

Hospital Wireless Network Design Guide

What you need to know before you deploy a high capacity, secure hospital wireless network



Table of Contents

Hospital Wireless Network Design Guide

- Overview.....3
- Radio Frequency (RF) Planning.....3-5
- Applications & Devices.....5-6
- Security.....7-8
- Network Infrastructure.....9
- System Management.....10-12
- Scalability.....12
- Location-Based Services.....13
- Redundancy & Reliability.....14-15
- Warranty & Support.....15-17
- How SecurEdge Can Help.....17-20

Overview

Hospital Wireless Network Design Guide

Whether it's increasing patient satisfaction, decreasing costs through better asset management or maximizing efficiency using location-based services, it's up to your network and the system you put in place that will determine if your business goals are successful or not. Your challenge is to build a hospital wireless network solution that will support your staff, patients and guests for many years to come. This document will give you some things to consider before you select the technology and put together your wireless deployment plan.

We've compiled this information from years of experience planning, deploying and supporting large scale, enterprise level wireless network infrastructures (we consider large scale 100+ access points), we hope this guide will help you be successful the first time. As we always say, "Plan twice, deploy once".

Radio Frequency (RF) Planning

The first thing to consider when deploying wireless is regarding Radio Frequency or RF and where you want to provide wireless access. It's not as easy as just broadcasting a strong signal for devices to associate to.

You'll have many different types of devices, users and areas to cover in a large scale environment. You'll need to consider three key things:

- **Coverage**
- **Capacity**
- **Performance**

Radio Frequency (RF) Planning

Hospital Wireless Network Design Guide

Capacity: Each wireless access point can handle a certain number of wireless clients or devices connecting to the network. This means that you need to consider the areas that may present a high number of users which means the deployment in that area is more important. Often, an organization will overlook things like, waiting rooms, nurse's stations, and large meeting rooms etc. These are high user density areas that present major issues if not planned properly.

Performance: Knowing a little about your RF environment will go a long way in helping to plan an optimal WLAN. This is where a site survey can come in handy. A site survey will uncover RF occurring already in your environment and advise accordingly. For example, if your site is already saturated with 2.4 GHz RF then moving your clients to the 5GHz spectrum might be advantageous. Also knowing how much bandwidth will be needed to accommodate the applications and clients that will be using the WLAN is also important. With 802.11ac offering the highest levels of performance and scalability today, it is advised to explore going with high speed rather than legacy Wi-Fi for all new deployments.

Applications & Devices

Knowing what devices and applications will be running over your hospital's wireless network is helpful in planning for the WLAN. Voice and video are two very demanding applications for a wired network much less a wireless one. Knowing the resource requirements of these and other applications intended for the WLAN will provide useful measurements for the planning of the network.



Applications & Devices

If you're reading this, then you are most likely planning what we call a "multi-media grade WLAN", which is to say you need the system to handle anything you want to put on it.

We recommend creating a list of applications and devices you'll need to operate on the network and assigning an order of priority to the applications and devices. The system should be engineered to support the most mission critical applications first.

For example, your Nurses' wireless VoIP phones will take priority over the wireless internet access for you guest users. Having these priorities will help design the hospital wireless system effectively.

<u>Devices</u>	<u>Quantity</u>	<u>Applications</u>	<u>Priority</u>
Cisco VoWLAN Phone	650	Wireless VoIP	1
Tablet PC	1000	MRI Imaging/Multimedia Streaming	2
Notebook	1200	Web & Email	3
RFID Tag	1500	Real Time Location Services	4



Security

In the past wireless security was considered to be inferior to wired security. This is no longer the case. Most often the wireless implementations can integrate with directory services, allowing you to control access at the user level. Here are some considerations to make when thinking about how to implement the highest level of hospital wireless security that's not only compliant but doesn't sacrifice the user experience as well.

