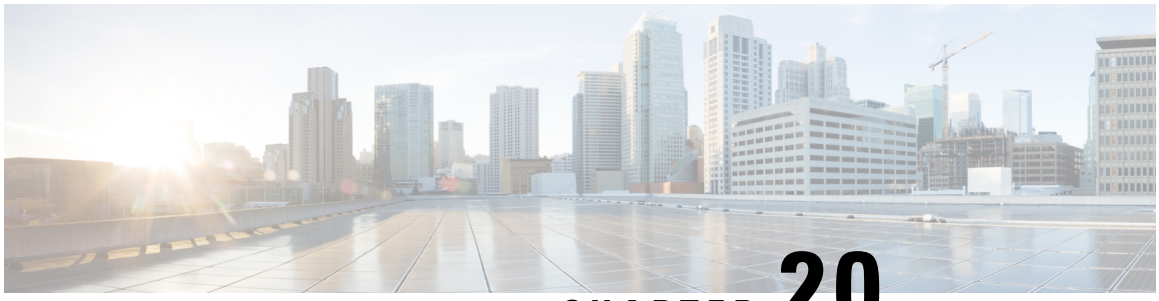
Feature Information for EoGRE: Inter-chassis HA

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 22: Feature Information for EoGRE: Inter-chassis HA

Feature Name	Releases	Feature Information
EoGRE: Inter-chassis HA	Cisco IOS XE Release 3.16S	The EoGRE: Inter-chassis HA feature converts the existing IP session to Dynamic Host Configuration Protocol (DHCP) session upon receiving DHCP control packets requested by the subscriber.



CHAPTER 20

Call Flows for Simple IP Users

This chapter provides various call flows for simple IP users.

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.

Simple IP Unclassified MAC Authentication (MAC TAL and Web Login) Call Flows

The MAC Transparent Auto Login (TAL) authentication method is associated with the web authentication method and is prevalent in public access control as used in public wireless LAN (PWLAN) applications or in limited usage as in broadband residential access. Here, many sessions are aggregated on a single VLAN or interface at the broadband remote access server (BRAS), and individual sessions are identified based on the source MAC address for the Layer 2 access subscriber.

MAC TAL enables the iWAG to authorize a subscriber on the basis of the subscriber's source MAC address. After authentication, the iWAG applies the auto-login services on the session and the subscriber will be able to access the service. If the initial authorization based on the MAC address fails, then the iWAG subscriber is redirected to the ISP's web portal, where the subscriber enters the ISP-assigned credentials (username and password) to complete the authentication in order to avail the ISP's services. The iWAG then applies the services that the subscriber selected from the portal, and provides the subscriber full access to those services.

This use case covers the following:

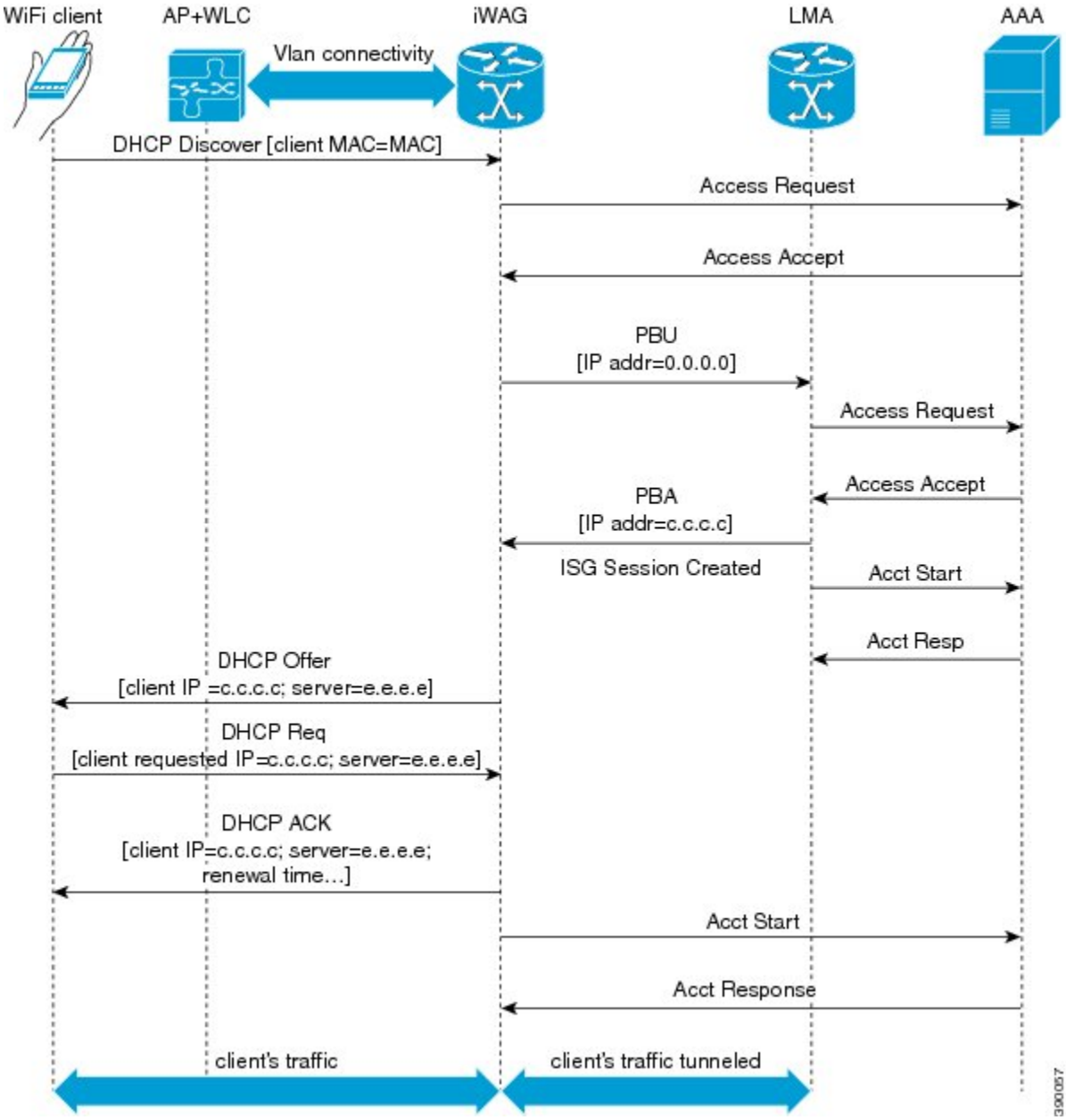
- iWAG session creation
- User authorization based on MAC address

