Wi-Fi® in Healthcare:

Improving the user experience for connected hospital applications and devices

Wi-Fi Alliance®
May 2013

The following document and the information contained herein regarding Wi-Fi Alliance programs and expected dates of launch is subject to revision or removal at any time without notice. THIS DOCUMENT IS PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. WI-FI ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES, CONDITIONS OR GUARANTEES AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY OR COMPLETENESS OF THIS DOCUMENT AND THE INFORMATION CONTAINED IN THIS DOCUMENT.

Executive Summary

Connecting medical devices to a hospital Wi-Fi® network can improve clinical workflows by providing wireless access to real-time patient data. When hospital applications rely on Wi-Fi connectivity, hospital staff must have confidence that all Wi-Fi connections are reliable and meet performance requirements dictated by the devices and applications used. To achieve these goals, hospital IT managers should use quality of experience (QoE) as a key performance metric when designing and managing their Wi-Fi networks.

Delivering the best possible user experience requires several key elements, including:

- Design and configuration of the Wi-Fi infrastructure to provide sufficient coverage and capacity for all devices;
- Incorporation of quality of service (QoS) features such as Wi-Fi Multimedia™ (WMM®) to improve the efficiency of traffic transmission;
- Ongoing management of Wi-Fi networks and devices, such as configuration management and change control processes, to flexibly adapt to changes in applications and devices used and to changes in environment.

A Commitment to the Best User Experience

Hospital Wi-Fi networks have a range of users, including a patient surfing the web, a staff member downloading a drug library to an infusion pump, and a clinician using a smartphone for clinical applications.

To satisfy users, Wi-Fi networks must support the wide range of clinical applications and meet the performance and reliability requirements of extensive coverage, high availability, and robust reliability.

QoS functionality through WMM is the first step toward achieving this level of performance, but QoE is a more encompassing concept. QoS metrics measure network performance. QoE metrics expand QoS to assess how network performance translates into user experience. QoS focuses on the network, QoE on the devices and applications. QoE measurements are more complex because they include subjective assessments of performance, but they are also more powerful in capturing how well the network serves the needs of its users.

To optimize QoE, hospital IT managers must implement QoS tools and adopt the best practices for the design, deployment and management of their Wi-Fi network.

This white paper discusses how hospital IT professionals can establish and maintain high QoE levels through network design, radio frequency (RF) design, infrastructure and client device configuration, and ongoing management. All of these recommendations are based on industry best practices and may be included as elements of a risk management plan as recommended by the International Engineering Consortium (IEC) 80001-1:2010 standard, “Application of risk management for IT-networks incorporating medical devices.”

Table of Contents

Introduction

Risk Management for IT Networks in Hospitals

The 80001-1:2010 standard, "Application of risk management for IT-networks incorporating medical devices," recommends the application of a risk management process in the design, deployment and management of an IT network as essential to the creation of a safe, secure and effective network for use in healthcare delivery organizations. In addition, the IEC standard IEC/TR 80001-2-3:2012 "Application of risk management for IT-networks incorporating medical devices – Part 2-3: Guidance for wireless networks" expands the concept of risk management to the design, deployment and management of wireless networks in healthcare.

Wi-Fi Alliance encourages IT organizations in the healthcare industry to adopt a risk management process as part of their wireless networking strategy.

Many hospitals have Wi-Fi networks, and the use of Wi-Fi in hospital environments continues to grow. At the end of 2010, 92 percent of North American healthcare facilities with more than 500 employees had Wi-Fi infrastructures in place, and that percentage is projected to be 100 percent by 2016, according to ABI Research.[1]

Today's hospital Wi-Fi networks provide network connectivity for a variety of computing devices. For patients and visitors, Wi-Fi networks provide convenient Internet access. For clinicians and administrators, Wi-Fi networks provide access to hospital networks and record-keeping databases from workstations on wheels, tablet computers, smartphones, and other computing devices.

In many hospitals, medical devices are beginning to share Wi-Fi networks with computing devices. Because medical devices are directly involved in patient care, it is imperative that medical device Wi-Fi traffic is prioritized ahead of general-purpose Wi-Fi traffic. Hospital IT managers should use quality of service (QoS) techniques based on Wi-Fi CERTIFIED™ Wi-Fi Multimedia (WMM) to give medical device Wi-Fi traffic the highest priority.

QoS is essential for ensuring that a Wi-Fi network can support all devices and applications, especially those that support clinical functions. QoS is a key element in ensuring that every user of a Wi-Fi device has a high quality of experience (QoE). To optimize QoE, you first must measure the user experience where it occurs – in running applications on client devices[2].

