Implementing a Wireless Network

BEST PRACTICES
Wireless Network Access....

It's everywhere and everyone WANTS it
- Staff, students, employees, customers and visitors EXPECT it...

- and they expect YOU to provide it.
The Best Practices Steps

Start with a Plan for wireless
Funding Justification
Planning considerations
WLAN Design
Sighting for optimization and installation
System pilot and installation
System operation, maintenance and growth
Start with a Plan for wireless

Before you start tacking up APs, it’s a good idea to think about the purpose of the WLAN in your environment.

Who are you serving?

What will they do over the WLAN?

Will it be just a convenience or will it become the primary service delivery system for network access?

Understanding how the WLAN might be used today and tomorrow can affect how you plan, design and fund your deployment.
Funding Justification

Wireless has been, and still is, viewed as a luxury by many corporate financial planners. As such, the ROI for wireless is often ill defined.

The fact is, for the new breed of mobile devices such as the iPhone, iPad, tablets, Skype phones, dual-mode handsets, portable screen projectors and the ubiquitous laptop, the primary means of network connectivity is Wi-Fi.

Additionally, as more people use Wi-Fi at home, they will become increasingly dissatisfied if wireless is not present or even available in the workplace.
Consider also the following justifications as they may apply to your environment:

Moves, Adds and changes — reduce cost; minimize disruption
Serving a mobile Society — Same convenience; lower cost
Enabling New media Services
Extending hotspot coverage and improving Service Quality
Moves, Adds and changes — reduce cost; minimize disruption

A WLAN can greatly mitigate the disturbance where moves, adds and changes are disruptive to daily business operation.

Faster to deploy - Without the hustle and bustle of laying Ethernet cables through walls or ceilings, wireless is definitely easier and faster to implement.

Reduce the cost of relocating an IT infrastructure

- The cost of rewiring a building can be as high as $3 per square foot or more. A WLAN infrastructure over the same space could be deployed at a fraction of the cost.
Serving a mobile Society - Same convenience; lower cost

The convenience of cellular is quickly reducing the desktop phone to a boat anchor at the expense of increased air-time and international roaming charges.

Mobility and Flexibility

◦ Users who are on the move could actually connect to the network in order to access information that enables them to perform their job more efficiently.

With the availability of dual-mode phones and fixed-mobile convergence (FMC) services realize substantial savings by implementing VoIP over Wi-Fi and still give employees the convenience of a single handset for mobile and fixed-line voice services.

Wi-Fi can also replace legacy two way radio systems with higher quality, full duplex communications while eliminating the cost of operating an additional infrastructure and associated devices.
Enabling New media Services

The availability of video handsets, multimedia laptops and high-quality portable cameras is enabling organizations to easily implement TV-quality video applications.

Deploying a video-capable WLAN will obviate future expenses associated with equipping a separate video delivery infrastructure.
Extending hotspot coverage and improving Service Quality

Proliferation of mobile devices with built-in Wi-Fi is spurring an increase in need to expand coverage and increase capacity to support the growth in user density and bandwidth consumption.
Proliferation of wi-fi devices
Planning considerations

It is critical to understand and validate the WLAN requirements in detail. To insure you’re delivering the highest quality WLAN experience, it’s a good practice to map out the following:

- Who and where is the potential wireless population to be served?
- What is the size of your user population?
- Where are they located?
- How and when are they likely to use wireless?
Synthesize design requirements

Knowing as much as possible about your wireless users will help you synthesize design requirements for access, performance and the scale of your WLAN infrastructure.

◦ What services will the WLAN support?
◦ Will wireless be an overlay to the existing wired network or will it be the primary network?

If the WLAN is mission-critical, you will need to factor in the requirements for fault tolerance, load management, and a comfortable performance margin.

Keep in mind that with a reliable wireless service, you may find your user population rapidly adopting it as their primary service vehicle.