- Default service activation (Internet)
- Auto-login service activation and access
- User redirection to the portal (on user authorization failure only)
- User authentication at the RADIUS server
- Profile download and auto-login service activation
- Access to features such as change of authorization (CoA), account logout, account stop, account ping

Simple IP Unclassified MAC with MAC TAL Authentication Call Flow

The following figure illustrates the unclassified MAC with MAC TAL authentication call flow for a simple IP user.

Figure 25: Simple IP Unclassified MAC with MAC TAL Authentication Call Flow



The following steps describe the call flow for a successful MAC TAL Web authorization for a simple IP subscriber:

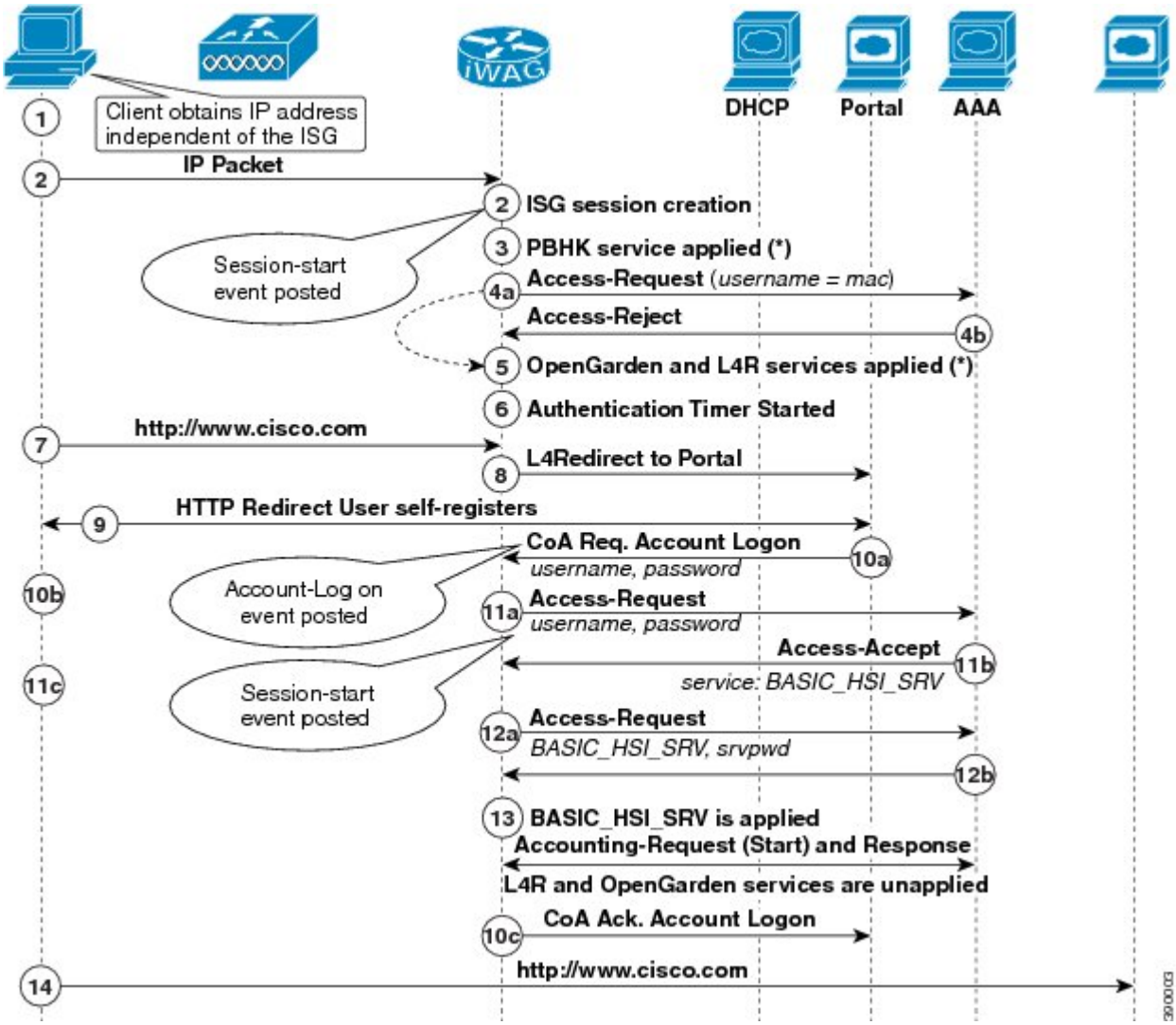
1. The subscriber initiates IP traffic to get connected to the Internet service. ISG notices a new subscriber address and creates an unauthenticated subscriber session.
2. ISG then sends an authorization request to the RADIUS server with the subscriber's MAC address as the username.
3. If the authorization is successful, the default Internet services are applied to the subscriber for the session.

4. The defined services are applied to the subscriber's session and the subscriber can start accessing the Internet.
5. The subscriber now has full access to the network.
6. An Accounting Start message is sent to the application provider to indicate the start of the subscriber's service. The subscriber can now access the Internet services applicable as part of the subscription.

