

Optimize the Cisco Unified Wireless Network to Support Wi-Fi Enabled Phones and Tablets

This white paper provides technical guidance and outlines recommended steps that IT teams can take to more effectively support Wi-Fi enabled phones and tablets on the Cisco Unified Wireless Network. This guidance is applicable for 802.11n-enabled devices such as the Apple iPhone 4, Apple iPad, or [Cisco® Cius™](#) tablet as well as any other phone, tablet, or device that has a wireless profile that includes single spatial streams, limited 20-MHz channel operations, or selected support of 2.4 or 5 GHz frequencies.

Using Wi-Fi Enabled Phones and Tablets on the WLAN

Many organizations are discovering that employees, end users, and partners are bringing consumer Wi-Fi enabled phones such as the Apple iPhone 4 and tablets such as the Apple iPad, BlackBerry PlayBook, or Android-enabled tablets such as the Samsung Galaxy Tab or Dell Streak on to the enterprise wireless network. Organizations are also looking at ways to enhance productivity by deploying business-ready tablets such as Cisco Cius for business applications and real-time communications, video, collaboration, and TelePresence (Figure 1). As organizations incorporate a greater variety and quantity of mobility-enabled devices on to the wireless LAN (WLAN), IT teams will need to more effectively manage network resources in order to maintain a robust, high-performance wireless network.

Figure 1. Cisco Cius Tablet



802.11n and Wi-Fi Enabled Phones and Tablets

With more and more Wi-Fi enabled devices using the enterprise WLAN, it is important that IT teams properly configure their wireless network to optimize its performance. In most cases, today's Wi-Fi devices are operating in a mixed client environment in conjunction with 802.11a/b/g or 802.11n client devices that are operating in 2.4- or 5-GHz using one to three spatial streams (antennas) and 20- or 40-MHz channels.

802.11n Protocol Overview

The 802.11n protocol includes several enhancements in the physical (PHY) and the MAC layer that helps improve 802.11n wireless performance as compared to legacy 802.11a/b/g wireless networks. The new capabilities

introduced with 802.11n dramatically improve the reliability of wireless communications, wireless coverage predictability, and overall throughput for wireless client devices. The four major enhancements introduced with 802.11n include:

- **Multiple-input, multiple-output (MIMO):** MIMO uses the diversity and duplication of signals from multiple transmit and receive antennas to improve performance for 802.11n clients.
- **Channel bonding:** The 802.11n standard supports the use of 40-MHz adjacent channels in both the 2.4- and 5-GHz spectrums. This feature helps significantly improve wireless data rates when combined with the reserved channel space. It is generally recommended for use in only the 5-GHz spectrum.
- **Frame aggregation:** The 802.11n standard uses frame aggregation to coalesce multiple packets together, helping reduce the overhead associated with 802.11.
- **Backward compatibility:** The 802.11n protocol is backward-compatible with 802.11a/b/g, making it possible for 802.11a/b/g and 802.11n devices to coexist on a single wireless network. This feature gives organizations the opportunity to phase in 802.11n access points or client migration while still supporting legacy 802.11a/b/g clients.

Cisco Enhancements to 802.11n

Cisco has improved upon the capabilities of 802.11n by offering an advanced solution called [Cisco ClientLink](#). Cisco ClientLink uses RF beam-forming techniques to improve downstream performance (from the access point to the client) for 802.11a/g clients. Independent testing of Cisco ClientLink by [Miercom labs](#) has shown that the technology increases throughput by up to 65 percent for existing 802.11a/g client devices connecting to a Cisco 802.11n network. The solution also increases the total available channel capacity by up to 27 percent because of an increase in throughput speeds for 802.11a/g client devices.

Cisco ClientLink enables a Cisco 802.11n access point to "hear" 802.11a/g clients better. Because it is common for Wi-Fi networks to support a mix of 802.11a/g and 802.11n clients, Cisco ClientLink helps address the challenges of mixed-client networks by making sure that legacy 802.11a/g clients operate at the best possible rates - especially when they are near access point cell boundaries. Thus legacy client reliability and performance are improved. In addition, the technology helps free critical bandwidth for clients such as the Apple iPad and Apple iPhone 4 because legacy 802.11 a/g clients get on and off the wireless network faster.

