White Paper

Wireless LAN Equipment in Medical Settings: Addressing Radio Interference Concerns

The proliferation of devices emitting and receiving radio frequencies in the 2.4-gigahertz (GHz) range has given rise to concerns about radio interference in this spectrum. This concern is often voiced in relation to wireless LAN (WLAN) technology operation around medical devices. Cisco Systems believes that interference between medical devices and WLAN technology can be mitigated with a properly conducted site survey and a well-designed network. Indeed, Cisco WLAN radios are operating in major medical facilities with no reported cases of interference from Cisco WLAN equipment.

This paper provides some background on wireless interference, describes preliminary test methodologies to determine interference, and describes installation best practices that serve to minimize or eliminate the potential for WLAN radio interference in medical environments. It concludes with an at-a-glance chart containing some of the medical devices that radios have been tested against for interference. This is, by no means, an exhaustive list.

The use of wireless technology in medical environments provides unique challenges for those installing wireless systems. They must deal with possible interference both to their own equipment, as well as to the equipment onsite.

To assist those installing wireless systems, Cisco has developed a quick ad hoc test method that is outlined in this document as well as a highly recommended, more thorough test procedure.

Understanding Wireless Interference

While there is no simple answer to the question, “If I install this in my hospital, will I have interference problems?” understanding the fundamentals of wireless interference can greatly assist those deploying wireless systems to manage or eliminate interference in medical environments. Interference problems are related to the location, frequency, output power, and radio frequency immunity level of the device(s).

Location, Frequency, and Power

The location, frequency, and operating power of networking products should be considered along with the radio frequency immunity level of the medical device before deploying wireless equipment in medical environments.

Radios using the 802.11b and 802.11standards operate in frequency bands referred to as the Industrial, Scientific, and Medical (ISM) and are allocated to these devices on a primary basis. Table 1 defines the frequency bands for WLAN in comparison to some of the ISM radio frequencies used.

Table 1 Frequency Bands Comparisons

Frequency	ISM	WLAN	U-NII	HyperLAN
902-928 MHz	Yes	Yes		No
2400-2483.5 GHz	Yes	Yes		No
5150-5350 GHz	No	No	Yes	Yes
5470-5725 GHz	No	No	No	Yes
5725-5850 GHz	Yes	Yes	Yes[1]	No

1. Currently UNII upper band stops at 5825 megahertz (MHz).

To put wireless LAN interference potential into perspective, it is worth noting that wireless radios are low-power devices. In other words, wireless LAN radios operate at power levels five to six times lower than most cell phones or handheld radios (Table 2), and operate on a non-interference basis. Non-interference means that they may not cause harmful interference but they must accept harmful interference (including interference that disrupts service).

Table 2 Wireless LAN Radios

Transmitter	Frequency	Power output
Very high frequency (VHF) hand held radio	150 MHz	3W EIRP
Cellular phone	860 MHz	600 mW EIRP
WLAN PCMCIA card	2.4 GHz	100 mW EIRP

Classic examples of location-related interference that have involved pacemakers and hearing aids are unlikely (although possible) with wireless networking. For example, the feedback condition that may sometimes result from cordless and cellular phones used in close proximity to hearing aids is unlikely to occur with WLAN devices because they are not likely to come into direct contact with a user's body during normal operating conditions. Furthermore, most of the pacemakers that registered notable interference levels were older models that did not have the level of radio frequency immunity found in newer systems. Additionally, interference was caused by systems operating in the 900-MHz band–certain cell phones operating below the 900-MHz spectrum have also caused similar interference. Changes to the design of pacemakers to increase their level of radio frequency immunity have helped eliminate some of the problems. In 1996, several of the Cisco radios were tested by Chicago Ingalls Memorial hospital to verify no problems would occur between Cisco 2.4-GHz radios and pacemakers. The summary report demonstrating compliance is on file at Cisco and available upon request.

Power levels also play a vital role in determining the potential for interference in medical environments. A 2.4-GHz transmitter operating with a 4-W Effective Isotropic Radiated Power (EIRP) could produce E fields exceeding 10V/m in the near field. Some devices may only be hardened to work three V/m fields. Therefore, when installing systems, the installer needs to keep in mind that the antennae should be kept at least two to three wavelengths away from sensitive equipment. Although it is worth noting that high power-levels are not alone in causing interference and other factors mentioned above such as location, frequency and radio frequency immunity levels must be considered along with power levels.