Simple IP Unclassified MAC with Web Login Authentication Call Flow

The following figure illustrates the unclassified MAC with web login authentication MAC TAL call flow for a simple IP user.

Figure 26: Simple IP Unclassified MAC with Web Login Authentication Call Flow



The following steps describe the call flow for a successful MAC TAL Web authorization for a simple IP subscriber:

1. The subscriber initiates IP traffic to get connected to the Internet service. ISG notices a new subscriber address and creates an unauthenticated subscriber session.
2. ISG then sends an authorization request to the RADIUS server with the subscriber's MAC address as the username.
3. If the authorization fails, services such as OpenGarden and Layer 4 Redirect (L4R) are applied to the subscriber for a temporary period of time.
4. ISG then redirects the subscriber to the portal where the subscriber enters the username and password. The subscriber's credentials are then sent to the ISG through the account login message.
5. ISG now authenticates the subscriber on the AAA server and retrieves the subscriber's profile, which may contain a few preconfigured auto-login services.
6. On successful authentication, ISG enables the user's auto-login services (Internet).
7. Assuming that the services for accessing the Internet are not cached on ISG prior to this session, ISG sends an access request to the corresponding service provider's AAA server to download the service definition.
8. The AAA server responds with the service definition.
9. The defined service is applied to the subscriber's session and the subscriber can start accessing the Internet. The subscriber now has full access to the network.
10. On successful account login, the L4R feature is unapplied for the subscriber in ISG to prevent subscriber traffic redirection to the ISP's web portal.
11. An Accounting Start message is sent to the application provider to indicate the start of the subscriber's service. Now, the subscriber is connected to the Internet.

Simple IP Unclassified MAC Authentication Call Flow Configuration

The following configuration is an example of a simple IP unclassified MAC call flow. This is applicable to both the MAC TAL and web logon authentication scenarios:

```
#-----------------------------------------------
# AAA and RADIUS
#-----------------------------------------------
aaa new-model
!
aaa server radius dynamic-author
 client 5.5.5.1 server-key cisco
!
aaa group server radius SERVER_GROUP1
server name RAD1
!
aaa authentication login AUTHEN_LIST group SERVER_GROUP1
aaa authorization network default group SERVER_GROUP1 local
aaa authorization network AUTHOR_LIST group SERVER_GROUP1 local
aaa authorization subscriber-service default local group SERVER_GROUP1
aaa accounting network List1 start-stop group SERVER_GROUP1
aaa accounting system default start-stop group radius
!
radius-server key cisco
!
```

```
radius server RAD1
address ipv4 4.4.4.1 auth-port 1645 acct-port 1646
#-----------------------------------------------
# Interface
#-----------------------------------------------
interface GigabitEthernet0/0/2.10    #Connected to the client, access interface.
 encapsulation dot1Q 10
 ip address 11.11.11.1 255.255.255.0
 service-policy type control TAL
 ip subscriber l2-connected
  initiator unclassified mac-address
!
interface GigabitEthernet0/0/3       #Connected to the RADIUS server
 ip address 4.4.4.2 255.255.255.0
 ip portbundle outside
!
interface GigabitEthernet 0/0/4 #Connected to the Web portal
 ip address 5.5.5.2 255.255.255.0
 ip portbundle outside
!
interface Loopback0                     #Loopback interface for PBHK service
 ip address 15.1.1.1 255.255.255.0
!
#-----------------------------------------------
# Port Bundle Configurations
#-----------------------------------------------
!
ip portbundle
 length 5
 source Loopback0
#-----------------------------------------------
# Service Definitions
#-----------------------------------------------
policy-map type service OPENGARDEN_SERVICE
 20 class type traffic ISG_OPENGARDEN
!
policy-map type service L4REDIRECT_SERVICE
 10 class type traffic L4REDIRECT
   redirect to group ISG_GROUP
   accounting aaa list IP_SESSION
!
 class type traffic default input
  drop

policy-map type service PBHK_SERVICE
 ip portbundle
!
#-----------------------------------------------
# Traffic Class Definitions
#-----------------------------------------------
class-map type traffic match-any ISG_OPENGARDEN
 match access-group output name ACL_OUT_OPENGARDEN
 match access-group input name ACL_IN_OPENGARDEN

class-map type traffic match-any L4REDIRECT
 match access-group input name ACL_IN_L4REDIRECT

class-map type control match-all IP_UNAUTH_COND
 match timer IP_UNAUTH_TIMER
 match authen-status unauthenticated
#-----------------------------------------------
# Redirect Group Definition
#-----------------------------------------------
redirect server-group ISG_GROUP
```

```
 server ip 10.10.33.166 port 80
#-----------------------------------------------
# Policy Map
#-----------------------------------------------
policy-map type control TAL
class type control always event session-start
  10 service-policy type service name PBHK_SERVICE
  20 authorize aaa list AUTHOR_LIST password cisco123 identifier mac-address
  30 service-policy type service name L4REDIRECT_SERVICE
  40 service-policy type service name OPENGARDEN_SERVICE
  50 set-timer IP_UNAUTH_TIMER 10
!
class type control always event account-logon
  10 authenticate aaa list IP_AUTHEN_LIST
  20 service-policy type service unapply name OPENGARDEN_SERVICE
  30 service-policy type service unapply name L4REDIRECT_SERVICE
!
 class type control UNAUTHEN_COND event timed-policy-expiry
  10 service disconnect
 !
#-----------------------------------------------
# ACL
#-----------------------------------------------
ip access-list extended ACL_IN_OPENGARDEN
 …
 permit ip any host 10.10.33.166
 …
ip access-list extended ACL_OUT_OPENGARDEN
 …
 permit ip host 10.10.33.166 any
….
ip access-list extended ACL_IN_L4REDIRECT
 …
 deny   tcp any host 10.10.33.166
 permit tcp any any eq www
 permit tcp any any eq 443
….
```

