The Value of Cisco Compatible Extensions (CCX) for Philips PageWriter Cardiographs

A White Paper from Philips Healthcare and Summit Data Communications

February 2009

Table of Contents

Executive Summary

Hospitals and other healthcare providers rely on medical devices, such as PageWriter cardiographs from Philips Healthcare, for patient care and patient safety. Connecting these devices to a hospital's network improves workflow on both the clinical path and the financial path, enabling the hospital to deliver better care to more patients, while billing those patients, and their insurance companies, quickly and accurately. By using wireless LAN, or Wi-Fi®, technology, medical devices can be connected to a hospital's network from anywhere in the hospital.

A Wi-Fi connection is provided by a Wi-Fi radio in the device. Because medical devices transmit and receive important and sensitive information, Wi-Fi radios in those devices must provide secure and reliable Wi-Fi connections.

IEEE and industry standards define how a Wi-Fi radio interoperates with a wireless LAN infrastructure, and the Wi-Fi CERTIFIED™ seal ensures interoperability. For many organizations that rely on medical devices, however, Wi-Fi CERTIFIED is not enough. These organizations need assurance that their medical devices will interoperate with a Cisco wireless LAN infrastructure and support Cisco wireless LAN innovations for enhanced security, mobility, quality of service (QoS), and network management. The Cisco Compatible seal gives organizations the assurance that they seek.

A client device earns the Cisco Compatible seal through a program called Cisco Compatible Extensions, or CCX. Like the Wi-Fi certification program, CCX:

- Includes a specification that defines a set of features that must be implemented in the hardware and software for a Wi-Fi radio or a device that uses a Wi-Fi radio
- Requires compliance testing conducted by an independent lab that is approved by the organization that manages the program
- Requires that a submitted radio or device pass all tests to be approved

The CCX specification is a superset of that used for Wi-Fi certification. Cisco has published several versions of its CCX specification, with each version building on the last. Today, medical devices, which are classified under CCX as application-specific devices (ASDs), are tested for version 4 (CCX V4). The specification for ASDs is a subset of the specification for laptops.

While CCX has been an overwhelming success in the laptop world, few medical devices carry the Cisco Compatible seal. Philips PageWriter cardiographs, which incorporate Wi-Fi radios from Summit Data Communications, have passed all tests for CCX V4 and earned the Cisco Compatible seal. That seal gives Philips Healthcare customers confidence that the PageWriter cardiographs interoperate with Cisco infrastructures and can take advantage of Cisco innovations for enhanced security, mobility, QoS, and network management.

Wi-Fi and Medical Devices

Medical devices play a critical role in patient care and patient safety. Today, nearly every hospital wants to connect these devices to its network, which is an information hub to which the hospital's healthcare and finance professionals can gain access from nearly anywhere in the hospital. Networking medical devices improves the workflow for everyone who uses the devices or relies on the data that that provide. For example, when a cardiograph is connected to a network, the hospital obtains workflow improvements on both the clinical path and the financial path:

- When a physician enters an order in a hospital system, that order can be downloaded to the electrocardiograph (ECG) where the test will be conducted.
- Immediately after a test, the cardiograph transmits the results to the ECG management system on the network, where the results are available to the physician for review.
- Transmitted results trigger an HL7 message that is sent to the electronic order system to clear out the order and initiate billing.

By putting medical devices on a network, a hospital can:

- Conduct more exams, with fewer errors, every day.
- Deliver better care to more patients, while billing those patients, and their insurance companies, quickly and accurately.

Wireless local area networks, also known as wireless LANs or Wi-Fi networks, are increasingly popular in hospitals. Rather than using Ethernet cables to transmit information to the network and receive information from the network, devices on a wireless LAN use radios that transmit and receive over the air. Wi-Fi devices can be connected to the network from anywhere in the hospital and can maintain their network connection even as they are moved from one location to another.

Wi-Fi Standards

Wi-Fi communication is handled by radios that use a specific type of radio frequency (RF) technology. A Wi-Fi radio in a device such as a PageWriter cardiograph interacts with a Wi-Fi radio in a network infrastructure device such as an access point, or AP. An AP typically has an Ethernet connection to the rest of the network and can be considered a bridge between the wireless LAN and the Ethernet network.