802.11n and Apple iPad, Cisco Cius tablet, and Apple iPhone 4

Each Wi-Fi enabled phone and tablet that supports 802.11n has specific antenna and channel configurations. Specifications for each device are listed on the manufacturer's website. Because these devices are 802.11n-enabled, they can use 802.11n enhancements such as MIMO and frame aggregation to help improve their upstream and downstream performance. The specifications for the Apple iPad, Cisco Cius, and Apple iPhone 4 follow:

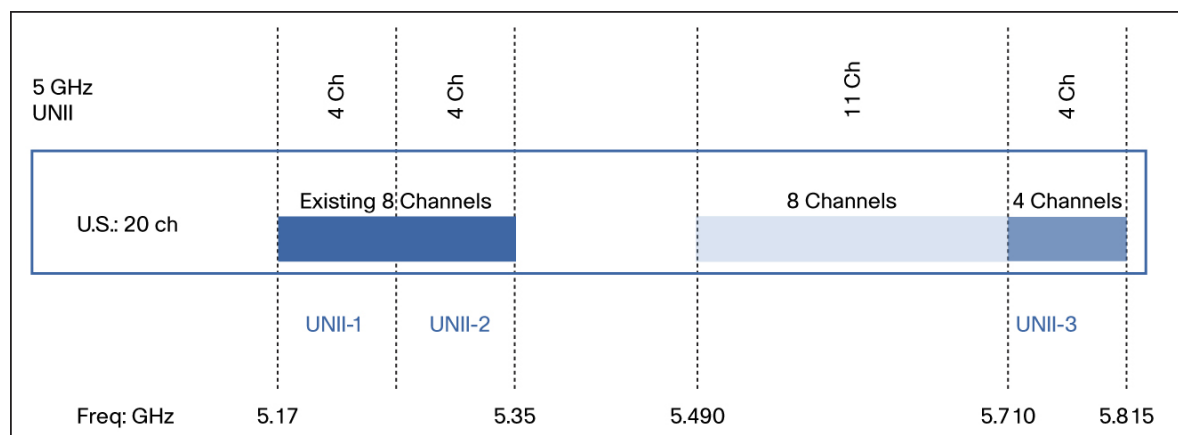
- The Apple iPad is a one-spatial stream (single antenna) 802.11n-enabled device that operates in 2.4- and 5-GHz spectrums using 20-MHz channels.
- The Cisco Cius tablet is a one-spatial stream (single antenna) 802.11n-enabled device that operates in the 2.4-GHz spectrum using 20-MHz channels and the 5-GHz spectrum using 20- or 40-MHz channels.
- The Apple iPhone 4 is a one-spatial stream 802.11n-enabled device that operates in only the 2.4-GHz spectrum using 20-MHz channels.

How to Optimize 802.11n WLANs to Support Wi-Fi Enabled Phones and Tablets

The following steps are recommended to help optimize a Cisco Unified Wireless Network 802.11n deployment to more effectively support the Apple iPad, Apple iPhone 4, Cisco Cius tablet, and other Wi-Fi phones, tablets, or clients with similar wireless profiles.