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

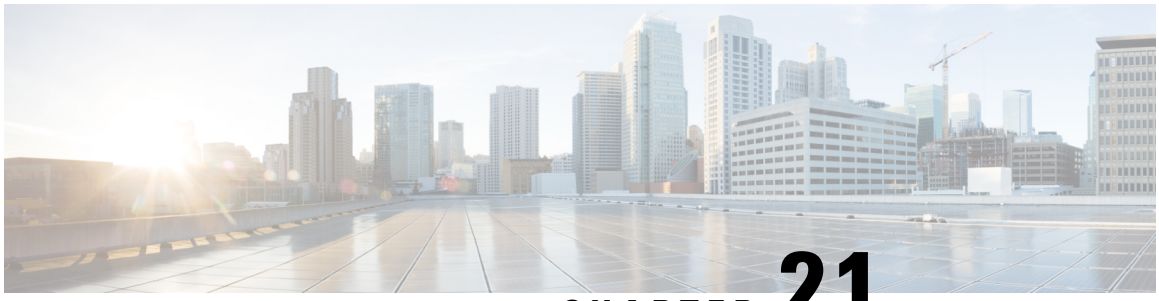
Feature Information for Call Flows for Simple IP Users

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

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

Table 23: Feature Information for Call Flows for Simple IP Users

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



CHAPTER 21

Call Flows for 3G and 4G Mobile IP Users

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

Finding Feature Information

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

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

3G DHCP Discover Call Flow

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

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

Figure 27: 3G DHCP Discover Call Flow (Part 1)

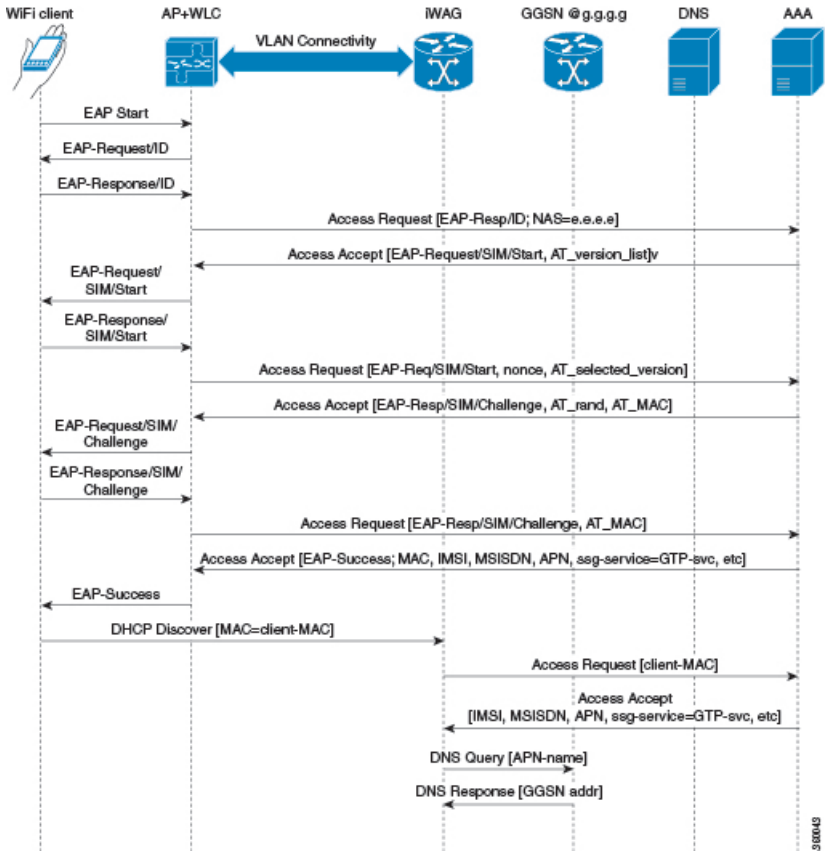
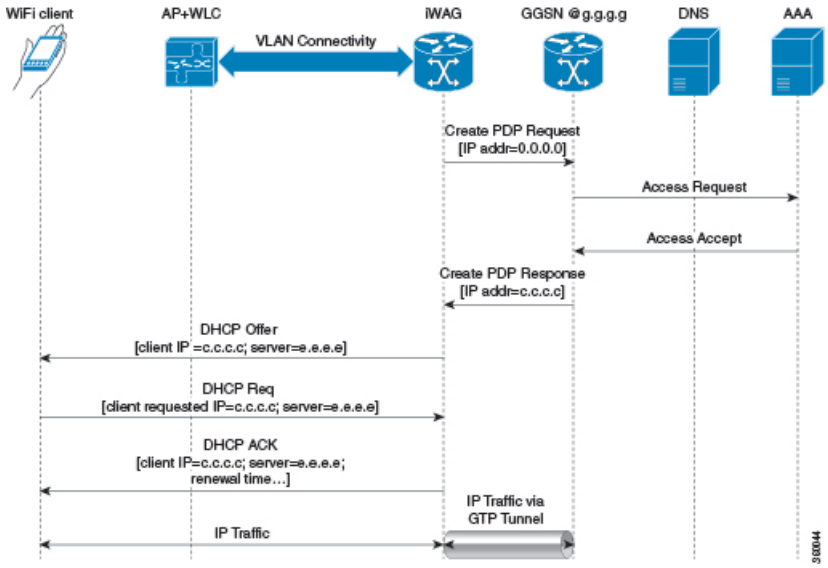


Figure 28: 3G DHCP Discover Call Flow (Part 2)



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

2. The AP or the WLC starts the EAP authentication process by sending an EAP Request ID to the mobile device.
3. The mobile device sends a response pertaining to the EAP Request ID back to the AP or the WLC.
4. The WLC sends a RADIUS Access Request to the AAA server asking it to authenticate the subscriber.
5. After the subscriber is authenticated, the AAA server caches its entire user profile that includes the information about IMSI, MSISDN, APN, and the Cisco AV pair having ssg-service-info set to GTP-service. The cached data also includes the client's MAC address, which is set as the calling-station-ID in the incoming EAP messages.
6. The AAA server sends the RADIUS Access Accept message to the AP or the WLC.
7. When the RADIUS Access Accept message comes back, the corresponding user profile in which the use of GTP-service is identified is obtained.
8. The WLC sends the successful EAP authentication message to the mobile device.
9. The mobile device sends a DHCP Discover message to the iWAG. In response to this DHCP Discover message, the DHCP goes into a new pending state to wait for the signaling on the MNO side to be completed, which assigns an IP address to the subscriber.