Nearly every Wi-Fi radio communicates by following a set of standards that are defined and ratified by the IEEE 802.11 Working Group[1], affiliated with the Institute of Electrical and Electronics Engineers – Standards Association (IEEE-SA). As a result, wireless LAN products often are referred to as 802.11 products. The base standards, or "air" standards, define how radios communicate with each other over the air. These standards include definitions of:

- Bands: The unlicensed frequency bands in which the radios can operate
- Modulation: Direct sequence spread spectrum (DSSS) and orthogonal frequency division multiplexing (OFDM)
- Data rates: Amount of data that can be transmitted, with rates measured in megabits per second (Mbps)

Table 1 on the next page provides an overview of the most popular IEEE air standards:

[1] For more information about the IEEE 802.11 Working Group visit http://ieee802.org/11/.

Standard	Year Ratified	Band(s)	Modulation	Top Data Rate
802.11a	1999	5 GHz	OFDM	54 Mbps
802.11b	1999	2.4 GHz	DSSS	11 Mbps
802.11g	2003	2.4 GHz	DSSS, OFDM	54 Mbps
802.11n	2009 (est.)	2.4 and 5 GHz	DSSS, OFDM	300 Mbps

Table 1: Popular IEEE 802.11 air standards

802.11b and 802.11g

The two most popular air standards are 802.11b and 802.11g. Radios that adhere to these standards operate in the 2.4 GHz band. Ratified in 1999, 802.11b specifies DSSS modulation and a maximum data rate of 11 Mbps. As 802.11b products became popular, demand increased for a standard that supports higher data rates and is also backward compatible with 802.11b. The answer was 802.11g, which was ratified in 2003. A superset of 802.11b, 802.11g specifies DSSS and OFDM modulation, the latter of which supports a maximum data rate of 54 Mbps. Today, 802.11g is the predominant standard. Wi-Fi devices that support 802.11g can interoperate with Wi-Fi devices that support 802.11b.

802.11a

While 802.11a was ratified at the same time as 802.11b, adoption of 802.11a was slowed by factors such as:

- Chipsets: Several popular wireless LAN predecessors to 802.11b operated in the 2.4 GHz band. As a result, 2.4 GHz radio chipsets were relatively plentiful. Competition among silicon providers and other suppliers brought down prices for components and chipsets for 802.11b radios. In contrast, few silicon providers produced chipsets for 5 GHz radios. As a result, 802.11a radios required more engineering work and had significantly higher prices than 802.11b radios.
- Range: Range is the distance from an infrastructure device such as an AP that a client device can establish and maintain a reliable connection. Because they operate at 5 GHz instead of 2.4 GHz, 802.11a radios deliver a lower range than 802.11b radios. In early wireless LAN deployments, relatively few access points (APs) were expected to cover large areas, and so it was important to maximize range.
- Data rate: Wireless LANs were first adopted in vertical markets such as retail, manufacturing, and distribution where mobile applications transmitted relatively small amounts of data. With its top data rate of 11 Mbps and typical throughput of 4-5 Mbps, 802.11b was more than adequate for these applications. 802.11a products were marketed primarily as delivering a higher data rate and more throughput, and demand for 802.11a remained relatively low. The debut of 802.11g in 2003 further diminished throughput-based demand for 802.11a, because 802.11g offers the same top data rate of 54 Mbps and, unlike 802.11a, is backward compatible to 802.11b.

As the 2.4 GHz band has become more crowded with Bluetooth headsets, baby monitors, some cordless phones, microwave ovens, and, of course, Wi-Fi devices, interest in Wi-Fi operation at 5 GHz has increased. 802.11a offers one option for 5 GHz operation. A second option is 802.11n, a forthcoming standard that will be ratified in 2009.

802.11n

Many people consider 802.11n a unifying standard that will dominate the marketplace in a few years. Although the standard is not ratified, dozens of infrastructure devices and mainstream client devices (such as laptops) use radios that are based on a draft of the standard. The Wi-Fi Alliance®, an industry consortium, is performing product interoperability testing and certification based on the draft standard.

802.11n radios operate at both 2.4 GHz and 5 GHz and can interoperate with radios that support 802.11n or any of the "legacy" standards of 802.11a, 802.11b, and 802.11g. Radios with 802.11n capability offer two primary advantages over radios that support both 802.11a and 802.11g:

1. Throughput can be up to 10 times greater
2. Consistent connections can be maintained at a higher data rate over a greater distance

The higher throughput of 802.11n is the result of a set of enhancements that include packet aggregation, block acknowledgement, wider channels, decreased spacing between sent packets, and MIMO (multiple input, multiple output) technology. To take full advantage of these enhancements, you must have 802.11n radios in both your infrastructure devices and your client devices. In contrast, you can obtain the benefits of greater range and more consistent connections even if you have 802.11n radios in your infrastructure devices but not in your client devices. Dual-band 802.11n radios for medical devices and other non-laptop devices are not expected to hit the market until 2010.

