White Paper

Wi-Fi Calling and the Support of IMS Services over Carrier Wi-Fi Networks

What You Will Learn

Carrier Wi-Fi deployments are helping mobile operators take advantage of already deployed evolved packet core (EPC)-based services for supporting trusted Wi-Fi access networks. Approaches include reusing P-GW -based accounting, policy enforcement, and regulatory services for supporting Wi-Fi users. With Wi-Fi calling, similar EPC-based services can be used to support IMS-based rich media services accessed over untrusted Wi-Fi networks.

This white paper contrasts the focus of carrier Wi-Fi-based EPC integration with Wi-Fi calling-based EPC integration, by demonstrating how they address complementary drivers for Wi-Fi integration for offloading data and providing service equivalency. Issues related to the simultaneous support of Wi-Fi calling and non-Wi-Fi calling flows are discussed, as well as techniques that support the coexistence of IPsec-tunneled Wi-Fi calling and Internet traffic. These topics are examined from a device perspective and an EPC-based carrier Wi-Fi perspective.

Introduction

The launch of Apple iOS 8 with its Wi-Fi calling capability may well be seen as a watershed moment in the user experience of heterogeneous networks, because it allows transparent access to IMS-based rich media communications over both LTE and Wi-Fi access networks. Apple iOS 8 delivers the standardized 3GPP capability to support access to IMS services over untrusted and unmanaged Wi-Fi networks. Although the capability was originally defined by 3GPP in 2005, widespread adoption has been seriously hampered by the lack of native support in a wide range of mobile handsets, a situation that the launch of Apple iOS 8 is sure to change.

The original 2005 definition of interworking WLAN specified by 3GPP considered all non-3GPP access networks to be untrusted and insecure. Since then, the mobile industry has embraced carrier Wi-Fi as an important complement to licensed radio access networks. Standards now allow carrier Wi-Fi to be integrated as a trusted WLAN (TWAN) into LTE's converged EPC. This allows operators to use a common set of equipment, services, and procedures to support access over both licensed cellular and carrier Wi-Fi radio access networks.

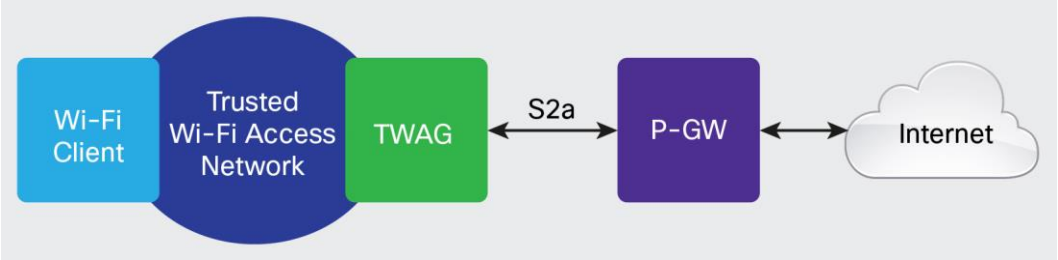
Adoption of the trusted Wi-Fi model allows mobile service providers to use EPC functions to support traffic generated by their users when they are attached to the carrier Wi-Fi infrastructure. But Apple iOS 8 Wi-Fi calling support allows Wi-Fi traffic, generated by those same users when attached to untrusted and unmanaged networks, to be tunneled over the Internet to a mobile service provider's EPC.

With these two different approaches to using an operator's EPC for supporting Wi-Fi traffic, how will the availability of Apple iOS 8 affect the adoption of carrier Wi-Fi-based EPC integration?

Trusted Wi-Fi-Based EPC Integration

When LTE's EPC was defined in Release 8, 3GPP allowed integration with non-3GPP access networks. In 2008, this original capability was focused on allowing integration with cdma2000 and WiMAX-based access networks. Since then, the same interfaces and architecture have been enhanced to support integration with trusted Wi-Fi access networks. From an architecture perspective, the 3GPP S2a interface is used to integrate the EPC with the carrier Wi-Fi access network using a trusted WLAN access gateway (TWAG), as shown in Figure 1.

