cisco

TOMORROW
starts here.

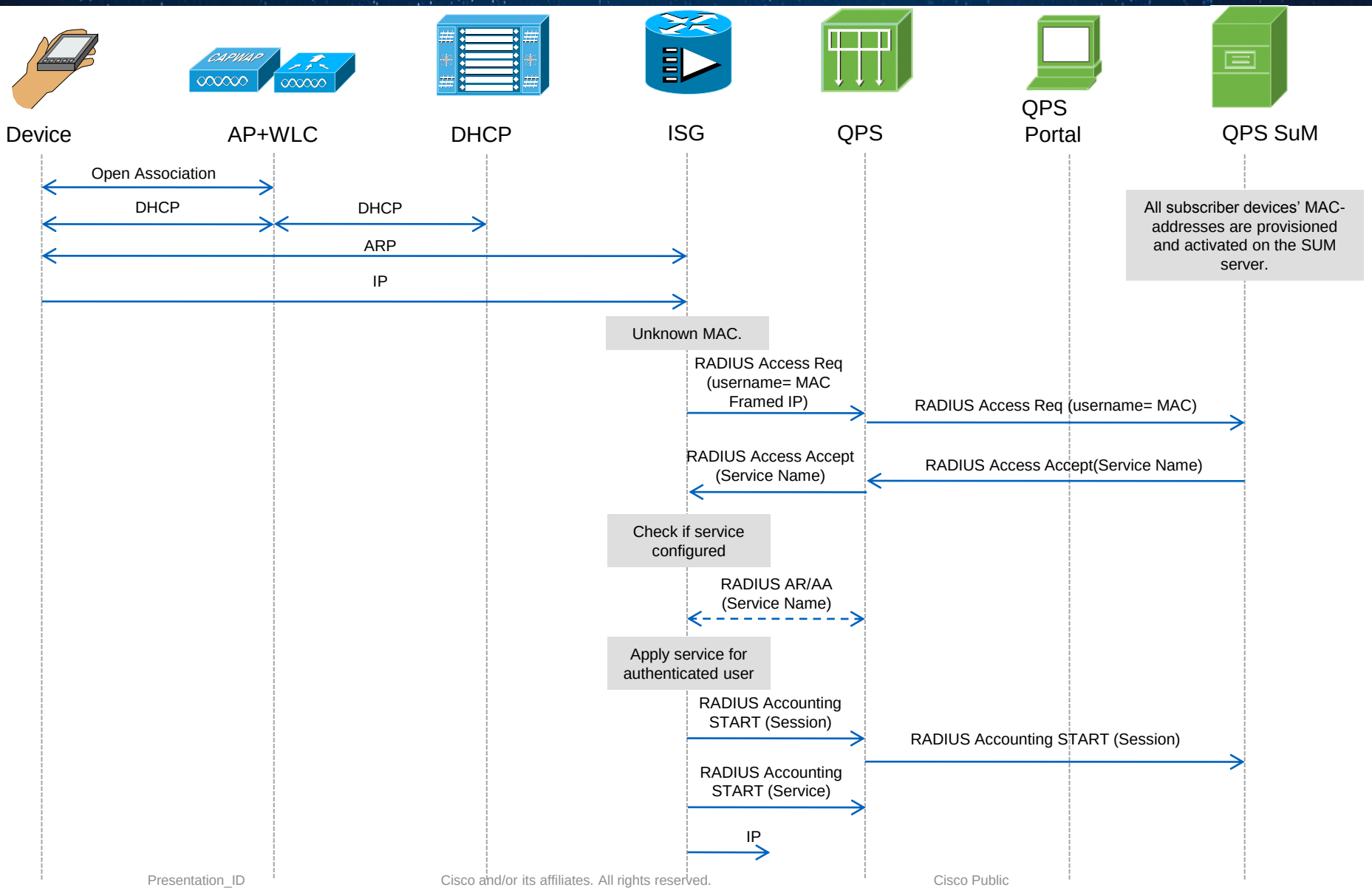
Cisco Connect
Split, Croatia

Cisco SP Wi-Fi solution: use cases and call flows

Djordje Vulovic
Consulting Systems Engineer
CCIE #16582

Local Breakout
using MAC TAL Authentication

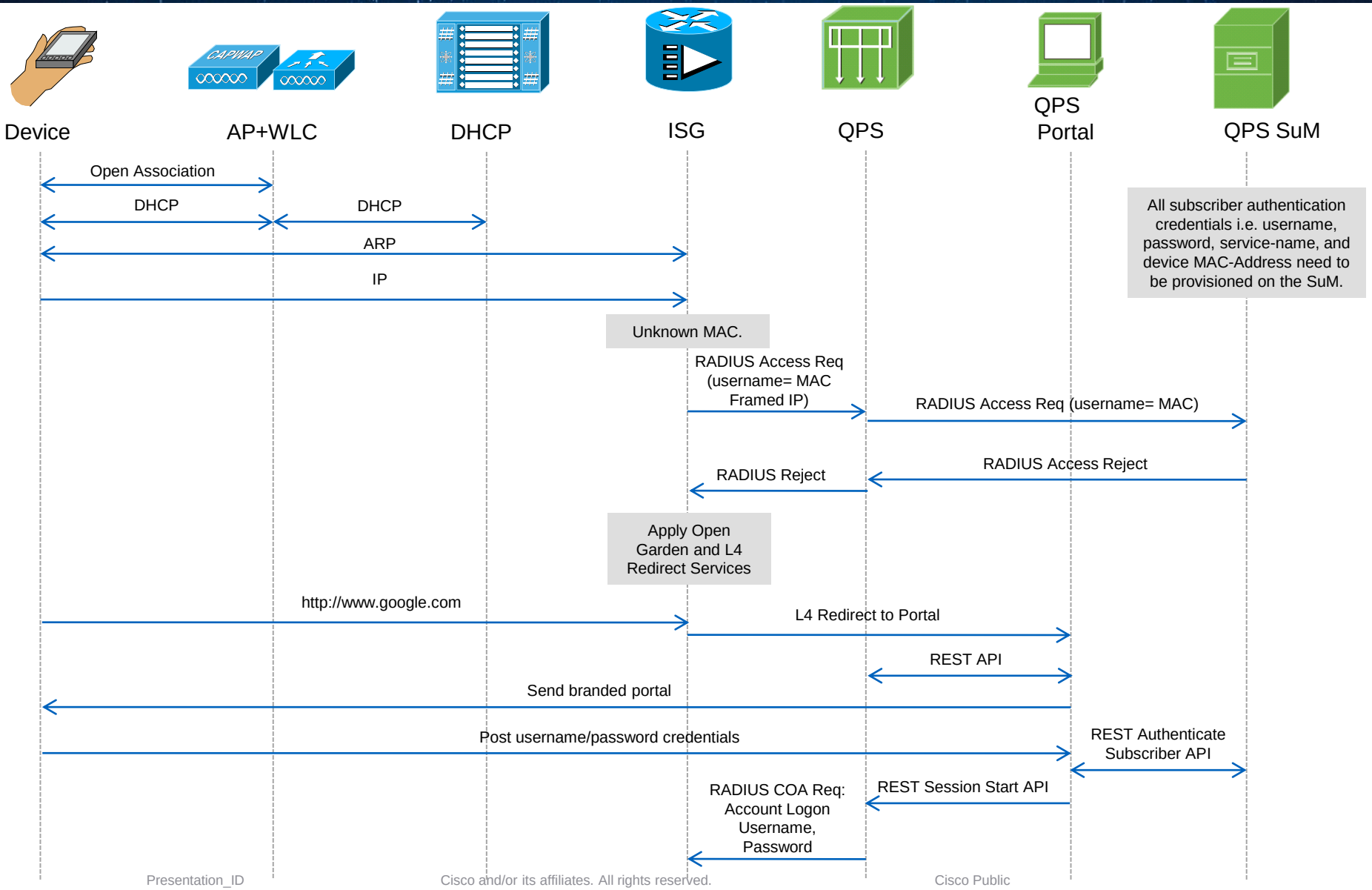
MAC TAL Authentication



Cisco and/or its affiliates. All rights reserved.

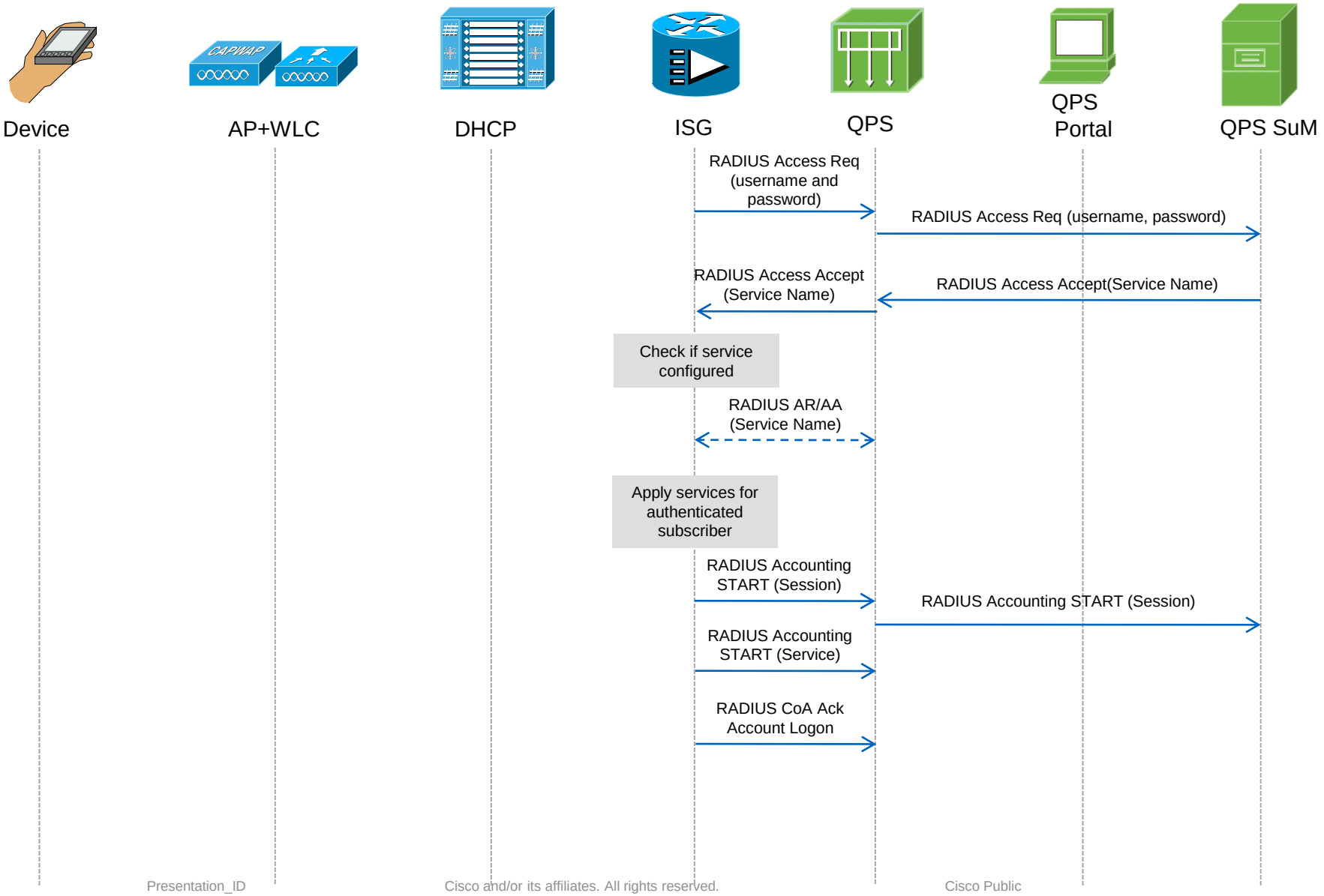
Local Breakout
using Web Authentication

Web Authentication following failed MAC-TAL (1/2)



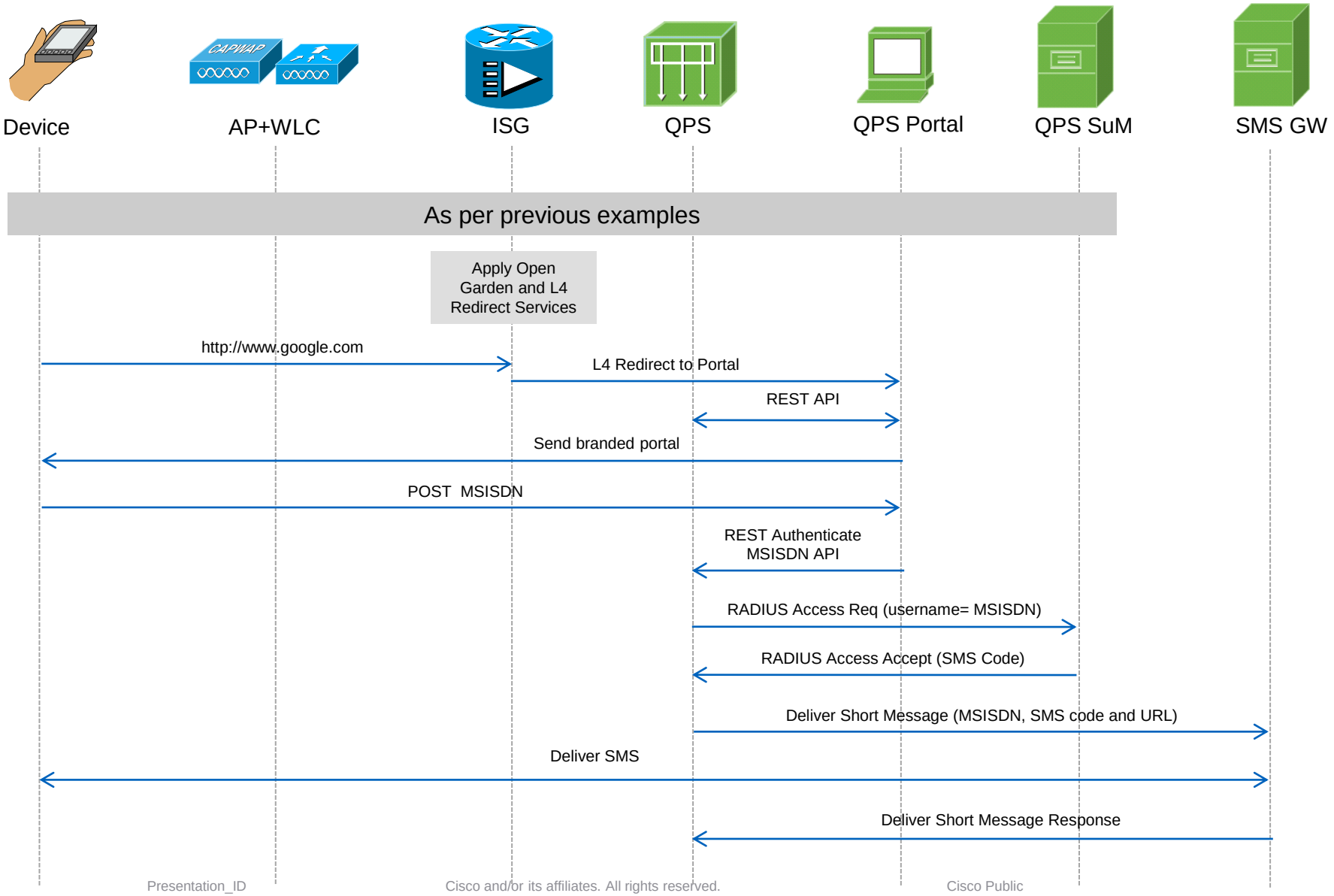
Cisco and/or its affiliates. All rights reserved.

