RF Spectrum Policy: Future-Proof Wireless Investment Through Better Compliance

Radio frequency (RF) spectrum is an overlooked but critical resource. It is through the spectrum between 800 MHz and 5.9 GHz that an organization will:

- Connect laptops and PDAs to the network
- Talk on cellular phones, cordless phones, and headsets
- Secure buildings with security cameras

Unless properly managed, many of these technologies will crowd the spectrum and negatively impact WLAN services. Because the spectrum is a shared resource, the need to monitor, manage, and secure it is imperative to optimal wireless reliability and performance. This paper focuses on the process of defining a spectrum management policy.

Defining a Spectrum Policy

Usage of the spectrum is not covered in most existing IT policies. Even if there is a wireless policy in place, extending the existing policy so that it addresses issues of spectrum management is the recommended initial course of action.

In addition to addressing interference problems generically, organizations will also need to define a spectrum policy for mitigating security vulnerabilities specific to the RF spectrum. Mitigating such threats is beyond the scope of basic wireless computing policies or policies describing the acceptable use of IT equipment.

Using the definition stage to take stock of the wireless and IT asset policies an organization has in place is the preliminary step. Once this is established, the next process is to adopt the guidelines described in this paper to meet the business's needs.

Crafting the Main Statement

Generally, it is best to start with a general statement defining the intended purpose and goals of the policy. **Here is a sample policy statement that refers to WLANs:**

[COMPANYNAME] provides secure wireless access to computing and information technology (IT) resources for employees, associates, and guests as part of the services offered to enhance productivity in the workplace. Wireless networks operate within a shared and finite radio spectrum. The IT department will maintain administrative rights over this spectrum to ensure fair and efficient allocation of the resource. Ensuring availability requires the careful management of traffic and the minimizing of interference in the RF environment.

Adding Specific Rules and Remedies

Once a general statement about the purpose of the spectrum policy is made, enumerate rules and remedies. **Here is an example:**

1. The IT department reserves the right to grant, limit, or restrict access to the wireless spectrum within the physical spaces and on grounds owned and operated by [COMPANYNAME].
2. IT reserves the right to monitor the spectrum on a continuous basis, and may/will regulate all wireless activities at all company sites, including remote offices and common areas.
3. Should any device create harmful interference, IT may request immediate deactivation of the device until such time as it can be reactivated without causing harmful interference.
4. Any individual knowingly and maliciously causing harmful interference will be subject to disciplinary procedures.[1]
5. All wireless spectrum use is subject to the same provisions contained in current Acceptable Use Policies.

If appropriate, cite the section and paragraph numbers of specific policies that are relevant.

Defining the Scope of the Policy: Frequency Ranges Covered

Next, define the scope of the policy. The most straightforward way to do this is to list the spectrum ranges to which the policy applies.

While defining the scope, it is better to define parameters in the policy by frequency range rather than product type. New wireless products are coming out all the time, so by specifying frequency ranges, you curtail the need to continually redefine the policy's scope every time a manufacturer introduces a wireless product.

List all the frequency bands that are used today, as well as those that might be used in the future. It is better to be overly comprehensive than to risk omitting a frequency band that later turns out to be important.

Here is an example of a frequency list:

[COMPANYNAME]'s spectrum usage policy applies to all device traffic and interference occurring in the following frequency ranges:

1. 800 and 900 MHz, industrial, scientific, and medical (IS) bands,, all modes
2. 21920–1930 MHz, all modes
3. 32.4–5 GHz, all modes
4. 4.9–6 GHz, all modes

Alternatively, you can include a chart like the one shown in Table 1. Digitally enhanced cordless telecommunications (DECT), unlicensed personal communications service (UPCS), and ultra wideband devices and applications are included in the example.

[1] It is recommended to link spectrum security violations to other security violations covered by your current security and HR policies. Many organizations have existing policies related to traditional denial-of-service (DoS) attacks, spam, and so on. This makes it easy to insert specific RF violations, such as RF jamming or the use of rogue or unauthorized access points.