1. **Configure 2.4-GHz for 20-MHz and three nonoverlapping channels:** Cisco recommends that the 2.4-GHz frequency remain configured for 20-MHz and three nonoverlapping channels. Some organizations have proposed changing the 2.4-GHz configuration to support one 40-MHz channel and one 20-MHz channel. Cisco does not recommend changing the configuration of 2.4-GHz to support a 40-MHz channel because having three nonoverlapping 20-MHz channels provides greater flexibility for access point placement and WLAN design than one 40-MHz channel and one 20-MHz channel. Maintaining three 20-MHz channels helps enterprise deployments better optimize wireless capacity and coverage.
2. **Improve client reliability and coverage by implementing Cisco ClientLink:** In mixed client environments, 802.11a/g clients may delay communications for 802.11n clients and reduce overall system performance. Organizations can improve the reliability and coverage for legacy 802.11a/g clients, assist these clients in operating at the best possible rates, and help ensure that these legacy clients get on and off the wireless network faster by implementing [Cisco ClientLink](#). Cisco ClientLink is easily enabled through the wireless LAN controller or Cisco Wireless Control System (WCS) control panel.
3. **Disable lower data rates in 2.4-GHz:** When 802.11b clients communicate on the WLAN, they pull down overall WLAN performance. Because most 802.11b-only clients are being phased out in favor of 802.11g or 802.11a/g/n devices, Cisco recommends that you consider disabling the lower 2.4-GHz data rates on the WLAN (such as 1 and 2 Mbps). This is highly recommended if you know that 802.11b clients will not be used on your WLAN. Data rates can be adjusted through the wireless LAN controller or Cisco WCS.
4. **Encourage clients to use 5-GHz by enabling Cisco BandSelect:** Encourage dual-band clients to operate in the 5-GHz frequency by turning on [Cisco BandSelect](#). Because 5-GHz has eight times the spectrum of 2.4-GHz, it is usually less congested. Cisco BandSelect helps encourage clients to use the 5-GHz bands, helping free 2.4-GHz bands in mixed client environments. When enabled, Cisco BandSelect encourages dual-band clients to operate in 5-GHz while the single-band devices such as the Apple iPhone 4 continue to operate in 2.4-GHz. Cisco BandSelect is enabled through the wireless LAN controller or Cisco WCS.
5. **Utilize all of the available 5-GHz Spectrum with Dynamic Frequency Selection (DFS):** In the FCC regulatory domain, DFS for radar avoidance is required in order to use the 5-GHz channels in the UNII-2 and UNII-2 Extended bands (Figure 2). For additional channel capacity, consider enabling the UNII-2 band (Channels 52 - 64). These channels can be safely enabled because the majority of 802.11a/n clients support the UNII-2 band channels. You can also consider enabling the UNII-2 Extended band (Channels 100-140) since many clients now support these frequencies including Intel's 5100/5300/6200/6300 radios, the Apple iPad, and Cisco Cius. Learn more about DFS by reading the [Cisco Bulletin: 2007 FCC Regulations Update](#).

Figure 2. 5-GHz Spectrum with Dynamic Frequency Selection



6. **Detect and mitigate wireless RF interference with Cisco CleanAir:** Interference from Wi-Fi and non-Wi-Fi sources can dramatically affect WLAN performance and end-user satisfaction. Cisco recommends that organizations regularly scan the RF environment and immediately address RF interference that affects the WLAN.

[Cisco CleanAir technology](#) is available to help organizations quickly detect, classify, locate, and mitigate sources of wireless RF interference. It automates the detection of a broad range of RF interference sources and takes automatic action to keep the WLAN operating at peak performance. Reducing wireless RF interference helps improve network reliability and performance for all Wi-Fi clients including the Apple iPad, Apple iPhone 4, and Cisco Cius.

7. **Implement Cisco Radio Resource Management (RRM):** For full spectrum management of your RF environment, properly use [Cisco RRM](#) to facilitate a controlled RF environment. Cisco RRM automates the optimization of channel reuse and helps deliver tighter management of access point power levels. With a finite RF spectrum (a limited number of nonoverlapping channels) and the innate ability of RF to bleed through walls and floors, RF is ever-changing. What might be an optimal access point channel and power scheme one moment might prove to be less than functional the next minute as the RF environment adjusts to client demands, interference, items that absorb RF, and signal attenuation.

Cisco RRM allows the wireless network to continuously analyze the existing RF environment and automatically adjust access point power levels and channel configurations to help mitigate events such as co-channel interference and signal coverage problems. Cisco RRM helps reduce the need to perform ongoing site surveys, increases system capacity, and provides automated self-healing functions to compensate for RF dead zones, unexpected access point failures, and unexpected client demand. When Cisco CleanAir access points are installed, Cisco RRM works seamlessly with Cisco CleanAir to detect, locate, and mitigate wireless RF interference. Cisco RRM is configured through the wireless LAN controller or Cisco WCS.