Web Authentication following failed MAC-TAL (2/2)



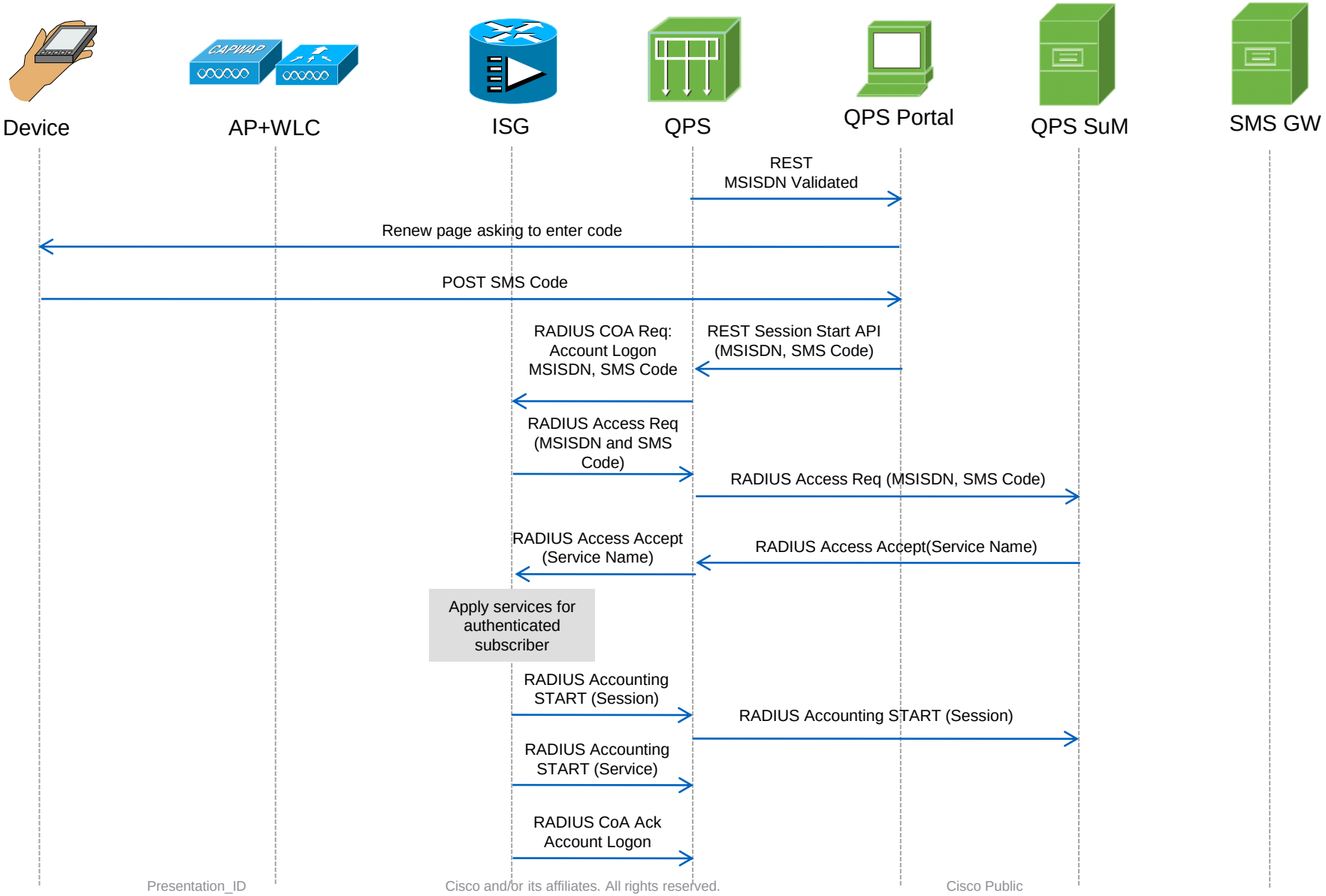
Cisco and/or its affiliates. All rights reserved.

Web Authentication with SMS delivery (1/2)



Cisco and/or its affiliates. All rights reserved.

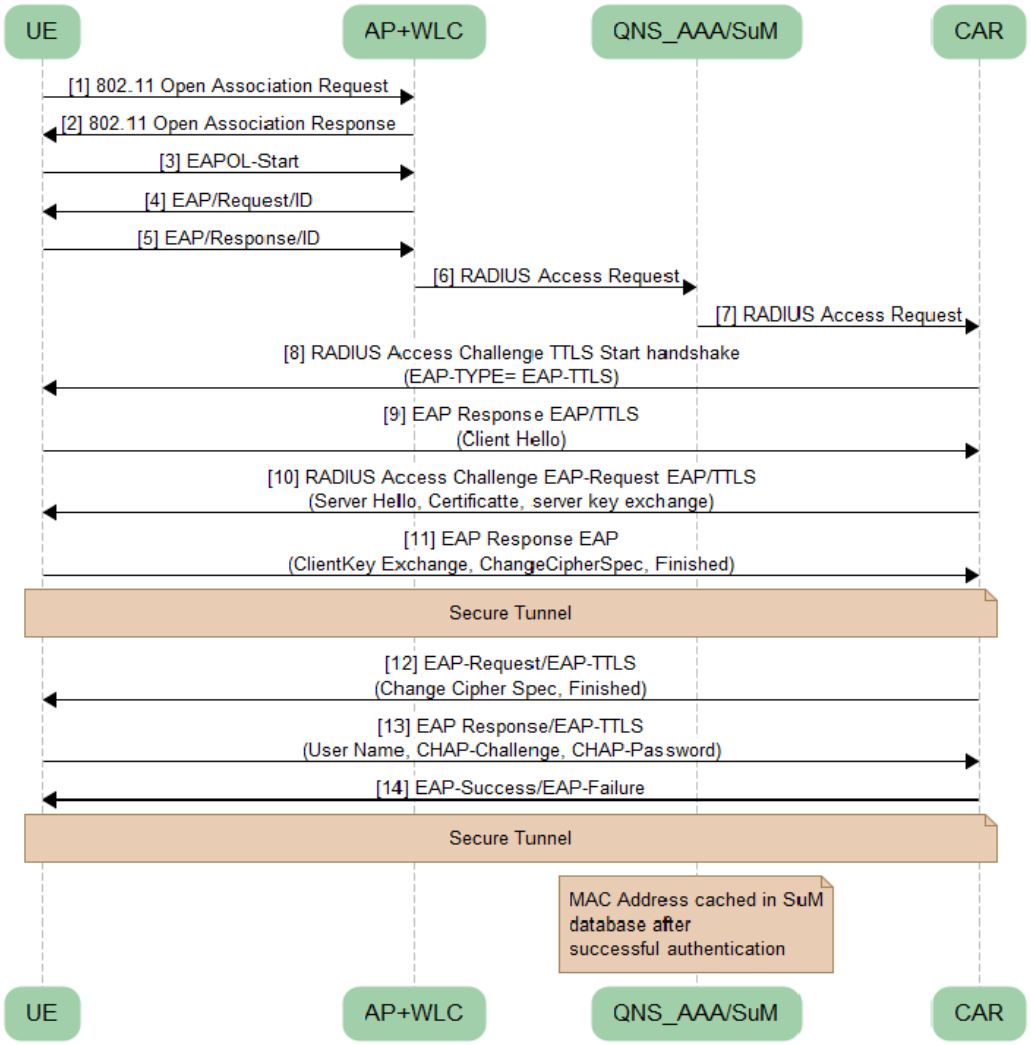
Web Authentication with SMS delivery (2/2)



Cisco and/or its affiliates. All rights reserved.

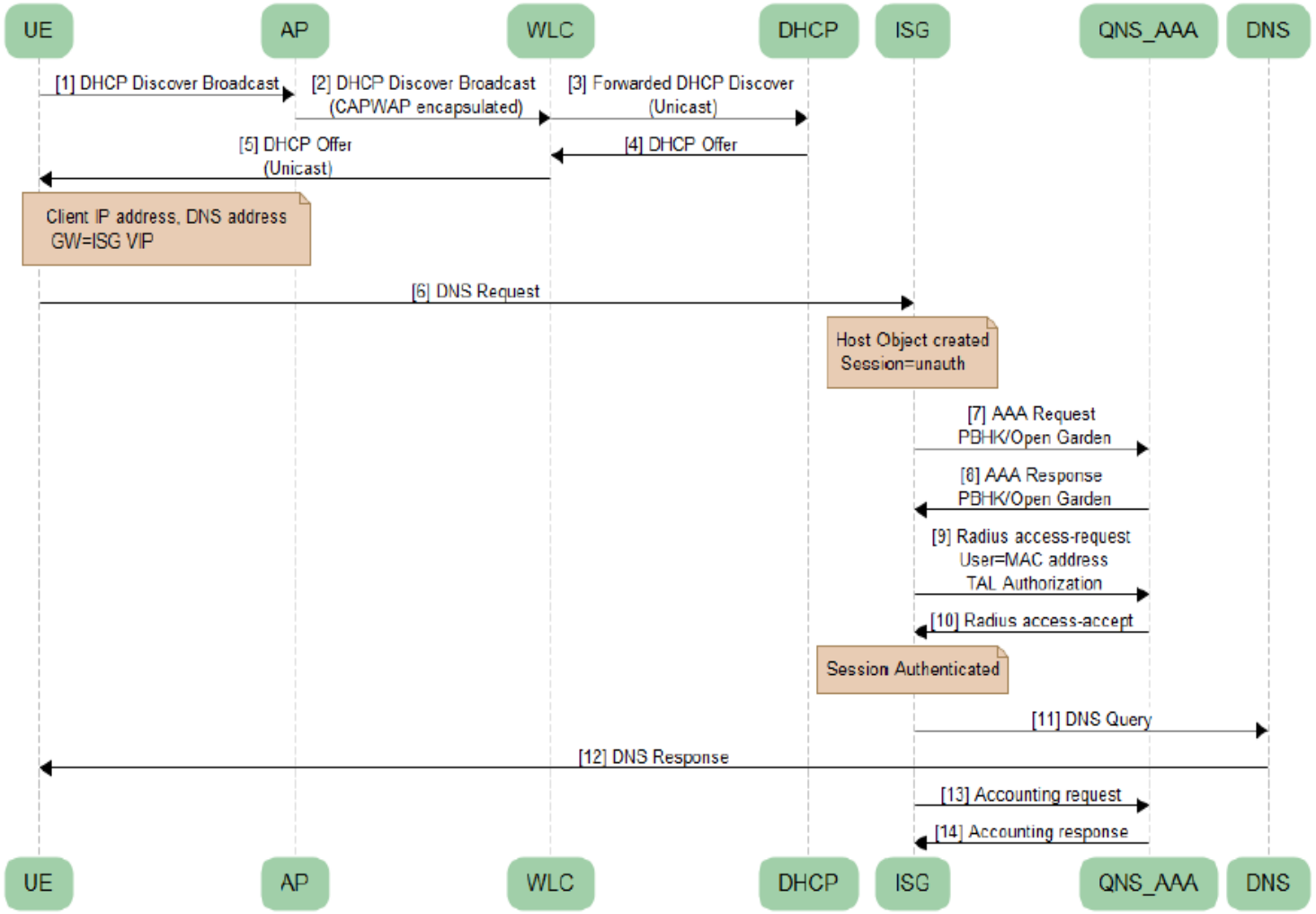
Local Breakout
using EAP Authentication

EAP-TTLS-based authentication (1/2)



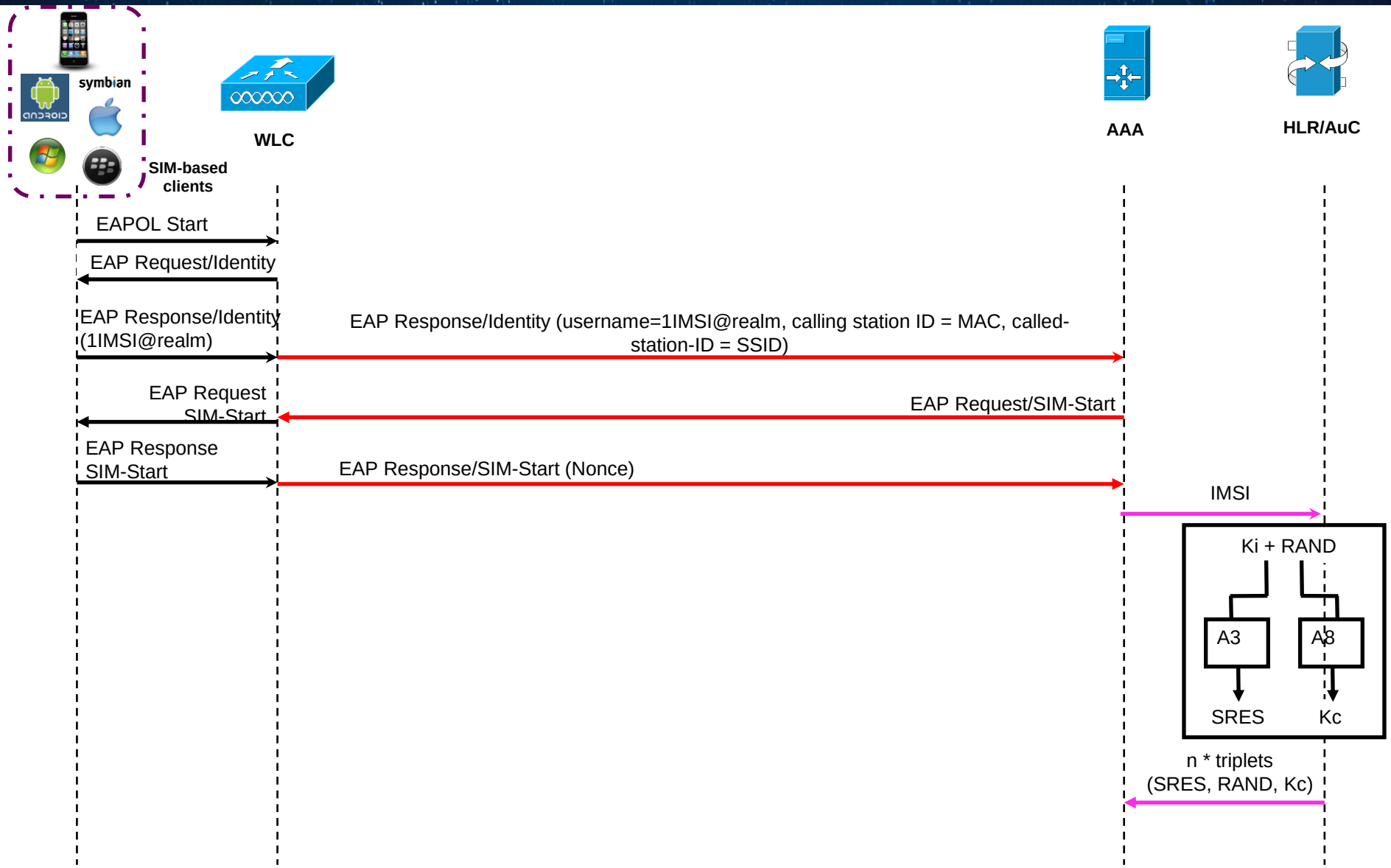
Cisco and/or its affiliates. All rights reserved.