Table 1. A Sample List of Frequency Ranges and Devices

Frequency Range	Band/Region		Devices
800 MHz	Cell	**Cell**	Cellular phones and devices
865-870 MHz	Europe ISM		Cordless phones, UHF-RFID, SCATA, wireless video
902-928 MHz	ISM		Cordless phones, UHF-RFID, SCATA, wireless video
950-956 MHz	Japan–ISM		Cordless phones, UHF-RFID, SCATA, wireless video
1850-1910 MHz	Cell		Cellular phones and devices
1880-1900 MHz	DECT–ETSI		European DECT cordless phones
1920-1930 MHz	UPCS–U.S.		U.S.–to DECT V.6
2.400-2.500 GHz	ISM		Cordless phones, Wi-Fi, Bluetooth, ZigBee, alarm systems, motion detectors, and others
2.5 GHz +	WiMAX		
3.1 GHz	UWB	**UWB**	UWB—Ultra Wideband applications currently approved for 3.1–10.1 GHz
4.94-4.99 GHz	U.S.–to public safety		U.S. and others
5.155.35 GHz	ISM/UWB		Wi-Fi—802.11a, video cameras, others
5.475.35 GHz	ISM/UWB		ETSI approved for use in Wi-Fi, soon to be FCC to approved; also contains radar, microwave links
5.7255.875 GHz	ISM/UWB		Wi-Fi, cordless phones, video, Hyper to LAN
10.1 GHz	UWB		UWB applications currently approved for 3.1-10.1 GHz

Including Contact Information

Be sure to include an e-mail address or phone number that department managers and others can call with questions about wireless devices.

A Checklist for Reviewing Policy Contents

Table 2 offers sample summary spectrum policy.

Table 2. A Sample Spectrum Policy

Summary	Sample Content
Explanation of purpose	Wireless technologies are and will continue to be important to the organization. To help ensure that wireless products can function properly, the IT department needs to protect the spectrum as a shared resource.
The IT department will manage the spectrum	The IT department will monitor and manage the RF spectrum and coordinate the use of the spectrum among departments. The IT department will grant access to the spectrum after assessing the impact that new devices and services will have the spectrum.
List of reserved frequency bands	List which frequency bands your organization has approved for devices such as cordless phones, which frequencies are reserved for other devices such as RFID scanners, and so on. This list will serve as a "spectrum map" for your organization.
IT has the right to take action against devices that threaten the spectrum	If the IT department discovers a device causing interference, the department has the right to shut down the device until a resolution can be reached.
IT has established a process for testing, approving, and deploying wireless technologies	Other departments should check with the IT department before purchasing and deploying new wireless products. IT needs to assess the effects of products on the spectrum. Unfortunately, managers cannot simply trust product packaging to accurately describe the frequencies at which a product emits energy.
IT guides users to not bring unapproved personal wireless devices into the workplace	There are a huge number of consumer wireless devices out there, and employees sometimes bring them into the workplace without understanding that they may cause RF interference. Employees need to be educated about the problems of spectrum interference and told not to bring in wireless gadgets that have not been approved by the IT department.
A warning to users about maliciously harming the spectrum	If an employee purposefully jams the spectrum or knowingly interferes with wireless services, he or she shall be subject to disciplinary action.
A reminder that IT will monitor the spectrum	The IT department will periodically survey the spectrum, catalog the devices affecting it, and take action accordingly.
Contact information	List the phone numbers, e-mail addresses, or Web sites that employees should refer to when they have questions about new wireless products, RF interference, or the spectrum policy in general.

Get the Facts: Don't Trust Product Packaging

In assessing the effect specific products will have on the spectrum, reliance on RF data printed on product packaging is not efficient.

Information on product packaging or even in product literature is often too general to be accurate. It sometimes omits important data about the frequencies at which a product operates.

For example, the box for a cordless phone or headset might say "2.4GHz or 5.8GHz DECT," suggesting that the phone operates in one range or the other. In reality, the phone might use both frequencies. In this case, the phone might use 5.8GHz DECT for caller ID and for dialing, and then switch to 2.4GHz frequency shift keying (FSK) (with a very high duty cycle that is harmful to WLANs) for call audio. Phones and headsets commonly use multiple frequencies this way.

The best source for accurate and detailed RF data about products can be found by researching the Federal Communication Commission's free, online database of product information, which you can find at: https://gullfoss2.fcc.gov/oetcf/eas/reports/GenericSearch.cfm

The database provides accurate, detailed profiles of wireless products.

