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 5 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

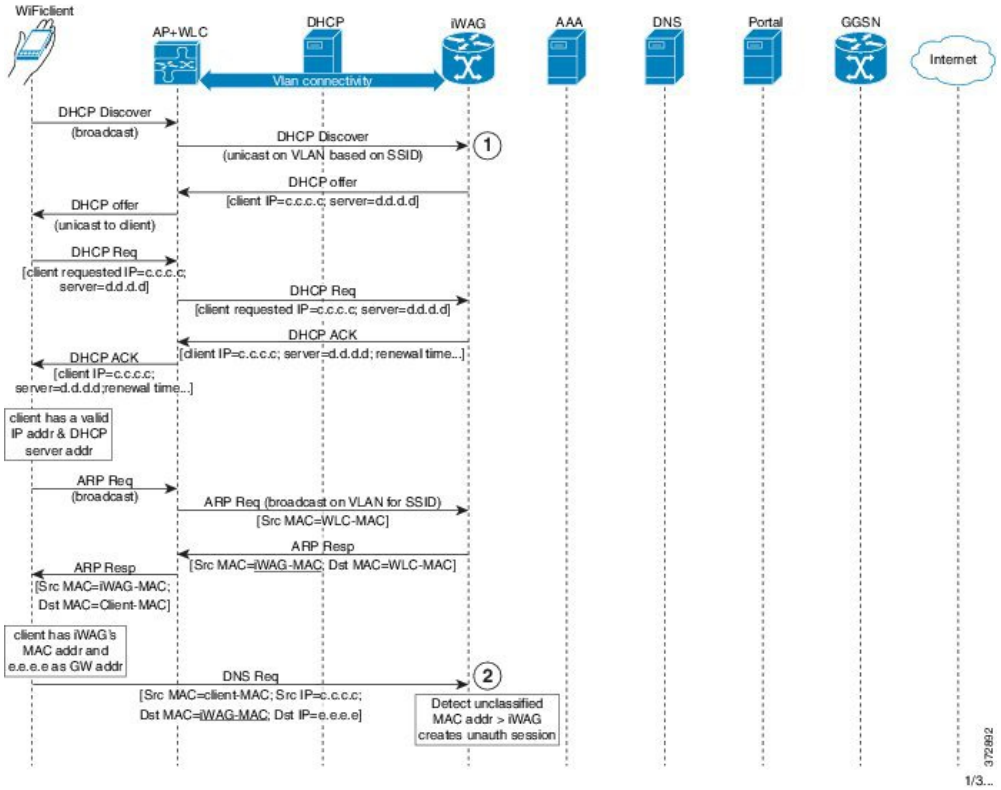
If an interface is configured as default gateway, the following events may occur on the configured interface:

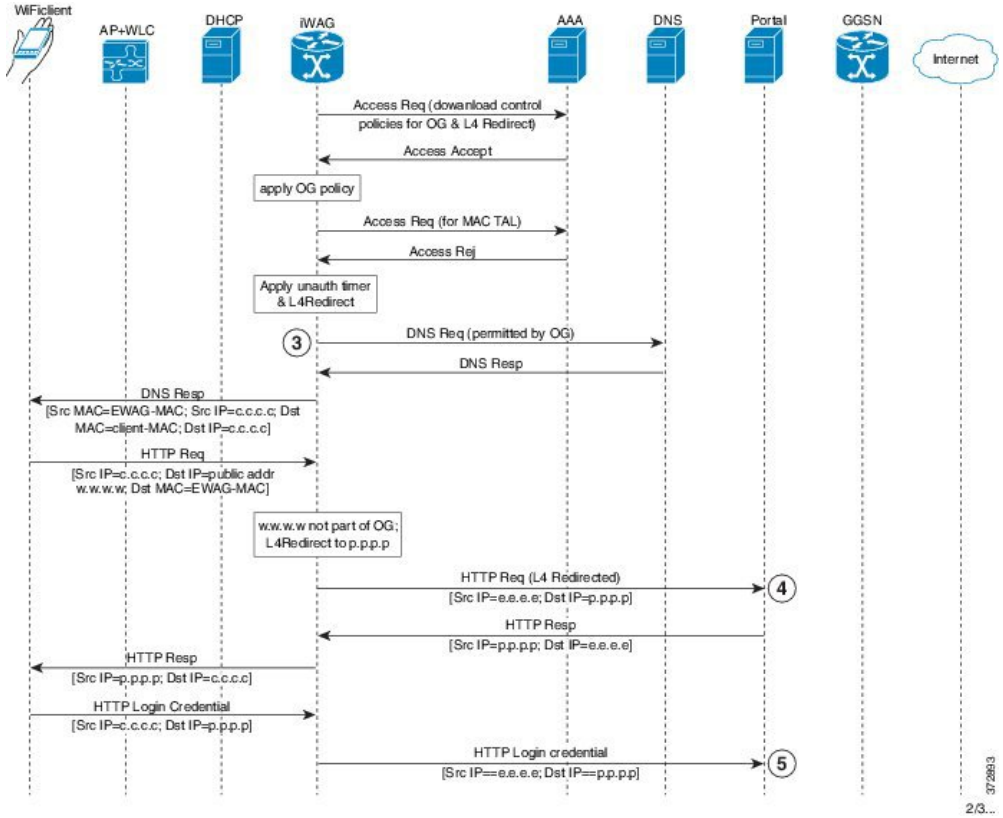
- If an IP address or a network mask on a configured interface is changed, the traffic may still continue, but the sessions may not be torn down by the DHCP clients depending on the idle timeout. New session setup requests may either continue through the default gateway if the subnet of the GTP Packet 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.

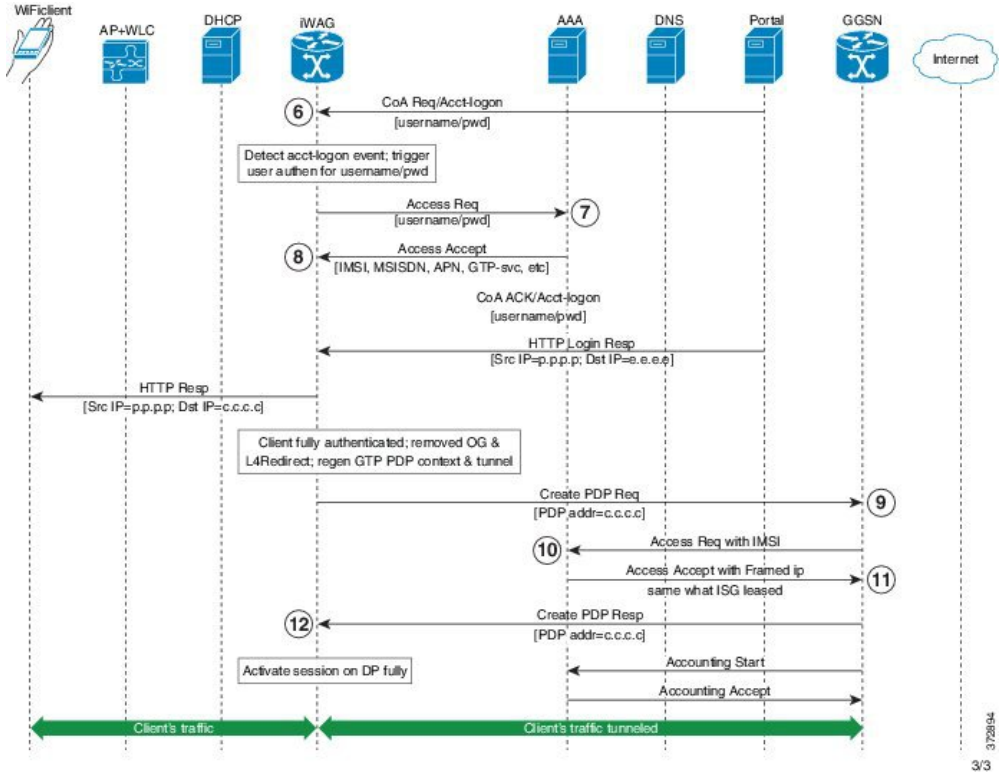
Web Authentication Support for iWAG-GTP Call Flow

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

Figure 1: 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 1: 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.