EAP-TTLS-based authentication (2/2)



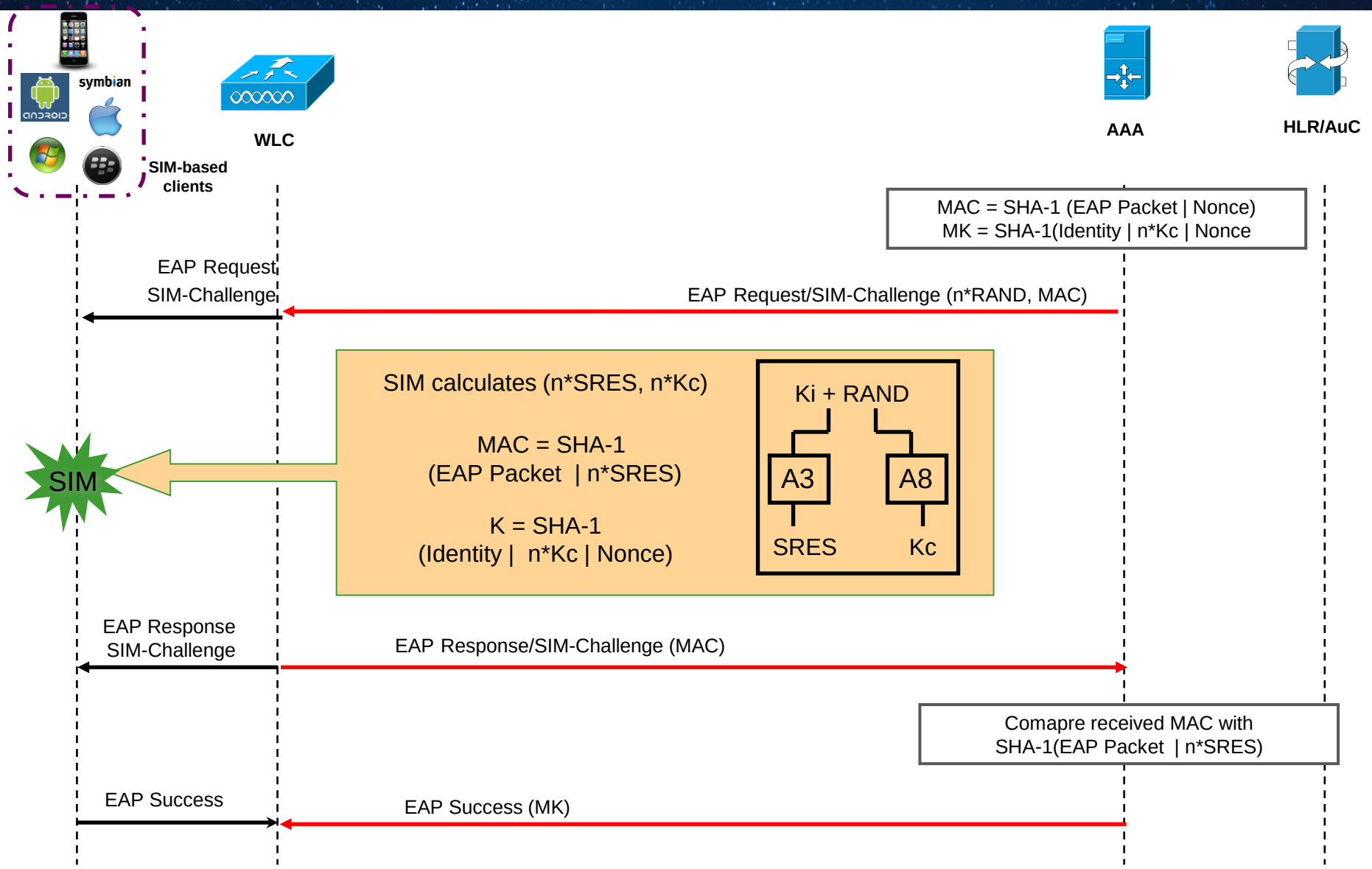
Cisco and/or its affiliates. All rights reserved.

EAP-SIM Call Flow (steps 1-3)



Cisco and/or its affiliates. All rights reserved.

EAP-SIM Call Flow (steps 4-6)



Cisco and/or its affiliates. All rights reserved.

Integration to Mobile Core
using intelligent Wireless Access Gateway
- iWAG

What is iWag

- Intelligent Wireless Access Gateway
- A transport/switching element with ISG Subscriber Awareness
- Radius-based Authentication and Accounting
- Policy-based subscriber routing for WiFi wholesale model
- Ethernet Access with PMIPv6 transport to 4G Mobile Core and with GTP transport to 3G Mobile Core
- Policy-based subscriber selective offload
- Provides a transparent access to WLAN users to connect to the 3G or 4G Mobile Packet Core without having any client application installed in the user-equipment(UE)

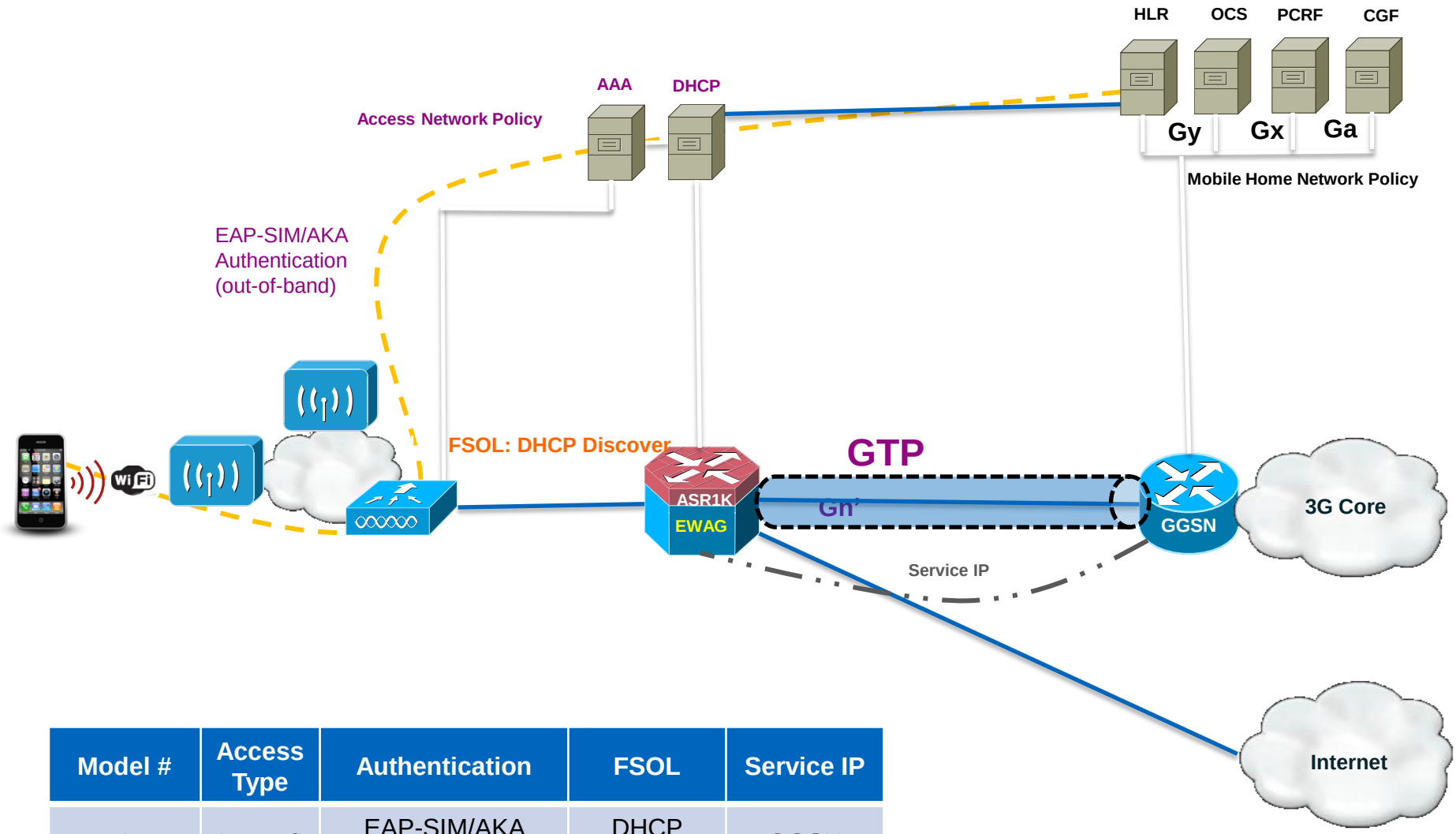
Cisco and/or its affiliates. All rights reserved.

iWAG models: Authentication and FSOL

No.	L2/L3 Access Method	ISG FSOL	Authentication
1	L2	DHCP Discover (Access-Request / EAP-Resp. done Out-of-Band)	EAP-SIM Out-of-band (EAP-SIM done via WLC to Mobile network, OOB from iWAG perspective)
2	L2	Radius Proxy (Access-Request/ EAP-Resp. done In-band to iWAG)/DHCP Discover	EAP-SIM In-band
3	L2	Unclassified MAC/DHCP Discover	Web Logon or TAL

Cisco and/or its affiliates. All rights reserved.

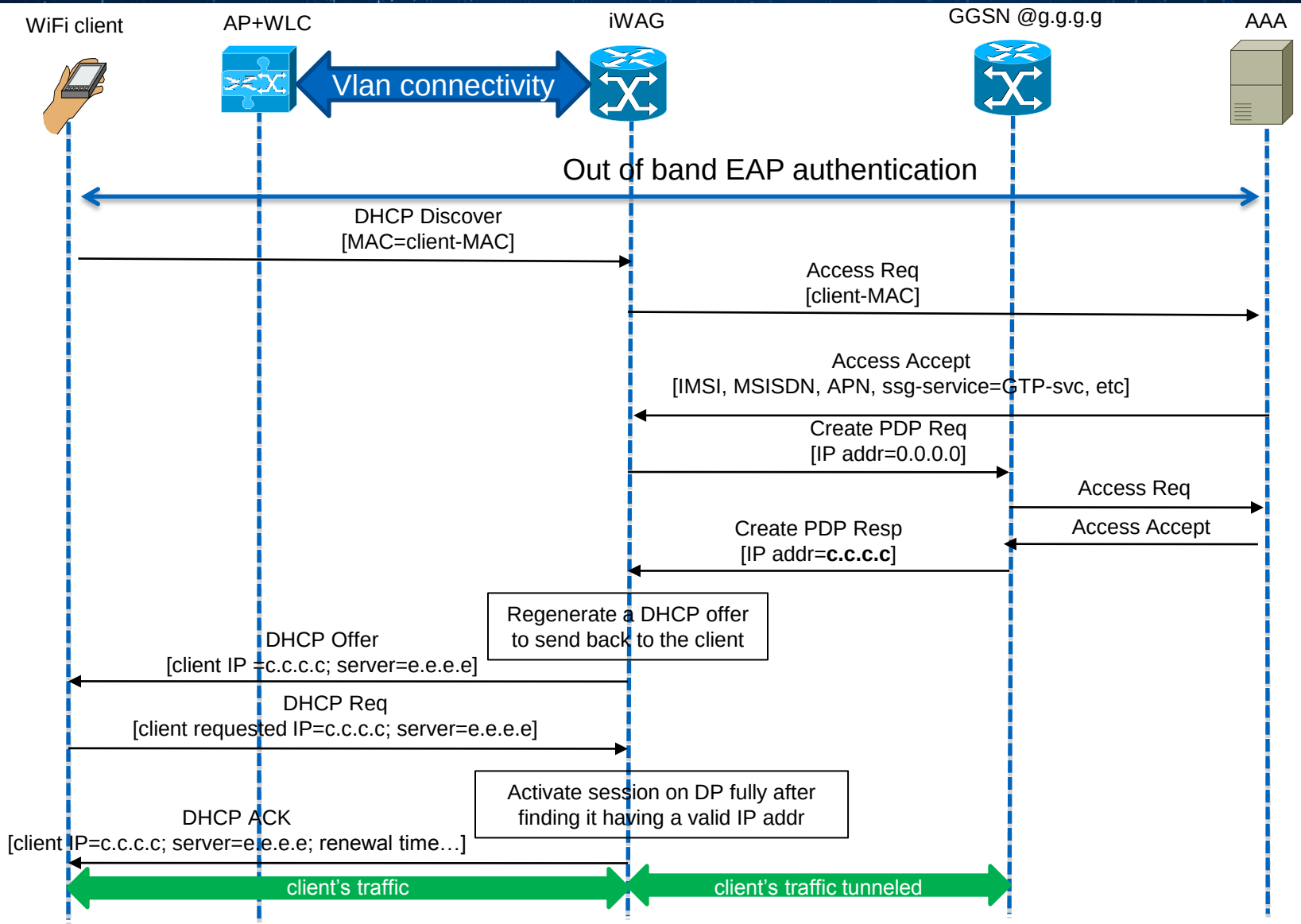
iWAG Deployment Model 1



Model #	Access Type	Authentication	FSOL	Service IP
1	Layer 2	EAP-SIM/AKA (out-of- band)	DHCP Discover	GGSN

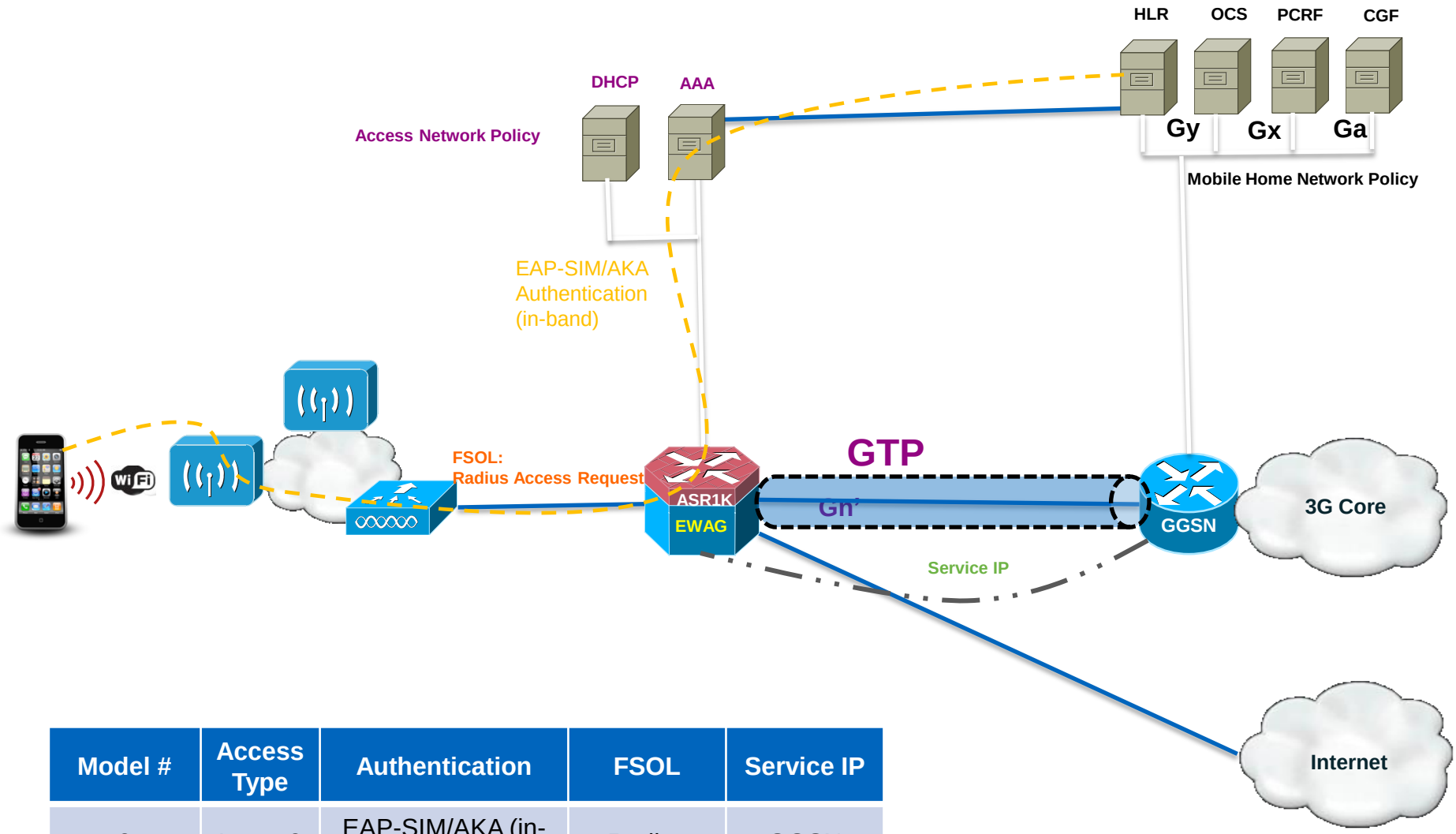
Cisco and/or its affiliates. All rights reserved.

