Wireless RF Interference Customer Survey Results

Executive Summary

Over 600 Cisco customers participated in an online survey about wireless RF interference and wireless network usage. The survey results confirmed that RF interference is affecting wireless network performance for a majority of companies. It also confirmed that the majority of companies now consider all or part of their wireless network to be mission-critical. With more companies relying on the wireless network for vital business functions, it is clear that minimizing the impact of RF interference and optimizing wireless network performance for enhanced reliability is critical for a company's operations, productivity, and success.

Survey Respondent Profiles

In April 2010, Cisco invited customers to participate in an online survey about RF interference and Wi-Fi network usage. Over 600 mid-market and enterprise customers participated in our survey. Survey respondents represented 28 different industry segments, including agriculture, arts, education (higher education and K-12 schools), financial services, government, healthcare, hospitality, manufacturing, oil/gas, and retail. Over 87 percent of the individuals completing the survey were IT managers or network engineers. Survey respondents were primarily from the United States, with some representation from Western and Eastern Europe.

Survey Results

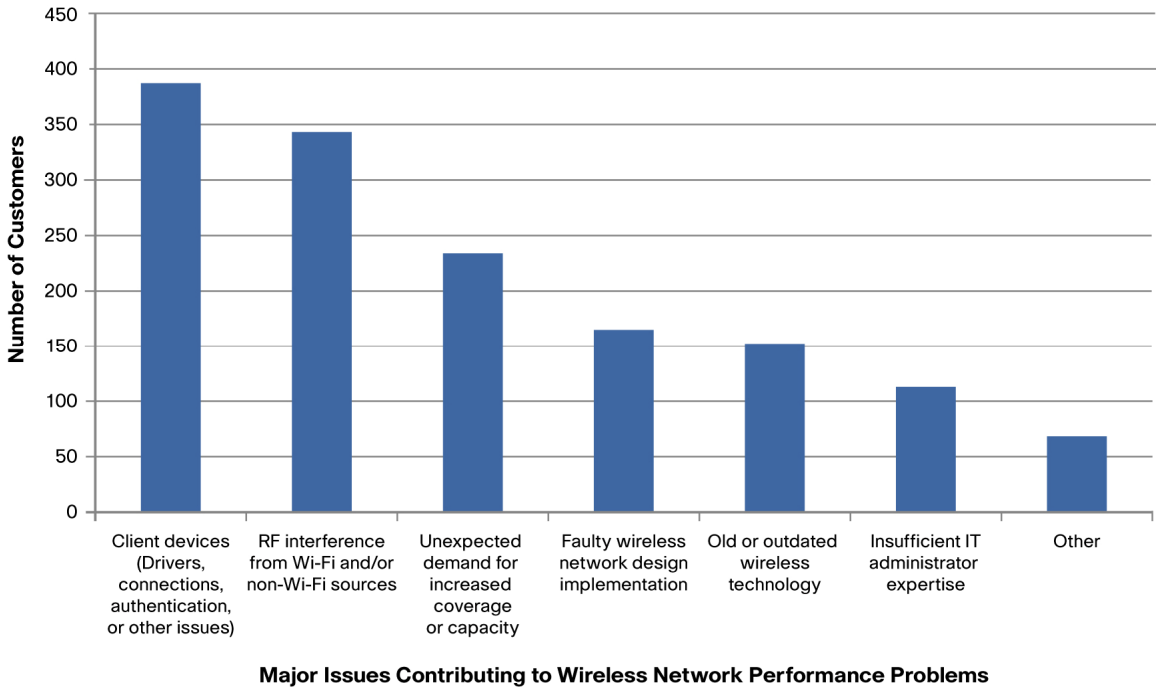
A variety of significant findings were generated from the wireless RF interference customer survey. Two of the most important findings of the survey were:

- 78 percent of companies now consider all or part of their wireless network to be mission-critical
- 54 percent of companies indicated that RF interference causes wireless network performance problems (and another 18 percent don't know if RF interference is impacting their Wi-Fi network)

The first finding confirms the growing pervasiveness of wireless in the workplace as a means to support mobile access to business-critical data and applications from anywhere, at any time. With over 42 percent of companies indicating that all or many of their employees use the wireless network as their primary network connection, it's clear that the trend towards enabling companywide wireless access will continue to grow.