Because the user experience encompasses more than a device's interactions with the Wi-Fi network, Wi-Fi QoE metrics must be restricted to those that can be addressed by making changes to Wi-Fi clients and Wi-Fi infrastructure devices. For some users, such as doctors and nurses, QoE should be prioritized ahead of QoE for other users, such as patients and guests. Also, QoE should be measured and monitored over time to gauge changes in user experiences.

The process by which a Wi-Fi network is designed, deployed, and managed is complex, but these tasks are key to QoE optimization. One driver of complexity is the multitude of devices with differing networking characteristics, performance capabilities, and requirements. Other factors

[1] ABI Research: "The Current State of Global Healthcare Wi-Fi,"

[2] Kalevi Kilkki, "Quality of experience in communications ecosystem," *Journal of Universal Computer Science*, Vol. 14, Issue 5, 2008.

include environment-specific RF propagation dynamics, the need to match logical interfaces to the wired network, and the highly configurable nature of Wi-Fi network deployments.

This paper provides an overview of the key steps in Wi-Fi network life cycle (Figure 1) and how IT managers in healthcare can use best practices, from the initial design to the management of a heavily used network, to optimize QoE and to ensure their Wi-Fi network meets user requirements and expectations. After these steps are followed during the initial deployment stage, the Wi-Fi network life cycle continues to offer a solid blueprint to maintain the performance levels in the network, as IT managers strive to enhance functionality, add support for new devices and applications, and meet increasing performance and traffic requirements.

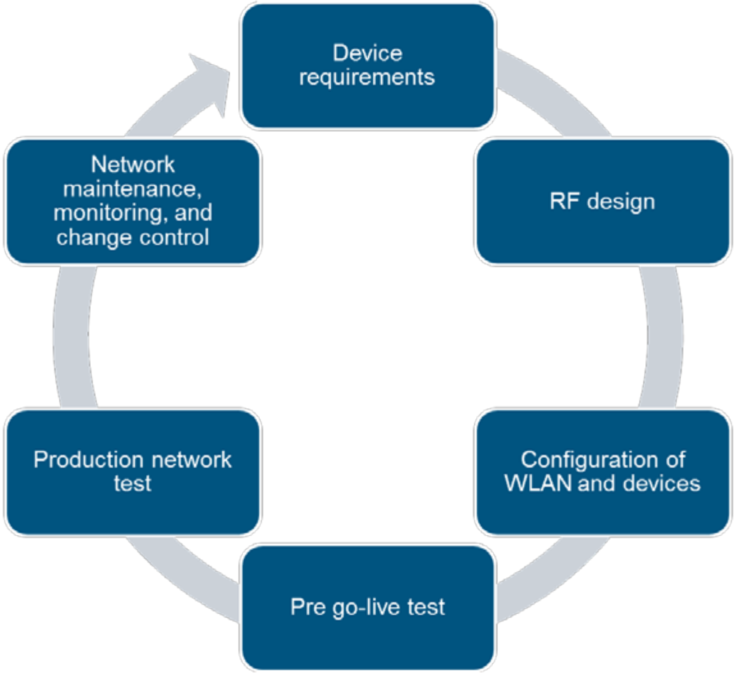
Device requirements
RF design
Configuration of WLAN and devices
Pre go-live test
Production network test
Network maintenance, monitoring, and change control

Figure 1: Wi-Fi network life cycle

Device requirements

Before adding a new client device type to a Wi-Fi network, administrators should understand the device's networking performance requirements and characteristics. This analysis enables them to define the appropriate device-specific service level agreement (SLA) in terms of networking performance and required functionality to manage traffic from this device and to assign a security classification to the device. Device networking requirements include packet delay, jitter and loss. Device characteristics include supported traffic types (e.g., Dynamic Host Configuration Protocol [DHCP] client, multicast, broadcast usage), data flows, and security capabilities (e.g., the Enterprise version of Wi-Fi Protected Access® 2, or WPA2™–Enterprise). IT managers should also consider a device's bandwidth needs, including supported data rates and required throughput.

A single device may have multiple data flows, each with its own characteristics in terms of usage (e.g., clinical mobile cart with video streaming). To define an SLA, IT managers have to capture the device's highest-priority traffic requirements for each application, and aggregate the networking requirements of all applications that run on the device. Because each device can support multiple applications with different requirements, it is not sufficient to consider the device attributes alone without reference to each application's requirements.