Call Flow



Cisco and/or its affiliates. All rights reserved.

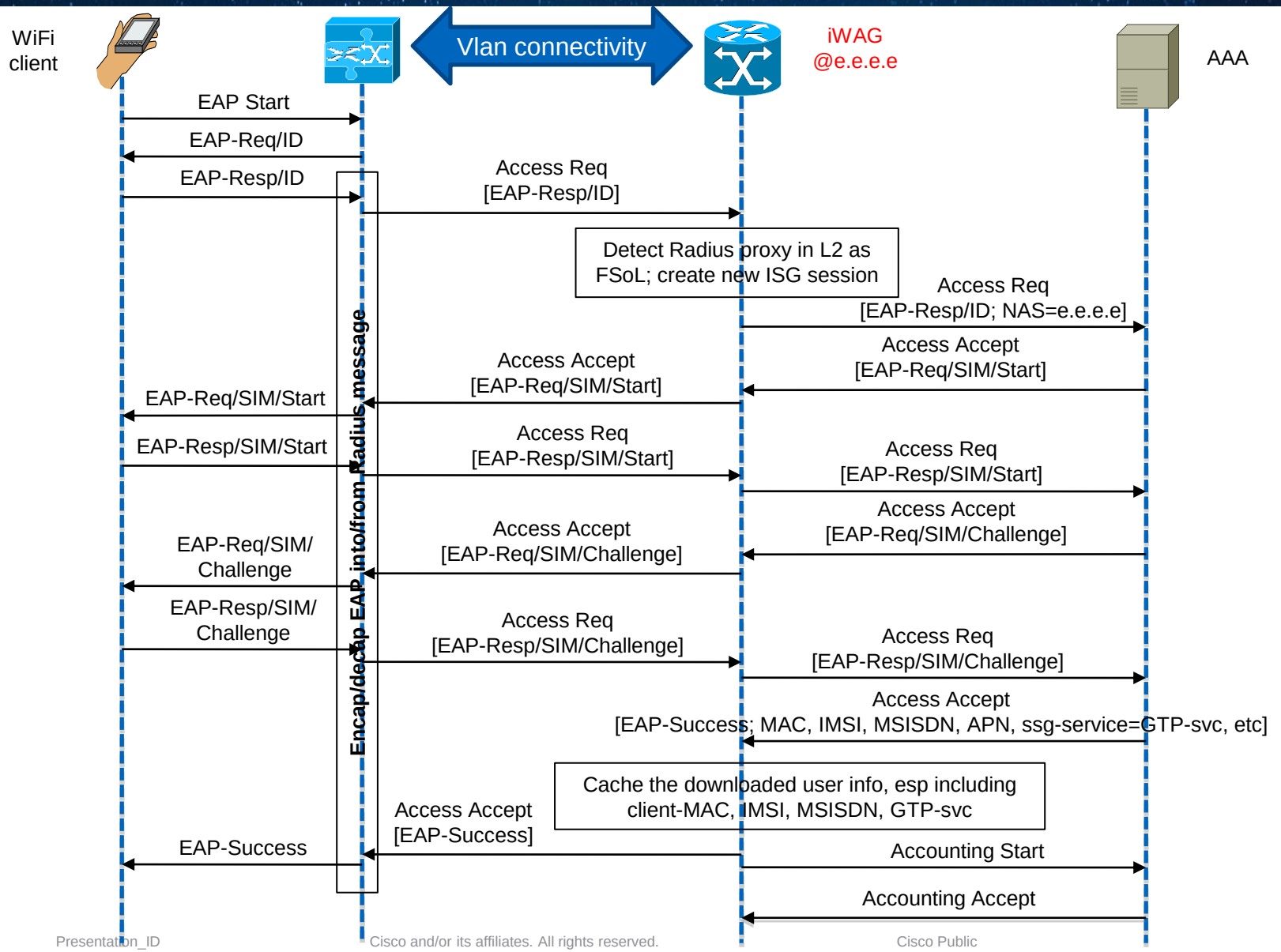
iWAG Deployment Model 2



Model #	Access Type	Authentication	FSOL	Service IP
2	Layer 2	EAP-SIM/AKA (in-band)	Radius	GGSN

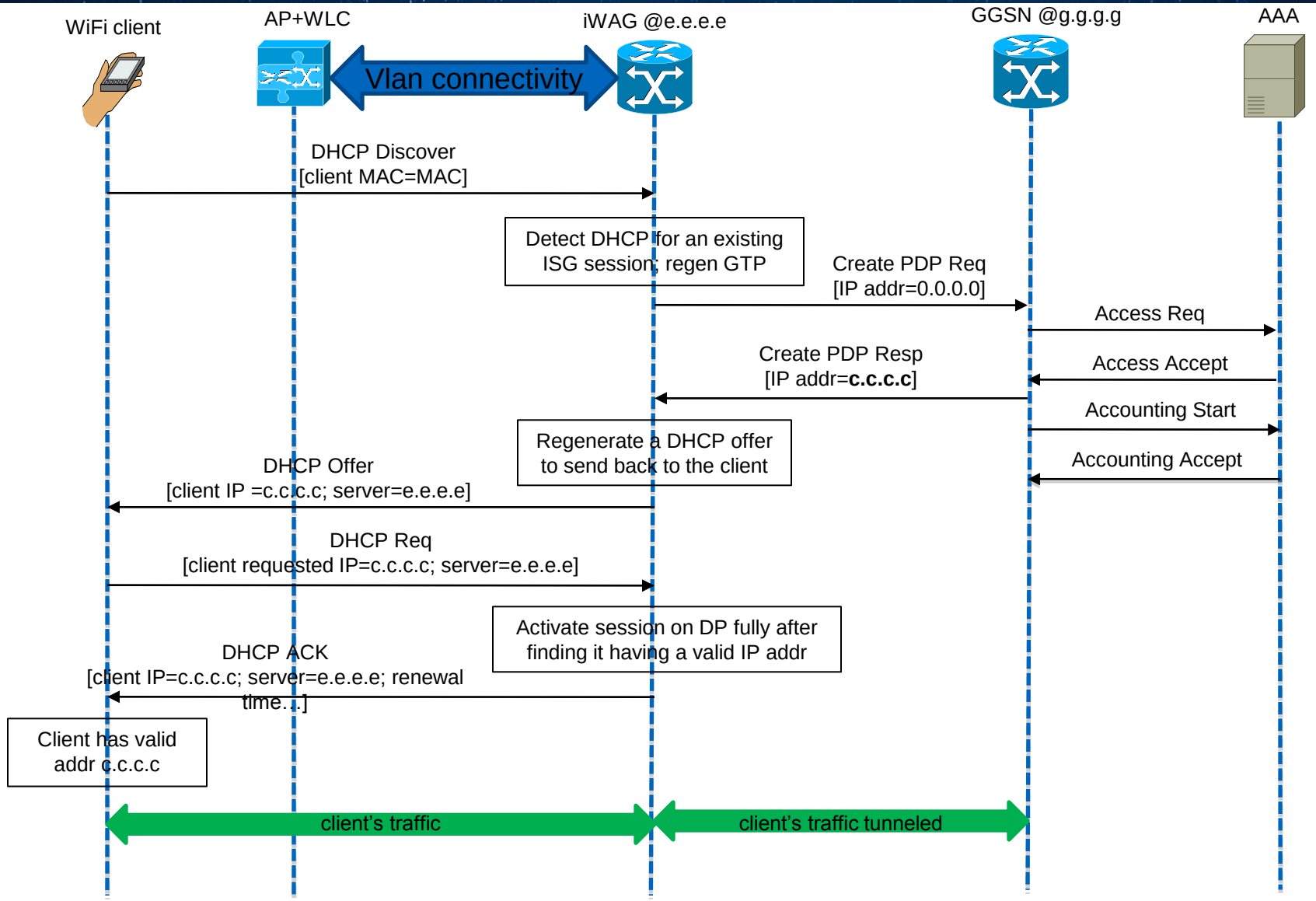
Cisco and/or its affiliates. All rights reserved.

Call flow (1/2)



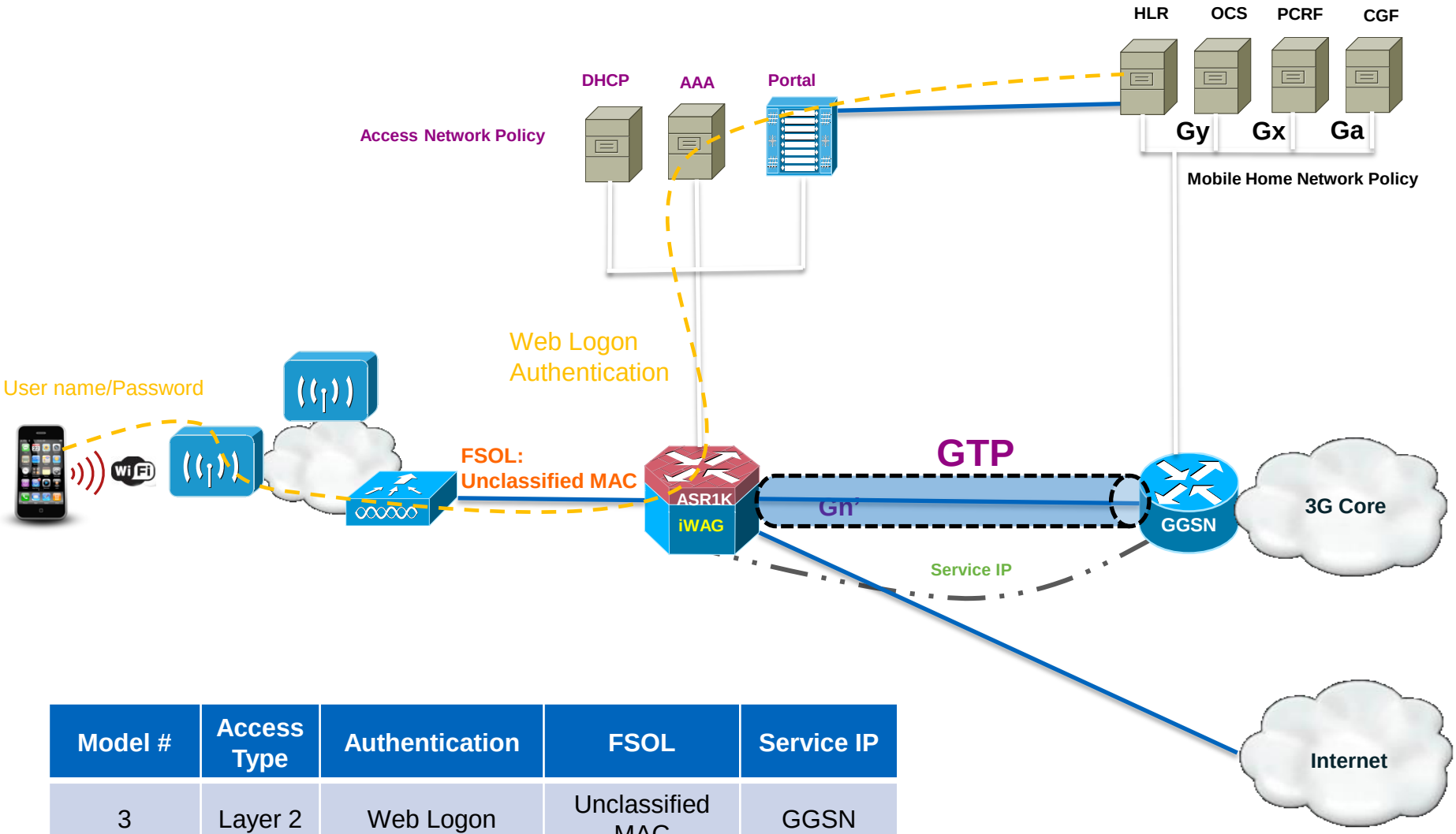
Cisco and/or its affiliates. All rights reserved.

Call flow (2/2)



Cisco and/or its affiliates. All rights reserved.

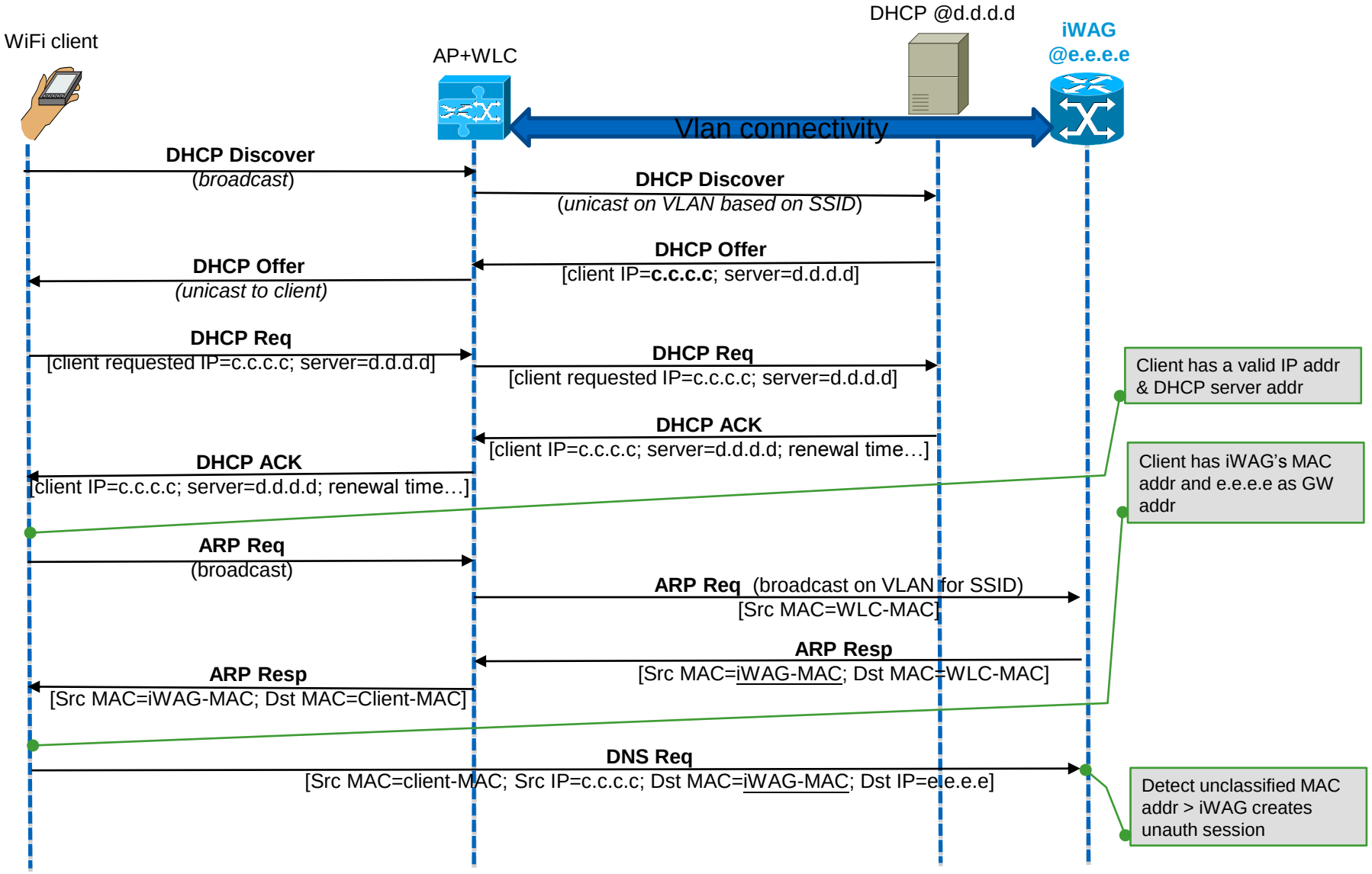
iWAG Deployment Model 3



Model #	Access Type	Authentication	FSOL	Service IP
3	Layer 2	Web Logon	Unclassified MAC	GGSN