   In response to this DHCP Discover message, DHCP goes into a new pending state to wait for the signaling on the MNO side to be completed, which assigns an IP address to the subscriber.
10. The iWAG finds a session associated with the subscriber MAC address and retrieves the subscriber IP address from the session context.
11. The iWAG sends a RADIUS Access Request to the AAA server asking it to authenticate the subscriber using the MAC address in it as the calling-station-ID, while also providing all other known subscriber information, IDs, and IMSI in this Access Request message.
12. When the AAA server sends back the RADIUS Access Accept message to the iWAG, the user profile in which the use of GTP-service is identified is obtained.
13. The iWAG sends a query to the DNS server to resolve a given Access Point Name (APN) to a GGSN IP address.
14. The DNS server sends the DNS-resolved GGSN address back to the iWAG.
15. After receiving the DNS-resolved GGSN address, the iWAG sends the Create PDP Context Request, in which the PDP context address is set to 0, in order to request the GGSN for an IP address assignment.
16. The GGSN sends a RADIUS Access Request to the AAA server.
17. Based on the cached information obtained from the EAP-SIM authentication, the AAA server replies with a RADIUS Access Accept message to the GGSN.
18. The GGSN sends the Create PDP Context Response that carries the assigned IP address c.c.c.c for the subscriber, to the iWAG.
19. The iWAG sends a DHCP Offer message to the mobile device.
20. The mobile device sends a DHCP Request message to the iWAG, and the iWAG acknowledges this request by sending a DHCP ACK message to the mobile device.
21. The WiFi subscriber traffic now has a data path through which it can flow.

3G DHCP Discover Call Flow Configuration

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

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

!
ip dhcp pool 2NETWORK
 network 10.0.0.0 255.0.0.0
 default-router 10.100.10.2
!
!
!
subscriber service multiple-accept
subscriber service session-accounting
subscriber service accounting interim-interval 1
subscriber redundancy dynamic periodic-update interval 15
subscriber authorization enable
!
!
spanning-tree extend system-id
!
username samipate nopassword
!
redundancy
 mode sso
```

```
redirect log translations extended exporter l4r-exporter
!
!
!
ip tftp source-interface GigabitEthernet0
ip tftp blocksize 8192
class-map type traffic match-any TC_TIMEOUT
 match access-group input name timeout_acl_in
 match access-group output name timeout_acl_out
!
class-map type traffic match-any TC_POSTPAID
 match access-group input name postpaid_acl_in
 match access-group output name postpaid_acl_out
!
class-map type traffic match-any TC_OPENGARDEN
 match access-group input name acl_in_opengarden
 match access-group output name acl_out_opengarden
!
policy-map type service OPENGARDEN_SERVICE
 10 class type traffic TC_OPENGARDEN
  accounting aaa list ACCT_SERVER
 !
 class type traffic default in-out
  drop
 !
!
policy-map type service SERVICE_POSTPAID
 20 class type traffic TC_POSTPAID
  police input 512000
 !
 class type traffic default in-out
  drop
 !
!
policy-map type service SERVICE_TIMEOUT
 25 class type traffic TC_TIMEOUT
  timeout absolute 10000
 !
 class type traffic default in-out
  drop
 !
!
policy-map type control ISG_GTP_CONTROL
 class type control always event service-stop
  1 service-policy type service unapply identifier service-name
 !
 class type control always event session-start
  10 service-policy type service name OPENGARDEN_SERVICE
  20 service-policy type service name SERVICE_POSTPAID
  25 service-policy type service name SERVICE_TIMEOUT
  30 authorize aaa list ISG_PROXY_LIST password lab1 identifier mac-address
 !
 class type control always event account-logon
  10 authenticate aaa list WEB_LOGON
  20 service-policy type service unapply name L4REDIRECT_SERVICE
 !
!
!
!
!
!
!
!
```

```
#-----------------------------------------------
 Configuring iWAG Access Interface
#-----------------------------------------------

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

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

interface GigabitEthernet0
 description To Management Interface
 ip address 5.28.8.10 255.255.0.0
 negotiation auto
!
mcsa # enabling mobile client service abstraction
 enable sessionmgr
!
ip default-gateway 5.28.0.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 5.28.0.0 255.255.0.0 5.28.0.1
ip route vrf Mgmt-intf 5.28.0.0 255.255.0.0 5.28.0.1
ip route vrf Mgmt-intf 223.0.0.0 255.0.0.0 5.28.0.1
!
ip access-list extended acl_in_opengarden # enabling access lists
 permit udp any eq 5555 any
ip access-list extended acl_out_opengarden
```

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

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

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