Auditing the Spectrum

In addition to communicating spectrum policy, actively monitoring the spectrum is critical to assessing how much "bandwidth" is available for new services.

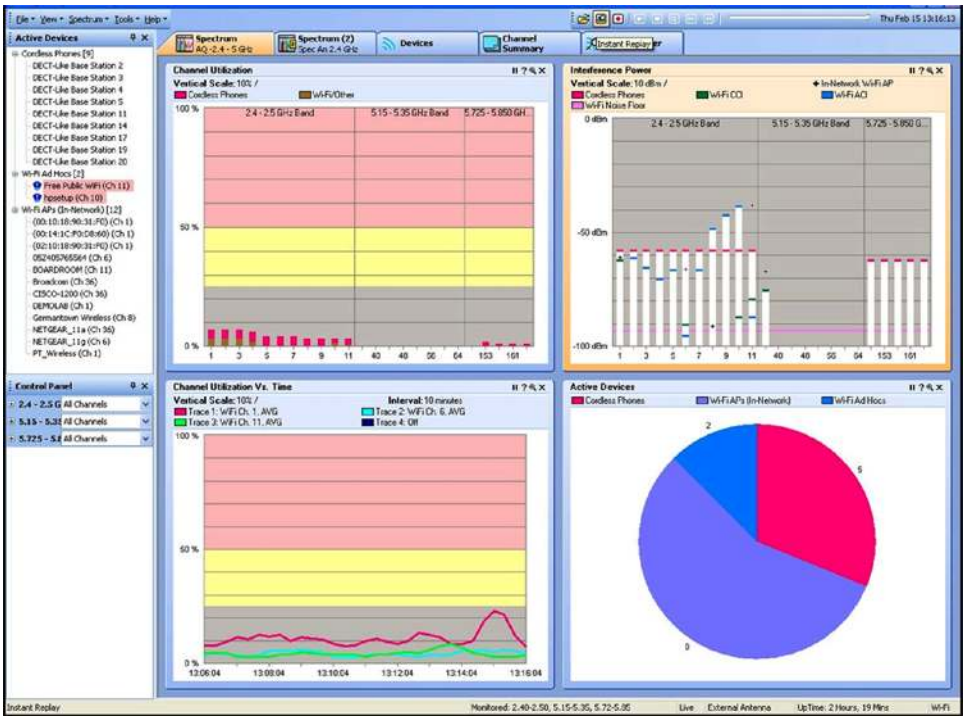
- **Audit the site using an RF analysis tool such as Cisco® Spectrum Expert Wi-Fi.**

  The Cisco Spectrum Expert Wi-Fi (Figure 1) is a laptop-based tool that monitors the wireless spectrum, identifies all the interferers present, and graphs the effect of those interferers on specific channels of your WLAN. Using the Device List in Cisco Spectrum Expert, you can make inventories of the types of cordless phones and other wireless devices transmitting in the spectrum. Save device lists, charts, and bar graphs for records, and establish a baseline of spectrum availability.

- **Periodically retest the spectrum to help ensure it is available for approved devices, and that no new sources of interference have arisen.**

  If a new device is detected, Cisco Spectrum Expert will help find its location, so that you can mitigate the harmful effects of the device either by shielding it, removing it, or replacing it.

Figure 1. Cisco Spectrum Expert Wi-Fi



Broadening Your Spectrum Policy

Once your spectrum policy is established, over time you may want to broaden—but not over broaden—the policy's scope. What else should you consider?

ISM Bands

Consider expanding the scope of the spectrum policy to include all ISM bands, which is a lot of spectrum to manage. Weigh broadening the policy to proactively give IT authority to act when problems occur, against taking responsibility for such a large area of spectrum and so many device types that the scope of the policy exceeds the department's ability to enforce it.

Airports and Hospitals

At airports and hospitals, special groups may be in charge of radios and other RF to emitting devices. IT managers and network engineers should meet with these other stakeholders to collaborate onsite to widen spectrum management policies.