The second finding demonstrates that RF interference is an important problem impacting wireless network performance and reliability. When asked to select from a list of major issues that contribute to wireless network performance problems, RF interference was a top concern (Figure 1).

Figure 1. Contributors to Wireless Network Performance Problems



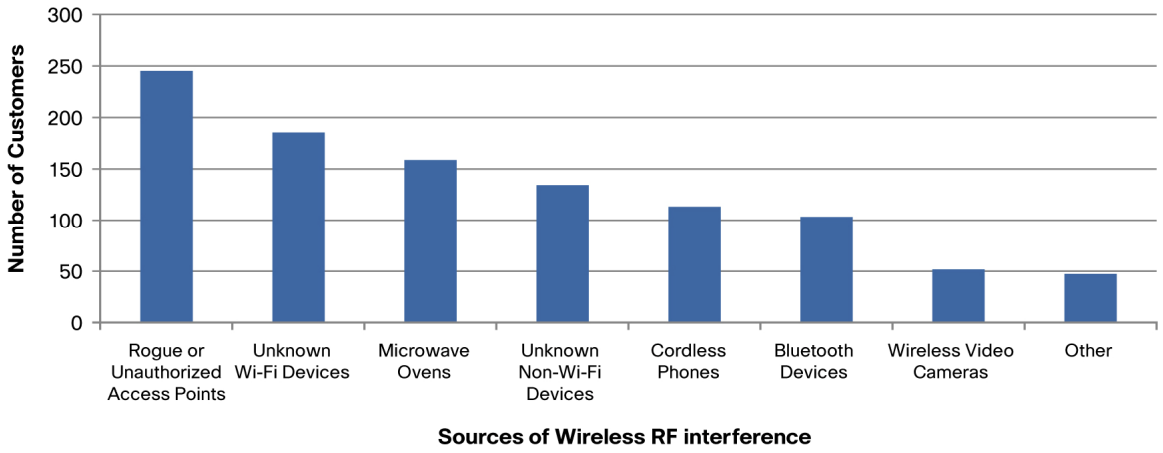
Note: Survey respondents had the option of selecting any or all of the issues listed. For the "Other" category, respondents listed issues such as lack of funding, lack of dedicated WLAN IT personnel, poor security implementation, application-related errors, bandwidth-IP address problems, and electromagnetic interference in manufacturing and transportation environments.

As shown in Figure 1, RF interference was listed as one of the top issues that contribute to wireless network performance problems. RF interference from Wi-Fi and non-Wi-Fi sources ranked higher than demands for increased network capacity, faulty wireless design, challenges with old or outdated technology, and insufficient IT administrator expertise. Only issues with client devices ranked higher than RF interference. This was expected since organizations continue to be challenged by misconfigurations of client devices and user errors that may or may not be related to the wireless LAN. The ranking of RF interference as a top issue contributing to network performance problems validates that it is an important concern for today's companies.

Primary Sources of RF Interference on the Wireless Network

To learn more about the types of devices causing RF interference problems on the wireless network, survey respondents were asked to identify their primary sources of wireless RF interference (Figure 2).

Figure 2. Primary Sources of Wireless RF Interference



Note: Survey respondents had the option of selecting any or all of the device types listed. Only responses indicating a frequency of occurrence daily, weekly, or monthly are included.