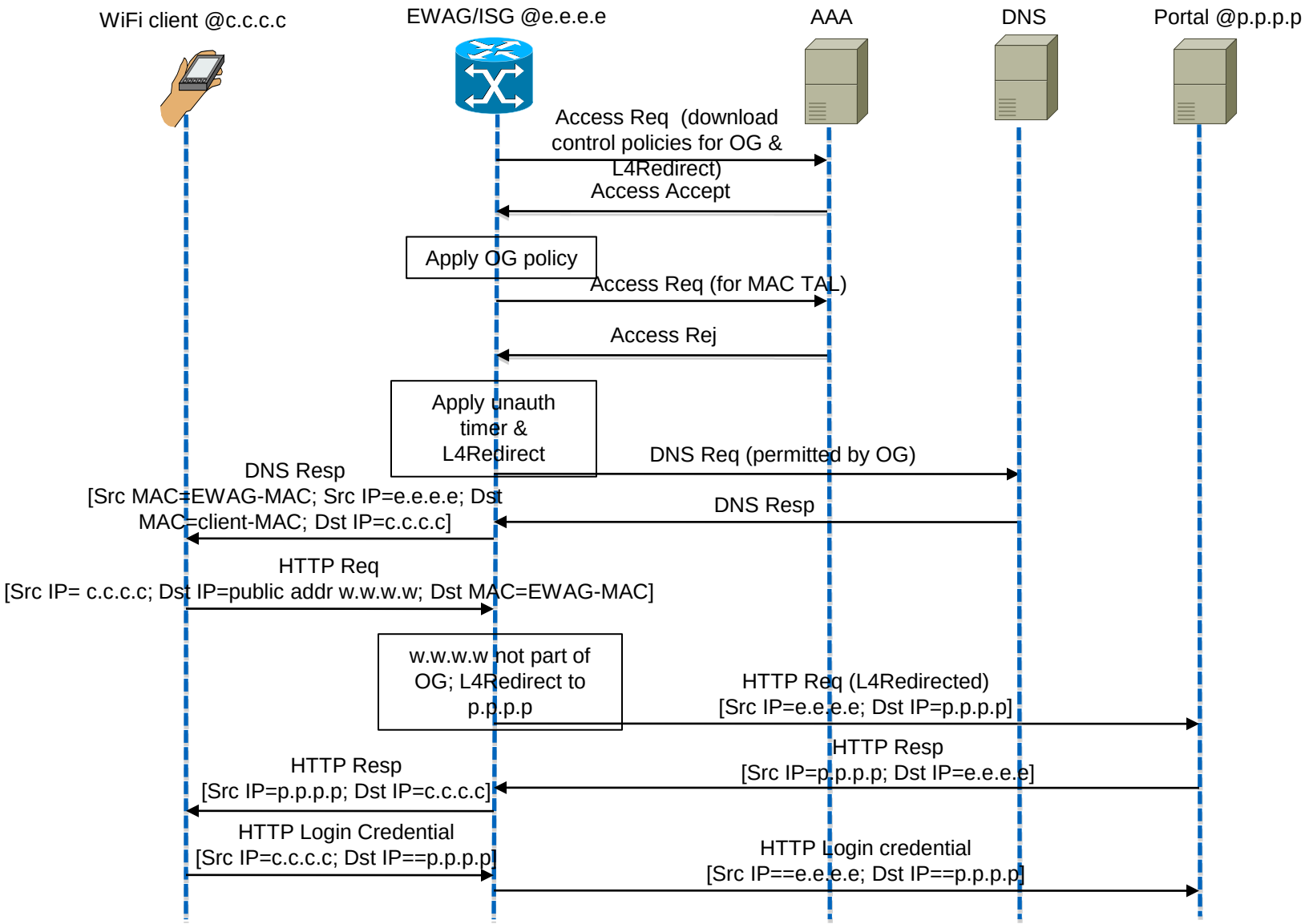
Cisco and/or its affiliates. All rights reserved.

Call flow (1/3)



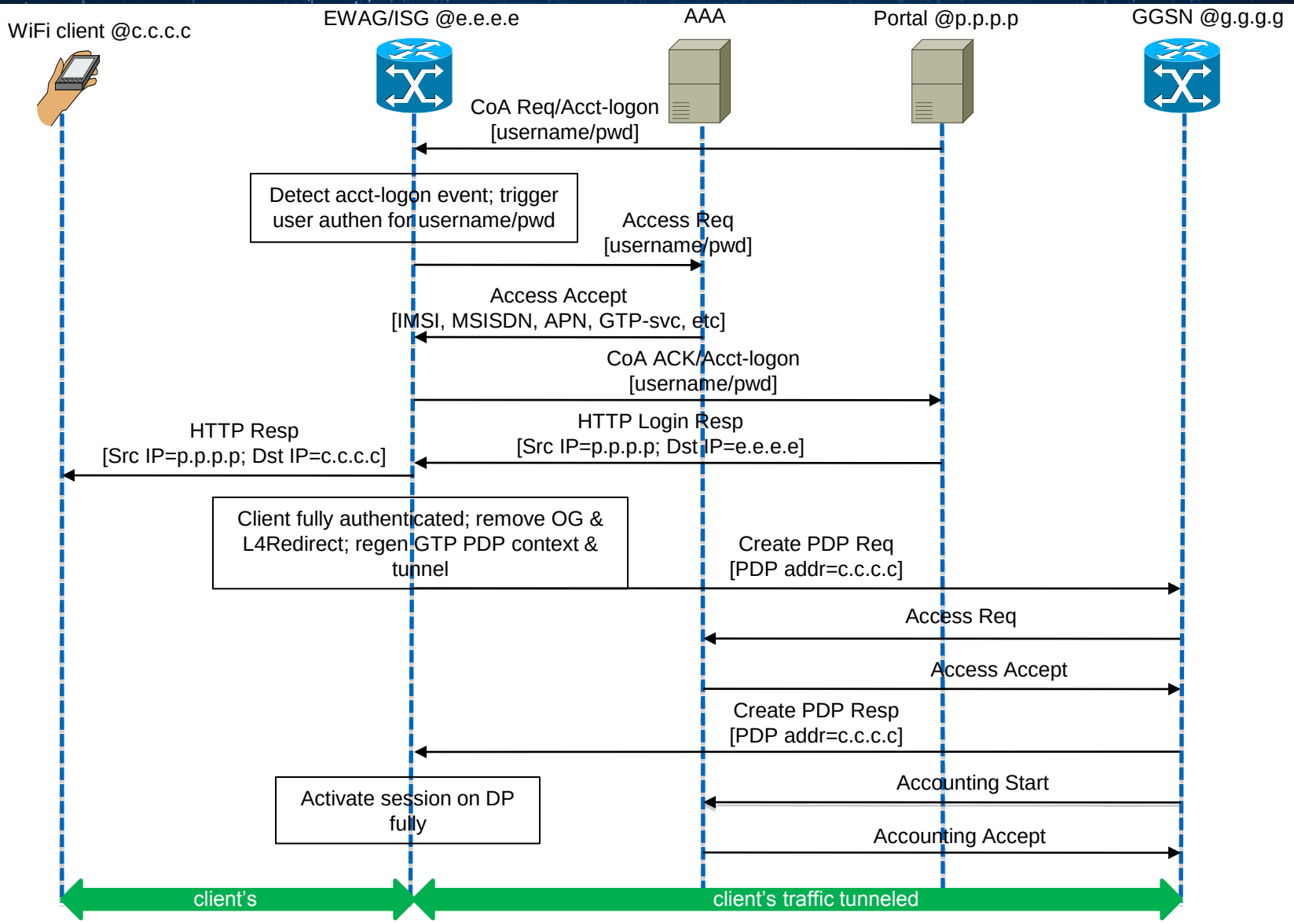
Cisco and/or its affiliates. All rights reserved.

Call flow (2/3)



Cisco and/or its affiliates. All rights reserved.

Call flow (3/3)



Cisco and/or its affiliates. All rights reserved.
Cisco Public

3G / 4G Mobile user Radius profiles

```
subscriber-profile gtp1 {
    access-accept {
     cisco-avpair { "cisco-mn-service=ipv4" }
     cisco-avpair { "cisco-mpc-protocol-interface=gtpv1" }
     cisco-avpair { "cisco-service-selection=cisco1.com" }
     cisco-avpair { "cisco-msisdn=49123456789" }
     3gpp {
          imsi 262020000000642
     }
    }
}
```

3G mobile user RADIUS profile *GTP based*

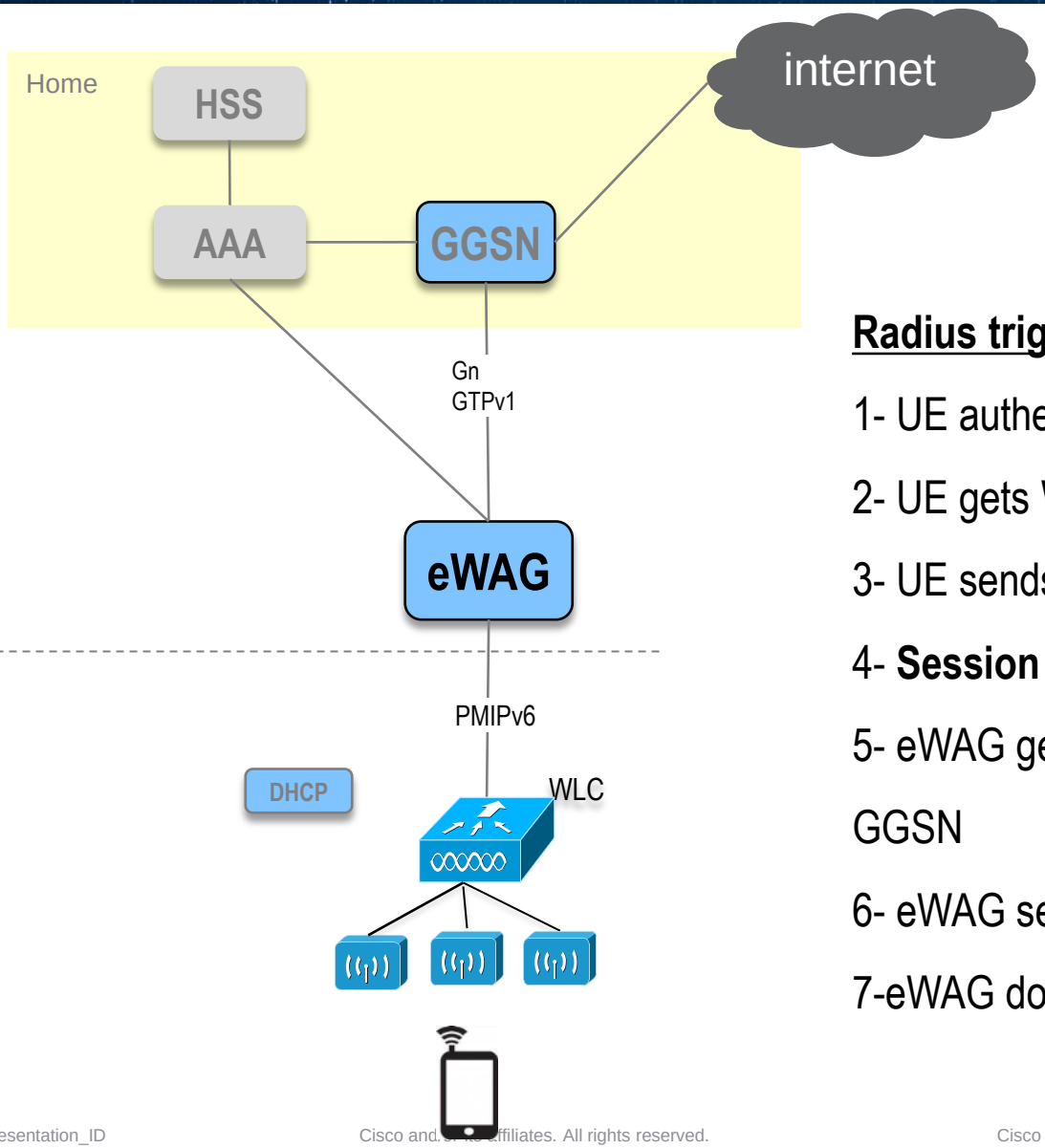
4G mobile user RADIUS profile *PMIPv6 based*

```
subscriber-profile pmip {
    access-accept {
    reply-msg "Default profile”
    cisco-avpair { "mn-service=ipv4" }
    cisco-avpair { "home-lma=LMA1" }
    cisco-avpair { "cisco-mpc-protocol-interface=pmipv6" }
    cisco-avpair { "home-lma-ipv6-address=9::2" }
    cisco-avpair { "cisco-downlink-gre-key=100" }
    cisco-avpair { "cisco-uplink-gre-key=100" }
    3gpp {
            mn-nai {
               username mn
               domain-name cisco.com
               start-at 1
            }
          }
    }
}
```


Cisco and/or its affiliates. All rights reserved.