Advantages of Direct-Sequence Radios

Direct-sequence radios have the following advantages over frequency hopping in interference mitigation:

1. Flexible channel programming: Direct Sequence Spread Spectrum (DSSS) radios can be programmed to operate on select channels to reduce interference. Unlike frequency-hopping radios that hop the entire spectrum, the DSSS radios can be programmed to operate on dedicated channels to avoid interfering with devices that might be susceptible to radios operating in certain parts of the band. Thus, Cisco DSSS radios can be programmed to avoid channels where devices could be sensitive to emissions.
2. Configurable power: Radio power management allows DSSS systems to be configured to operate at lower power levels, which reduces the likelihood of interference to installed medical equipment. Power output levels can be reduced to as low as 1mW if required to reduce radio cell sizes and coverage reach.
3. Compliance with conservative emission requirements: Products are designed to the more stringent Class B spurious emission requirements which contribute to lower out-of-band emissions that can also affect medical devices.

The fact that many medical facilities have deployed 2.4-GHz WLANs in close proximity to medical equipment operating in the 900- and 2.4-GHz range is further testimony to the safety of DSSS wireless products in medical environments when operated in compliance with best practices outlined in this document.

Radio Frequency Immunity Levels

Interference is not necessarily due to problems with the transmitting device, in this case, the WLAN equipment. Interference may be caused by a medical device that is not properly hardened from the operating frequencies and power levels of the radio device. The relative immunity of the medical device to radio interference may depend on when the device was manufactured. Newer devices tend to be designed for more radio immunity than older devices. Cisco strongly recommends that you work closely with your biomedical engineering department to identify all devices that may be susceptible to radio interference and quantify their radio immunity. By doing this, you and the biomedical engineering department can come up with a frequency management plan to use in conjunction with a professional site survey. The following example illustrates why frequency management plans and professional site surveys are always a good idea. A report once suggested that electronic toys were possibly causing interference to certain medical devices. Naturally, hospitals considered disallowing these toys into wards where children were on certain monitoring machines. Had radio interference tests and installation best practices been adopted, the potential for immunity-related interference could have been identified or avoided before the interference occurred.

Medical EMC Standards

The Electromagnetic community (EMC) recently adopted a harmonized standard for equipment operating in medical environments. The requirements must meet the emission and immunity requirements of the International Electrotechnical Commission (IEC) 601-1.2. Cisco WLAN radios are evaluated to this standard as part of their system qualifications.

Please note that compliance with IEC 601-1-2 does not mean that the transmitter will not interfere with any medical device, but that the device's digital emissions are compliant with the industry limits and the device's digital portion has sufficient protection from interference from other electronic devices.

Though newer medical systems deployed in hospitals are designed and tested to the latest standard, it is possible that older systems that have not been evaluated to this standard have been deployed as well. Hence the need for working closely with the biomedical engineering department and technical staff to get all information on installed equipment and their levels of radio frequency immunity.

To date, there have been no reported cases of EMC interference to medical devices from Cisco wireless LAN equipment deployed in hospitals.

Ad Hoc Test Methodology for Determining Interference

Below, we outline an ad hoc test methodology to determine WLAN interference in medical environments. It should not substitute a professional site survey. The ad hoc test is merely a preliminary test to determine the radio frequency immunity of medical devices against WLAN infrastructure, but it is strongly recommended that this test be followed up by a professional site survey. The test procedure below was developed to provide an onsite ad hoc test as opposed to the more rigorous lab test. For a more in-depth test methodology than that outlined below, contact your sales support representative. The test methodology below is for verifying the ability of the medical equipment to operate without any malfunctions with the radio in close proximity.

General Test Requirements

1. The test should be done in a lab in a way that replicates the real-time operations as closely as possible. It should allow the WLAN to be set up and tested at distances ranging from 10 centimeters (cm) to three meters (m) or greater at a 360-degree angle around the device. For this test, an open room is highly recommended to isolate sources of interference.
2. The device that is being evaluated against the radio should be configured with all necessary accessories for this test, including any carts where it will be used. The medical device should be configured to operate as it would in its normal environment.
3. Configure the WLAN system to operate in its normal mode of operation and select the lowest operating frequency that the system operator plans to deploy.
4. The WLAN antenna should be set at a minimum distance of 10 centimeters (cm) from the medical equipment being tested. The reason we specify this distance is because 10 cm is the separation distance specified in American National Standards Institute (ANSI) Standard C63.4 for equipment under test and surrounding equipment.
5. Choose at least 16 equal points around the circumference of the unit to perform measurements.
6. Define the basis for a pass or fail of the medical device. This should be determined by the biomedical engineering team of the hospital, and, if necessary, as defined by the manufacturer of the medical device.