```
end
```

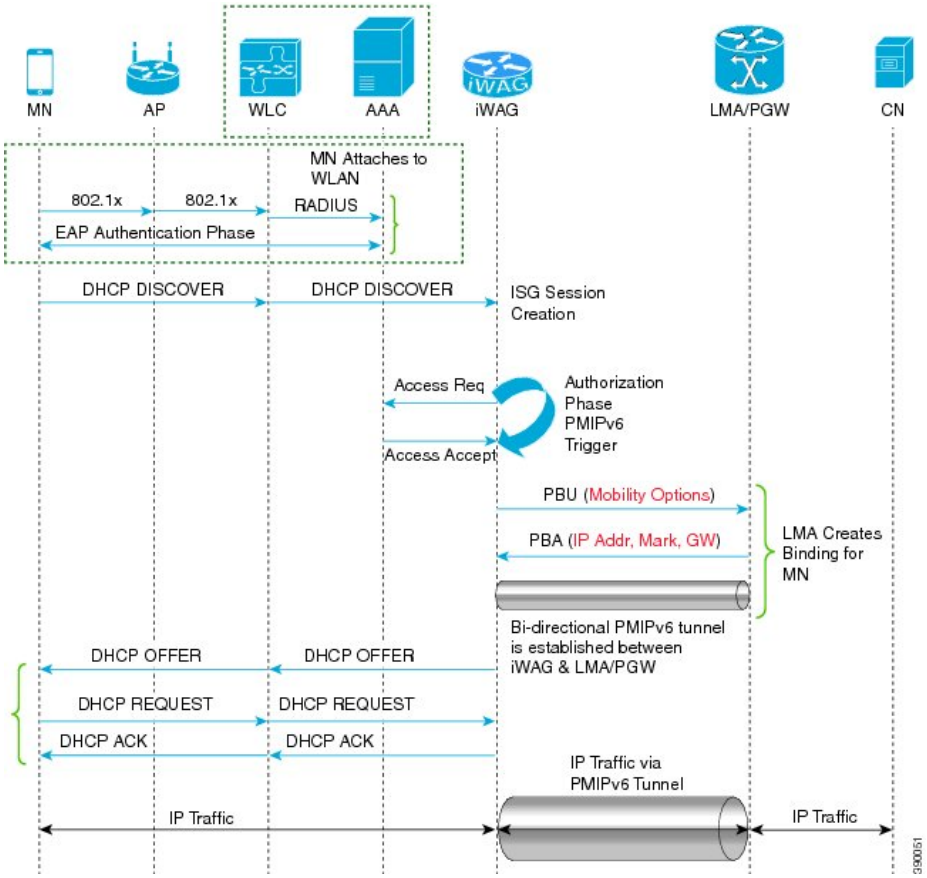
4G DHCP Discover Call Flow

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

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

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

Figure 29: 4G DHCP Discover Call Flow



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

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

10. The iWAG offers an IP address to the mobile node through a DHCP OFFER message.
11. The mobile node accepts the IP address by sending a DHCP Request.
12. The iWAG, which also hosts the DHCP server, acknowledges the mobile node's request by sending a DHCP ACK message.
13. The iWAG finally creates a DHCP binding.
14. The mobile node configures the IP address that was offered on its wireless interface.
15. The mobile node seamlessly exchanges data traffic with the correspondent node.

4G DHCP Discover Call Flow Configuration

The following is a 4G DHCP session initiator configuration:

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

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

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

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

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

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

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


!
```

4G Roaming Call Flow

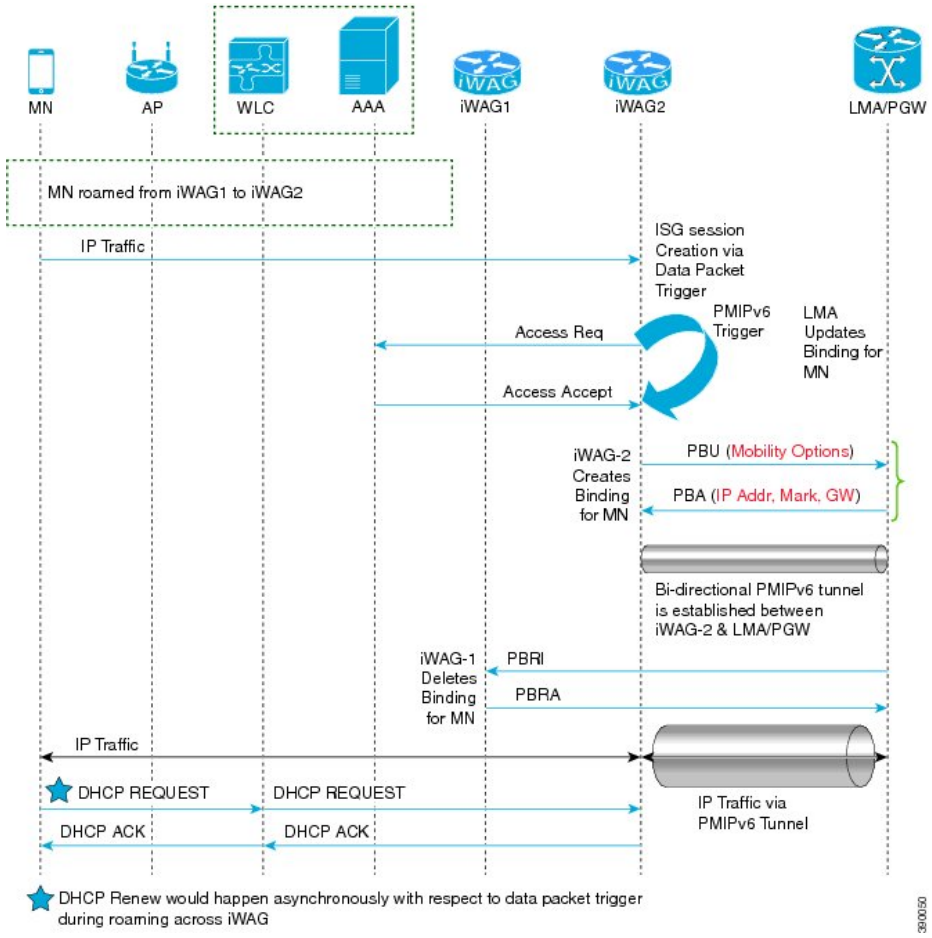
After roaming from one iWAG to another, the mobile node sends traffic to the iWAG. On receiving the unclassified MAC address, the iWAG creates a session and sends an Access Request message to the AAA server. The iWAG downloads mobility parameters from the AAA server through an Access Accept message.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