Integration to Mobile Core
using enhanced Wireless Access Gateway
- eWAG

ReWAG



Radius triggered (ReWAG)

1- UE authenticated by AAA (EAP-SIM)

2- UE gets WiFi IP address from DHCP

3- UE sends Accounting start (radius)

4- **Session is triggered**

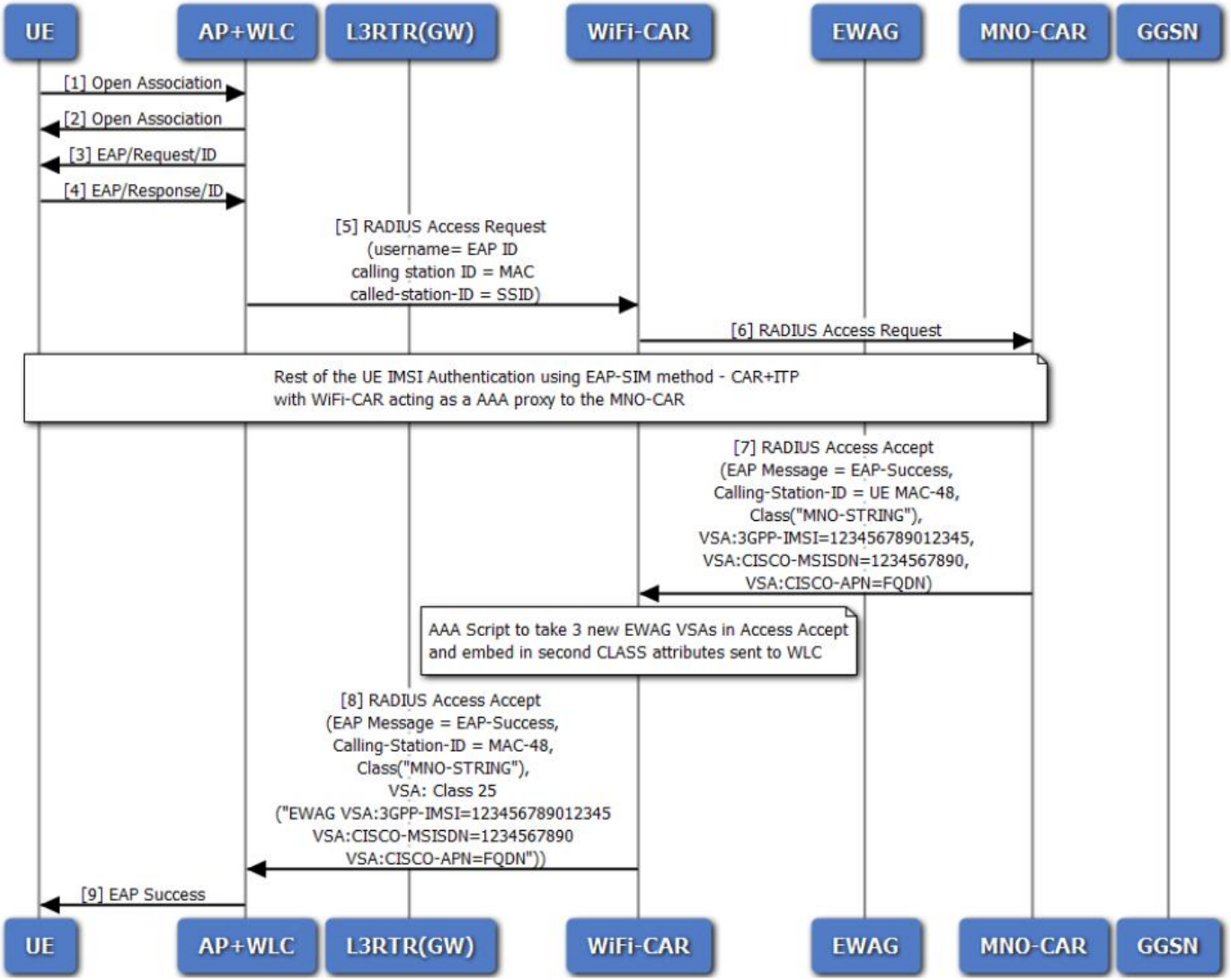
5- eWAG gets mobile IP address from GGSN

6- eWAG sets up tunnel

7-eWAG does NAT

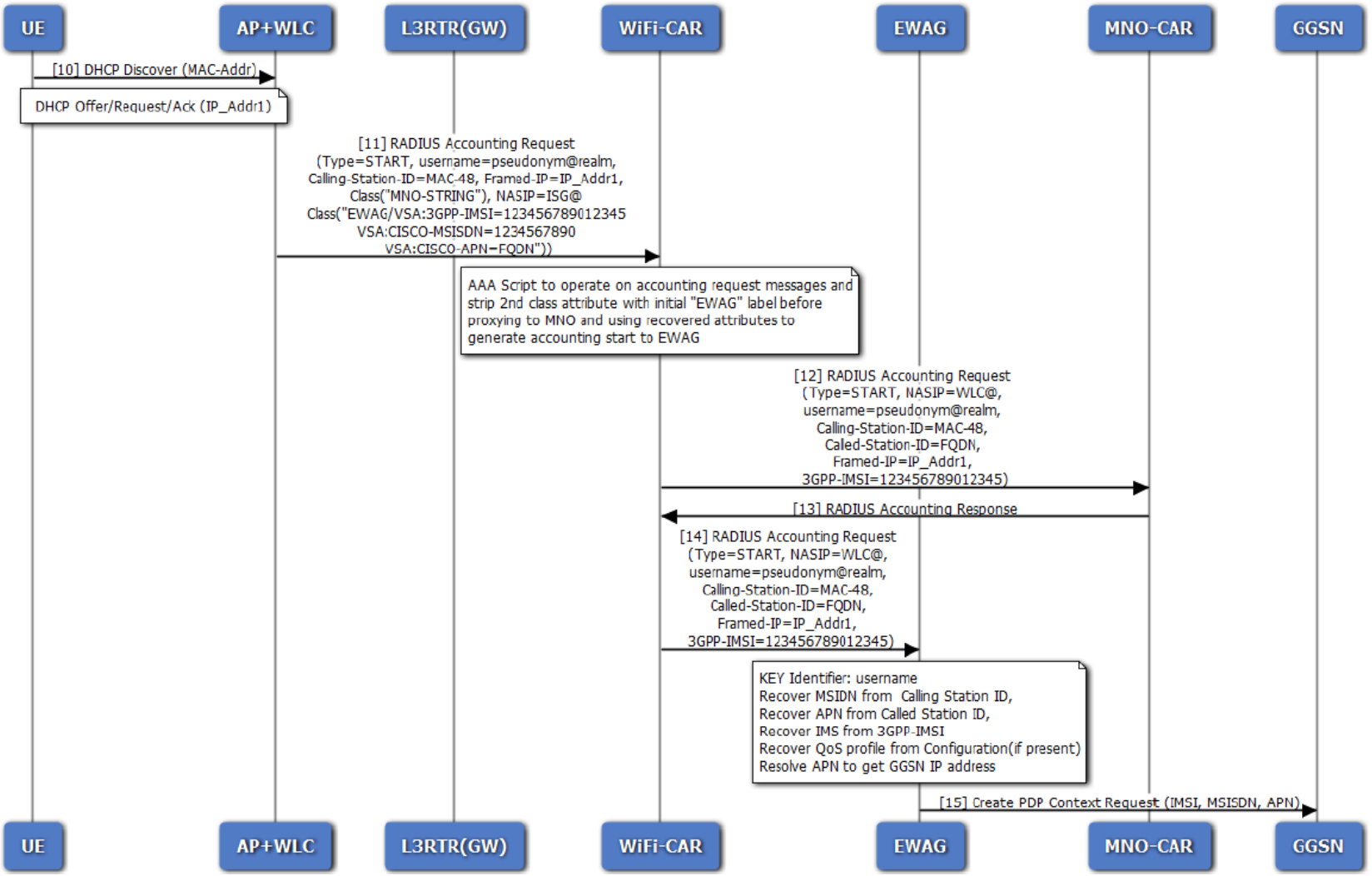
Cisco and/or its affiliates. All rights reserved.

Radius-based eWAG (ReWAG) w/o ISG 1/3



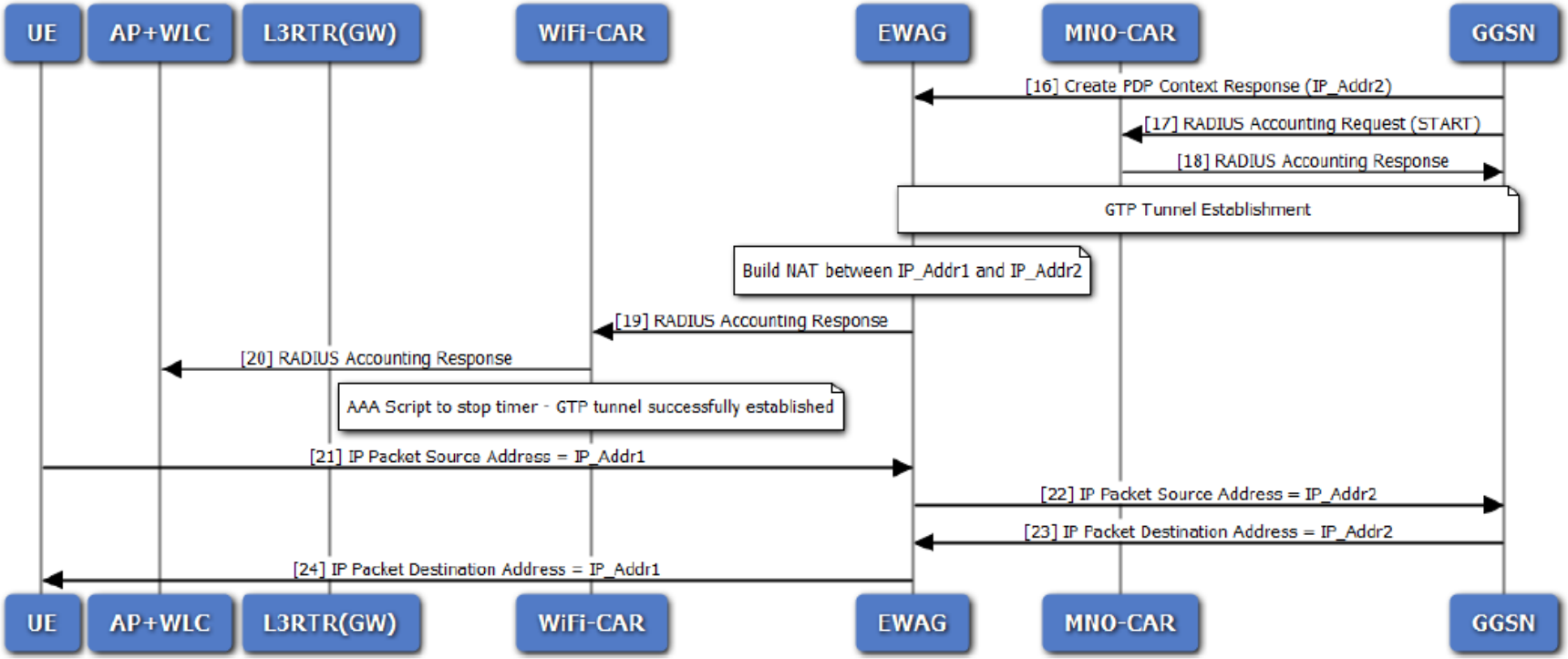
Cisco and/or its affiliates. All rights reserved.

Radius-based eWAG (ReWAG) w/o ISG 2/3



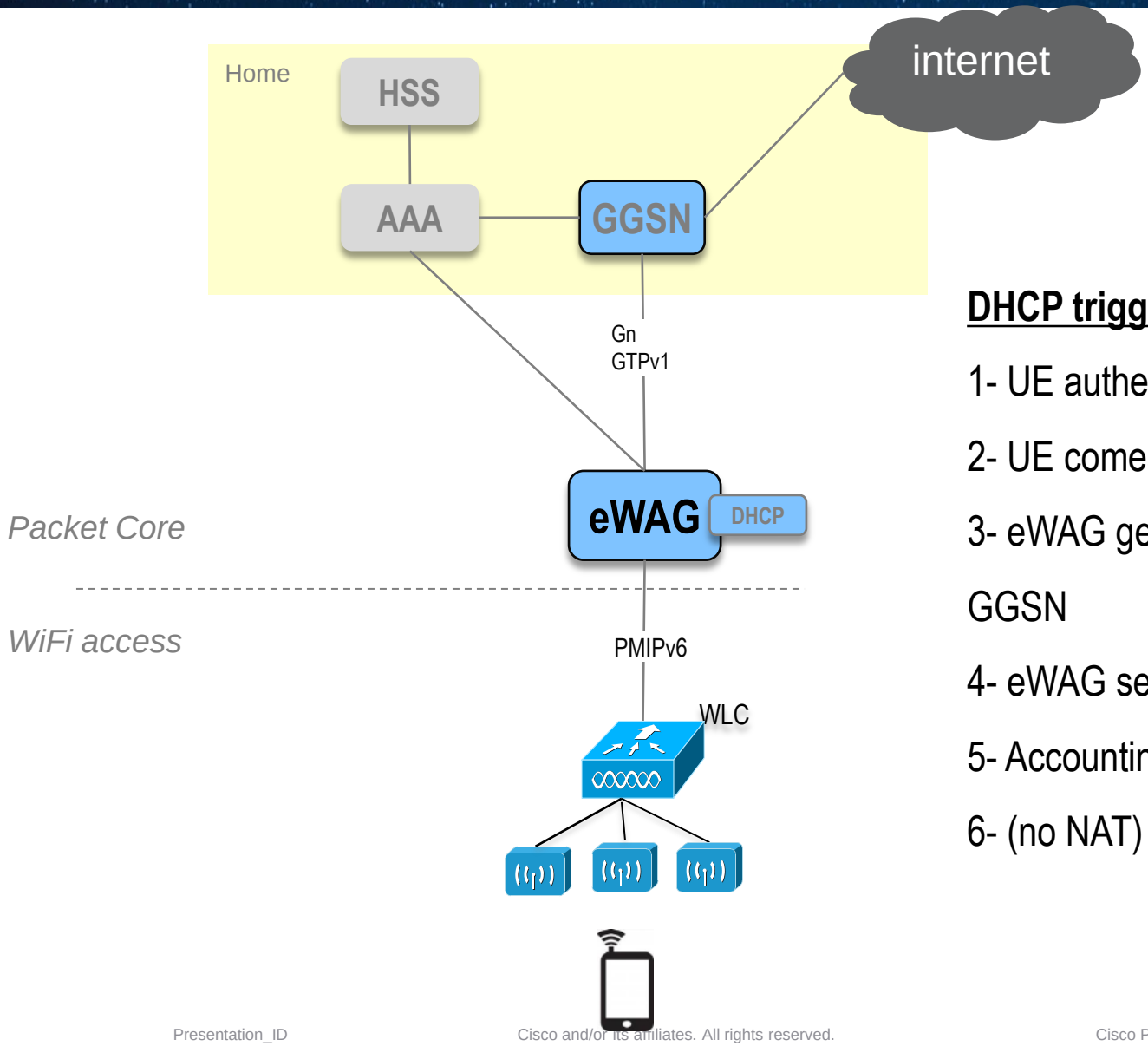
Cisco and/or its affiliates. All rights reserved.

Radius-based eWAG (ReWAG) w/o ISG 3/3



Cisco and/or its affiliates. All rights reserved.