Figure 1. 3GPP Trusted Wi-Fi Integration



Two versions of S2a have been defined. Initially, in Release 8, PMIPv6 was specified as the protocol for supporting the S2a interface. In 2012 (3GPP release 11), the architecture was enhanced to allow use of the GTPv2 protocol. Equipment vendors quickly enhanced their Wi-Fi solutions to support TWAG and S2a functions. For example, Cisco currently supports TWAG and S2a functionality in a range of different equipment, including:

- TWAG/S2a support integrated into the Cisco ASR 5000 Series S2a Mobility over GTP (SaMOG) Gateway
- TWAG/S2a support integrated into the Cisco ASR 1000 Series Integrated Wireless Access Gateway (iWAG)
- TWAG/S2a functionality integrated into the wireless LAN controller (WLC)
- TWAG/S2a functionality integrated into Cisco Videoscape™ OpenRG residential gateway software

From a Wi-Fi device perspective, parallel developments by the Wi-Fi Alliance and Wireless Broadband Alliance have led to the accelerated availability of smartphone devices that are Wi-Fi CERTIFIED Passpoint™. These devices can establish secure connections to carrier Wi-Fi networks using existing smart card credentials. From a device requirements perspective, this baseline functionality is then sufficient for a device on a trusted Wi-Fi network to access EPC-based functionality, including P-GW-based accounting, policy enforcement, and regulatory services.

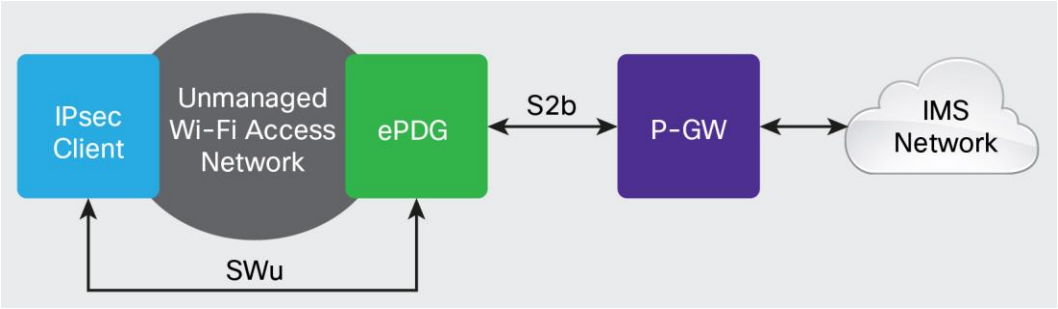
Because no additional device functionality is assumed by the Release 11 architecture, the TWAN can use DHCP to provide the device with a single address that has been allocated by the P-GW. This addressing capability contrasts with the licensed radio access network's approach, which defines functionality to support multiple IP addresses on a single device, each associated with a separate PDN connection. Support for multiple PDN connections is associated with access point name (APN) signaling, functionality that is not defined in 3GPP Release 11 trusted Wi-Fi.

For an EPC, the flows supported over the TWAN are normally associated with a "default APN" that is then defined to support Internet-type traffic. In the majority of carrier Wi-Fi deployments, this is entirely appropriate, as operators are looking to use their Wi-Fi networks to offload a significant volume of Internet traffic from their licensed radio networks.

Wi-Fi Calling-Based EPC Integration

Apple iOS 8 Wi-Fi calling supports access from untrusted networks. This requires new device functionality that establishes an IPsec tunnel between the iPhone and an ePDG in the carrier's network over the SWu interface. Figure 2 shows how the ePDG then uses the S2b interface to integrate with the carrier's existing P-GW where services can be applied to the IP flows from a particular device.

Figure 2. SWu-based Access to Wi-Fi Calling Applications



Unlike the Release 11 trusted Wi-Fi use case that placed no requirements on the device for supporting concepts of PDN connectivity, 3GPP has defined enhanced communication between the client and ePDG to support APN signaling. This allows the concept of a PDN connection to different APNs to be supported over the SWu interface. For Wi-Fi calling, this functionality allows the device to request access to the IMS-APN, so the P-GW can provide connectivity to the IMS-defined SIP servers, XCAP servers, and media gateways.

