White Paper

Cisco Voice over Wi-Fi Solution

Motivation for Voice over Wi-Fi

Wi-Fi connectivity is the most pervasive radio technology worldwide. In many areas there is more available Wi-Fi spectrum and access technology than licensed radio systems. Most of us have very good Wi-Fi access at work, school, shopping, and at home. Wi-Fi offers an excellent coverage and capacity augmentation for service providers to offer enhanced customer satisfaction in a very cost-effective manner.

In mobile networks, unlicensed Wi-Fi has been used primarily as a data-only radio system. Voice has almost always been carried on licensed spectrum. There has been UMA/GAN technology for Wi-Fi voice calling since 2005. This early system was heavily customized and was not well integrated into the UE handset. Hand-in to Wi-Fi and hand-out to licensed radio did not work all that well.

After several iterations of this technology and some new standardization and handset advancements, voice over Wi-Fi (VoWi-Fi) has been rolling out to many carriers worldwide. VoWi-Fi now offers transparent hand-offs from Wi-Fi to licensed radio for voice calls. Apple iOS (since iOS 8) and Samsung Android support this capability natively in the handset. This represents a huge inflection point in acceleration of mobile voice services. Since early adoption announced by Everything Everywhere and T-Mobile in late 2014, the list of global operators deploying VoWi-Fi has been growing rapidly.

The Cisco Visual Networking Index from 2016 shows that VoWiFi will surpass VoLTE by 2016 and VoIP by 2018 in terms of minutes of use. By 2020, VoWiFi will have 53 percent of mobile IP voice, up from 16 percent in 2015. VoLTE is expected to surpass VoIP minutes of use by 2019. In addition, Wi-Fi traffic from both mobile devices and Wi-Fi-only devices together will account for more than half (53 percent) of total IP traffic by 2019, up from 41 percent in 2014.

The main factors for VoWi-Fi include:

- **A cost-effective solution to complement macro coverage:** As many operators continue to deploy LTE networks, there will be areas where coverage is suboptimal, including indoor areas. As a result of these coverage constraints, traditional voice services might be less than optimal. VoWi-Fi can be deployed to support voice services and can complement cellular coverage.
- **Customer retention:** Voice calling with roaming services can be expensive, and users often turn to OTT providers or services to offset these costs. Because OTT applications use “best effort” bandwidth to support their services, the user experience can be inconsistent and at times suboptimal. VoWi-Fi enables roaming services to be supported at a lower unit cost and with a consistent, transparent voice service.
- **Single telephone number access:** Enterprise employees are mobile and want to be able to easily communicate anywhere, often on their own devices. There has been an increase in interest by employees to be reached from either their desk phone or their mobile phone using a single number. VoWi-Fi services enables single telephone number access on the mobile devices using the same number as the desk phone.

- **Voice calls on non-SIM devices:** Currently, voice calls are only available on devices that support cellular coverage or OTT applications. VoWi-Fi expands the number of voice-capable devices to cover non-SIM Wi-Fi-only devices. With VoWi-Fi, users can make and receive calls on their non-SIM tablets, enhancing additional revenue streams.

VoWi-Fi Solution Technology Overview

VoWi-Fi is based on the i-WLAN solution as defined in 3GPP 23.402. Voice and text message data is sent over Wi-Fi using an IPSec tunnel from a native smartphone client to an ePDG gateway in the mobile core. The native client and interface to ePDG are named, respectively, the SWu client and interface. Following the IPSec tunnel establishment, an IMS-APN is invoked, and all IMS-related traffic (voice, text) then goes through the SWu client and interface. All non-IMS traffic will either go to the LTE PDN or to a local Wi-Fi interface.

There is no need to install any VoWi-Fi application on the smartphone because:

- The SWu client is supported natively in the smartphone.
- The same phone application is used for 3G/VoLTE/VoWi-Fi calls. It is up to the phone to select which access to use for the voice call. The MSISDN number is used for 3G/VoLTE/VoWi-Fi calls.
- VoWi-Fi calls use the same IMS infrastructure and application deployed for VoLTE.

Depending on handset capabilities, handover between VoLTE and VoWi-Fi is supported. This means that for any voice call starting in Wi-Fi, the call will be continued when the user moves to LTE and vice versa.