RF design

Coverage and capacity

A client device cannot connect to a Wi-Fi network if the device is outside the coverage areas for that network. In a congested network, a device may experience difficulty in connecting to a Wi-Fi network or in using some applications, and the user experience may be impaired. When designing the infrastructure for a Wi-Fi network, hospital IT personnel must work with vendors to ensure that the network provides sufficient coverage and capacity in all areas where client devices require network connections.

Wi-Fi network coverage is adequate when signal strength, RSSI and/or SNR, everywhere in the coverage area allows a client device to establish and maintain a network connection that satisfies the device SLA. The signal strength that a client device requires depends on the type of device, the type of data that it transmits and receives, the data rates it requires, and the Wi-Fi frequency band in which it operates.

While many devices may operate at signal strengths down to the published sensitivity limit of the application or device, IT managers should determine the recommended minimum signal levels to achieve their desired data rates and bandwidth needs with the assistance of the device and infrastructure vendors. For the highest level of available capacity, the signal strengths should be designed for the use of maximum data rates.

Real-world deployments involve many RF propagation challenges, such as physical obstructions, interference, and multipath effects, all of which influence both signal strength and quality. One example is the need for coverage in patient bathrooms and procedure areas, which might not have been taken into account during the initial planning of the network and which present a more complex RF environment than other areas in a typical hospital. The clinical users of the medical devices should be consulted to understand where and how the devices will be used, in order to determine what level of coverage is needed in these areas. On the basis of this analysis, network design can be tailored to provide the required signal levels for RF coverage for each area within the hospital and to provide an adequate buffer for propagation challenges, enabling a more reliable and consistent level of performance.

Wi-Fi network capacity is adequate when devices can obtain immediate connections to the Wi-Fi network and send and receive packets in a timely manner according to the device SLAs. IT managers have to carefully plan for levels of network capacity and access point (AP) density needed to meet unexpected peak usage traffic loads and to allow for future growth in traffic levels.

Wi-Fi network capacity design must factor in the transmission settings of the APs. Wi-Fi has automatic data-rate switching capabilities to adapt modulation to channel conditions. For instance, as a user moves away from the AP and channel conditions gradually deteriorate, the radio adapts and uses a less complex modulation scheme to send data. This results in a range increase that is accompanied by a reduction in transmission data rates. As devices switch to these lower data rates, they will need to remain connected for a longer time to transmit or receive the same amount of data, thus negatively affecting the capacity of the network.

The impact on network capacity is not limited to the single device that requires a less efficient modulation scheme, but to the entire network because only one device can communicate with an AP at a time. To improve the overall throughput of the network, IT managers can disable lower data rates, but only if all client devices can connect and maintain application performance without those disabled rates, and only if network coverage and capacity are sufficient to support the modulation schemes needed to support the higher data rates.

Broadcast and multicast traffic impact on network capacity

Another design consideration for capacity and bandwidth usage is the amount of broadcast and multicast traffic in the network. Because broadcast and multicast traffic is directed to all devices or to a subset of them, and sent from multiple APs in the network, it uses more network resources than unicast traffic, especially when transmission is at a lower rate.

Broadcast and multicast traffic can also be a burden on battery-operated devices or devices with limited processing capability, because it forces these devices to exit their power-saving mode and connect so they can listen to and decipher these broadcast and multicast messages, even though the messages may not be intended for those specific devices.

IT managers can mitigate the impact of broadcast and multicast traffic using different approaches:

- Transmit broadcast and unicast traffic at the highest data rate that is supported by all associated client devices, instead of using the typically lower basic or mandatory data rate as defined for a given AP. If an AP uses the highest data rate set in this way for broadcast and multicast traffic, the time used to transmit the data will be substantially reduced and, as a result, more network resources will be available for unicast traffic.
- Enable Internet Group Management Protocol (IGMP), an Internet Engineering Task Force (IETF) protocol to improve the efficiency of Internet Protocol (IP) multicast. With IGMP, transmission of broadcast and multicast traffic can be limited to the APs that have associated devices for which the transmission is intended.
- Enable proxy address resolution protocol (ARP) to handle ARP requests. Proxy ARP allows the network to resolve ARP requests more efficiently by eliminating unnecessary broadband and multicast traffic.

Channel planning

In most countries depending on the regulatory regimes, Wi-Fi operates in three non-interfering, non-overlapping frequency channels in the 2.4 GHz band, and up to 24 channels in the 5 GHz band. Wi-Fi networks use multiple non-overlapping channels to avoid co-channel interference and, hence, optimize performance. However, in dense, high-capacity deployments, co-channel interference may occur and cause degradation in performance.