For hospitals with an established wireless LAN infrastructure, upgrading to 802.11n requires careful planning in at least three areas:

1. APs: The vast majority of APs that support pre-802.11n radios do not support 802.11n radios, and so those APs must be replaced.
2. Uplinks: Because 802.11n APs support throughput of greater than 100 Mbps, they should be connected to the wired network —not with the 100 Mbps Fast Ethernet uplinks that are prevalent in hospitals today —but with Gigabit Ethernet uplinks.
3. Power: 802.11n APs with simultaneous support for 2.4 GHz and 5 GHz operation have power requirements that exceed the maximum supplied by the current standard for power over Ethernet, 802.3af. Until 802.3at, the successor standard to 802.3af, is ratified by the IEEE in 2009, hospitals that want to deploy dual-band 802.11n APs must use vendor-specific solutions or creative approaches to ensure that AP power requirements do not exceed the power supplied to those APs.

Wi-Fi CERTIFIED

Since 802.11b standard was ratified in 1999, wireless LANs have become extremely popular worldwide. The foundation of the wireless LAN boom is interoperability, which ensures that the Wi-Fi radios in client devices will interoperate with the Wi-Fi radios in infrastructure products, such as APs and routers, regardless of who makes the radios, the client devices, or the infrastructure products. Interoperability results from all products supporting the same standards for communication and interoperation.

While the IEEE defines the standards for how wireless LAN radios operate, it has no mechanism for enforcing these standards. Interoperability of wireless LAN products from different vendors is ensured by the Wi-Fi Alliance, a non-profit industry association of more than 300 member companies. The Wi-Fi Alliance determines how well products implement IEEE 802.11 standards by developing rigorous interoperability tests and running those tests against products from different vendors. Since the introduction of the Alliance's certification program in March 2000, more than 4,000 products have passed all required tests and are designated as Wi-Fi CERTIFIED.

Wi Fi CERTIFIED

Radios in select Philips PageWriter cardiographs are Wi-Fi CERTIFIED.

Wi-Fi Security

As mentioned in the previous section, Wi-Fi radios send data to each other over the air, using radio waves. These radio waves do not travel in a direct line but spread out over a wide area. They "bleed" through most types of walls, ceilings, and floors, and they reflect off some metallic surfaces. Wi-Fi

transmissions can be viewed by any computing device that is in the vicinity, provided that the device is equipped with the following:

1. A Wi-Fi radio
2. An antenna that provides sufficient gain to enable the radio to "hear" the Wi-Fi packets
3. A commonly available software application called a Wi-Fi sniffer, which makes the contents of Wi-Fi packets viewable

Wi-Fi Security Threats

Without proper Wi-Fi security in place, a hacker can use intercepted Wi-Fi packets to do one or more of the following: view sensitive information, gain access to the wireless LAN, or trick users into communicating with him instead of the network.

The first threat of weak Wi-Fi security is **data exposure**. Some of the data packets that travel between a Wi-Fi client and a wireless LAN may contain sensitive information such as patient-private information. If the packets are not scrambled, or encrypted, so that they cannot be deciphered by a hacker, then the hacker can view sensitive information just by sniffing and viewing the packets.

Weak Wi-Fi security also can lead to **network exposure**. In addition to data packets, control packets travel between Wi-Fi clients and a wireless LAN. When wireless LAN access is not governed by a strong authentication mechanism, then a hacker can use the control information in sniffed packets to pose as an authorized user and gain access to the wireless LAN. Once on the wireless LAN, the hacker may be able to gain access to sensitive information on the network.

A third threat of weak Wi-Fi security is **man-in-the-middle attacks.** When Wi-Fi clients are not required to use strong authentication methods, a hacker's laptop posing as an AP may be able to trick clients into associating with it instead of a trusted AP. Once a Wi-Fi client associates with a hacker's laptop, the hacker may be able to steal information from the client, including sensitive information and information required to gain access to the trusted network.