VoWi-Fi Solution Architecture

Figure 1. VoWi-Fi Solution Architecture

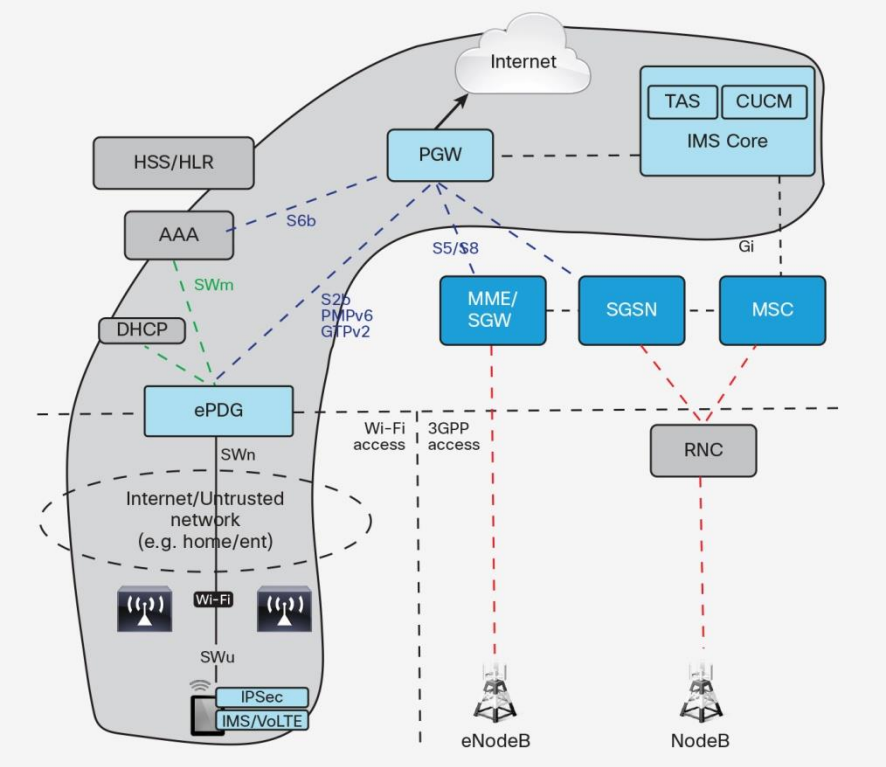


Figure 1 depicts the end-to-end VoWi-Fi solution and its relationship with the mobile core and Wi-Fi access networks:

- An IPSec tunnel is established over Wi-Fi and the Internet between the native IPSec/SWu client on the smartphone to the ePDG.
- Although 3GPP standards mention that the Wi-Fi access network is untrusted (hence the need for a secure tunnel), in reality it can be trusted (SP managed) or untrusted (unmanaged).
- The ePDG is located in the core network. Its Internet-facing interface has public IP addresses that can be resolved from ePDG FQDN from UE using DNS. ePDG performs EAP-AKA-IKEv2 authentication and IPSec SA establishment with the UE. After the IPSec tunnel has been established, the ePDG creates a GTPv2 tunnel with the PGW.
- 3G/VoLTE and VoWi-Fi use the same phone application/dialer for a voice call. The VoWi-Fi phone application on the device communicates with VoLTE IMS infrastructure over the IPSec tunnel and PGW for VoIP call setup. The actual voice packets also travel through the IPSec/PGW to other IP destinations.
- AAA or 3GPP AAA supports the SWm interface toward the ePDG for EAP authentication. It communicates with the HSS using the SWx interface. In order to support handover, the S6b interface to the PGW is supported.

VoWi-Fi for Business: Challenges and Opportunities

Opportunities

As VoWi-Fi deployments accelerate, and its use gains in popularity, more calls will likely be made over nonresidential systems, including community Wi-Fi, hotspots, hot zones, large venues, business Wi-Fi networks, and city Wi-Fi networks. Therefore, it is critical that mobile operators provide consistent VoWi-Fi service in residential, business, and other venues.

Improving indoor radio coverage for business venues has been top of mind for mobile operators for several years. Small cells and DAS are among the most popular solutions deployed today. VoWi-Fi presents a very cost-effective alternative to indoor coverage improvement for businesses, especially when they require support for multiple carriers. The Wi-Fi network, already a must have in most businesses, can support VoWi-Fi service with multiple mobile service providers, whereas a small cell solution typically supports only one mobile service provider. In addition, there is significant difference in terms of CapEx/OpEx between Wi-Fi and small cell/DAS in business venues.