To mitigate the effect of co-channel interference, IT managers have to carefully plan the AP and channel deployment in consultation with their selected vendors, and they must address the specific physical environment, capacity requirements and coverage requirements of the Wi-Fi networks.

In hospitals with multiple floors, Wi-Fi signals from one floor can extend to floors above and below, so both the vertical and horizontal dimensions should be considered. APs within range of each other should always be set to non-interfering channels to minimize co-channel interference to avoid performance degradation.

Because of the spectrum limitations in the 2.4 GHz band, hospitals and other enterprises may find it difficult to avoid co-channel interference while meeting coverage and capacity requirements. To address this issue, Wi-Fi networks in hospitals and other healthcare locations should use both the 2.4 and 5 GHz bands. With a higher number of available channels, the 5 GHz band allows for greater flexibility and higher density in Wi-Fi network layouts.

Furthermore, IT managers should also verify that spectrum channels in the 5 GHz band are non-overlapping. In many regulatory domains, the 24 channels in the 5 GHz band are considered non-overlapping because there is 20 MHz of separation between the center frequencies of each adjoining channel. However, the lack of a protective guard band may create interference from adjacent channels. A careful channel allocation (Figure 2) can address this issue by using these guideline principles:

- Channel allocation in adjacent and partially overlapping APs should be two channels apart (i.e., channels should be separated by 40 MHz).
- Separate but adjacent channels should be separated by at least one AP (i.e., there is no overlap between the two cells).
- The same channel should be separated by at least two APs. For example, note the channel represented by “A”. There is minimally two different channel cells between each reuse of channel “A”.
- Channels should be staggered between APs on adjacent floors.

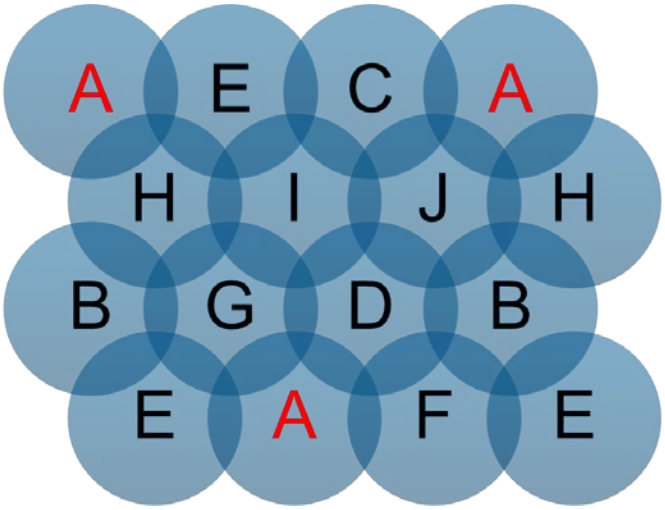

Figure 2. Generic channel planning allocation

In many countries, regulation may limit the number of 5 GHz channels available because the spectrum is shared with other technologies and services. For instance, in the US and other countries, Unlicensed National Information Infrastructure–2 (UNII-2) frequencies (5.25–5.35 GHz) are used by radar systems, and Wi-Fi networks operating in those bands are required to employ a radar detection and avoidance capability.

IT managers are required to determine if the 5 GHz channels they plan to use are subject to these regulatory restrictions. The IEEE 802.11h standard addresses this requirement by adding support for dynamic frequency selection (DFS) and transmit power control (TPC) on every channel in these sub-bands.

If a Wi-Fi AP detects a radar system on a channel with DFS enabled, the AP must announce to the attached client devices that it is vacating the channel on which the radar is detected, and it should send a request to the devices that they move to a different channel. The client devices must immediately vacate the channel and reattach on a new channel. Since the AP is the only element in the network required to be aware of radar transmissions, it is responsible for managing the client device behavior on the Wi-Fi network. In countries with DFS channels, Wi-Fi client devices are not allowed to do active probes on a DFS channel and must only passively scan (i.e., listen) for the presence of an AP in these channels.

Accommodating mobility

Client devices can be defined as stationary, nomadic, or mobile. Stationary devices almost never move. Nomadic devices may be moved but may not require an active or robust network connection during transport. Mobile devices frequently move about the facility and require an active network connection while in motion. In a network that properly supports mobility, mobile devices are able to roam from one infrastructure AP to another while maintaining a network connection.