To thwart the first two threats, you must employ a Wi-Fi security system that prevents a hacker from viewing transmitted data and from gaining access to the network where data resides. Such a security system is shown in Figure 1 on the next page. To thwart the third threat, you must ensure that every Wi-Fi client uses strong authentication to be sure that it interacts only with a trusted wireless LAN and not an intermediary.

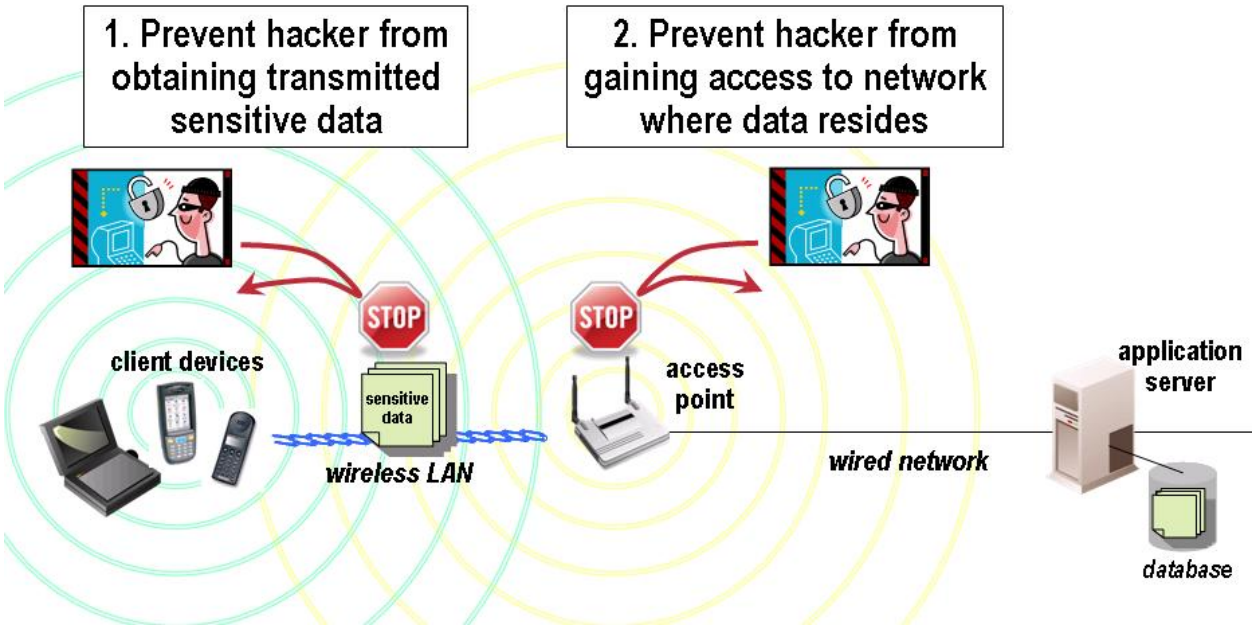


Figure 1: Solid Wi-Fi security protects sensitive data.

WEP: Insufficient

As a part of the 802.11a and 802.11b standards, the IEEE defined a security mechanism called Wired Equivalent Privacy (WEP). This security mechanism focuses on scrambling, or encrypting, transmitted data through the use of an encryption key, called a WEP key, that is shared among all devices that want to participate in a wireless LAN. While WEP seemed sufficient when it was defined in the late 1990s, security experts quickly realized that WEP does not offer sufficient security, for reasons that include:

- **No access control:** While it defines a means to encrypt transmitted data, WEP provides no means to control access to a wireless LAN. If you know the WEP encryption key, then you can gain access to the wireless LAN.
- **Vulnerable keys:** Due to weaknesses in WEP, a hacker can "crack" or decipher a WEP key by collecting WEP-encrypted data packets and running them through a WEP-cracking tool. Today, using sophisticated tools, even a 104-bit WEP key can be cracked in less than an hour.
- **Static keys:** The only way to avoid the use of a WEP key that has been cracked by a hacker is to change all WEP keys regularly, which today means more frequently than every hour. Because the most common way of deploying WEP keys is to define them statically on all devices that used them, changing WEP keys is an administrative nightmare.

WPA and WPA2

In 2001, the IEEE formed a task group, called the 802.11i task group, to define a standard for stronger wireless LAN security. The task group took several years to define, debate, finalize, and ratify the standard. In the meantime, the market grew increasingly impatient for something better than WEP. The Wi-Fi Alliance responded to market pressure by teaming with the 802.11i task group to create WPA, which the Alliance termed "a significant near-term enhancement to Wi-Fi security". WPA made its debut in 2003.