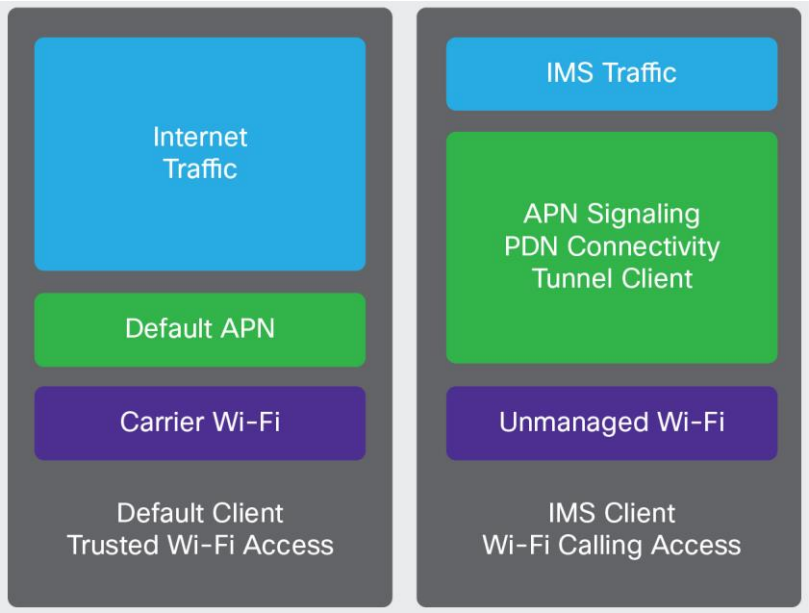
Because equivalent concepts of APNs and PDN connectivity are supported over Wi-Fi access using the ePDG and the existing cellular network, full integration with APN-defined services can be supported. These services include the IMS-based rich media services used to support the Wi-Fi calling service. Release 11 trusted Wi-Fi architecture, in contrast, cannot support APN signaling and simultaneous PDN connectivity. Hence, it is unable to simultaneously support IMS services and Internet-type traffic over the trusted Wi-Fi network.

Coexistence of Release 11-Based Carrier Wi-Fi and Wi-Fi Calling-Based EPC Integration

The two approaches to EPC integration have different focuses (Figure 3). The focus of trusted WLAN integration and carrier Wi-Fi is on offloading Internet traffic from the licensed radio network when the user is in the vicinity of a carrier Wi-Fi access point. The focus of Wi-Fi calling is on enabling access to IMS APN-based services, including the traffic associated with IMS-based media, from devices active on any Wi-Fi access network.

According to 3GPP standards, for the device to trigger an SWu tunnel to the ePDG, it must determine that the Wi-Fi access network is "untrusted." Given this definition, and the inability of Release 11 trusted Wi-Fi networks to support multiple PDN connections, Wi-Fi calling can only strictly be accessed over unmanaged Wi-Fi networks and not the carrier's own trusted Wi-Fi Access network.

Figure 3. Comparing Trusted Wi-Fi and Wi-Fi Calling Propositions

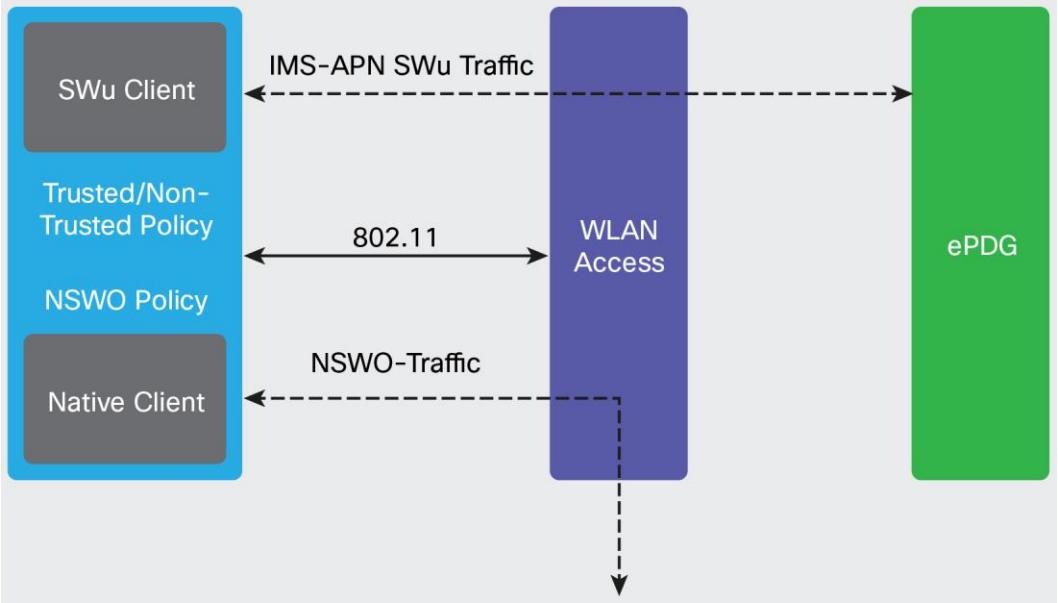


For coexistence, the decision as to whether a Wi-Fi network is considered “trusted” or “untrusted” is critical. The decision can be based on dynamic information signaled by a mobile operator in EAP-AKA signaling or based on a preconfigured policy in the smartphone. Hence, if a smartphone is configured with a policy that considers all Wi-Fi networks to be untrusted, it can help ensure that the Wi-Fi calling service is supported over both unmanaged and carrier Wi-Fi networks.

