



Cisco® CleanAir technology uses silicon-level intelligence to create a spectrum-aware, self-healing and self-optimizing wireless network that mitigates the impact of wireless interference and offers performance protection for 802.11n networks.

In today's business world, the wireless network is more than just a convenience; it's mission-critical. Wireless operates in a shared spectrum with a variety of applications and devices competing for bandwidth in enterprise environments. More than ever, IT managers need to have visibility into their wireless spectrum to manage radio frequency (RF) interference and prevent unexpected downtime.

## Interference: A Threat to Your Wireless Network

Microwave ovens, cordless phones, RF jammers, motion detectors, neighboring wireless networks, and wireless security cameras are just a few sources of interference that can shut down your wireless network, bringing business productivity to a halt. Because the RF spectrum involves many variables that are constantly changing, IT managers need to have visibility into the spectrum to prevent unexpected downtime. As latency-sensitive applications like voice and video make their way into the enterprise, IT managers have an even greater need to be aware of interference. Resolving RF problems requires not only the right tools but also the right training. Many enterprises lack the in-house resources and expertise for effective RF troubleshooting.

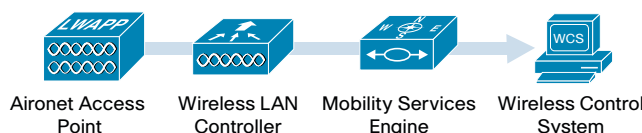
## The Value of Cisco CleanAir Technology

Cisco CleanAir technology delivers the performance of 802.11n and the reliability required to support mission-critical applications, all while intelligently avoiding the impacts of interference. CleanAir technology is a system-wide feature of the Cisco Unified Wireless Network that streamlines operations and improves wireless performance by providing complete visibility into the wireless spectrum. CleanAir has the unique ability to detect RF interference that other systems can't see, identify the source, locate it on a map, and then make automatic adjustments to optimize wireless coverage. CleanAir gives you access to real-time and historic information about devices and assets located anywhere in the

wireless network. Now IT managers can enforce policies and quickly take action to improve network performance based on intelligent information.

CleanAir technology is enabled by the advanced silicon design of the Cisco Aironet® 3500 Series Access Points, as well as Cisco wireless controllers, the Cisco Wireless Control System (WCS), and the Cisco 3300 Mobility Services Engine (Figure 1).

Figure 1. Components of CleanAir Technology and the Cisco Unified Wireless Network



Cisco CleanAir technology enables organizations to:

- Automatically optimize the wireless LAN for better reliability and performance
- Perform remote troubleshooting for fast problem resolution and less downtime
- Detect non-Wi-Fi security threats and resolve issues in real time
- Look at historic interference information for back-in-time analysis and faster problem-solving
- Set and enforce policy with intelligent identification of wireless devices

## Self-Healing and Self-Optimizing Wireless

With CleanAir technology, if an interference source is strong enough to completely jam a Wi-Fi channel, the system will change channels within 30 seconds to avoid the interference and resume client activity on another channel outside of the affected area. The system remembers intermittent interference from a microwave oven, bridge or wireless video camera and avoids the channels where these devices operate to prevent future interference.

Many companies claim they have an integrated interference detection system, yet their products can't decipher between Wi-Fi and non-Wi-Fi interference. Spectrum intelligence products from other manufacturers may falsely interpret any network noise as interference and

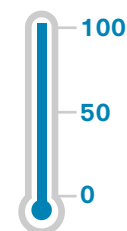
randomly switch channels, which jeopardizes network stability and may reduce overall network performance. Cisco CleanAir technology uses silicon-level intelligence to precisely detect and classify over 20 interference types, changing channels only if it determines that the interference is severe enough to impact network performance. If CleanAir changes channels it takes the entire network channel strategy into account and only then determines the preferred channel change. All of these intelligent features create a self-healing and self-optimizing wireless network that offers performance protection for 802.11n networks.

## Troubleshooting Forensics for Faster Interference Resolution and Proactive Action

CleanAir technology provides full visibility into the performance and security of the wireless spectrum, with an easy-to-read Air Quality Index. The index identifies problem areas and locates them in the context of access point, floor, building, and campus (Figure 2).

Figure 2. An Air Quality Index Providing a Snapshot of Network Performance and the Impact of Interference

Air Quality Index: 95



CleanAir reduces downtime. Network administrators can set alerts so that they are notified when air quality falls below a desired threshold. The system can also be configured to automatically enforce security or management policies. Cisco CleanAir generates reports to help network administrators prioritize interference issues that require immediate attention and easily drill down into the details for further network analysis.

Reports include a summary of the worst RF conditions, recent security risk interferers, threshold alarms, and historical charts. By proactively monitoring Air Quality Index charts and 30-day interference reports, administrators can establish normal behavior and monitor network trends which may indicate warnings of future problems before they affect network performance.