8. **Improve multimedia and video with Cisco VideoStream technology:** Video is expected to account for nearly 90 percent of all Internet traffic by 2012. The quality of the video experience when delivered over Wi-Fi must be enterprise-class and must be capable of supporting multiple video, audio, and data streams in a reliable, synchronized manner without disruption. When delay, packet loss, and jitter enter visible thresholds, the usefulness of video quickly drops to zero. Video must be intelligible to be useful.

Extending video over Wi-Fi has certain challenges compared to wired networks. These challenges arise because Wi-Fi introduces a set of network performance characteristics including variable data rates, packet loss, and multicast unreliability that work against some of the traditional approaches to guaranteed quality of service (QoS).

If you are using real-time multicast video, [Cisco VideoStream technology](#) provides a significant improvement over standard WLAN solutions by delivering important traffic prioritization, protection, monitoring, and adaptability features for video over the wireless network. Cisco VideoStream technology is a system wide set of features for the Cisco Unified Wireless Network that takes advantage of the benefits of [Medianet](#) and incorporates critical enhancements for scalable, high-performance, high-quality enterprise video over Wi-Fi. Cisco VideoStream is enabled from the wireless LAN controller or Cisco WCS.

9. **Use the Cisco WCS client troubleshooting tools:** Cisco WCS includes a built-in client troubleshooting tool that provides a step-by-step method to analyze problems for all client devices. This tool helps speed the resolution of trouble tickets for a variety of Wi-Fi client device types. It helps quickly address a variety of problems, including authentication key mismatches, wrong credentials, expired certificates, policy manager state, and Dynamic Host Configuration Protocol (DHCP)/IP addressing. This robust tool can also assist with client trending analysis.

When [Cisco Compatible Extensions](#) clients and Cisco CleanAir technology are used, additional client troubleshooting diagnostic tools are available to support enhanced analysis of connection problems. Learn more

about using the Cisco WCS client troubleshooting tool by reading the section [Troubleshooting Client Issues with WCS](#) in the technical guide Cisco Unified Wireless Network: Troubleshoot Client Issues.

10. **Properly configure high-density wireless deployments:** For areas with a large number of end users or devices simultaneously accessing the WLAN, it is important to properly design and configure the wireless network for high-density usage. The following RF design best practices are recommended to help properly deploy a high-density wireless network:
 - i. **Accurately assess end-user bandwidth requirements:** Determine the bandwidth required for each user and the number of users to be supported by each access point.
 - ii. **Determine total bandwidth for each access point:** Calculate the total bandwidth required for each access point by multiplying the bandwidth required by the number of users to be supported by each access point.
 - iii. **Assess available access point channels:** Determine the number of channels available for each access point and the bandwidth available for each channel. Each Wi-Fi spectrum (2.4- and 5-GHz) has a limited number of channels based on the 802.11 specification, the size of the channel, and country-specific regulations.

For example, in the United States, 2.4-GHz supports three nonoverlapping channels, with each channel supporting 7 Mbps for 802.11b, 13 Mbps for 802.11b/g, 25 Mbps for .11g/a, and 150 Mbps for 802.11n. In all cases, 5-GHz channels will be critical to success, with between 4 and 22 additional nonoverlapping channels available in most regulatory domains.
 - iv. **Perform a thorough site survey:** A site survey helps define the contours of RF coverage for each area within a building and on campus. By performing a thorough site survey, organizations can discover building regions where multipath distortion is occurring and uncover campus areas where RF interference is high. The site survey also helps organizations more accurately determine the number of access points required to meet business and operational requirements. Learn more about performing successful wireless site surveys by reading the [Wireless Site Survey FAQ](#).
 - v. **Accurately define access point placement:** Determine the best placement for each access point and the distance between access points based on the site survey results, channel availability, and the total bandwidth required for each access point. In general, the closer each access point is to its neighboring access point, the more important it is to control the RF environment. In most high-density WLAN deployments, access points are placed 20 to 25 feet apart. This distance is closer than standard business Wi-Fi deployments, where access points are usually placed at an average distance of 50 feet apart. The exact distance between access points is determined during the site survey. Placing access points at a distance of less than 20 feet apart is not recommended.
11. **Properly configure Wi-Fi enabled phones and tablets:** Each Wi-Fi enabled phone or tablet supports a variety of configuration options and profiles. The following configurations are recommended for successful deployment of Wi-Fi enabled phones and tablets.
 - i. **Configure Cisco AnyConnect™ Secure Mobility Client:** For devices that use VPN, [Cisco AnyConnect Secure Mobility Client](#) makes the VPN experience more transparent and secure. Cisco AnyConnect Secure Mobility Client supports the always-on VPN experience across a broad set of PC and smart-phone mobile devices, including Apple iOS 4 devices. As mobile workers roam to different locations using always-on and intelligent VPN, the client can automatically select the most optimal network access point and adapt its tunneling protocol to the most efficient method.