According to the Alliance, WPA is "a specification of standards-based, interoperable security enhancements" that ensures data protection through encryption and wireless LAN access control through

authentication. WPA was designed to be supported in software by Wi-Fi CERTIFIED products that previously had supported WEP.

There are two versions of WPA: Personal and Enterprise. Both versions encrypt and decrypt transmitted data using Temporal Key Integrity Protocol, or TKIP. Like WEP, TKIP uses RC4 encryption, but TKIP is designed to address all known vulnerabilities of WEP by providing these enhancements:

- Longer initialization vector, which minimizes the chance that a key will be reused during a session
- Key hashing, which results in a different key for each data packet
- Message integrity check, which ensures that the message is not altered in transit between sender and receiver

The key used for TKIP encryption and decryption is derived dynamically from the information exchanged between the Wi-Fi client and the wireless LAN during the authentication process that proceeds the client's connecting to the wireless LAN. With WPA-Personal, authentication is done through a four-way handshake using a pre-shared key (PSK) or passphrase. If the PSK on the Wi-Fi client matches the PSK on the AP to which the client is trying to associate, then the authentication succeeds, and an encryption key for that client is derived and stored on the client and the AP.

While PSKs are easy to implement on small networks, a hacker can "guess" a short PSK using a dictionary attack. In such an attack, the hacker captures packets that were created using the PSK and then, using a dictionary of potential PSKs and the published algorithm for WPA, tries to recreate the capture packets. If he is successful, then he has determined the PSK, and he can use it to gain access to the wireless LAN. The IEEE and various researchers recommend that, if you use a PSK, that PSK should be a random string of at least 20 characters, including characters other than letters and digits.

While WPA-Personal relies on a pre-shared key or passphrase for authentication, WPA-Enterprise relies on IEEE 802.1X, a ratified standard for network access control. 802.1X supports a set of Extensible Authentication Protocol, or EAP, types for mutual authentication of the client device and the network to which it is trying to connect. 802.1X authentication with an EAP type such as PEAP or EAP-TLS is extremely strong.

In July 2004, the IEEE approved the full 802.11i specification. Soon after that, the Wi-Fi Alliance introduced a new interoperability testing certification, called WPA2 that incorporates the key elements of 802.11i. WPA2 is essentially the same as WPA, with TKIP replaced by a stronger encryption method based on the Advanced Encryption Standard (AES) cipher. In March 2006, the WPA2 certification became mandatory for all new equipment certified by the Wi-Fi Alliance.

Figure 2 provides an overview of WPA-Enterprise and WPA2-Enterprise:

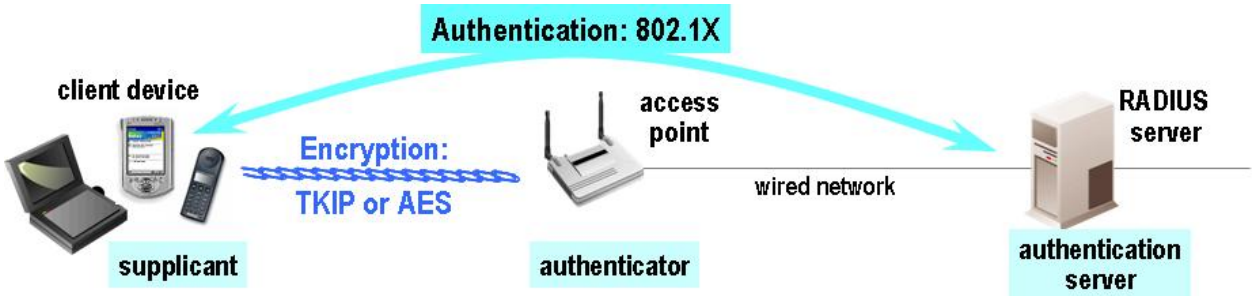


Figure 2: WPA-Enterprise and WPA2-Enterprise

Table 2 on the next page compares popular EAP types that are used with 802.1X authentication:

Type	Credential(s)	Database(s)	Pros and Cons
LEAP	Microsoft password	Active Directory (AD)	No certificates Strong password required
PEAP with EAP-MSCHAP	Microsoft password	AD	Native support in Windows, CE CA certificate on every client device
PEAP with EAP-GTC	Password, one-time password, token	AD, NDS, LDAP, OTP database	Broad range of credentials CA certificate on every client device
EAP-TTLS	Wide variety	Wide variety	Broad range of credentials Not widely supported
EAP-FAST	Microsoft password, others	AD, others	No certificates Complex provisioning process
EAP-TLS	Client certificate	Certificate authority (CA)	Very strong authentication Native support in Windows, CE CA, user certificates on every client device