IT managers need to decide whether to support mobility in their Wi-Fi networks and how to manage it. To accommodate roaming in mobile devices, the coverage area of adjacent APs must partially overlap and support the same service set identifiers (SSIDs). The area of overlap must be sufficient to accommodate the roaming process, which includes the following steps:

- Determine that the current AP's signal strength is becoming weak
- Scan for other APs that support the same SSID
- Select a new AP
- Roam to that AP

The extent of the coverage area overlap needed depends on the speed at which mobile devices move within the network. IT managers should work with their vendor or implementer to determine what amount of overlapping coverage is adequate in their environment.

When 5 GHz channels include DFS channels, the requirements to do passive scans of DFS channels can increase the time required by a mobile client to identify potential roaming targets and select the AP to which to roam. This increase in scanning time may prevent some clients from keeping their connection active while roaming across APs. In this case, it is preferable to avoid the use of channels in which DFS use is mandated, even if this leads to less flexibility in managing co-channel interference. IT managers should be able to retain a separation of adjacent channels by at least one cell even if these channels are not utilized.

Transmit power control

The design of a Wi-Fi network plays an important role in optimally balancing the requirements of transmit power from client devices and from network infrastructure. In networks with mobile devices, power transmission requirements are even more prominent. This is because design constraints (e.g., small battery and small antenna) are responsible for a common asymmetry, with the typical transmit power of a smartphone being significantly lower than that of an AP. When planning their networks, IT managers need to consider the transmit power requirements of both APs and the supported devices.

The AP transmit power should be set so that the client devices receive the required minimum signal strength. The higher a deployment's AP density, the lower the transmit power should generally be set, in order to prevent co-channel interference. Lack of control over transmit power may result in reduced range, increased error rates, interference among devices, and limitations in roaming capabilities. IT managers need to ensure that the transmit power is set appropriately, both to mitigate interference and to enable client device connectivity and performance according to the established SLAs.

Many enterprise-grade Wi-Fi APs support methods to adjust transmit power separately at each AP, with some supporting dynamic, automatic adjustments based on RF conditions. When the AP transmit power can change, all client devices that support TPC can adjust their transmit power to match that of the AP. This ensures that the client's coverage radius matches the AP's and that the mobile device's power level settings can be changed when the device roams to another AP with different power level settings.

Maximum allowable AP transmit power settings vary by band and by channel, and among countries. In addition, maximum supported power output levels vary by AP manufacturer. IT managers should work with their vendor or implementer to ensure that they comply with local regulations.

Interference

Interference on a wireless network may originate from many sources. Microwave ovens, Bluetooth devices, cordless phones, wireless video cameras, wireless motion detectors, and rogue and neighboring APs are among the many potential interfering RF sources in Wi-Fi networks. In general, devices that employ or emit common frequency RF signals within a given radio coverage area will have the potential to cause unwanted signal interference.

RF spectrum analyzers can help identify the sources of such interference. Once identified, multiple approaches are available to mitigate interference:

- Remove the interfering devices from the network area.
- Change the channel setting of the interfering device to avoid conflict with the surrounding APs.
- Change the channel of the surrounding APs to avoid as much co-channel overlap with the interfering device as possible.

A documented facility-wide RF usage policy will help control sources of RF energy. Ideally, any RF-generating device should have prior approval before introduction onto the property or installation in any building or structure.

Multipath and signal distortion

Multipath transmission occurs when a radio signal reaches the receiver by more than one path due to factors such as reflection or refraction. In a hospital environment, this can be caused by physical barriers such as walls, ceilings, equipment and other structures. Multipath is a frequent occurrence in locations with installed metal, such as storage areas, or, in healthcare, around diagnostic equipment like X-ray and magnetic resonance imaging (MRI) machines. Multiple converging wave fronts may be received as a signal that is either attenuated or amplified. In some instances, if the signals arrive at the receiver exactly out of phase, the result is a complete cancellation of any RF signal.

Multipath distorts the signal and generates interference in networks using legacy Wi-Fi Physical/Medium Access Control (PHY/MAC), such as IEEE 802.11a, b, and g. Multipath can cause network throughput degradation, which leads to high error rates and packet retries. In turn, this can lead to severe wireless network quality impairment.

In the newer IEEE 802.11n and 802.11ac standards, the signal distortion caused by multipath is beneficial since it can be used to improve performance. Devices incorporating these more advanced features use multiple radios and antennas with multiple-input, multiple-output (MIMO) technology that leverages multipath effects to obtain increased range and overall throughput. For new deployments or network expansions, Wi-Fi Alliance® recommends deploying networks and client devices, if appropriate, that support Wi-Fi CERTIFIED n and Wi-Fi CERTIFIED ac. Devices certified under these programs provide more capacity and throughput, better coverage, and lower latency.

