Wi-Fi Calling

Why Wi-Fi Calling?

More and more of your employees are opting to make calls from their mobile devices using Wi-Fi Calling. The benefits for them are multifold, but what's in it for you and your organization? How can you make sure that your network is properly equipped for Wi-Fi Calling? How can you choose a Wi-Fi Calling solution that is secure, inexpensive, and easy to deploy? Cisco has the answers.

What Is Wi-Fi Calling?

Wi-Fi Calling, or voice over Wi-Fi (VoWi-Fi), is a setting on many mobile devices that enables calls to be made over a Wi-Fi network rather than the cellular network.

This setting is automatically available on Apple devices, provided they are running iOS 8. For Android devices, making calls over Wi-Fi can be a bit more complicated. These phones require the user to download an app compatible with the device and the service provider.

The main benefit your employees get from using VoWi-Fi is that it saves money, as it allows for inexpensive international roaming services. Aside from the cost factor, adopters of VoWi-Fi also enjoy:

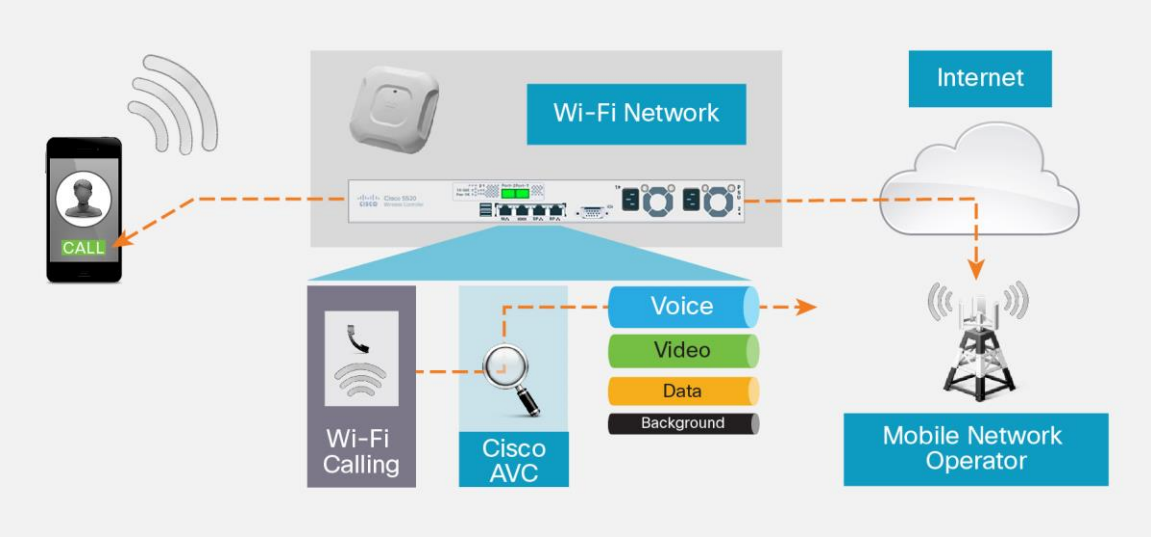
- Better coverage: While finding indoor cellular coverage can be a struggle, VoWi-Fi eliminates that challenge. Wi-Fi can be found in many indoor public and private locations.
- The ability to make calls with non-SIM devices: With VoWi-Fi, tablet users can make and receive calls as if they were using a mobile phone.

The convenience and cost savings are great for your employees, but how do you and your organization benefit from VoWi-Fi? Here are a few reasons to support Wi-Fi Calling:

- With many devices offering Wi-Fi Calling, this is a nice perk for mobile device users. Also, voice packets have very low bandwidth requirements.
- By designing a VoWi-Fi network, you create your own network fail-safes. For security reasons, some companies have regulatory issues that require cell calls to go through a specific corporate system. You can create these regulations yourself to keep in compliance.
- Despite the low amount of bandwidth needed for VoWi-Fi, businesses still need to control their bandwidth usage. Controls can be set up to prioritize or limit the use of VoWi-Fi so that it will not eat a large chunk of your bandwidth. For example, if you block any external service provider (ESP), Wi-Fi Calling will be blocked for that ESP too. You can also exert bandwidth control over an ESP by designating a certain amount of bandwidth per Service Set Identifier (SSID). Anything over that amount will be blocked, effectively limiting the consumable bandwidth.
- Cellular service providers are beginning to heavily promote this service, so it is something that a majority of your employees will be using very soon. Getting ahead of the curve will make your life easier down the road.

How Does Wi-Fi Calling Work?

Figure 1. Wi-Fi Calling



The technology behind how the service works isn't overly complicated: voice and text message data is sent via an IP Security (IPsec) tunnel from a native smartphone client to a gateway called the Evolved Packet Data Gateway (ePDG) in the mobile core. Once IPsec connection verification is completed, all native voice and text traffic is funneled through this tunnel (Figure 1). If IPsec connection verification fails, non-IP Multimedia Subsystem (IMS) traffic will go either to the LTE public data network (PDN) or to the local Wi-Fi interface.