Table 2: Comparison of popular EAP types

In late 2008, two German researchers reported that a vulnerability in TKIP could enable an attacker to decrypt individual packets that are encrypted with TKIP. The same vulnerability does not exist with AES-CCMP, the encryption algorithm used with WPA2. In other words, the researchers confirmed that WPA2-Enterprise offers stronger security than WPA-Enterprise. Given that a broad range of client devices support WPA2-Enterprise, every organization should rely on WPA2-Enterprise instead of WPA-Enterprise.

The use of WPA2-Enterprise addresses the security threats discussed earlier:

- **Data exposure:** To prevent the data in Wi-Fi packets from being viewed by a hacker, the sender of those packets must encrypt the data in such a way that only the intended recipient can decrypt the packets and view the data in its unscrambled, clear-text form. WPA2 provide proven mechanisms for ensuring that all transmitted data is protected from being viewed by a hacker.
- **Network exposure:** When every Wi-Fi client uses WPA2 with 802.1X authentication to the network, a hacker cannot glean from sniffed packets any information on how to gain access to the network.
- **Man-in-the-middle attacks:** When every Wi-Fi client is configured to use a strong EAP type for mutual authentication to the trusted wireless LAN, no client will associate inadvertently to a hacker's laptop that is posing as an AP.

WPA2-Enterprise protects all sensitive data and the networks that house that data. Reliance on the Enterprise version of WPA2 is a foundational element of a sound wireless LAN security strategy. To achieve the Enterprise level of Wi-Fi certification, a product must pass a set of tests that demonstrate support for WPA2-Enterprise.

CCX

Organizations that run business-critical applications on mobile devices demand that those devices be Wi-Fi CERTIFIED. For many of these organizations, however, Wi-Fi CERTIFIED is not enough.

The vast majority of wireless LAN infrastructure systems in today's hospitals and other healthcare facilities use products from Cisco Systems, Inc. As a result, most healthcare facilities want to ensure that their medical devices and other mobile devices interoperate with a Cisco wireless LAN infrastructure and support Cisco wireless LAN innovations for enhanced security, mobility, quality of service, and network management.

Nearly all mobile device vendors claim that their devices work well with a Cisco wireless LAN infrastructure. Fortunately, you don't have to take a vendor's word for it. Since 2003, Cisco has managed a program by which Wi-Fi radios and mobile devices with those radios can earn the Cisco Compatible logo. The logo signifies that a radio or device interoperates with a Cisco wireless LAN infrastructure and supports Cisco innovations. The program is called the Cisco Compatible Extensions (CCX) program.

Within CCX, Cisco licenses a specification of IEEE standards and Cisco innovations. A licensee, typically a firm that offers wireless LAN radios for client devices, implements support for all required elements of the specification in the software for a Wi-Fi radio. The licensee then submits the radio, or a client device that uses the radio, to an independent lab for rigorous testing. Only by passing all tests does the radio or device earn the Cisco Compatible seal.

Select Philips PageWriter cardiographs are certified for CCX V4.

CCX and Standards

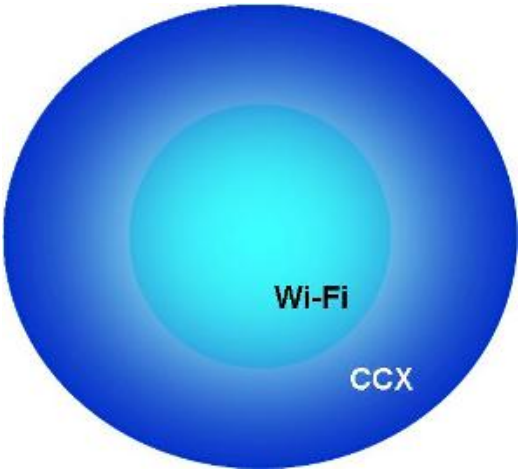
The CCX program has a structure that is similar to that of the Wi-Fi certification program. With both programs:

- One or more specifications define what features must be implemented in the hardware and software for a Wi-Fi radio or a device that uses a Wi-Fi radio.
- Compliance testing is conducted by an independent lab that is approved by the organization that manages the program
- A device must pass all tests to be approved

While the Wi-Fi certification program is for any type of product that uses Wi-Fi technology, CCX is restricted to client devices used by businesses, as well as the Wi-Fi radios used by those devices. In CCX compliance testing, client devices and their radios are tested as they interact with the Cisco wireless LAN infrastructure products that are used by businesses and other organizations.