Wireless Intrusion Detection & Prevention - WIDS is the acronym we use in reference to Wireless Intrusion Detection & Prevention. WIDS is very helpful in being proactive with wireless security in the healthcare environment. An integrated WIDS system in your WLAN can detect and prevent varying degrees of attacks and hacks that are used to acquire access to your hospital's network. It is also useful in something as innocuous as the dreaded "Rogue AP" which is installed by well meaning, but poorly informed employees seeking to gain mobile freedom in the workplace.

Roles & Policies - It helps to think of your user groups in terms of what they need access to and then create security policies that limits their access to only those systems. An Executive role would include a security policy that allows them access to the financial servers, while a nurse would have limited access to sensitive servers.

Security

Hospital Wireless Network Design Guide

Directory Services Integration - Integration with your directory services is a critical step to provide wireless security by being able to authenticate each user connecting to the network. The credentials created for each person inside your directory services should also be used to authenticate the user on the wireless infrastructure so that you have one database of users accessing the network.

Role Based Access Control - RBAC is the process of being able to assign a specific security role (for example: Nurse or Patient) to a user or groups of users that connect to the network. In order to do this your system must have directory services integration and then be able to assign a role to that user.



Wireless Firewalls - Your system needs to be able to segment traffic by user groups similar to the way a LAN firewall segments VLANs. For example, a guest user should be denied all internal servers and only be able to access the internet gateway to surf the web and check email.

Network Infrastructure

Hospital Wireless Network Design Guide

The following items are important pieces to the success of any WLAN implementation in Healthcare. Know them and making sure you have the right infrastructure in place will ensure an optimal wireless experience for you and your users.

Switching - New 802.11AC access points have potential for Gigabit speeds. If these AP's are connected to 10/100 Mbps switchers the potential cannot be realized. We advise and recommend Gigabit switches preferably with PoE+ for connectivity with the AP's.

DHCP & DNS - Static IP networks can present issues with AP and wireless client functionality. It's advised and preferred to have a dynamic IP network. Static IP networks can work but will prove in the end to be an administrative headache. Locally hosted DNS is also preferred as AP's will be dependent on name resolution to find their controllers over layer 3 networks. If your network is a flat layer 2 network then this is not as critical.

PoE & Power - Access points can be powered by PoE (Power over Ethernet) which makes the installation of cabling to the AP's very clean and eliminates the need to have AC power locally at the AP location. Surge protected power will be needed at the location of the PoE adapters or switches that are providing power to the AP's.

System Management

Hospital Wireless Network Design Guide

The biggest challenge with a large scale hospital wireless implementation is trying to manage the users and devices after the system is installed. The RF environment and user patterns are dynamic, if you don't have the ability to manage them from one interface, your hospital operations costs will go up, your staff's efficiency will go down and your patient's satisfaction will drop as well. You need to be able to build the infrastructure once, then be able to grow it, adjust it, and even provide compliance reporting in some cases.



We suggest varying levels of management based on several criteria and the needs of the organization, but here is a starting point for you to consider:

User & Device Management - You need to be able to assign "Bandwidth Contracts" to users and/or devices. A policy might be: each user is assigned 1Mbps of bandwidth from 8am to 5pm but 3 Mbps of bandwidth per user after 5pm.

System Management

Hospital Wireless Network Design Guide

Adaptive Radio Management - RF is dynamic; your system should also be dynamic. You'll want to see RF coverage maps in real-time so that you know how to trouble shoot any issues. This is a critical component for those running the user help desk.



System Management

Hospital Wireless Network Design Guide

Change Management - In the old days you had to configure each access point on your network separately (can you imagine managing just a 50 AP network?). Today you can configure one management console and then push the configuration out to every AP. Likewise, you should also be able to grow the wireless network simply by installing a new AP and having it join the WLAN automatically.

Help Desk/Administrative Access - There should be an option to set up levels of access for the management interface. Guest provisioning should be handled by administrative staff or help desk users. But write access for the major system configuration should come with high level privileges.

Reporting & Compliance - Process logs, device level reporting, trending, network monitoring, RF health, and alerts are all different ways to proactively manage your WLAN and your management system can provide them.