A further consideration for coexistence is the device’s behavior concerning how non-IMS traffic is supported. 3GPP has defined nonseamless WLAN offload (NSWO) as the ability for a device to send traffic directly to the Wi-Fi access network, compared with the traffic associated with the Wi-Fi Calling application that is tunneled using IPsec towards the ePDG. 3GPP permits smartphone devices to include static policies that are used to determine which flows are routed towards the ePDG and which are routed using the local IP address allocated by the WLAN access network.

Hence, a smartphone configuration can define NSWO policy for supporting non-IMS APN traffic and use a blanket configuration of all Wi-Fi access technology as being “untrusted” to allow simultaneous support for different traffic types, as illustrated in Figure 4.

Figure 4. Preconfigured Smartphone Policy for Supporting SWu and NSWO Traffic



Besides these smartphone policy techniques that allow simultaneous support for IMS-APN traffic over the SWu tunnel and non-IMS APN traffic over the local IP interface, a mobile operator deploying a carrier Wi-Fi network can use TWAG functionality to enable EPC-based functionality to be reused for supporting carrier Wi-Fi users. These capabilities include P-GW-based accounting, policy enforcement, and regulatory services.

Figure 5 shows a device supporting Wi-Fi calling attached to a carrier Wi-Fi network that is being supported using an S2a-based EPC integration. In this case, the NSWO-enabled client capability enables the coexistence of the trusted Wi-Fi access network with the Wi-Fi calling application.

Figure 5. Coexistence of Carrier Wi-Fi Access with Wi-Fi Calling

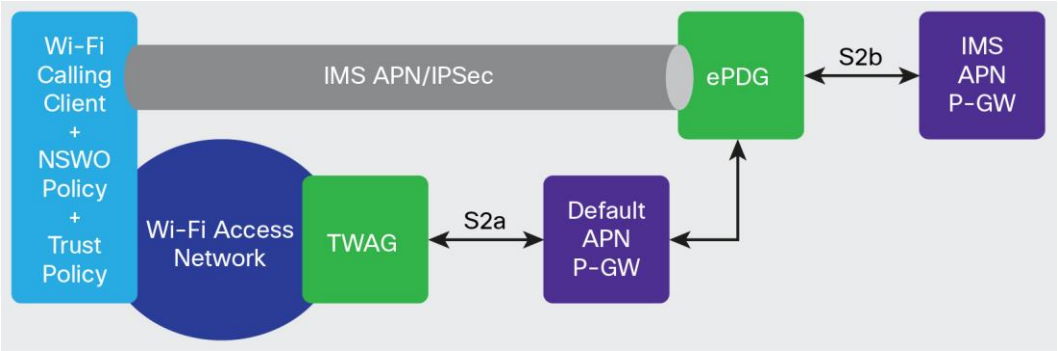
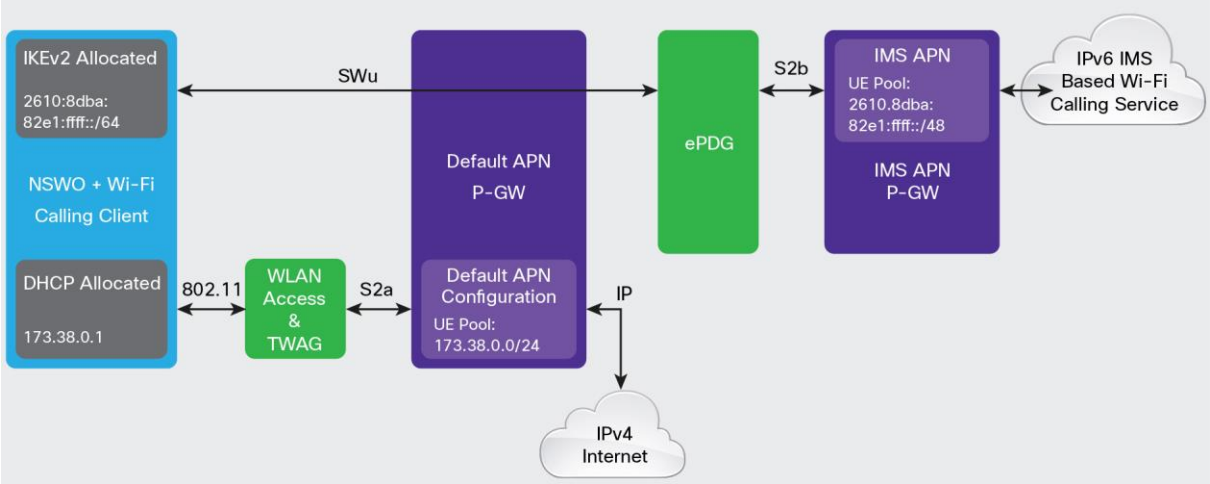