While the CCX specification includes Cisco-defined technologies and features, its core is the specification used for Wi-Fi compliance. In other words, the CCX specification is a superset of the Wi-Fi specification. In fact, a device cannot be certified as Cisco Compatible unless that device or the Wi-Fi radio that it uses is Wi-Fi CERTIFIED.

The CCX specification also includes some IEEE standards that are not ratified and have not been incorporated into Wi-Fi compliance testing. Cisco uses CCX as a way of introducing and proving innovative solutions that Cisco then takes to the appropriate IEEE 802.11 task groups as proposed standards.



The CCX specification is a superset of the Wi-Fi specification

Because it requires program participants to implement support for both established and emerging IEEE and industry standards, CCX encourages support for standards in the market. As vendors vie for

prominence in CCX by striving to be the first to implement support for new CCX versions, support for standards is accelerated across a broad range of mobile devices.

Key CCX Features

The CCX specification defines the features that a Wi-Fi radio, or a client device that uses a Wi-Fi radio, must support to be deemed "compatible" with a Cisco wireless LAN infrastructure. Cisco has published five versions of its CCX specification, with each version building on the last. Today, a product can be certified only at one of the two most recent versions: Version 4 (V4) or V5. CCX V5 is aimed at laptops. Non-laptop devices, which Cisco calls application-specific devices or ASDs, are certified for CCX V4.

In each version of CCX some features are classified as optional for ASDs. Examples of ASDs are medical devices, mobile computers, smartphones, and printers. The CCX specification for ASDs is a subset of the CCX specification for laptops. Some CCX features are not required for ASDs because many ASDs lack the computing power or operating system foundation required to support the features.

Table 3 below shows the primary features of CCX V4 for ASDs. Most of these features, such as CCKM, were introduced in versions of CCX before V4. Cisco's controller-based wireless LAN infrastructure solution, which is known as the Cisco Unified Wireless Network, will not support CCX features such as CCKM with a client device unless that client device (or its radio) is certified for CCX V4. As a result, CCX V4 certification is essential for all devices that want to use CCX features with the Cisco Unified Wireless Network.

Feature Type	Feature	Standard?
Interoperability	Wi-Fi certification for device or radio in device	Yes, Wi-Fi Alliance
Security	WPA and WPA2	Yes, Wi-Fi Alliance
Security	Support for at least one of the following EAP types: LEAP, EAP-FAST, and EAP-TLS	LEAP: Cisco-defined Others: Published
Mobility	AP-assisted roaming	No, Cisco-defined
Mobility	Fast 802.1X reauthentication using the Cisco Centralized Key Management (CCKM) protocol	No, Cisco-defined
Management	Support for multiple SSIDs and VLANs on an AP	No, Cisco-defined
Management	AP-specified maximum client transmit power	No, Cisco-defined
Management	Client-based RF scanning and reporting	No, Cisco-defined
QoS and Voice	Wi-Fi Multimedia (WMM)	Yes, Wi-Fi Alliance
QoS and Voice	Call admission control, to improve voice quality	Yes, IEEE 802.11e
QoS and Voice	Unscheduled Automatic Power Save Delivery, to improve battery life and reduce network congestion	Yes, IEEE 802.11e
QoS and Voice	Voice metrics, to tune networks for voice performance	No, Cisco-defined

Table 3: Key features of CCX V4 for ASDs

The Value of CCX for Medical Devices

For network administrators, CCX reduces costs, complexity, and risks. By using CCX devices, an administrator has the assurance that the devices will interoperate with a Cisco wireless LAN infrastructure. In fact, because the CCX specification incorporates all key requirements for Wi-Fi certification, the Cisco Compatible seal provides the assurance of interoperability even with non-Cisco wireless LAN infrastructures. And because many of today's Cisco innovations are likely to become tomorrow's IEEE and industry standards, an administrator may be able to change the infrastructure in the future without having to abandon the CCX features exploited by today's infrastructure and clients.