Network Card Testing

1. Place the WLAN unit with the antenna 10 cm from the edge of the unit, antenna polarized horizontally at the first test point.
2. Verify the medical device is operating normally as per the established definitions of normal operations done in the previous steps.
3. Turn the WLAN transmitter on and verify it is operating properly. If possible, adjust the transmitter to send maximum packet lengths or operate at 100 percent duty cycle with modulation turned on to test for worst-case scenarios.
4. Let the transmitter operate for five minutes.
5. Observe any changes in the operation of the medical device. If a problem occurs, note the problem, and observe if the problem goes away when the transmitter is turned off. If no problem occurs in a period of five minutes, then the chance of interference to that device from the radio is remote at this test point.
6. If the medical device has a problem, then move the transmitter out to the next test distance below and repeat test. If a problem occurs at the next distance, repeat the test at this point at each incremental test distance as specified below until the problem no longer occurs or the operation of the system is no longer impaired. If no problem occurs at the test distance selected, move transmitter antenna to the next test point around the circumference of the medical device.
7. Repeat this test series for each selected test point around the system and then repeat with the network card antenna polarized vertically. Conduct each test for five minutes.

- Test at a minimum of 10 cm
- Test at 20 cm
- Test at 50 cm
- Test at 100 cm
- Test at 1-m distance
- Test at 3-m distance
- Test at distances greater then three m if system still fails in 1-m increments
- Repeat test for each planned frequency of operation of the installation

The test suites for an access point or bridge is the same but must be repeated for each different antenna gain being deployed for the system.

Pass-Fail Criteria

The determination of pass-fail criteria for a device is addressed one of two ways. The first is to verify what the manufacturer of the equipment states as the pass-fail criteria for the device or installation.

The second method is to have the hospital biomedical engineering staff determine the pass-fail criteria. Suggested examples of minor or catastrophic failures are listed below.

Minor failure could include:

- Screen flicker
- Display color changes

Catastrophic failures could include:

- System reset
- System records inaccurate data
- Total system shutdown

Recommended Best Practices to Minimize the Potential of Interference

While there is a possibility of interference between medical equipment and WLAN infrastructure, this is minimal if the best practices outlined below are followed.

1. Have a certified installer perform a professional site survey of the facility. This should include a comprehensive study of all devices operating in the radio frequency spectrum in the facility.
2. Have the system installed by qualified professionals.
3. Review the overall layout of the facility and determine areas containing devices prone to interference from wireless as well as various internetwork status monitor (ISM) equipment. From this review, you can design antenna "keep out zones," in which access point antennae are mounted several meters away from sensitive equipment to avoid possible problems.
4. Use only properly certified components for the system. This includes only using antennae certified for use with the radios. Do not use amplifiers for the systems because Cisco radios are not certified with external amplifiers.
5. Develop a frequency-management plan based on the spectrum survey to avoid interference from or with ISM and other onsite wireless equipment.
6. Consider reducing power or reorienting antennas if problems exist or appear.
7. Consider performing some live tests based first on the ad hoc test methodology that is outlined in this document and then by conducting the more formal test procedure developed by Cisco Corporate Compliance. We also recommend having either the manufacturer of the medical device in question or a third-party lab evaluate the system for operation in an environment with a WLAN. It is highly recommended that the ANSI C63.18 procedure be used. If this is not available at the test lab, a copy of the recommended Cisco test procedure for performing onsite electromagnetic interference (EMI) testing with medical equipment may be obtained from Cisco.

Medical Devices Tested Against 900 MHz and 2.4 GHz Wireless Radios

Tests of WLAN equipment against medical devices is done on an ongoing basis by a number of parties such as hospitals, medical device manufacturers, and even radio vendors. Below is a list that highlights just a few of the commonly used medical devices that have been tested against wireless radios. This list is by no means exhaustive and will be updated periodically as additional devices and radio tests become available from those parties.

Medical Device Medical Device Testing		
The following list of devices was tested with WLAN radios. Neither radios nor medical devices showed degradation in normal operation at close proximity.		
Hewlett-Packard M2350A M1176A 78553A Pressure Monitor 78554 Data Management Monitor 78551D Hemodynamic Module 78670A Defibrillator 78500 Series Central Station 78100 Analog Telemetry Unit 43100A Defibrillator M2300 (CCM) Component Central Monitor M1403A Digital Telemetry Model 54 Merl in Bedside Monitor Codemaster XL M1723A Defibrillator	**BIO-TEK** Lionheart Simulator **Motorola** HT 90 (462550 MHz) **ZETRON** 64 DAPTPLUS Paging **NEC** V2 Paging System **EST** IRC -3 Fire Alarm System **Kendall** SCD5320 BDIAEDSIDE Monitor **First Temp Genius** Sherwood IMS	**McGraw Horizon** Infusion **Code Centry System 2** Dialysis Control Unit **Mansfield** 3001 IABP Cardiac Arrest Unit **Model 3000** Digital Thermometer **Marquette Mac 8** EKG **Putitan Bennet** 7200 Ventilator System **Siemans Cathcor** Catheterization Monitor

Conclusion

Cisco is committed to networking the medical environment. Cisco participates in various standard committees and partners with engineering (test and verification) teams at leading medical equipment vendors in order to minimize or eliminate the occurrence of wireless interference in deployments of Cisco wireless networking solutions.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

12/02 BW8740