Figure 6 shows an example of IP addressing in the coexistence scenario, illustrating how the default APN of the trusted Wi-Fi access is defined as supporting IPv4 addressing. The example shows address 173.38.0.1 being allocated to the Wi-Fi device using DHCPv4. This address is then used by the device to establish an IKEv2 connection with the ePDG, which is then used to allocate an IPv6 prefix associated with the IMS APN. The device next uses this IPv6 address to access Wi-Fi calling services, tunneling IPv6 packets over the SWu IPsec connection being transported by the default APN P-GW.

Figure 6. Example IP Addressing for Supporting Coexistence

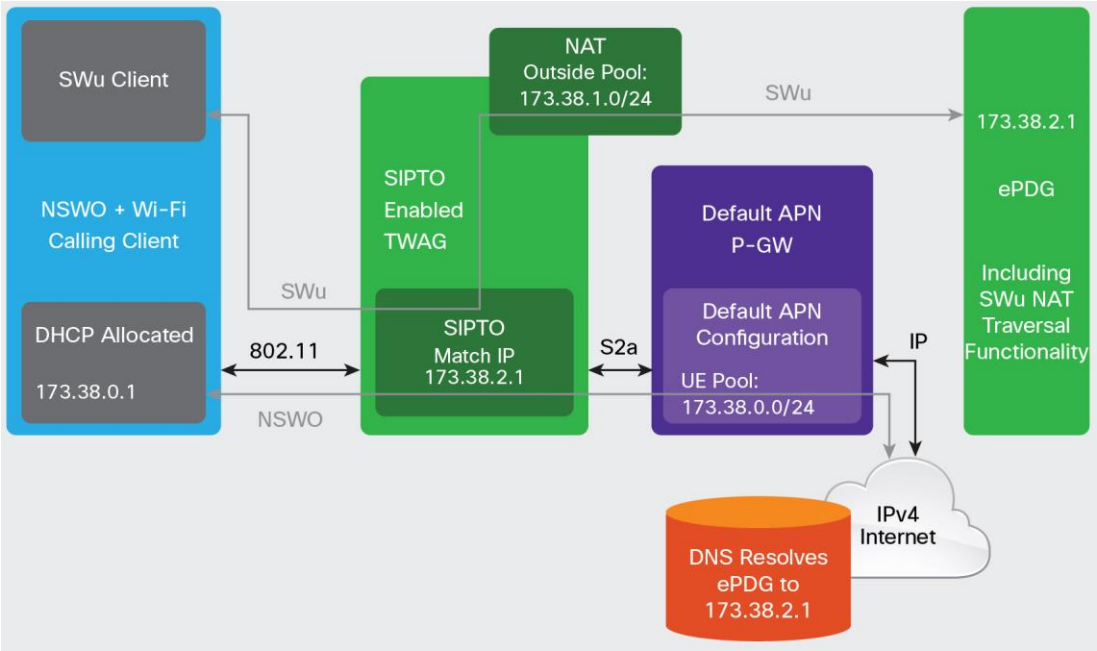


Architectural Optimization

In the baseline coexistence scenario shown in Figure 6, it is evident that the IMS-APN traffic is processed by both the default-APN P-GW and the IMS-APN P-GW. Because the latter function provides the accounting, policy enforcement, and regulatory services for the IMS-APN traffic, operators may be able to optimize the system by avoiding the IMS-APN traffic from transitioning through the default APN P-GW. This can be achieved by using 3GPP-defined selective IP traffic offload (SIPTO) functionality.