VoWi-Fi offers the opportunity for fixed-mobile convergence use cases for businesses. With integration between mobile operators' IMS and UCaaS/PABXaaS solutions, mobile phones can act as an extension of the office. Fixed-mobile convergence not only enhances business user experience but also improves mobile-operator/business stickiness. It adds differentiation to mobile operator's service offerings.

Challenges

Studies have shown that 90 percent+ of the time that mobile users use Wi-Fi, they are at home, work, or school, where low-cost or free Wi-Fi is readily available. Apart from their homes, mobility customers spend most time in their office. The primary challenges for deploying VoWi-Fi in the business environment are:

- Security: VoWi-Fi requires an IPSec tunnel to be built over the network between the mobile phone and the ePDG. Some businesses choose to block IPSec by default. There are some security concerns about IPSec tunnels because they are very secure and do not allow for any monitoring, whereas with SSL connections, IT personnel can preshare keys to owned devices and monitor them. This is especially true with laptops and servers. The mobile UE already has access directly to the Internet using a 2G, 3G, or 4G mobile data connection without monitoring in place. Furthermore, the VoWi-Fi architecture is a very secure connection back to the mobile operator's ePDG. The UE has to authenticate to the ePDG gateway for access before getting routed through to the IMS system, which usually restricts connections to just voice or video. Getting data from the IMS system to the Internet is often difficult.
- Network performance/QoS becomes even more critical in the office/business environment. Factors affecting network performance for VoWi-Fi in the office environment are:
  - Traditional Wi-Fi networks are designed to carry data. In order to support VoWi-Fi, Wi-Fi networks are required to carry the smaller size voice packets as well as the regular-sized data packets. In Wi-Fi, overhead and collisions of small periodic VoWi-Fi packets significantly reduce the MAC efficiency, while cochannel interference (CCI) limits the bandwidth allocated to voice packet transmission. This affects the VoWi-Fi call capacity in a Wi-Fi cell.
  - VoWi-Fi with high mean opinion score (MOS) requires higher packet error rate (PER) than pure data. This affects the Wi-Fi cell size.
  - Complexity arises when VoWi-Fi users with active voice call move among different Wi-Fi cells. In order to maintain the voice call, smartphone and Wi-Fi network are required to perform inter-AP roaming more quickly and more efficiently.

  Overall, the network performance challenge for VoWi-Fi relates to how to deliver a consistent user experience regardless of load, user location, and environment.
- VoWi-Fi QoE. Businesses will naturally require high QoE for VoWi-Fi calls in compliance to their company policy. MOS values for VoWi-Fi calls and call success rates are the likely QoE parameters required by business.

VoWi-Fi Solutions for Businesses

Security

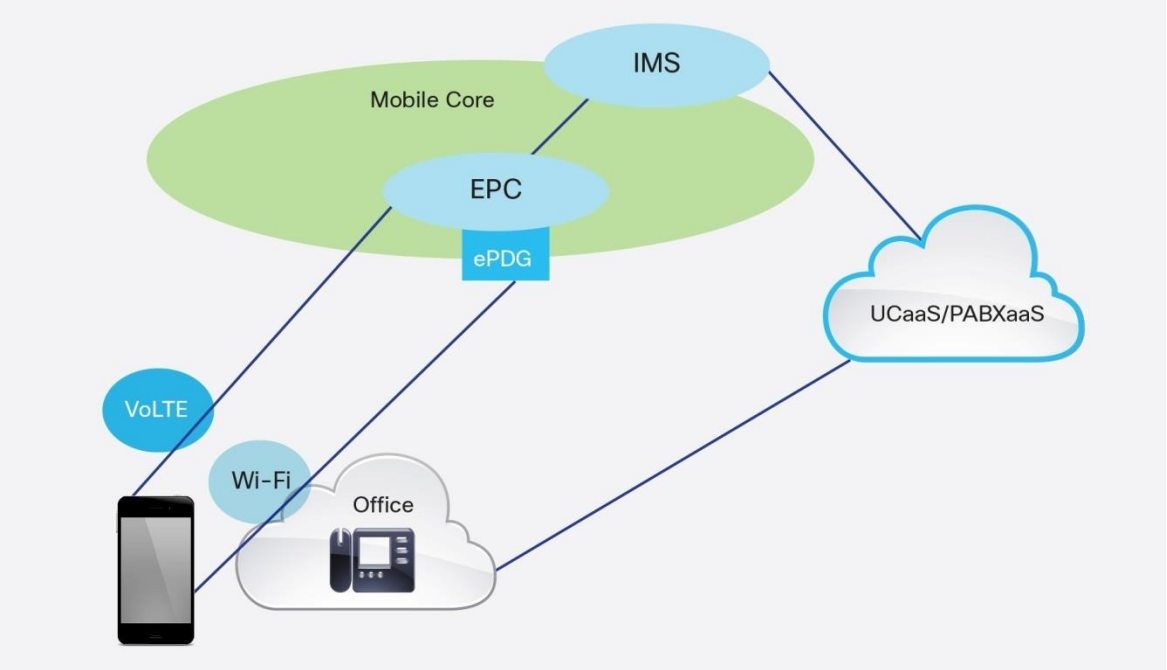
Businesses will have various views regarding risk associated with IPSec. Some businesses would just naturally allow IPSec traffic. Others will allow IPSec as long as it is for VoWi-Fi and the destination for the IPSec tunnel (ePDG IP address) is well defined. There is no one-size-fits-all solution for security in VoWi-Fi for businesses. The following is a range of security solutions from easy to hard for deploying VoWi-Fi in the business environment:

- Make no restriction on IPSec ports. Many small and medium businesses allow IPSec. VoWi-Fi IPSec does not face any obstacles in these situations.

- Offer a separate Wi-Fi SSID for VoWi-Fi with firewall IPSec ports open to carrier ePDG ports or no filtering at all. In this approach, users have no access to the corporate intranet. Similar to a guest Wi-Fi SSID, mobile VPN is needed to access mail, calendar, and other corporate content. This approach offers access to the corporate network using VPN or SSL similar to that one would experience in the macro radio network with the added benefit of Wi-Fi coverage and capacity.
- Enable IPSec just for VoWi-Fi. In this approach the businesses allow IPSec connections in their firewalls to ePDGs belonging to trusted service providers. A list of trusted ePDG addresses is given to the enterprise by the service provider to be added to their firewall. The service provider typically will block nonvoice/video traffic to the Internet and can offer additional protection.

Fixed-Mobile Convergence for Business Users

Figure 2. VoWi-Fi for Fixed-Mobile Convergence



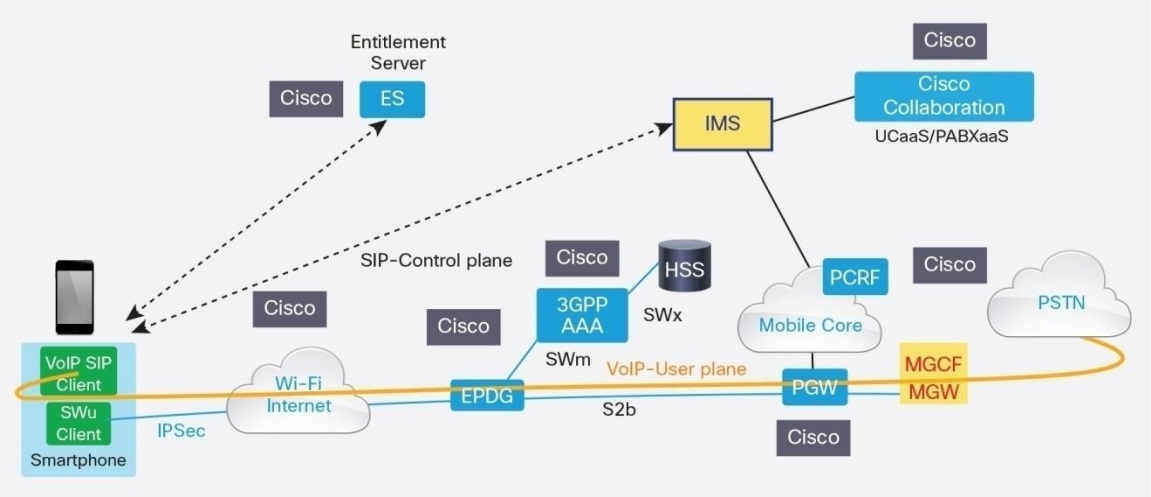
The architecture shown in Figure 2 enables fixed-mobile convergence between businesses and the mobile network. Mobile operators use UCaaS/PABXaaS to provide cloud-based IP telephony and collaboration applications to businesses. With integration to mobile IMS, smartphones can become an extension to the office.

To help illustrate the FMC experience, here are a few example use cases enabled by the FMC architecture:

- A mobile user can call colleagues based on the business dial plan (short number dialing).
- When calling an external party, the caller ID shown will be the business caller ID.
- When someone calls the business or mobile number, both desk/softphone and mobile phone will ring.
- Users can hand over the voice call between devices.
- Midcall voice recording.