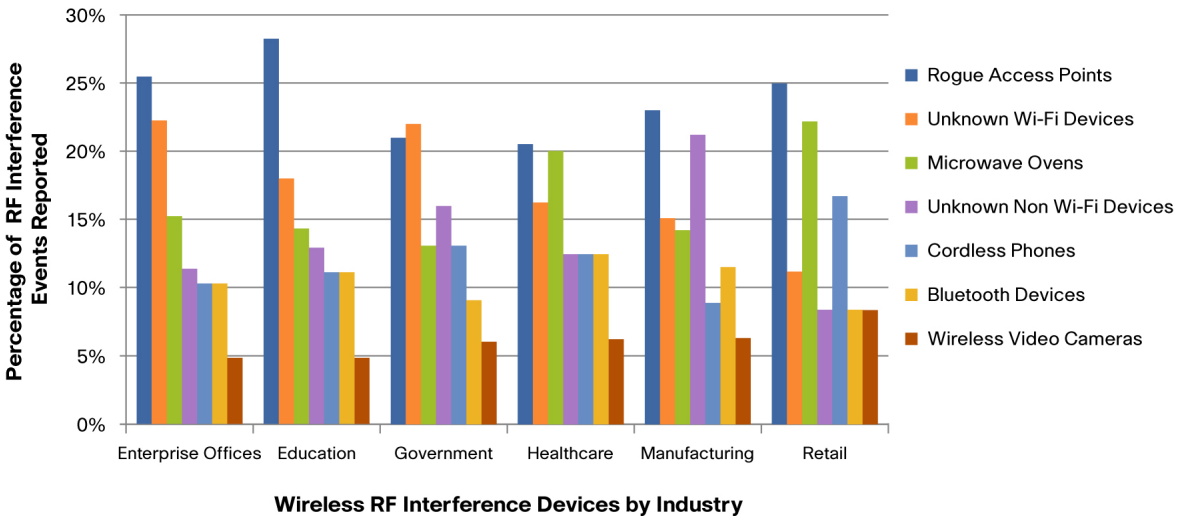
As confirmed in Figure 2, rogue access points, unknown Wi-Fi and non-Wi-Fi devices, and microwave ovens were found to be the primary sources of RF interference on most wireless networks. Together, these devices accounted for over 70 percent of the reported RF interference. Also important were cordless phones, Bluetooth devices, and wireless video cameras, which accounted for 26 percent of the reported RF interference.

An unknown Wi-Fi and non-Wi-Fi device is one that generates interfering events for which companies are unable to find the source of the interference. Unknown Wi-Fi devices are usually neighboring networks, Wi-Fi personal area networks (ad-hoc, peer-to-peer), wireless bridges (Wi-Fi-based), Wi-Fi devices left by previous tenants, Wi-Fi devices not removed after testing sessions, or devices performing malicious activity on the wireless network. Unknown non-Wi-Fi devices (operating in 2.4 GHz and 5 GHz) include microwave ovens, cordless phones, Bluetooth devices, continuous transmitters (video cameras, phones), game controllers (Xbox controllers), radar, consumer AV devices, wireless bridges (WiMAX, Canopy, or proprietary transmission schemes), or jammers.

Devices Causing RF Interference as Reported by Specific Industries

The devices identified as the primary sources of RF interference varied by industry. Figure 3 shows the devices causing wireless RF interference as reported by major industries.

Figure 3. Devices Causing Wireless RF Interference as Reported by Major Industries



Note: Survey respondents had the option of selecting any or all of the device types listed. Only responses indicating a frequency of occurrence daily, weekly, or monthly are included. Total respondents per industry: Enterprise Offices [business services, consultants, financial Services, legal, marketing, real estate, telecommunications, computer industry] (108), Education [K-12 and higher education] (102), Government [state, local, national, and military] (54), healthcare (88), manufacturing (64), and retail (23).

As shown in Figure 3, rogue access points were the primary source of wireless RF interference as reported by most industries, followed by unknown Wi-Fi devices, microwave ovens, and unknown non-Wi-Fi devices. While the information provided by survey respondents represents the most likely RF interference trends for each industry, it is not a complete representation of the RF interference occurring on the WLAN.

Most organizations only scan for RF interference intermittently in selected locations on the wireless network. They do not have the tools to pervasively scan and mitigate RF interference that may occur daily or hourly across the entire WLAN. Also, the tools that are in use may detect only a limited range of RF interference device types such as rogue access points or microwave ovens. These tools may not detect Bluetooth devices, radar, Xboxes or other types of RF interference. The tools also rely on on-site, in-person usage which can be costly for an organization and difficult to perform in remote locations. Alternatively, an organization may not use any RF tools and instead their RF interference sources are identified by on-site visual inspections of areas where RF interference is suspected. As a result, the RF interference reported by each industry may be under reported or devices causing interference may be completely missed or mislabeled as unknown. Based on this information, it is clear that organizations need a comprehensive tool that helps them detect, identify, and mitigate a wide range of devices that are causing RF interference and affecting wireless network reliability and performance.

Wireless RF Interference Summary by Industry

A review of the wireless RF interference reported by each industry is below.