DeWAG



DHCP triggered (DeWAG)

1- UE authenticated by AAA (EAP-SIM)

2- UE comes to eWAG for DHCP (VLAN)

3- eWAG gets mobile IP address from GGSN

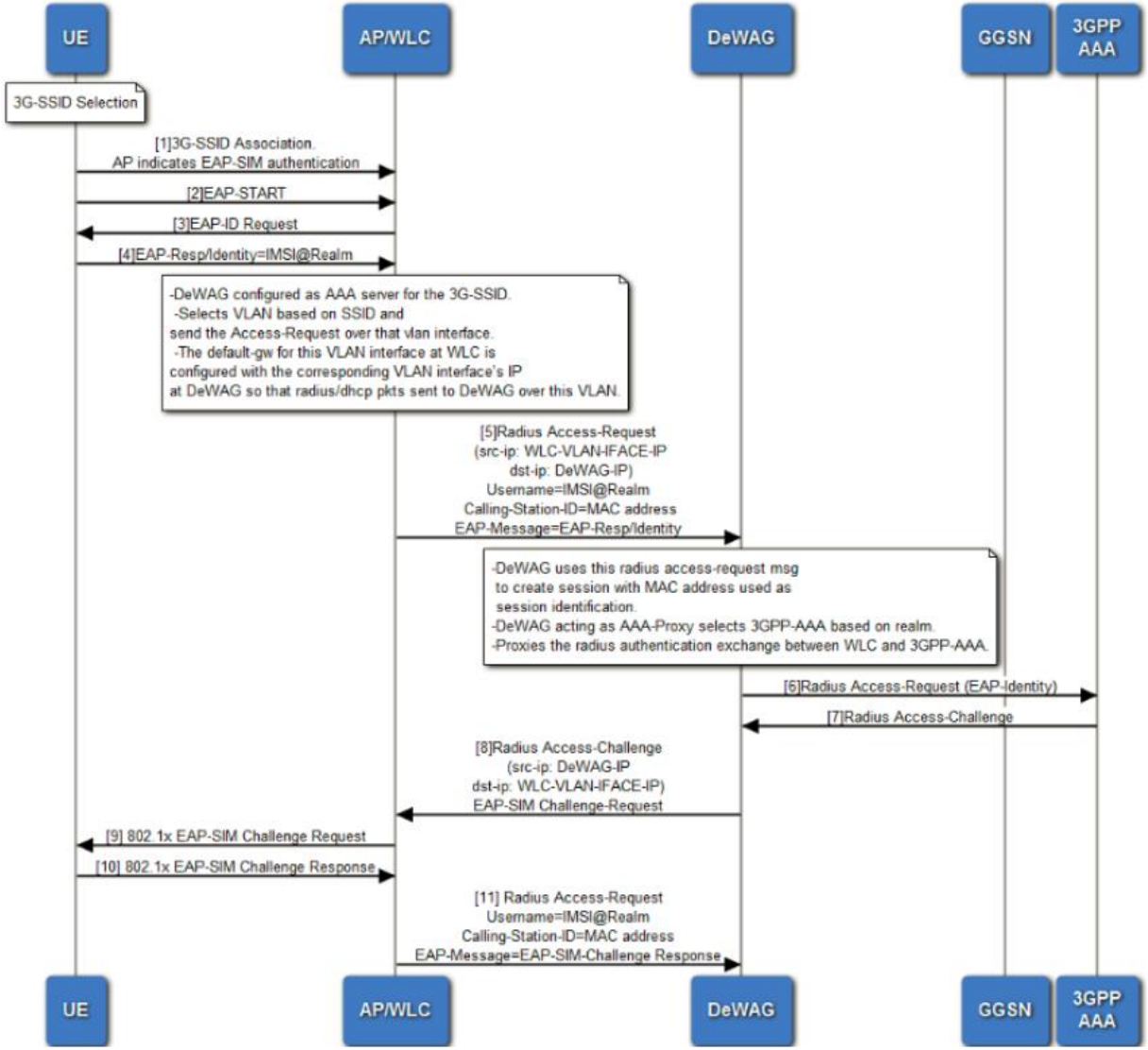
4- eWAG sets up tunnel

5- Accounting is started

6- (no NAT)

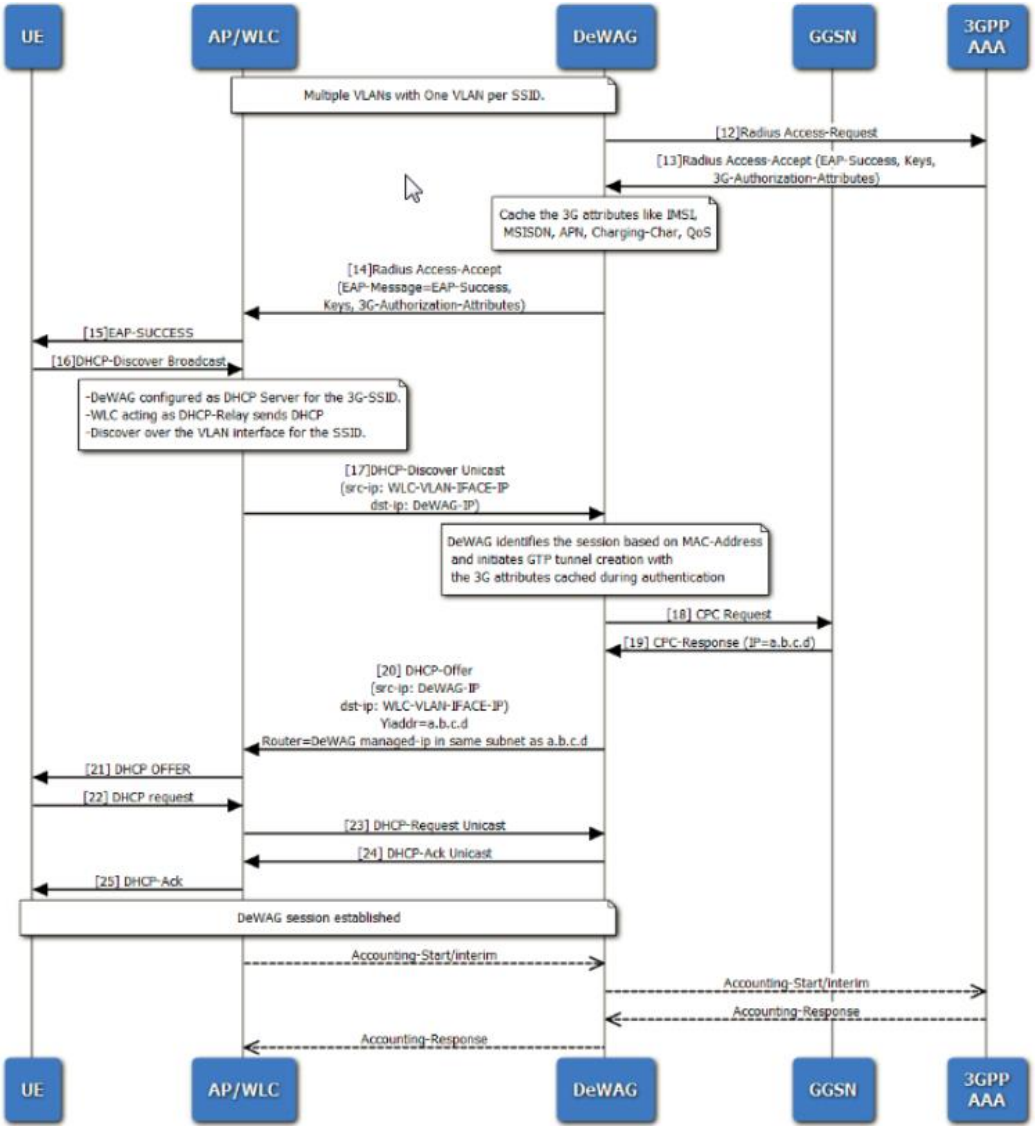
Cisco and/or its affiliates. All rights reserved.

DHCP-based eWAG (DeWAG) 1/3



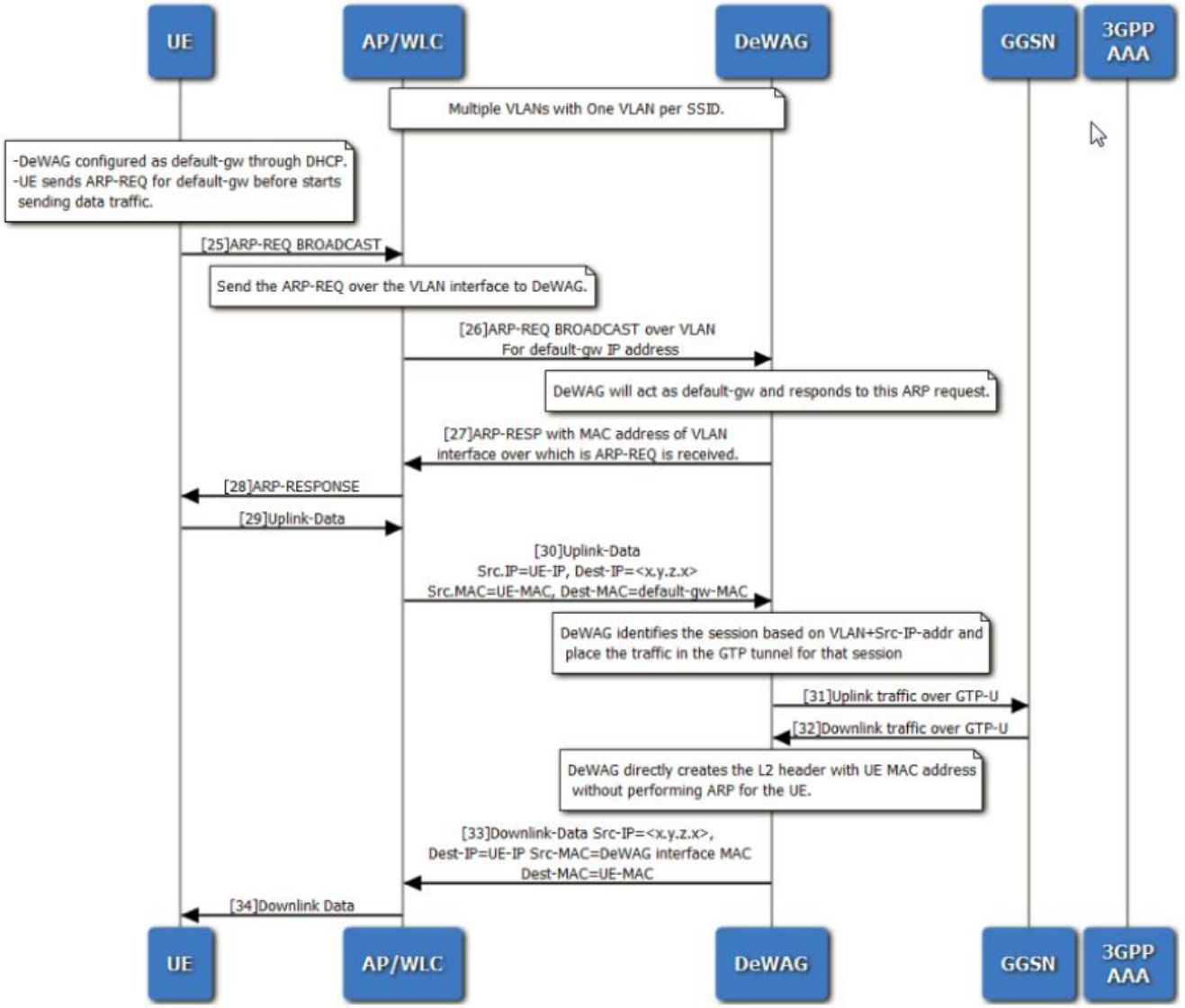
Cisco and/or its affiliates. All rights reserved.

DHCP-based eWAG (DeWAG) 2/3



Cisco and/or its affiliates. All rights reserved.

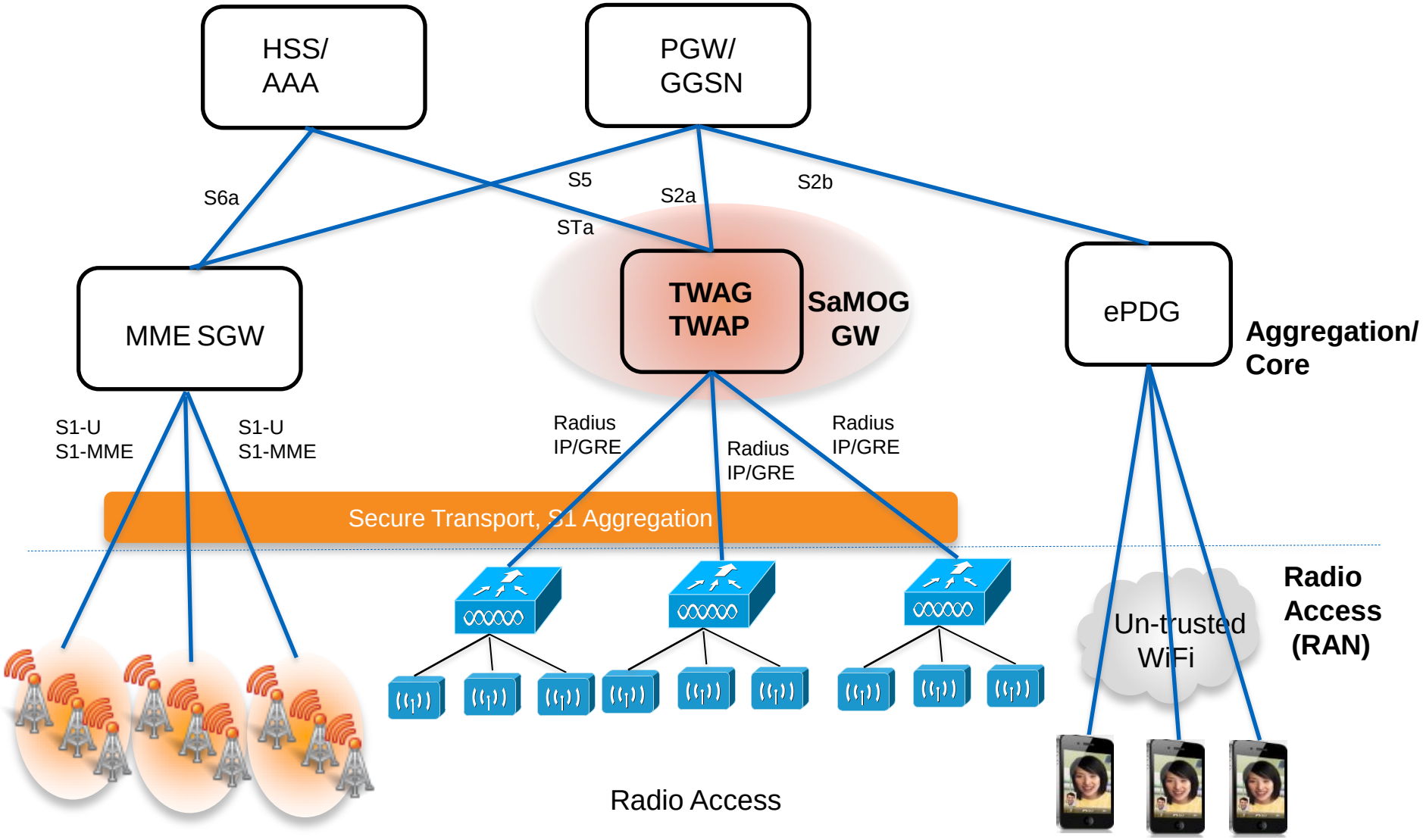
DHCP-based eWAG (DeWAG) 3/3



Cisco and/or its affiliates. All rights reserved.

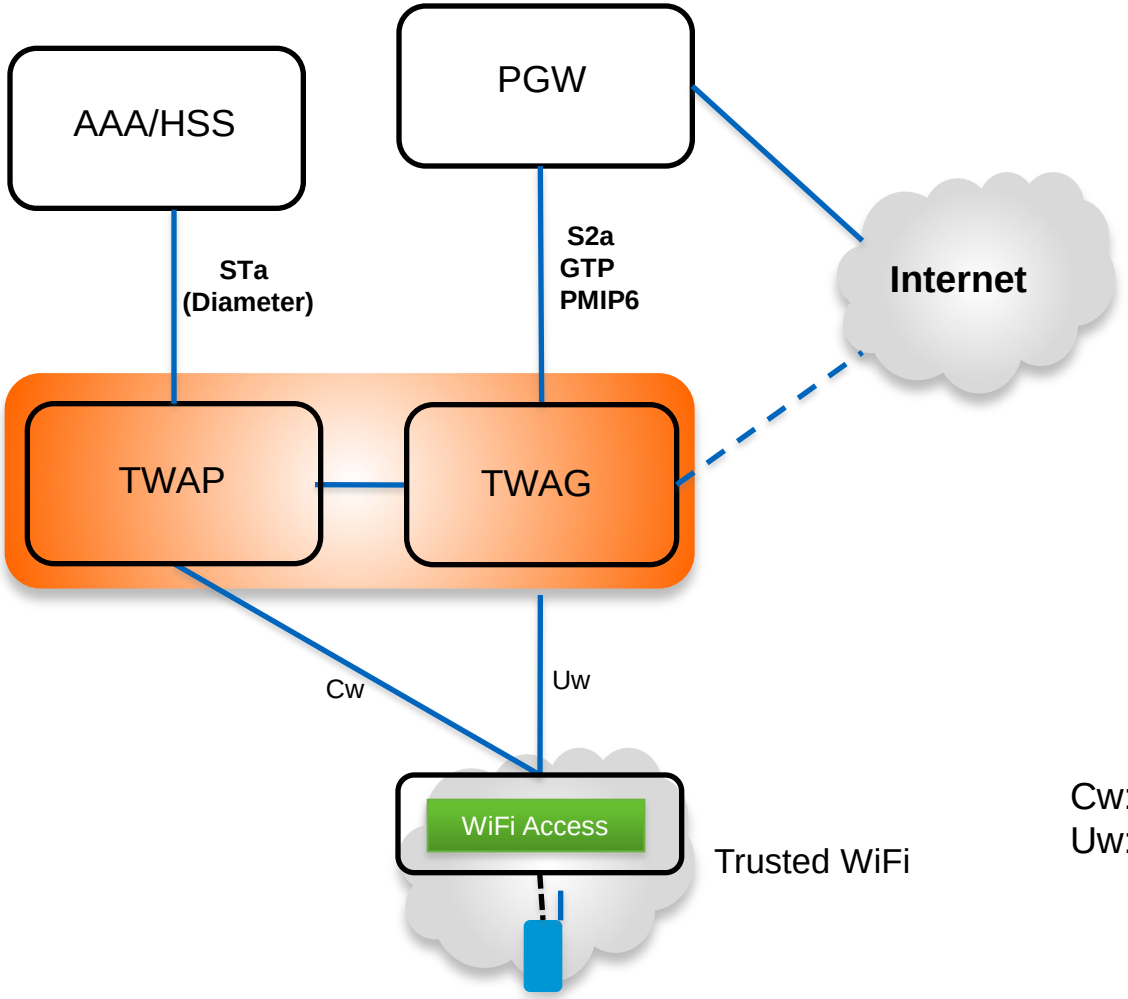
Integration to Mobile Core
using S2a Mobility Gateway
- SaMOG

EPC, Trusted wifi & Untrusted wifi Architecture



Cisco and/or its affiliates. All rights reserved.