Cisco AnyConnect Secure Mobility Client provides reliable and easy-to-deploy encrypted network connectivity from any Apple iOS 4 device, including Apple iPhone 4, delivering persistent corporate access for mobile users. The client can also enable built-in web security and malware threat defense. Download the Cisco AnyConnect Mobility Client for the iPhone from iTunes at <http://itunes.apple.com/us/app/cisco-anyconnect/id392790924?mt=8>.
 - ii. **Configure the Apple iPad and Apple iPhone 4 wireless security profiles:** The Apple iPad and Apple 4 support a variety of 802.1x authentication methods for enterprise environments. Wi-Fi networks are automatically displayed by each device, or they can be located under the Wi-Fi settings profiles. The correct 802.1x method is automatically selected for each wireless Service Set Identifier (SSID), or it can be

manually chosen at Settings > Wi-Fi > Security. If no digital certificate is required, users simply enter their user ID and password in order to gain secure access to the enterprise wireless network. If the organization's authentication method requires digital certificates, IT can create configuration profiles and send them to the Apple iPad and Apple iPhone 4. For more information about configuring the Apple iPad and Apple iPhone 4, please read the [Apple iPad in Business - Deployment Scenarios and Device Configuration Overview](#) or visit the website [Apple iPhone in Business](#).

- iii. **Configure Apple FaceTime:** The Apple iPhone 4 and Apple iPad include support for a feature called FaceTime, which uses the Wi-Fi network to place video calls to other Apple devices enabled with FaceTime. In order to properly enable this feature, Apple devices should be running the [Apple iOS 4.1 software upgrade](#). The enterprise IT department may also need to make adjustments to the enterprise network infrastructure to accommodate FaceTime calls. For more information, please read the Apple documents [iPhone 4 and iPod Touch \(4th generation\): Using FaceTime Behind a Firewall](#) or [iPhone and iPod Touch: Troubleshooting Wi-Fi Networks and Connections](#).

Summary

Organizations will continually experience the introduction of new wireless client devices that bring innovative collaboration and communication opportunities to businesses. The robust nature of the Cisco Unified Wireless Network makes it easy for companies to smoothly integrate these new devices, such as the Apple iPad, Apple iPhone 4, Cisco Cius, and Android-enabled devices, onto the secure enterprise wireless environment.

IT teams can optimize the performance of the Cisco Unified Wireless Network to help ensure a wireless environment that meets and exceeds their mobility needs by implementing the steps outlined in this document. These steps will help IT teams maintain a robust high-performance wireless network for all mobile users - especially those early adopters who bring new and exciting Wi-Fi enabled devices on to the enterprise WLAN and expect them to just work.

Why Cisco

With wireless LANs moving to mission-critical status, IT managers need a flexible wireless network that addresses their individual business, technical, and operational needs while also quickly adapting to changing business priorities. The Cisco Unified Wireless Network with CleanAir technology meets these exacting requirements by providing the industry's best 802.11n network performance, integrated RF interference services, and built-in easy-to-use tools. By effectively using all capabilities of the Cisco Unified Wireless Network, IT teams can deploy a self-healing, self-optimizing wireless network that automatically addresses RF interference problems and keeps the network operating at peak performance.

For More Information

- Cisco CleanAir Technology: <http://www.cisco.com/go/cleanair>
- Cisco wireless products: <http://www.cisco.com/go/wireless>
- 802.11n: The Standard Revealed white paper:
http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_c11-427843_v1.pdf
- Cisco demonstration of network applications on the Apple iPad:
<http://www.youtube.com/watch?v=XVjB3x7eQzg>



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)