## Quick and Accurate Interference Detection to Reduce False Positives

Interference can be difficult to track because most devices are constantly moving or they turn on and off quickly. Even in very busy RF environments where hundreds of devices are operating simultaneously, CleanAir can classify over 20 different types of interference within 5 to 30 seconds. The accuracy and speed of CleanAir classification is a key differentiator because it reduces reports of interference when none exists ("phantom interference"), and eliminates duplicate reporting of the same device detected by multiple APs. It also reduces mislabeling of interference sources, saving administrators time often wasted in searching for the wrong type of device.

## Remote Access for More Efficient Problem Resolution and Reduced Travel

For remote troubleshooting, Spectrum Expert Connect mode provides an expert view of low-level spectrum plots from an individual access point's coverage area. While the CleanAir technology provides a great deal of higher-level analyzed data, including reports that classify devices and assess the wireless air quality, there will always be cases in which it is desirable to look at the real-time, raw spectrum data to help with a difficult-to-diagnose interference problem. This is particularly helpful if the type of interference is not included in the standard classification list.

## Effective Policy Enforcement

Enforcing policies to prohibit devices that interfere with the Wi-Fi network has been a challenge for network administrators. 2.4-GHz phones can disable handheld scanners that are used for inventory tracking in retail environments. College campus networks become unusable when Xbox games are active. With CleanAir technology, network administrators now have the ability to track network performance, locate and see the impact of non-Wi-Fi devices, and enforce policies that prevent known interference sources from taking down their networks or jeopardizing network security.

## Robust Security

From a security perspective, tracking devices on a map lets you know immediately where to dispatch your security personnel. There are a number of threats to your network that are invisible to traditional IDS/IPS systems—because they can only be detected at the RF level. These threats include proprietary wireless bridges, and older standards such as 802.11FH that may represent intrusion points on your network. These threats also include malicious Wi-Fi devices that operate on nonstandard operating frequencies or that use nonstandard modulation. And of course, there are always denial-of-service type attacks that can occur from jamming devices.

In addition to viewing security-impacting devices on a map, administrators can configure customized alerts based on device or location. This is a powerful feature since certain devices may be considered a threat in some areas of your building (for example, in trading wing), but not in other areas, such as the building lobby.

## Market Differentiators

Cisco CleanAir technology provides complete visibility into the wireless spectrum and optimizes wireless coverage to work around interference. Since wireless interference at the RF physical layer accounts for as much as 75 percent of wireless performance lags and connectivity disruption, gaining complete visibility into the spectrum is crucial in maintaining business-ready wireless application services. Cisco CleanAir delivers three distinct advantages that other interference solutions can't come close to matching:

- **Custom silicon implementation.** Only Cisco has invested in creating a custom chipset optimized to allow detection of non-Wi-Fi wireless transmissions while simultaneously serving network traffic. Because the detection and classification takes place on inline silicon and because it has access to rich low-level data not available with standard Wi-Fi chipsets, the CleanAir technology produces interference visualizations that are much more detailed and precise than those produced by competing systems.

- **High-definition interference visualization:** CleanAir is uniquely broad in its ability to detect 20 different interferers, and uniquely granular in its ability to visualize interference impact. These capabilities support more intelligent decisions and policies, for automatic remedial action and faster troubleshooting.
- **Systemwide integration.** Rather than managing interference on one access point at a time, CleanAir aggregates the impact of interference across the entire network. It can provide both real-time and historical views of interference across controllers, with reports on performance and the flexibility to remotely reconfigure access points to act as sensors that analyze RF.

## Summary

With CleanAir technology, the Cisco Unified Wireless Network correlates sources of interference across the network, allowing intelligent decisions and policies for faster troubleshooting and automatic RF interference avoidance. CleanAir makes it easy for network administrators to assess service disruptions, receive notices about performance degradation, and research resolutions and quickly take action to improve network performance. CleanAir is part of the industry's most adaptive, reliable, and high-performance wireless network—a network that has the ability to adjust automatically to changes in its environment, without the need for time intensive or costly human intervention. With Cisco CleanAir, organizations have the tools to support a truly mission-critical wireless network while simplifying ongoing operations. Business benefits include the ability to:

- Protect user productivity with reliable and secure performance for business applications
- Reduce troubleshooting time from days or weeks to hours, saving IT resources and protecting business productivity
- Consume fewer IT resources with automatic interference mitigation and faster troubleshooting
- Prevent costly downtime with a self-healing Wi-Fi network
- Seamlessly integrate mobile services and simplify the transition to 802.11n networking with Cisco partners and [Cisco Wireless LAN Services](#)