3GPP SaMOG Functional Architecture



Cw: AAA Radius
Uw: Tunnel, native IP

Cisco and/or its affiliates. All rights reserved.

Trusted WLAN AAA Proxy (TWAP) Functions

- Relaying the AAA information between the WLAN Access Network and the 3GPP AAA Server
- Establishing Binding of UE IMSI with UE MAC address on the WLAN Access Network into (IMSI, MAC) tuple via snooping on the AAA protocol messages
- Detecting L2 Attach of UE to the WLAN Access Network via snooping on the AAA protocol for EAP-Success message
- Detecting L2 Detach of UE from the WLAN Access Network via snooping on the AAA protocol for Accounting-Request STOP message
- Informing the Trusted WLAN Access Gateway of WLAN Attach and Detach events for UE with (MAC, IMSI) tuple

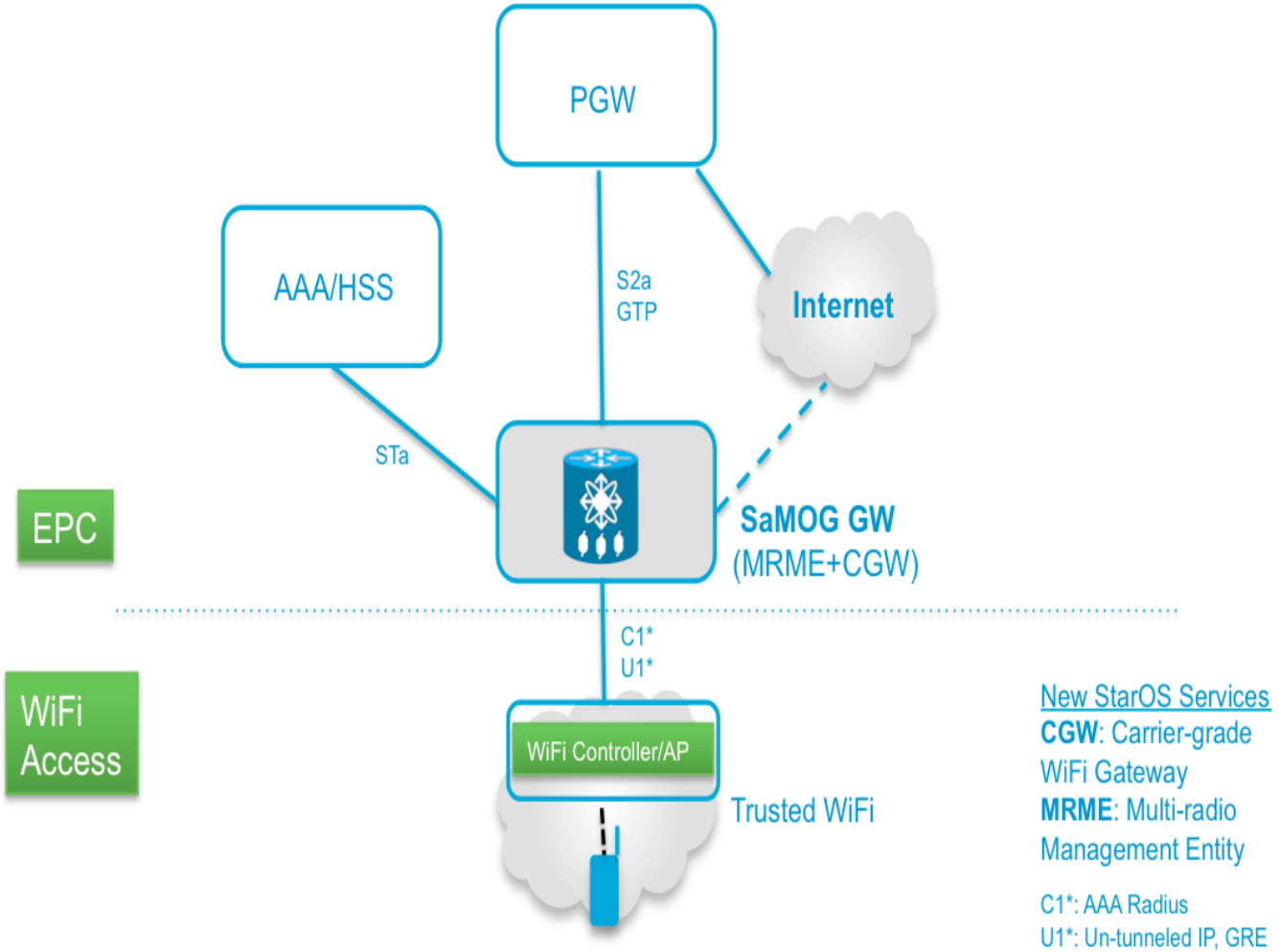
Cisco and/or its affiliates. All rights reserved.

Trusted WLAN Access Gateway

- For IPv4:
  - ✓ Default IPv4 router
  - ✓ Allocates the IP address received from P-GW to the UE (Direct or indirect)
- For IPv6:
  - ✓ Default IPv6 Router
  - ✓ Advertises the IPv6 prefix received from P-GW to UE (Direct or indirect)
- WLAN Access side connectivity
- S2a connectivity towards PGW
- Support for LBO in case of NSWO

Cisco and/or its affiliates. All rights reserved.

ASR5K based SaMOG GW (TWAG/TWAP)



Multi-Radio Management Entity (MRME)

- New StarOS service for access control and session management
- Basic Functions
  - Trusted WLAN AAA Proxy (**TWAP**)
  - EAP-AKA(’) over Radius termination (support EAP-SIM as well)
  - Diameter STa interface to 3GPP AAA Server
  - UE session management (Attach, Detach, Mobility)
- Enhanced functions (roadmap)
  - GW selection (for 3G, 4G users)
  - session continuity (Anchor PGW selection)
  - access admission control
  - Closed Subscriber Group support

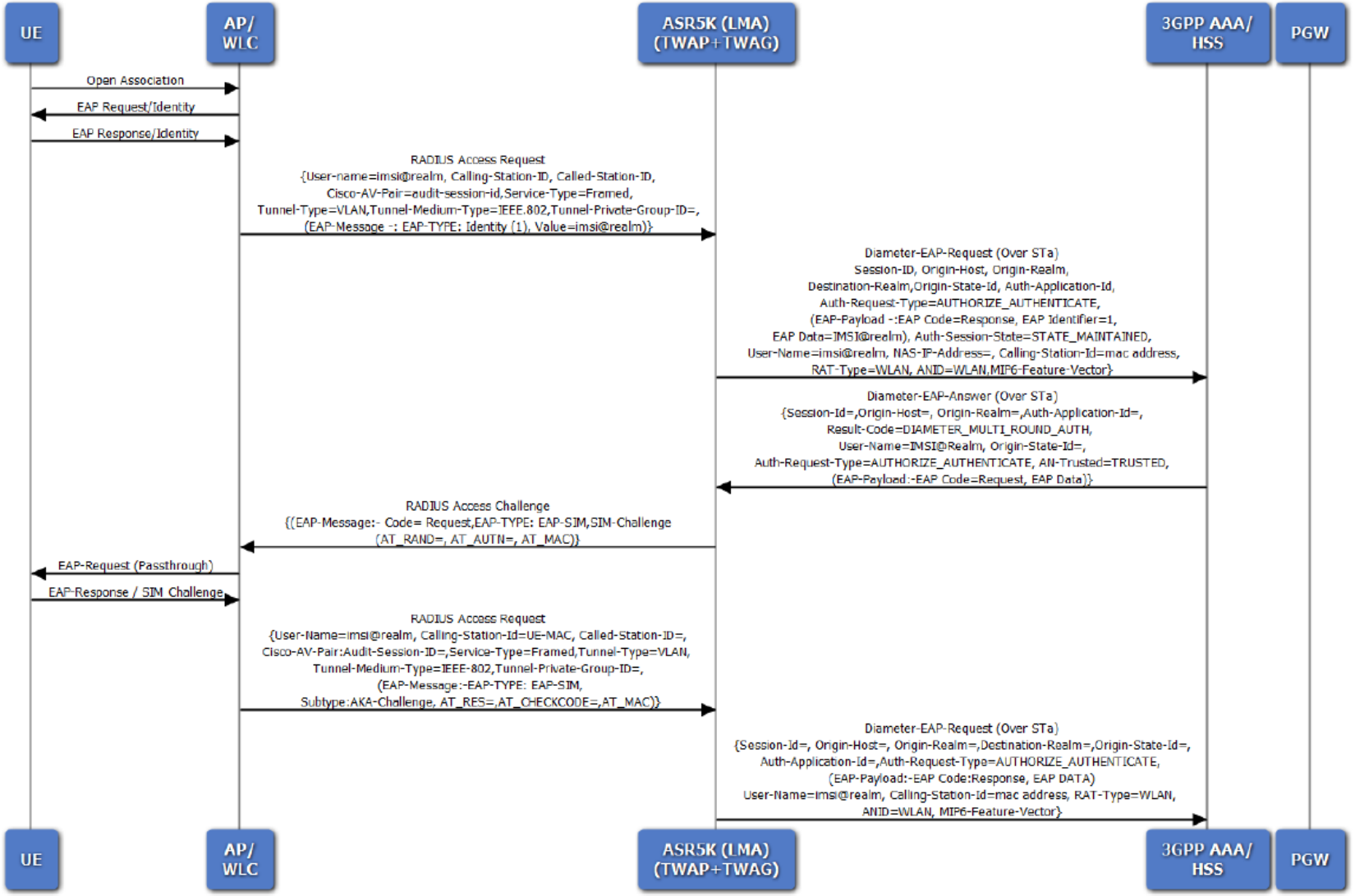
Cisco and/or its affiliates. All rights reserved.

Converged Access Gateway (CGW)

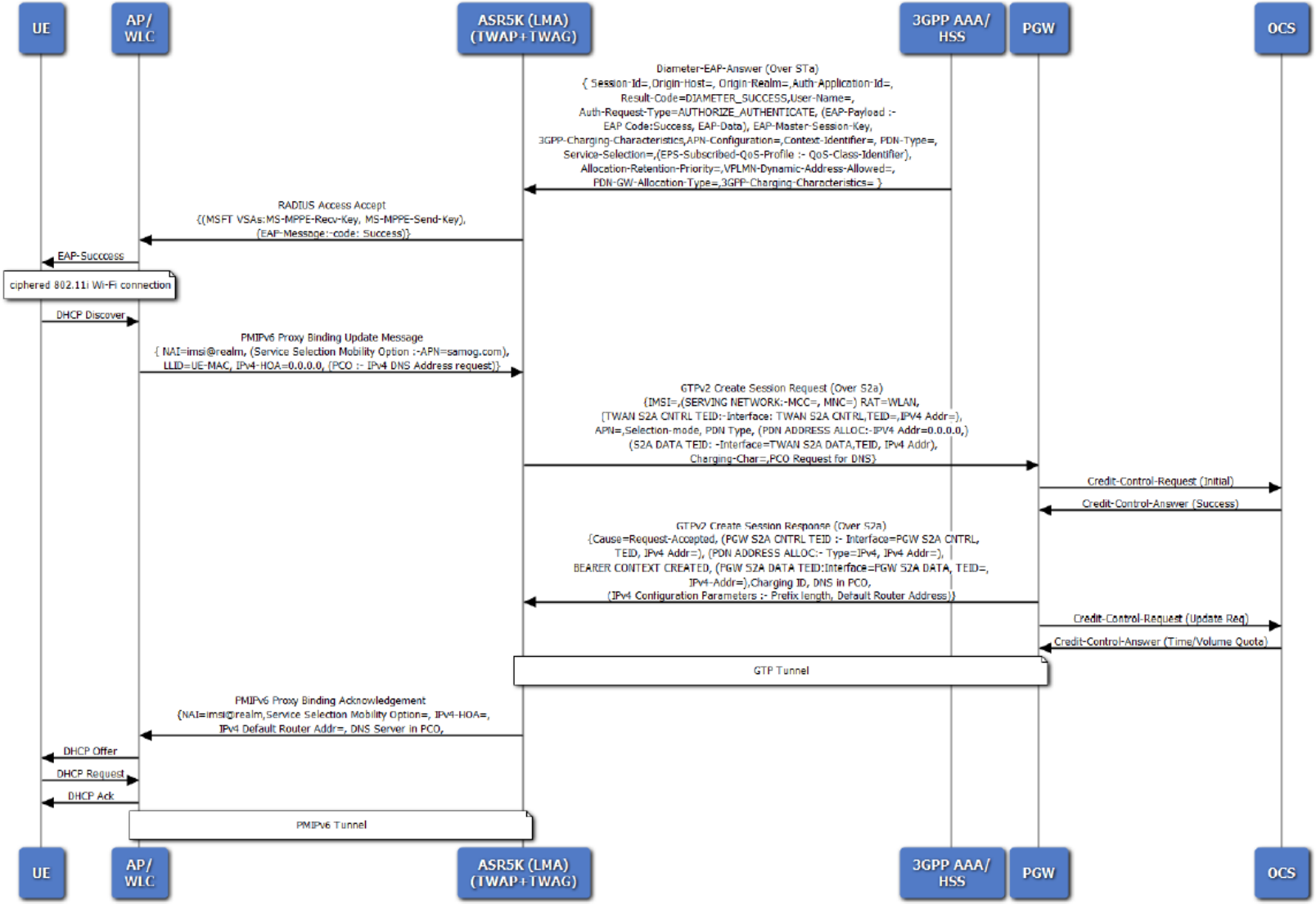
- New StarOS service for Trusted WLAN Access Gateway
- 3GPP **TWAG**
- Ingress (towards the WiFi AP)
  - IP-in-IP-GRE termination
  - Un-tunneled operation
- Egress (towards Mobile Gateway)
  - GTPv2-C, GTP-U

Cisco and/or its affiliates. All rights reserved.

SaMOG Session Establishment w/EAP-SIM 1/2



SaMOG Session Establishment w/EAP-SIM 2/2



CISCO
TM