For enterprise offices, the primary devices causing wireless RF interference were reported to be rogue access points and unknown Wi-Fi devices. Most rogue access points detected in this environment are from neighboring Wi-Fi networks and unauthorized employee-installed WLANs. For businesses, RF interference can be challenging because IT departments need to centrally manage local and remote sites that may span national and international locations. In the comments section of the survey, a business IT manager had this to say about RF interference:

> *Our global wireless networks are managed centrally and need a cost-effective way to monitor the RF remotely. At this time I have no way to get a handle on interference.*

In education, rogue access points and unknown Wi-Fi devices were reported as causing a high prevalence of RF interference on the wireless network. These rogue and unknown devices could be neighboring business WLANs, unauthorized deployments from students or faculty, or malicious activities on campus. This finding correlates with this comment from a university IT manager:

> *Since we're a university, we have a lot of rogues on and off our network. Most of our users are transient, so we don't get reports of WLANs down due to interference since the user usually moves to a new location within the hour. So some of our interference is most likely unreported. The rogue problem exists in residences and campus buildings next to businesses with Wi-Fi.*

Healthcare environments are especially challenging for Wi-Fi because of the prevalence of Wi-Fi-enabled devices and specialized equipment that generates signals affecting the 2.4 GHz or 5 GHz range. Rogue access points, microwave ovens, and unknown Wi-Fi devices were reported as the leading causes of RF interference for healthcare, with unknown non-Wi-Fi devices, microwave ovens, and Bluetooth devices also playing a role. The unique nature of the healthcare environment makes it challenging to identify the source of RF interference, as noted by this healthcare IT manager:

RF interference is always a potential player whenever there is a wireless issue in a particular area. We have two scenarios where we know we have interference but cannot determine the source.

Respondents from local, state, and national U.S. government agencies and the U.S. military indicated that unknown Wi-Fi devices and rogue access points were prevalent on the wireless network. Additionally, state and local government agencies, which represent the largest portion of the government responders, indicated that unknown non-Wi-Fi devices, microwave ovens, and cordless phones were also causing RF interference on a regular basis.

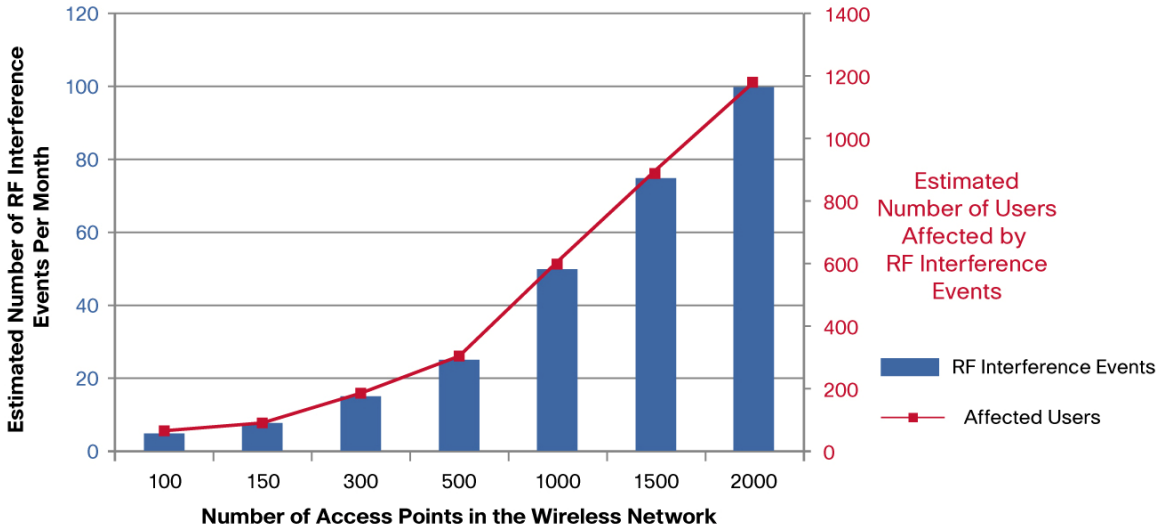
Retail respondents indicated that rogue access points, microwave ovens, and cordless phones generated the majority of wireless RF interference. This finding correlates with the expectation that neighboring WLANs, consumer or commercial microwave ovens, and cordless phones used by store personnel contribute significantly to the RF interference experienced by retail businesses located in shopping malls, business hubs, and store environments.