This call flow covers the following:

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

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

Figure 30: 4G Roaming Call Flow



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

1. A mobile node roams from iWAG 1 to iWAG 2. The mobile node directly sends the IP packet to iWAG 2. The iWAG 2 creates sessions and send access request to the AAA server.
2. The iWAG 2 downloads mobility parameters from the AAA server through an Access Accept message.
3. On receiving mobility parameters from the AAA server, the iWAG 2 initiates PMIP signaling by sending a Proxy Binding Update (PBU) message to the LMA. The LMA responds with the PBA message that

contains the IP address, mask, and gateway. Now a PMIP tunnel is established between iWAG 2 and the LMA.

4. The LMA sends a PBRI message to iWAG 1 to delete the binding from iWAG 1. iWAG 1 deletes the binding for mobile node and responds with a PBRA message.
5. iWAG 2 acknowledges the same IP address to the MN through a DHCP ACK message.
6. The MN seamlessly exchanges data traffic with the correspondent node.

4G Roaming Call Flow Configuration

The following is a 4G Roaming call flow configuration:

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

     ipv6 address 2001:DB8::1/64
     ip address 10.8.24.101 255.255.255.0 secondary
    subscriber default
    exit
    apn serviceprovider.com
      selection-mode sent-by-ms
      accounting-mode none
      ip context-name pgw
      ip address pool name PMIP_POOL_TME
      ipv6 address prefix-pool v6_pool
    exit
    lma-service lma1
      no aaa accounting
      reg-lifetime 40000
      timestamp-replay-protection tolerance 0
      mobility-option-type-value standard
      revocation enable
      bind address 2001:DB8:0:0:E000::F
    pgw-service pgw1
      plmn id mcc 100 mnc 200
      session-delete-delay timeout 60000
      associate lma-service lma1
    exit
    ipv6 route 2001:DB8::/48 next-hop 2001:DB8:0:ABCD::1 interface lma1
    ip route 10.8.0.0 255.255.0.0 10.8.24.8 lma1
  port ethernet 17/1
    boxertap eth3
    no shutdown
    bind interface lma1 pgw
end
#-------------------------------------------------
IWAG2 (ASR 1000)
Local Profile without AAA (Simple Configuration using the MN’s MAC)
#-------------------------------------------------
!
ipv6 unicast-routing
! !
policy-map type control PROXYRULE
 class type control always event session-start
  10 proxy aaa list RP
```