When only CCX-certified devices are permitted to connect to the wireless LAN, the infrastructure can have a single configuration that supports a rich set of capabilities in key areas such as security and mobility. On the security front, the network can require the use of WPA or WPA2 with the organization's preferred choice of an EAP type. To ensure application persistence on mobile devices, the network can require the use of CCKM for fast EAP re-authentication. In contrast, when the wireless LAN must accommodate devices that lack support for some CCX features, network administrators have to do one or more of the following:

- Introduce security risks by using weaker security schemes supported by devices not certified for CCX
- Increase network complexity and costs by creating additional wireless LANs for non-CCX devices and tying those wireless LANs to network VLANs to protect sensitive data on the network
- Deploy additional software to maintain network connections on devices with inferior mobility

Because CCX brings key benefits to network administrators, those administrators want the assurance that all of their devices, including medical devices, support CCX. While many device vendors claim support for CCX, the only guarantee that a device is certified for CCX is the use of the Cisco Compatible seal with that device. Given that Cisco is the market leader for enterprise wireless LAN infrastructure and enjoys high brand awareness among customers, medical device vendors that fail to earn the Cisco Compatible seal may find themselves losing deals to competitors that do have the CCX seal.

Challenge: Achieving CCX on Medical Devices

CCX has a considerable success in the laptop world. According to Cisco, the top five vendors of laptop and notebook computers participate in the CCX program. When a new version of CCX is introduced, the first devices to support it are laptop and notebook computers, even though the required feature set for those devices is broader than that for ASDs.

While scores of firms manufacture medical devices, only a few offer medical devices that are certified for CCX. Why? It's not because CCX features offer more value on laptops than on medical devices. Security features are important on all types of devices, and features that enhance mobility, such as CCKM for fast 802.1X re-authentication, offer more value on medical devices than on laptops because medical devices often run applications that can fail without a constant network connection.

With both laptops and medical devices, support for CCX features is implemented primarily in the Wi-Fi radio software that runs on the device. The primary software components are a device driver, a security supplicant, and an administrative utility. Supporting CCX requires the following software development tasks:

- Modify the radio device driver to add support for driver-based CCX features
- Integrate a security supplicant that offers support for CCX security features
- Create an administrative utility for configuring settings required for various CCX features

In the laptop world, the required software development is done not by laptop vendors but by silicon providers. Once a silicon provider implements CCX support in the software for a laptop-ready radio, the laptop vendor can achieve CCX compliance simply by including the radio and its software in the laptop. The laptop vendor makes no hardware modifications or software modifications.

While laptop-ready CCX radios are plentiful, no silicon provider offers a CCX-certified radio for medical devices. To achieve CCX certification on a medical device, a firm must take a Wi-Fi radio and software designed for mainstream devices such as laptops and do the following:

- Port the software to the operating system that runs on the medical device.

- Modify the software to add support for CCX features.
- Create an administrative utility for configuring settings required for various CCX features.
- Test the resulting software set on the medical device and make modifications as necessary.

The challenge is too great for most medical device vendors. Fortunately, a viable alternative exists for medical devices that run Windows CE, Windows Mobile, or Windows XP. Radios from Summit Data Communications are certified for CCX on those operating systems. By using a Summit radio within a medical device, the manufacturer is assured that the medical device will pass all CCX tests and earn the Cisco Compatible seal.

Philips PageWriter Cardiographs and CCX

Hospitals are under increasing pressure to perform more ECG tests while reducing costs. At the same time, hospital administrators need solutions that reduce errors while enabling the hospital to capture billings to deliver care faster and more efficiently. By putting cardiographs on a wireless LAN, a hospital can enable its cardiology department and its administrators to achieve their goals of more exams with fewer errors, better care to more patients, and faster and more accurate billing.

To deliver these benefits without introducing risks and hidden costs, Wi-Fi cardiographs must address the increasingly stringent requirements of hospital information technology departments. Those requirements include strong, standards-based security that protects sensitive information, whether that information is transmitted through the air or housed on the hospital network. While the Wi-Fi CERTIFIED seal provides an assurance of interoperability and support for security standards, it is insufficient for many hospitals, especially those with Wi-Fi infrastructure products from Cisco. Increasingly, hospitals look for the Cisco Compatible seal, which demonstrates tested support for Cisco infrastructure devices and Cisco Wi-Fi innovations. That's why Philips PageWriter cardiographs have been a leader in supporting Wi-Fi industry standards and are the first cardiographs in the market to have earned the Cisco Compatible (CCX) seal.