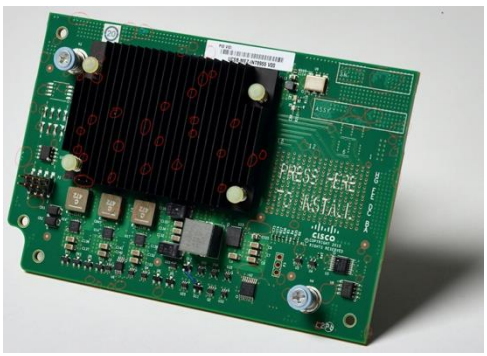
Cisco Solution for VoWi-Fi

Figure 3. Cisco VoWi-Fi Solution



The Cisco® VoWi-Fi solution (Figure 3) includes the following components:

- **Wi-Fi access infrastructure:** Cisco Universal Wi-Fi is a carrier-grade solution that features a portfolio of 802.11ac indoor and outdoor access points and the 8500 Series Wireless Controller. Cisco Universal Wi-Fi includes High-Definition Voice Experience (HDVX) technology, including interference management, radio resource management, beamforming, and fast roaming to vastly improve the quality of voice calls over Wi-Fi.
- **ePDG:** Cisco StarOS ePDG is supported on multiple platforms
  - Our world-leading ASR5500 platform offering a very high performance, secure, and stable solution. This solution uses onboard hardware IPSec crypto chips for high VoWi-Fi performance.
  - Our new virtualized EPC platform “Ultra,” which offers very flexible implementations based on x86 server architectures. We have further enhanced this offering by adding optional crypto daughter cards in our Cisco UCS® x86 platform. These crypto cards offer great improvements in VoWi-Fi capacity as well as the ability to customize the ePDG capacity to suit operator needs.



- **AAA:** Cisco Prime™ Access Register for EAP authentication, SWm, SWx, and S6b (for VoLTE/VoWi-Fi handover). Cisco Prime Access Register is very flexible, and its function can be extended easily. Working with Cisco ePDG, it supports UE VoWi-Fi access blocking and geolocation checking.
- **PGW:** Cisco's StarOS PGW is supported on multiple platforms such as the ASR 5500 as well as the PGW based on the virtualized evolved packet core (vPC).
- **UCaaS/PABXaaS:** Cisco has very extensive collaboration solutions that offer IP telephony, meeting room, instant messaging, and file sharing as a service with our service provider partners. In particular, Cisco Collaboration can be integrated with IMS to enable VoWi-Fi fixed-mobile convergence services for businesses.
- **Policy Suite:**

  Cisco PCRF: Cisco Policy Suite is a fully virtualized, carrier-grade policy, charging, and subscriber data management solution that is uniquely designed to support the scale, performance, and latency requirements for VoLTE control plane processing. It operates on COTS hardware and operates as a virtual application in the service provider cloud today.

  Cisco Access Selection: The Cisco Access Selection solution allows personalized, network-aware device access to network selection policies that run in real time on each user device. Access Selection is relevant for service providers that want to manage which Wi-Fi is connected to for specific subscribers' VoLTE and other data flows, in select times and places, for an "always best connected" subscriber experience. Access selection policies are assigned using the user's profile and current user location. As part of the Cisco end-to-end access policy solution, the Access Policy Server supports flexible business logic and selection rule configurations that are an essential part of access selection use cases and business outcomes. In addition, the Access Policy Solution provides a network-based server that supports an open device and client or clientless approach.
- **Entitlement Server:** Cisco's Entitlement Server is a product developed in close design and test collaboration with Apple. The Entitlement Server is a new architectural node defined to enable carrier-driven feature activation and device policy control on Apple SIM and non-SIM devices. The relevant carrier features controlled and managed by the Entitlement Server include Facetime, tethering, IMessage, VOLTE, VoWi-Fi and Apple's Cellular Continuity (companion device calling on cellular).

  The Entitlement Server by design can allow/restrict on a per-user, per-SIM, and non-SIM device basis which of the preceding features can be used in the carrier network or not and can drive autoprovisioning of such user/devices into the carrier network as needed. This enables an optimal user experience for new feature activation and an optimal carrier service management approach for new users in the carrier network.