SIPTO allows particular IP flows to be routed directly to their destinations without transitioning a mobile core network. This approach is enabled by Network Address Translation (NAT) and packet inspection, based on operator policies. In particular, SIPTO functionality can be supported on the TWAG for packets matching a predefined policy, for example, identifying packets being sent to or from the ePDG, as illustrated in Figure 7. The SIPTO NAT function can be automatically accommodated by the NAT traversal capability already integrated into the SWu tunnel establishment procedures, allowing SWu flows to avoid being routed through the default APN P-GW.

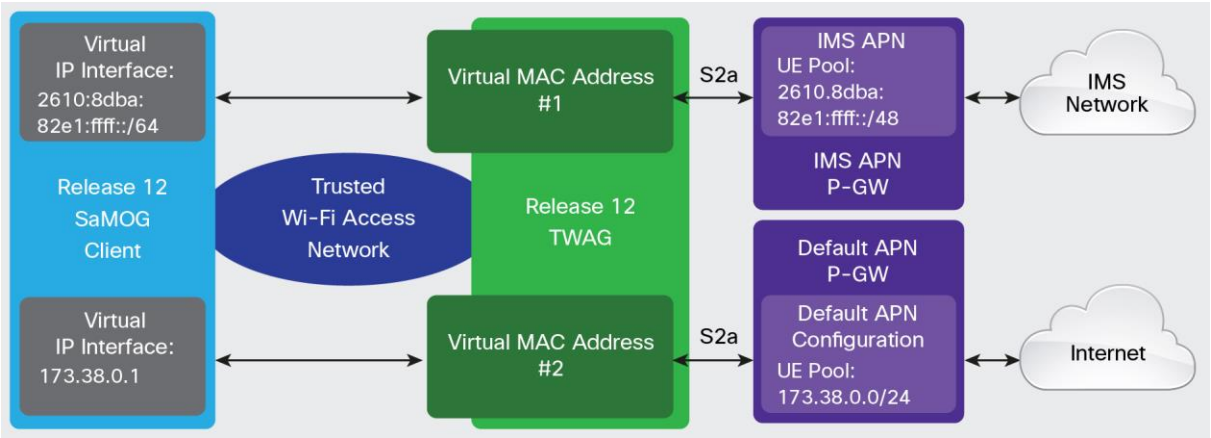
Figure 7. SIPTO-Based TWAG Optimization



Architectural Evolution

As described earlier, device policy techniques to allow simultaneous support of IMS-APN and NSWO traffic are necessary because the 3GPP Release 11 architecture does not support APN signaling and multiple PDN connections over the trusted WLAN access network. This deficiency is being addressed in 3GPP Release 12 which defines new client and network capabilities to support such functionality. These client functionalities include support for multi-PDN devices that can support simultaneous PDN connections, in parallel to NSWO, over a trusted Wi-Fi access network. Figure 8 illustrates the new capability that includes multiple virtual interfaces on the device, so it can allow multiple IP addresses associated with multiple PDN connections to be supported. In addition, it provides enhanced virtual MAC-based encapsulation over the trusted Wi-Fi network, allowing the TWAG to correctly identify which packets are associated with the different PDN connections.

Figure 8. Enhanced Multi-PDN Capability in 3GPP Release 12 trusted WLAN



To migrate from today's Release 11 EPC-based trusted Wi-Fi architectures, a wholesale upgrade to deployed clients will be required to support the Release 12 multi-PDN capability. This enhancement would then see a corresponding upgrade to the client policy definitions. These changes will enable the coexistence of the current Apple iOS 8 ePDG-based Wi-Fi calling and the Release 12 supported IMS-APN access over the trusted Wi-Fi access network. The client must support the dynamic indication of trust to determine whether to support IMS calling applications over the SWu tunnel to the ePDG or the virtual MAC connection to the TWAG.

Carrier Wi-Fi and Wi-Fi calling now provide mobile operators with two contrasting approaches to integrate Wi-Fi traffic into their EPC infrastructure. Carrier Wi-Fi's trusted WLAN access network enables already deployed EPC-based services, including P-GW-based accounting, policy enforcement, and regulatory services, to be re-used for supporting the Internet-type traffic associated with a default APN. The Wi-Fi calling approach tunnels rich-media traffic associated with the IMS-APN using an IPSec connection over untrusted and un-managed Wi-Fi networks. This white paper compares the architectures for supporting these alternative approaches and demonstrates techniques to enable their co-existence, both from a device perspective and EPC-based carrier Wi-Fi perspective.

For More Information

http://www.cisco.com/go/spwifi

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-733136-00 10/14