Scalability

Don't paint yourself into a corner when choosing a solution for your hospital's WLAN implementation. Make sure that whatever solution you choose will be able to easily accommodate your future wireless growth. In our experience as soon as you introduce wireless to your users they will want it everywhere. When planning take into account a full campus or wireless everywhere plan even though you may only have the budget for a few select locations. This will give you an idea of how big you may need to grow and what solutions can achieve this and accommodate the future scaling.



Location-Based Services

A location-based service, often known as Real Time Location Services (RTLS), is the ability to physically locate a user or device on a wireless network. Think of it as GPS inside a building.

There has been considerable debate about whether a Wi-Fi Network can handle the capacity of RTLS and if it is accurate enough to locate a device within a reasonable distance. The answer to the capacity question is that the right platform can easily handle the load as the data traffic from a Wi-Fi enabled RFID tag is very minimal.

As for accuracy, the system uses wireless access points to "triangulate" on a user or device, so the more access points that are deployed the more accurate the system will be.

If your hospital is considering RTLS, we recommend defining how accurate you need the system to be, for example: within 20 ft.

It's important to work with a wireless partner that is experienced in RTLS systems (like us) that can help you define how dense an access point deployment you're going to need to successfully support your specific goals.

Redundancy & Reliability

Hospital Wireless Network Design Guide

Wireless when implemented correctly will quickly become your user's main means of connectivity and they will become reliant on it, **HEAVILY!** Because of this it will be important to you and your users that you have ensured High Availability for your WLAN. In order to achieve High Availability you will need to build in redundancy and other means of reliability for the system. For many of our healthcare customers if their network goes down, critical functions are interrupted (this is especially true for hospital networks). Consider the cost of downtime and how it will impact your hospital's operations during the design process. Then work with an expert to design as much high availability into the system as necessary.

See our sample design for an example of redundancy below:

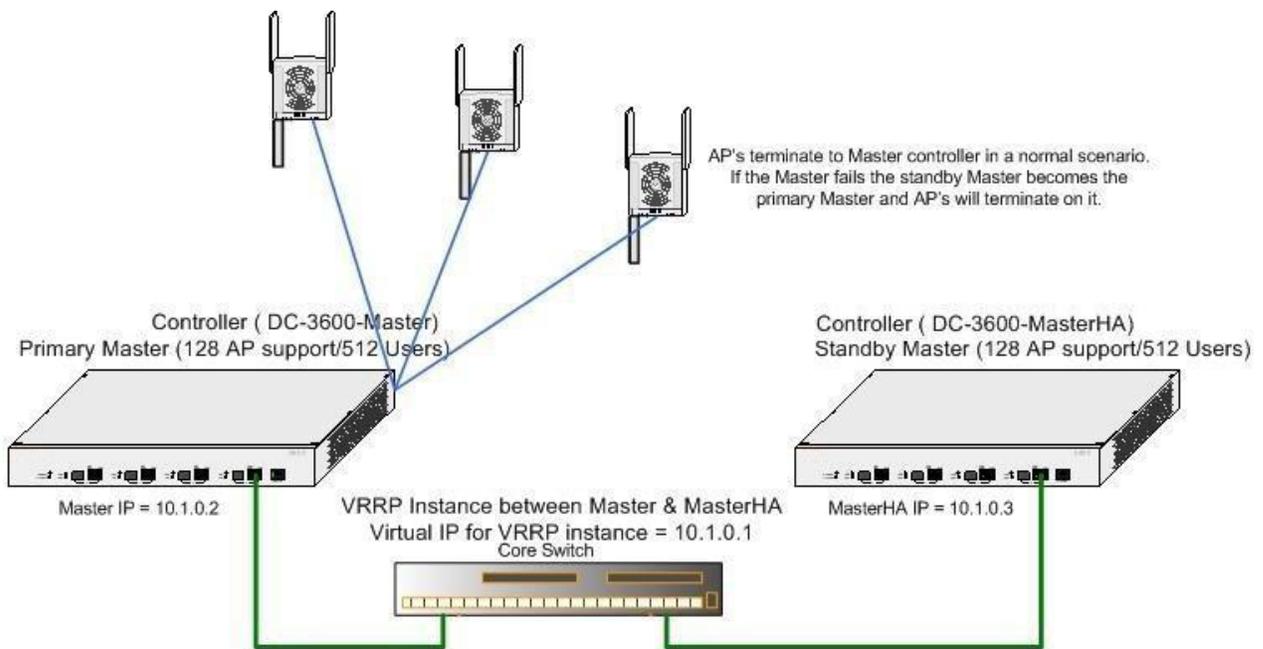


Fig A.

Redundancy & Reliability

Hospital Wireless Network Design Guide

See our sample design for an example of redundancy below:

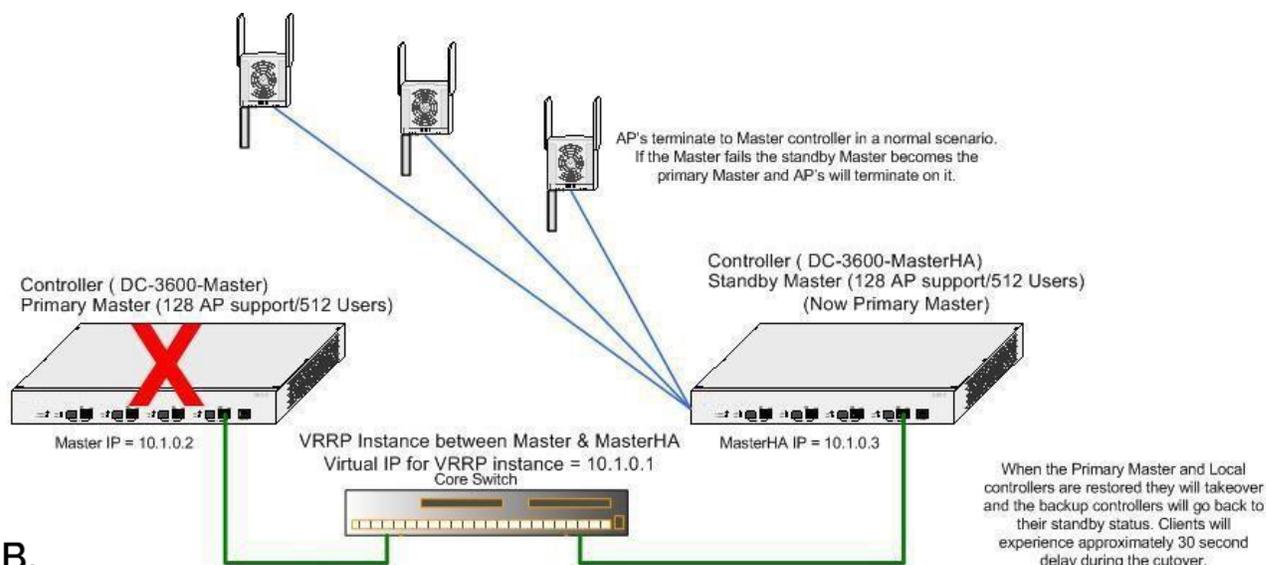


Fig B.

Warranty & Support

One of the most critical steps to building a reliable wireless network in healthcare is making sure you have the proper level of support to meet your requirements. Murphy's Law of critical systems is that something will go wrong eventually. For example: One of our healthcare customers had a water pipe break directly above a data closet housing a critical part of their WLAN system. These things don't happen often but you have to be prepared like they are. Here are some things to think through to make sure you're ready.

Warranty & Support

Hospital Wireless Network Design Guide

Hardware/Software Replacement - Your wireless network will have many different components. You need to understand what happens if something fails or is damaged.