Site survey

A site survey should be done once a network deployment is complete to validate that all minimum RF performance requirements discussed above are met. The ability of the network to meet these requirements – or updated requirements due to the introduction of new devices or applications – should be periodically rechecked as an ongoing maintenance activity, to ensure that coverage and performance have not degraded over time and that they meet the current traffic demand.

Commercial tools are available to measure signal strength and quality information in all locations of the facility that have Wi-Fi coverage. Many Wi-Fi vendors include a survey diagnostic tool integrated into their equipment.

The site survey ensures that the wireless network is optimally designed and configured to support all device types and applications. This is done by assessing AP placement, cell overlap, channel allocation/reuse, packet transmission quality, packet retry rates and other deployment key performance indicators (KPIs). Many site survey tools offer additional security functionality – for instance, by checking for rogue APs. They can also verify that the SSID, data rate configuration, and security and QoS mechanisms are correctly set; if they are not, the survey tools can detect and correct configuration problems.

The site survey results provide guidance that helps IT managers address coverage and performance issues by adding and/or relocating APs, or by reassigning channels to change the RF environment. When these adjustments are made, an additional site survey has to be performed to confirm that the changes address the coverage and performance issues as expected, and that they have not had any unexpected adverse impact elsewhere in the network.

Network and device configuration

Once the design of the RF network is completed, IT managers have to configure APs and client devices to optimize performance and meet QoE requirements. Key network and device configuration areas include SSID management, security credentials, virtual LAN (VLAN) assignment, security, and WMM and RF management capabilities.

Multiple SSIDs and VLANs

Most enterprise-grade wireless infrastructure can support multiple, simultaneous SSIDs across APs and within each AP. These separate SSIDs are treated as logically distinct overlapping Wi-Fi networks. However, the SSIDs share the same RF frequency, so the total bandwidth remains constant regardless of the number of SSIDs used. Multiple SSIDs provide a method to separate wireless traffic streams that have different security or QoS needs, and, to a certain extent, traffic from different devices or device types.

Separate SSIDs can be configured to offer different levels of QoS to the attached clients. This allows separation of mission-critical applications from lower-priority, best-effort network uses, or assignment of priority to voice and video uses over other data uses, or provisioning of guest network access to visitors or patients with lower service-level expectations. It can also be used to isolate multicast and broadcast traffic between devices.

Although multiple SSIDs are useful for separating traffic, they also generate more beacons (low-bandwidth broadcast messages used to manage traffic), and hence more management traffic; this, in turn, reduces the time available to transport data traffic. To limit the impact of multiple SSIDs on network performance and complexity, IT managers should deploy only as many SSIDs as required for proper network operation.

WMM

Wi-Fi networks that implement WMM optimize the allocation of shared network resources among competing applications by prioritizing media access depending on the traffic type. This approach brings flexibility in networks that have concurrent applications with different latency and bandwidth requirements. For these networks, Wi-Fi Alliance recommends the adoption of APs and client devices that are certified for WMM.

To fully benefit from WMM and the QoS functionality it brings to Wi-Fi, IT managers need to establish a QoS policy based on WMM. In a hospital environment, WMM can prioritize voice and video traffic with more stringent latency, jitter and packet loss requirements over other types of data traffic (e.g., browsing, email, file transfers), or clinical traffic over less-critical network traffic (e.g., from guests or patients). WMM defines four access categories corresponding to decreasing priority levels:

- WMM voice
- WMM video
- WMM best effort
- WMM background

Although the four access categories were designed with specific types of traffic in mind, WMM relies on the application to assign the appropriate access category for the traffic it generates and on the AP to manage traffic on the basis of the adopted QoS policy. Once the application assigns the traffic it generates to the appropriate access category, packets are added to one of four independent transmit queues in the AP and in the client device.

WMM-Admission Control

WMM-Admission Control allows the AP to manage its available airtime based on traffic requirements submitted by associated clients, and rejects connection requests if resources are not sufficient to meet the transmission requests at the required priority level defined by the access category. Wi-Fi Alliance recommends the adoption of Wi-Fi CERTIFIED WMM-Admission Control equipment to avoid over-subscription of the AP, therefore preserving and protecting QoE for all associated devices.