  Because of the interface requirements, session processing, and scalability requirements of the Entitlement Server, Cisco is using the proven Cisco Policy Suite virtualized software platform for this new carrier application module.
- **Cisco HDVX Wi-Fi Access for VoWi-Fi:** A single VoWi-Fi call does not place a heavy data load on the network (in the iOS 8 VoWi-Fi calling example, this will typically be around 250 kbps), but latency and jitter and other applications on the network can affect voice quality. Wi-Fi AP-to-AP mobility/AP-selection, Wi-Fi band selection, VoWi-Fi Wi-Fi access QoS, network element resilience, AP throughput under load, and radio performance and cellular hand-off are issues that can affect the user experience. The Cisco Universal Wi-Fi solution with High-Definition Voice Experience (HDVX) features provides remedies to these issues for an excellent VoWi-Fi user experience.

Why Cisco for VoWi-Fi

Proven Solution and Leader in VoWi-Fi

Cisco has been at the forefront of the 3GPP Wi-Fi standardization activity based on many years of deploying Wi-Fi in the service provider market. Cisco has the most deployed VoWi-Fi solution on the market and is currently in use with VoWi-Fi solution with mobile operators around the globe.

Multiservice Software

The Cisco ePDG is based on StarOS. With the multiservice nature of StarOS, Cisco supports the deployment of HNBGW, PGW, SaMOG gateway, and ePDG in the same node/platform. This provides huge flexibility to operators as the network requirements evolve. Cisco is the only vendor to support all mobility functions in a single HW platform.

Multiplatform: Virtual, Highly Scalable Gateway

The Cisco ePDG is available in the following platforms:

- ASR 5500: proven, dedicated, and highly scalable platform
- VPC: virtual gateway and can be deployed on any x86 platform

Hybrid Trusted/Untrusted Solution

Support coexistence of trusted Wi-Fi (3GPP SaMOG) and untrusted Wi-Fi (3GPP iWLAN/VoWi-Fi). Cisco StarOS supports SIPTO, which can optimize the routing for VoWi-Fi traffic in a SaMOG environment.

Enhanced VoWi-Fi Core

Cisco ePDG supports Wi-Fi network visibility features, which allow roaming access white/blacklisting. Because ePDG is normally deployed at the Internet edge, it is subject to attack. Cisco ePDG supports an assortment of measures to protect the system from Internet DOS attack.

The Cisco Policy Suite is a fully virtualized, carrier-grade policy, charging, and subscriber data management solution that is uniquely designed to support the scale, performance, and latency requirements for VoLTE control plane processing (RADIUS, Sh/Sp, Gx, Sd, Rx, APIs). The policy solution supports converged policy control processing for both 3G/LTE and Wi-Fi access types, enabling converged subscriber experiences and monetization opportunities.

Proven Enterprise VoWLAN Solution

Although VoWi-Fi is a relatively new technology deployed on smartphones, VoWi-Fi/WLAN is nothing new in the enterprise. As the leading enterprise Wi-Fi solution provider, Cisco has accumulated a vast amount of experience on deploying voice over Wi-Fi in the last decade. The keys for successful VoWi-Fi deployment to provide a good user experiences are:

- Coverage
- Throughput
- QoS
- Inter-AP mobility

Cisco Universal Wi-Fi provides the best-in-class Wi-Fi infrastructure available for VoWi-Fi and other enterprise data applications. Featuring HDVX technology, Cisco Universal Wi-Fi offers 802.11ac throughput, enhanced Wi-Fi network mobility through fast roaming, and efficient smartphone battery use to enhance the VoWi-Fi experience. The Cisco Advanced Service team is also available to work with enterprises to optimize their Wi-Fi network design to support VoWi-Fi.

Fixed-Mobile Convergence Use Cases for Business

With integration between mobile operators' IMS and collaboration services, mobile phones can act as an extension of the office. Fixed-mobile convergence not only enhances business user experience but also improves mobile-operator/business stickiness. It adds differentiation to mobile operators' service offerings. Based on Cisco's vast portfolio of solutions covering Wi-Fi access, VoWi-Fi, and collaboration, it is the one stop for a fixed-mobile convergence solution.

Conclusion

VoWi-Fi demand is poised to grow dramatically, with both the combination of voice demands on the networks and the pervasiveness of Wi-Fi. Operators are well positioned to take advantage of these growths given their relationship with consumer and business customers. And the combination of Cisco's years of experience deploying Wi-Fi for operators with the complete VoWi-Fi solution enables those operators to address VoWi-Fi demands on their network today and build deeper relationships with their customers.

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 C11-736770-00 02/16