Be aware that if a call is dropped on the Wi-Fi network, the handover between VoWi-Fi and voice over LTE (VoLTE) is not always seamless and depends on the service provider. For an uninterrupted back-and-forth conversation over the VoWi-Fi and VoLTE networks, a transfer roaming handoff will work better with a 4G LTE connection. This means that the caller will not detect any difference in service. If the device does not employ the 4G network and instead uses a 2G network connection, for example, the likelihood increases that a call will drop as it roams from VoWi-Fi to VoLTE.

How Can Cisco Help?

Creating a Wi-Fi Calling network using Cisco® products is simple because it is made up of equipment that is cost-effective, easy-to-use, and packed with Cisco expertise and reliability. Cisco Aironet® access points offer a purpose-built, innovative chipset with best-in-class RF architecture. The Cisco 802.11ac access points - like the Cisco Aironet products - offer not only greater range and reliability than offered by the competition, but also Cisco High Density Experience, which consists of a subset of features including Cisco ClientLink 3.0 and Cisco CleanAir®. High Density Experience allows more users to connect while providing a better user experience by reducing RF interference and optimizing signal quality and performance. This helps to improve battery life for all mobile devices attached to the network.

The following components are needed to deploy Cisco's VoWi-Fi solution:

- Robust, enterprise-class Wi-Fi access infrastructure
- Optional firewall to selectively block some Wi-Fi calling providers

Before we get into the actual setup of Cisco's VoWi-Fi solution, it's important to discuss cell design, which promotes good roaming. In order to have a robust VoWi-Fi solution, you need to think about your network design in terms of voice efficiencies. There are three rules to a proper and efficient design:

1. Create cell conditions optimized for voice, which can be broken down into these four key areas:
   - Coverage
   - Throughput
   - Quality of service (QoS)
   - Inter-access point mobility
2. Design a cell edge that matches your device and application needs
3. Implement the protocols that help a device roam efficiently

When it comes to answering the question "when will the device roam?" the easy answer is that it depends on the device. However, it's a bit more complicated than that, as devices typically probe for a new network once they get to the cell edge. The cell edge is defined as the region within the service area of a cell where the quality of the signal offered by the access point servicing the cell becomes lower than the quality needed by the client device. There is a chance that there could be another cell behind that first cell, but there might not be.

For Apple devices, cell roaming starts at -70 decibels per milliwatt (dBm), and because of this, you should reduce your cell edge to -65 dBm for real-time applications. Android devices aren't so cut-and-dried, as there is no overarching setting. Android roaming commonly starts around -75 dBm, which means cell edge reduction should be set at -67 dBm for real-time applications.

For a much more efficient roam, consider deploying a Wi-Fi solution that has implemented the IEEE standards 802.11k and 802.11v. When you support these standards, devices that support 802.11k/v will benefit and unsupported devices won't be affected. Any Apple device with iOS 7 or later, most LG high-end clients, and Samsung and Sony Xperia devices support 802.11k and 802.11v. Some devices support 802.11r, which helps roaming and expedites the correct authentication and security exchanges. However, this is not a standard feature in all devices, and you should do further research to determine whether you should move to this standard.

To make sure that the Wi-Fi Calling network is running correctly, follow these best practices for VoWi-Fi deployment:

1. IPsec: The enterprise firewall policy needs to enable User Datagram Protocol (UDP) ports 500 and 4500 for IPsec to work properly.
2. RF coverage: The Cisco rule of thumb is one access point per 3000 square feet. This allows for a seamless transition between access points. Your access points also need to be positioned wisely. Creating a point where the first access point signal drops below -65 dBm and the next access point is visible from an iOS 8 client and from the first access point is a good way to start setting up your access points.
3. Capacity planning: The recommended number of calls should be limited to 20 on 5-GHz radio access point and 15 on 2.4-GHz radio access points.
4. Band Select. Since 5 GHz offers more channels, you should enable Band Select. This will cause access points to delay their response to probe requests in the 2.4-GHz band, resulting in roaming delay. If cells are designed with consistent coverage in the 5-GHz band, you will avoid 5-GHz to 2.4-GHz roaming events.
5. QoS profile: Enable the Platinum Profile to help ensure that VoWi-Fi packets receive prioritized treatment between the access point and client.

6. Fast transition: Enable this feature if your WLAN supports 802.1X-based security, because it allows clients to roam faster between access points.
7. Assisted roaming: Implement 802.11k and 802.11v assisted roaming on your WLANs.
8. Optimized roaming: Cisco recommends enabling optimized roaming on WLANs that support VoWi-Fi. Receive Start of Packet (RX-SOP) is not required for VoWi-Fi as long as optimized roaming is configured.
9. Load balancing: Aggressive load balancing should not be enabled for Wi-Fi Calling deployments. It's useful for data- and bandwidth-intensive applications, but it may delay roaming.
10. Battery life: Enable the 802.11v Network Power Save feature.

Network Impact

Wi-Fi Calling will have an impact on your network design. The assumption is that iOS 8 will roam to the next Basic Service Set Identifier (BSSID) only if its signal is at least 8 dB better than the previous one. To avoid frequent 5-GHz to 2.4-GHz roams, make sure that the SSID is limited to one band (5 GHz if possible). Dual-band SSIDs are more apt to see frequent 5-GHz to 2.4-GHz roams.

For more information on Wi-Fi Calling and VoWi-Fi, go to http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white-paper-c11-733136.html.

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 C11-735826-00 09/15