Pre go-live test

After finalizing the Wi-Fi network and client device configurations, IT managers have to test how the client devices interact with the Wi-Fi network infrastructure. Before conducting tests on a production network, it is prudent to conduct tests on a physically isolated test network with the same configuration as the production network. A typical setup may include an enterprise-class controller and two or three APs. To confirm that the network supports the expected QoE levels, the test network should include the devices with the most demanding requirements.

If a separate test network is not available, IT managers can use a small portion of the Wi-Fi network that does not include clinical or other mission-crucial areas (e.g., lobby or office area), and logically isolate the test environment with the creation of a test VLAN and Wi-Fi network and SSID served by the enterprise controller.

Production network test

After testing new devices, isolated from the production network, as outlined in the pre go-live section above, IT managers can test on the Wi-Fi network using the following guidelines:

1. The Wi-Fi network should be configured as necessary for production operation (SSID, security, QoS, etc.), but the devices themselves should not be used for clinical use (e.g., they should not be connected to patients).
2. Backend servers or computers that support clinical devices and applications (e.g., nursing stations, database servers, etc.) should also be configured and available for testing, without disrupting their ongoing clinical functions. Verifying that the end devices are able to connect and send data to these servers and computers reliably is an essential component of the test.
3. Tests should be conducted in an area where interruption of the clinical workspace can be kept to a minimum.

4. IT managers should establish a back-out or emergency plan in case of network outages due to testing on the live IT network.

Maintenance, monitoring, and change control

The IT change control process should take into account the specific requirements driven by the clinical usage of the devices and applications, and involve the clinical end users. Failure to include the clinicians in the preparation and planning of network changes might affect patient safety and clinical effectiveness. An increase in IT and clinical staff during network software or hardware changes is a widely used control measure to support maintenance, monitoring, and change control processes. As in the case when production testing, an emergency plan should be available in case of extended network downtime.

Networking off-the-shelf tools are commercially available for monitoring and reporting on Wi-Fi network performance and reliability. Hospital IT managers need real-time visibility into the performance of end-to-end networking components (e.g., switches, routers, wireless controllers) in addition to the Wi-Fi APs. Some client devices may also allow access to network monitoring applications such as those that use Simple Network Management Protocol (SNMP), to provide information about the client devices and network KPIs. Degradation of connectivity performance in a medical device ranges from a non-issue (e.g., in the case of minor delays with infusion pump library updates) to potential for patient harm (e.g., if there is a delay between alarm–triggering events and alarms). Proactive network and device monitoring in a hospital network, especially when wireless connectivity is crucial to clinical activities, is a best-practice risk control measure that IT managers should adopt.

Maintenance of the hospital network goes hand-in-hand with monitoring the network's health. Many of the best practices discussed in this paper – such as periodic RF site surveys, pre go-live testing, combined clinical and IT change control processes, and monitoring the network health – lead to a robust and reliable medical IT network. Implementing these best practices as part of documented network maintenance policies provides a high level of confidence in the ability of the network to meet the needs not just of general computing devices, but also of the critical use of medical devices.

Conclusions

This white paper covers a wide range of issues that IT managers face when designing and operating a Wi-Fi network with strict end-to-end QoE requirements driven by medical and non-medical users, and it provides guidance in configuration management.

IT managers should collaborate with their vendors to consider the recommendations in this paper. Many of these measures may be included when implementing the risk management plan recommended by IEC standard 80001-1:2010.

To ensure that the Wi-Fi network meets evolving user requirements, IT managers have to continuously measure QoE indicators, and use device and application requirements to design, operate, maintain, and update their network, following a continuous life cycle of network performance improvements. The table on the next page provides a reference and summary of the key metrics to consider when planning, deploying and operating a Wi-Fi network in a healthcare environment.

Ensuring QoE in Wi-Fi networks: a reference list of key planning and operation considerations for healthcare IT managers

Key metric	Notes and recommendations
RF Design	
PHY/MAC	Options: Wi-Fi CERTIFIED a, b, g, n, and ac Recommended: Wi-Fi CERTIFIED n and ac as the future dominant PHY/MAC, with support for legacy a, b, and g
Spectrum band	Preference for the 5 GHz band for mission-critical devices 2.4 GHz band reserved for guest access and noncritical devices
RF site survey	Signal strength (RSSI and/or SNR) should be measured initially during the planning phase and repeated periodically to guide network evolution and performance improvement
Co-channel separation	Can be used in the 5 GHz band to mitigate interference
Wireless capacity	Measured through time to monitor the network's ability to meet demand from devices and applications, and expectations from users
QoE management	
QoS	Recommended adoption of WMM infrastructure and client devices
SSID assignment	Use for segmentation of clients into different network usage policies
SSID broadcast	Recommended, especially if DFS channels are mandated by regulations
VLAN mapping	Required to map traffic to wired LAN via SSID
WPA2	WPA2-Enterprise required, with WPA2-Personal pre-shared key (PSK) recommended to support mobile devices
Network management	
Pre go-live testing	Recommended, to test network and devices without impacting clinical operations
Production network test	Recommended second phase of testing for network and devices in live network, but controlling for impact on clinical operations
Change control process	Recommended, to support clinical applications
Continuous RF monitoring	Recommended for both 2.4 GHz and 5 GHz band to evaluate sustained performance and QoE through time