- **How long is the warranty on the wireless network components (access points, antennas, software etc.)**
- **How quickly can you get replacement parts?**
- **How will they be installed when something does go wrong?**
- **How does the system react/adjust to a component failure?**
- **What is involved in adding the replacement to the network?**

Support - Being able to get an experienced engineer on the phone to help handle critical support issues is a vital asset to maintaining a large scale wireless network. Support specialists should understand your specific requirements and be able to respond and resolve issues quickly.

Maintenance/Managed Services - Your hospital's wireless network will have software and firmware that needs to be updated and maintained on average of once per quarter. We call this a quarterly refresh of the system. This keeps it up to date and ensures that the system has the latest security patches and updates available. This can be a tricky process because typically with each new release it brings additional features and potentially additional bugs in the software.

Warranty & Support

Hospital Wireless Network Design Guide

Maintenance/Managed Services Continued - Consider utilizing an engineer that is an expert on that particular platform to assist with issues or even provide the service ongoing to free up your internal resources. Many times utilizing an expert on a monthly or quarterly basis is more cost effective than figuring things out internally.

How SecurEdge Can Help

There is a lot to consider when deploying a large scale hospital wireless network and mobility infrastructure. We recommend getting an expert to help ensure you complete a successful roll out. At SecurEdge Networks we have many years of experience designing, deploying, and supporting large scale wireless infrastructure inside the healthcare environment. Here are a few things that make us unique.

Specialty Focus - One-stop shopping works well in some retail environments, but it's our belief that it's very difficult to achieve in the technology world. In our experience customers want a technology solutions partner that understands the exact problems they're facing specific to their industry. SecurEdge is committed to providing only the solutions we are experts in, serving the markets we have significant expertise in. We have even developed industry specific solutions and best practices. We believe this philosophy and approach creates the most value for our customers.

How SecurEdge Can Help

Hospital Wireless Network Design Guide

We Are Client-Centered not Product-Centered - At SecurEdge, we take our comprehensive knowledge and experience to determine which type of solution will be the best fit for your organization. Many companies who manufacture products do a great job at marketing their products. The challenge becomes when they recommend it for everyone even though it's not the best fit for the customer's specific environment. SecurEdge has the ability to work on the client's behalf, cut through a lot of the marketing jargon, and recommend a solution that will best support the customer's specific goals and needs.

Our Methodology

Analyze - We have industry and solution specific experts empowered with software tools to help understand a customer's current environment. This is the basis to build any wireless solution.

Design - We offer complete solution design services to help address the challenges. Our design recommendations are based upon your end goals, as well as industry and solution specific knowledge.

Deploy - We deploy many solutions turnkey or we can work with your team to provide guidance on deployment best practices and customer specific integration services.

Support - We offer custom fit support services that includes managed services, unmanaged or hybrid support which encompasses online portal access and support tools to help you manage any portion or all of your system.



About SecurEdge Networks

Yes, it's true, we're geeks. But the real reason we're passionate about wireless is because of what it can do.

Mobile devices and other mobile technologies have changed the fabric of what it means to be alive today. There's not one area of our lives that has not been touched by the possibilities and intelligence that wireless and mobile have created. The best part is, in many ways, we're just getting started.

However, wireless doesn't just work, although many people seem to think it should. It's a very complex and constantly changing system that inherently comes with many critical security challenges. How safe has your data been lately?

Fortunately, there are people (like ourselves) that really want to help make sure that your business is getting it right, the first time.

At SecurEdge, it's our life's work to educate you on how you can leverage wireless to help your business succeed.

Our goal is to provide the infrastructure, services, and support organizations need to do all the cool and cutting edge things they want to do to drive their business forward.

We live by one simple truth, intelligent mobility can make it happen.

Deploying or expanding your wireless network?

[Register for a wireless design and assessment here!](#)

For the latest on mobility, security and how wireless can help drive your business goals, **Connect with us!**



[SecurEdge on LinkedIn](#)



[Subscribe to the SecurEdge Blog](#)

Contact Sales

704.688.9360 #1

Contact Support

704.688.9360 #2