The New UPCS Band

The UPCS band is a new addition to the unlicensed space. It is located at 1920 MHz to 1930 MHz. What runs there? DECT 6.0 does. This is the band in which cordless phones and headsets are starting to move after the FCC made this band available in April 2006. Addition of the UPCS space is not a complete panacea for your cordless phone and headset problems, however. The space is only 10 MHz wide, and there is a practical limit to how many DECT devices can share that spectrum in a given area. Different manufacturers have different guidelines for how their products can be used in the UPCS band. Become familiar with them.

DECT

Consider specifying the technology that can be used in a cordless phone or headset. Digitally enhanced cordless telecommunications (DECT) devices have three very nice attributes that stand out:

- **Privacy:** DECT has encryption built in, although it is not a mandatory part of the specification. Many implementations have focused on security as a feature and enhanced operation significantly.
- **Visibility:** DECT uses a 5-byte address to identify an associated handset with the base station. This address is visible in Cisco Spectrum Expert and can be used to audit from the air.
- **Standards-based:** In the cordless phone market, traditionally there have been very few standards and virtually no interoperability between manufacturers. DECT Version 6.0 should significantly reduce that trend.

Wireless Headsets

Call center staff, inside sales teams, and other workers who spend long hours on the phone will all eventually want wireless headsets, if they do not already own them. To meet the demand, you can roll out the headsets in a controlled fashion, mixing 900-MHz and 1.9-GHz models to minimize interference with other headsets and with WLANs operating at 2.4 GHz or 5 GHz.

Video Cameras and Motion Sensors

Which other wireless devices might create problems for your spectrum? Video cameras are a possibility, as well as motion sensors for alarms and automated lighting applications. It is far easier (and often less conspicuous) for the security team to install a wireless camera than to have cables run. But video cameras, in particular, can produce a very disruptive signal. These devices run rampant in the 2.4-GHz frequency—the same frequency used for 802.11b/g WLANs. Test such devices before deploying them. If WLAN performance suffers, use an RF analysis tool to check for the effects of cameras, motion sensors, and other physical plant infrastructure to determine if they're playing a role in the problem.

Bluetooth Devices

There's little need to be concerned about a single Bluetooth headset. However, 200 headsets operating in an auditorium whose AV system runs over 2.4 GHz can create a real problem. Keep in mind that with numbers come congestion. Multiple Bluetooth devices can crowd the airwaves, potentially disrupting other services.

It is also important to watch for security risks introduced by Bluetooth devices. Many well-meaning users have inadvertently but efficiently defeated a WLAN's Wireless Application Protocol (WAP) security simply by adding a nifty Bluetooth headphone to a laptop. The headset's installation CD usually offers to install a handy Bluetooth access point at the same time that it loads the headset's drivers. Most users will simply just keep clicking "Yes" until music comes out, not realizing that by converting their laptop to a Bluetooth access point, they're creating a backdoor that hackers can use to access the WLAN.

Educating users about security risks like these is as important as setting policies for managing the spectrum.

Devices That Fall Outside the Spec

Electrical devices sold in the United States must meet FCC part B certifications, which verify that devices have been correctly designed, and that they do not inadvertently transmit RF interference. But the physical condition of a device—even a device that passes certification—can change over time. Especially if a device has received little maintenance or improper maintenance, it may end up performing in unexpected and potentially harmful ways.

When age or improper maintenance causes a device to fall out of specification and transmit RF energy that congests your spectrum, you won't be able to detect the problem by referring to the FCC database or checking product specifications. This is a problem that can only be discovered and diagnosed through an RF audit of the spectrum itself, using a tool like Cisco Spectrum Expert Wi-Fi. You need to see what's really happening in your airwaves. Through FFT (Fast Fourier Transform) charts and other reporting tools, RF spectrum analysis can reveal problems such as out-of-spec products. RF spectrum analysis will also enable verification of whether a product is performing correctly again, after it has received maintenance or an upgrade.

Conclusion

By establishing a spectrum policy and following the best practices advocated in this paper, an organization can proactively improve the management and security of the wireless spectrum. Defining a policy and enforcing it with periodic RF audits is the best way to help ensure that organizational benefits from advances in wireless technology last for years to come.

For more information on the effects of interference and spectrum solutions, visit:

http://www.cisco.com/en/US/products/ps9393/index.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 C11-449282-01 10/09