```
 !
ip dhcp pool pmipv6_dummy_pool
!
ipv6 mobile pmipv6-domain D1
 replay-protection timestamp window 200
 lma lma1
  ipv6-address 2001:DB8:0:0:E000::F
 nai mn1@example.com
  apn example.com
  lma lma1
  int att WLAN l2-addr 0024.d78e.21a4
!
ipv6 mobile pmipv6-mag M1 domain D1
 discover-mn-detach 100 10
 role 3GPP
 address ipv6 2001:DB8:0:1:FFFF:1234::5
 interface GigabitEthernet 0/1/0.3074
!
interface GigabitEthernet1/3/0
 ip address 10.27.52.1 255.255.0.0
 negotiation auto
 ipv6 address 2001:DB8:0:1::1 link-local
 ipv6 address 2001:DB8::1
 ipv6 nd ra suppress
 ipv6 eigrp 100
 service-policy type control PROXYRULE
 ip subscriber l2-connected
  initiator dhcp
  initiator unclassified-mac
!
```

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

Additional References

Related Documents

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

MIBs

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

Technical Assistance

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

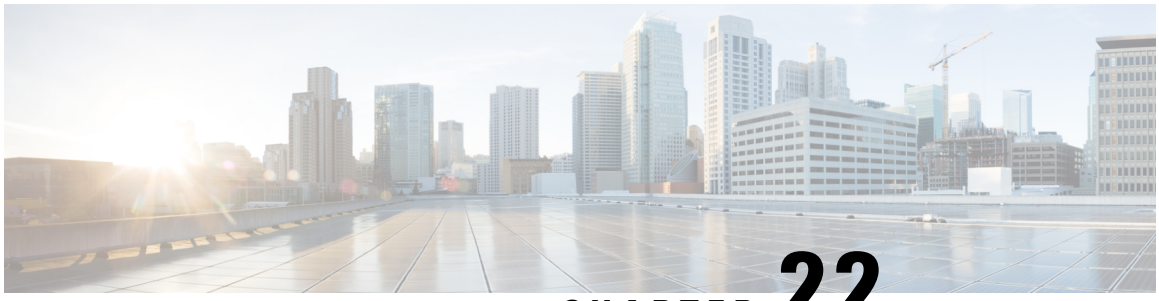
Feature Information for Call Flows for 3G and 4G Mobile IP Users

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

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

Table 24: Feature Information for Call Flows for 3G and 4G Mobile IP Users

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



CHAPTER 22

iWAG Scalability and Performance

The infrastructure of a service provider must be capable of supporting the services that an enterprise customer or Internet service provider (ISP) wants to offer its subscribers. The service provider must also be able to scale up to an expanding subscriber base. You can configure IWAG on the Cisco ASR1000 Series Routers for high scalability and performance.

iWAG Scaling

The ASR 1000 Series Routers can be deployed as an IP session aggregator. The maximum number of IP sessions that can be supported depends on the hardware combination.

Table below lists the iWAG scaling numbers and maximum number of IP sessions supported on the ASR 1000 hardware:

- Hardware combination and the maximum number of IP sessions that are supported when used for SP WiFi applications.

The session limits apply to all variety of IP session initiators: DHCP, unclassified Mac address, unclassified IP, and radius proxy.

- Hardware combinations for SP WiFi applications and the corresponding Simple IP use case scale numbers for authenticated and walk-by users.

Note Other hardware variants are not supported for SP WiFi applications. For more information, see Restrictions for iWAG Scalability, page 3

The scale numbers provided in the table below assumes the following reference configuration:

- Walk-by users: A maximum of three traffic classes on the default session.

- Authenticated users: There are no traffic classes for authenticated users.

Any deviation from the conditions mentioned above may result in different scale numbers. The scale limits and the hardware combinations listed in the next table requires 16GB of DRAM on ASR1000 Route Processor 2 (RP2).

Table 25: iWAG Scale: Maximum Number of IP Sessions Supported on ASR 1000 Hardware

Chassis	RP	ESP	Walk-by Users	Authenticated Users	Total number of Session (combined Authenticated and Walk-by Users)
1001	Integrated + 16 GB	ESP-2.5G or ESP-5G	16000	8000	24000
1001-X	Integrated + 16 GB	ESP licensing from -2.5G, 5G, 10G, or 20G	16000	8000	24000
1002-X	Integrated + 16 GB	ESP licensing from 5G, 10G, 20, or 36G	128000	32000	160000
1001-HX	Integrated + 16 GB	44G to 60G	128000	32000	160000
1002-HX	Integrated + 16 GB or 32 GB	44G to 60G	256000	128000	384000
1004, 1006, 1006-X, 1009-X, 1013	RP2 + 16 GB	ESP-40G	192000	64000	256000
1006-X, 1009-X, 1013	RP3 + 16 GB or 32GB or 64GB	ESP-40G	192000	64000	256000
1006, 1006-X,1009-X, 1013	RP2 + 16 GB	ESP-100G	256000	128000	384000
1006-X,1009-X, 1013	RP3 + 16 GB, or 32GB or 64 GB	ESP-100G	256000	128000	384000
1009-X, 1013	RP2 + 16 GB, or RP3+ 16GB or 32GB or 64 GB	ESP-200G	256000	128000	384000

Restrictions for iWAG Scalability

The following are the restrictions pertaining to iWAG scalability:

The Intelligent Wireless Access Gateway (iWAG) feature is not supported on the following hardware.

- RP1 with ESP10 or ESP20
- ASR1002
- ASR1002F

Layer 4 Redirect Scaling

The ASR 1000 supports the ability to redirect IP traffic within an ISG traffic class. Layer 4 redirect scaling is performed by the Quantum Flow Processor (QFP). The scaling limits are dependent on the ESP.

Table 26: Maximum Number of Per-Session Limit Per ESP

Chassis	RP	ESP	L4 Redirect Translations	Default Per-Session Limit
1001	Integrated	ESP-2.5G	256000	128
1002-X	Integrated	ESP-5G ESP licensing from 5G, 10G, 20, or 36G	256000	128
1004, 1006, 1013	RP2	ESP-40G	1 Million	128
1006, 1013	RP2	ESP-100G	1 Million	128

Configuring Call Admission Control

The Call Admission Control (CAC) feature is configured to protect the ASR 1000 processing resources that must be configured. CAC can restrict creation of new sessions when system resources exceed configured thresholds.

For examples about configuring the CAC for IPoE feature, see the “Call Admission Control” section in the Intelligent Wireless Access Gateway Configuration Guide located at:

http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/IWAG_Config_Guide_BookMap_chapter_01001.html

Walk-by User Support for PWLAN in iWAG

In public wireless LAN (PWLAN) setups, a high number of ISG sessions might be unauthenticated sessions from wireless devices that do not use the PWLAN service. These sessions are referred to in this document as walk-by sessions, and users that use these sessions are referred to as walk-by users.

Walk-by sessions, if not dealt with in an optimized way, may consume a large portion of the hardware resources. This resource utilization may lead to an increase in the number of ISG routers required for a given PWLAN deployment. The concept of light-weight sessions is introduced to provide an optimization for walk-by sessions.

The features for walk-by users are configured on a default session acting as a template. Walk-by users are then assigned light-weight sessions that inherit features from a default session. The features are configured only once on the default session, thereby optimizing the resource usage.

A lite session is a light-weight unauthenticated ISG session that inherits default session services. Lite sessions are created on ISG to support walk-by users and optimize resource usage. A timer may be specified to limit the duration for which the lite session can utilize the public wireless LAN (PWLAN) services while remaining unauthenticated.

On the ASR 1000 Series router, the Layer 4 Redirect (L4R) feature supports a maximum of 16 translation entries per walk-by session. For more information on the limit for the total number of translations on the system, see Layer 4 Redirect Scaling, on page 185.

For platform-independent restrictions pertaining to the walk-by sessions and information on how to configure the Walk-By User Support for PWLAN in ISG feature, refer to the following URL: http://www.cisco.com/en/US/docs/ios-xml/ios/isg/configuration/xe-3s/isg-wlkby-supp.html

Additional References

Related Documents

Related Topic	Document Title
Control Plane Policing	*Quality of Service Solutions Configuration Guide*
Using ARP for Keepalive Messages and Using ICMP for Keepalive Messages	Intelligent Services Gateway Configuration Guide Cisco IOS XE Release 3S
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at this URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

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 iWAG Scalability and Performance

Feature Information for IWAG Scalability and Performance table lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note Feature Information for IWAG Scalability and Performance 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.

Table 27: Feature Information for IWAG Scalability and Performance

Feature Name	Releases	Feature Information
iWAG Scalability and Performance	Cisco IOS XE 3.11S	In Cisco IOS XE Release 3.11S, this feature was introduced on the Cisco ASR 1000 Series Router.