Wi-Fi Alliance certification programs relevant to healthcare Wi-Fi networks

From its inception, Wi-Fi Alliance has promoted interoperability across vendors through its Wi-Fi CERTIFIED program, which certifies client devices and infrastructure equipment that meets the specifications and performance requirements established by Wi-Fi Alliance, based on the IEEE 802.11 standard. Users' confidence that Wi-Fi CERTIFIED devices can connect to any Wi-Fi CERTIFIED AP to deliver a reliable connection and a high-quality experience has made Wi-Fi ubiquitous in PCs, laptops, tablets and smartphones, and increasingly available in other consumer electronics (CE) devices.

With effortless interoperability as its core target, the Wi-Fi Alliance certification program has expanded to include the building blocks that support a richer and safer user experience with mobile devices:

- **Wi-Fi CERTIFIED n** leverages multiple-in, multiple-out (MIMO) technology in IEEE 802.11n Wi-Fi CERTIFIED products to enhance performance and capacity in Wi-Fi networks.
- **Wi-Fi CERTIFIED ac** further improves Wi-Fi performance over Wi-Fi n, by increasing throughput, lowering latency, and improving coverage, by leveraging wider channels in the 5 GHz band, and with MIMO and beamforming technologies.
- **Wi-Fi Multimedia (WMM)** provides quality of service (QoS) functionality to enhance the user experience with real-time applications, such as streaming video and voice applications.
- **Wi-Fi Protected Access 2 (WPA2)** is required in all Wi-Fi CERTIFIED devices and infrastructure equipment and provides IEEE 802.1X controlled access, secure Extensible Authentication Protocol (EAP)–based authentication and connectivity through encryption of over-the-air traffic.
- **WPA2 with Protected Management Frames (PMF)** provides a WPA2 level of protection for unicast and multicast management action frames, strengthening privacy protection for data frames with mechanisms that improve the resiliency of mission-critical networks.

References

- The Building Blocks of Enterprise-Grade Wi-Fi®: An Overview of Wi-Fi CERTIFIED™ Programs for the Enterprise (2012)
- Wi-Fi® in Healthcare: Security Solutions for Hospital Wi-Fi Networks (2012)
- Wi-Fi® in Healthcare: The Solution for Growing Hospital Communication Needs (2011)
- Wi-Fi CERTIFIED™ n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks (2009)
- 802.11n: Enterprise Deployment Considerations (2008)
- Wi-Fi CERTIFIED™ for WMM® (2004)

These papers are available for download at the Knowledge Center on the Wi-Fi Alliance website (www.wi-fi.org).

Further information resources

An up-to-date list of certified products can be found in the Wi-Fi CERTIFIED products database on the Wi-Fi Alliance website (www.wi-fi.org), where users can search for Wi-Fi CERTIFIED equipment by multiple criteria, including product category, manufacturer, certification date and features supported, and can view the interoperability certificate for certified products.

For further information on the Wi-Fi Alliance certification program and for white papers on Wi-Fi–related topics, please visit the Knowledge Center on the Wi-Fi Alliance website (www.wi-fi.org).

The Wi-Fi CERTIFIED logo makes it easy to identify trusted Wi-Fi products

About Wi-Fi Alliance

www.wi-fi.org

Wi-Fi Alliance® is a global non-profit industry association of hundreds of leading companies devoted to seamless connectivity. With technology development, market building, and regulatory programs, Wi-Fi Alliance has enabled widespread adoption of Wi-Fi® worldwide. The Wi-Fi CERTIFIED™ program was launched in March 2000. It provides a widely-recognized designation of interoperability and quality, and it helps to ensure that Wi-Fi-enabled products deliver the best user experience. Wi-Fi Alliance has certified more than 15,000 products, encouraging the expanded use of Wi-Fi products and services in new and established markets.