In manufacturing, where rogue access points and unknown non-Wi-Fi devices were reported as the primary sources of RF interference, one company stated that they have RF interference on their wireless network that they have been unable to track back to a specific device because they lack the tools to identify the proper source of the RF interference.

Projected RF Interference Events per Month

With 54 percent of companies indicating that RF interference causes wireless network performance problems, it was important to ascertain the number of RF interference events occurring on a company's wireless network. Based on the survey data, it was determined that five interfering events are occurring per month (average value) for every 100 access points. On average, 12 wireless users are affected by each interference event. Figure 4 presents the projected rate of RF interference events per month with a correlating projection of the number of affected users based on the size of the wireless network.

Figure 4. Projected RF Interference Events Per Month and Number of Users Affected by RF Interference Events



As indicated in Figure 4, a network with 300 access points will experience an average of 15 RF interference events per month, affecting an estimated 180 users. For a larger network of 2000 access points, an average of 100 RF interference events will occur per month affecting an estimated 1200 users. With millions of new Wi-Fi devices expected to be released each year and more businesses deploying companywide WLANs, organizations will be challenged to keep their networks free from the disruption and potential performance degradation caused by wireless RF interference events.

Cost Impact of Wireless RF Interference for Businesses

The cost impact of wireless RF interference is an important consideration. In response to the survey, 34 percent of companies indicated that a portion of their current trouble tickets are due to RF interference issues. With each interfering event having the potential to generate trouble tickets or help desk calls from users experiencing dropped connections, poor throughput, or connectivity issues, it is important that companies take the potential effects of RF interference seriously. An increase in trouble tickets can lead to an increase in IT and operations costs and a decrease in business productivity.

With the proper tools, IT teams can find and mitigate wireless RF interference, helping to reduce trouble tickets, improve productivity, and make the WLAN more reliable. An IT manager from a leading university provided this comment regarding the need for tools to help find and mitigate RF interference.

> *We really need a better tool to give us RF interference information, so I will know the extent of RF interference in our network. RF interference could be a very minor problem or a significant problem, I just don't know for sure.*

With 18 percent of companies reporting that they don't know if RF interference is impacting their Wi-Fi network, it's very likely that the number of trouble tickets attributed to RF interference is currently underreported.

Finally, over 22 percent of companies indicated that the cost of addressing RF interference problems has affected their decision to expand their wireless network. This finding is significant, since 78 percent of companies now consider all or part of their wireless network to be mission-critical. The fact that companies may delay the expansion of their wireless network because of RF interference is a primary concern. In today's competitive business environment, it is imperative that organizational growth is not impacted by WLAN performance issues - especially issues that can be easily addressed by putting the proper tools in place. This finding underscores how important it is that companies immediately address RF interference occurring on the wireless network.

Summary

The unprecedented growth of Wi-Fi and non-Wi-Fi devices that can cause interference in the unlicensed RF spectrum is challenging IT teams in their efforts to maintain peak wireless network performance. With the majority of wireless networks now considered mission-critical, companies need to address the impact that RF interference has on wireless reliability, business functions, employee productivity, and operational costs. Clearly, a solution is needed to help companies find and mitigate RF interference, maintain an optimized wireless network, and continue to ensure the success of the organization.

Why Cisco?

To address the RF interference issues validated as business critical by the results of the Wireless RF Interference Customer Survey, Cisco® CleanAir technology is now available. Cisco CleanAir technology allows organizations to quickly address RF interference events occurring on the wireless network. Cisco CleanAir technology protects 802.11n network performance by creating a self-healing and self-optimizing wireless network that detects, classifies, locates, and mitigates RF interference. Based on custom ASIC-level intelligence and fully integrated with the Cisco Unified Wireless Network, CleanAir technology automates the detection of a broad range of RF interference sources, provides systemwide maps, and takes automatic action to make the optimal corrections. With CleanAir technology, companies can easily and cost-effectively address RF interference issues and keep their wireless network operating at peak performance.

For More Information

- Cisco CleanAir Technology, visit: http://www.cisco.com/go/cleanair
- Cisco wireless products, visit: http://www.cisco.com/go/wireless
- The Cisco Unified Wireless Network, visit: http://www.cisco.com/go/unifiedwireless

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 C11-609300-00 07/10