Will it be ready?
Information gathering

Assess performance requirements
Applications and services
Indoor and Outdoor
Security
Growth
Personnel
Assess performance requirements

To assess performance requirements, it is important to determine the applications and services that may be used over the WLAN.

Will you support applications with real-time, latency sensitive traffic such as video and voice?

Will you serve outdoor spaces as well as indoor?

What is your security policy?

Have you really looked into the future?

Personnel considerations
Applications and services

Will you support applications with real-time, latency sensitive traffic such as video and voice?

- Real-time services demand guaranteed delivery times; furthermore, video can consume a great deal of bandwidth.
- You must determine the extent to which your population will use these services, during what times and in what locations.
Will you serve outdoor spaces as well as indoor?

Deploying outdoor Wi-Fi requires additional considerations including:

- The WLAN’s proximity to the wired network,
- Topography,
- The potential AP locations/mounting options. Outdoor WLAN equipment is expensive and deployment requires personnel with RF expertise.

Experience has shown that many buildings enclose outdoor areas of interest, making it possible to serve an outdoor space from an indoor window. This can greatly reduce the cost and complexity of providing outside coverage.
What is your security policy?

Security can be a mixed bag.

Everyone wants it but many are not willing to tolerate the overhead it imposes on access or IT administration.

You must determine the tradeoff that your organization is willing to make.

Most likely, some form of network access control will be required. Standards such as 802.1x enable per user access control of wireless users through external authentication servers such as RADIUS or Active Directory (AD).

Guest access is a desirable service, giving temporary and limited authorization to select users whose access time is bounded. Typically a captive portal is used as a convenient, web based front end to provide guest credentials.
Access control is often not enough

Some form of encryption “over the air” is desired to insure the integrity and privacy of the wireless content.
  - Wi-Fi link layer encryption can provide the answer through standards such as WPA and WPA2, depending on the desired strength.

These encryption methods require a pre-shared key to be given out to each WLAN client.
  - Key administration is an overhead that needs to be factored into the ongoing operational cost of the WLAN.
Have you really looked into the future?

Don’t underestimate the user appetite for wireless.

- If your coverage is not ubiquitous on day one, at least spend time up front to verify that your WLAN design is scalable to provide ubiquitous access when the need arises.
- Multimedia support may not be a current concern. However, applications and devices are converging. It is just a matter of time that the network will be tasked to support converged services — video, audio, graphics, interactivity, etc.
- Fortunately, 802.11n, a new Wi-Fi standard for delivering several times the capacity of current 802.11g is available in business class 802.11n products.
- Nevertheless, a solid QoS implementation is always a necessary insurance that the network can support diverse traffic types, applications, devices and users.
Personnel considerations

With every new technology comes the requirement for skilled resources to plan, design, install and maintain that technology.

- Wireless is no different in that regard.
- Choosing a WLAN offering whose features and support minimize the need for additional skilled personnel could be a top priority.
WLAN Design

With the detailed requirements in hand, you can now design a WLAN that meets your capacity, coverage and performance goals today with a path for expansion whenever the demand arises.

Determining the required capacity

In general, a typical wireless user consumes no more than 250Kbps bandwidth on average.

Here are some typical service rates:

<table>
<thead>
<tr>
<th>Network Need</th>
<th>Sustained data rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Casual Data</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>Mission Critical Data</td>
<td>10 Mbps</td>
</tr>
<tr>
<td>Voice/Video</td>
<td>20 Mbps</td>
</tr>
</tbody>
</table>
Bandwidth

Voice doesn’t take much bandwidth but it requires guaranteed bandwidth.

Video on the other hand will create a major impact on bandwidth consumption.

Surveillance video requires less bandwidth as frame rates and resolution are typically much lower. However, low cost surveillance cameras do not have the latest compression technology so the bandwidth required is not insignificant either.

A good assumption to use in AP capacity planning is 1-2 Mbps per user for data and 5-10 if you think video will dominate. The average TCP throughput of 11g APs is approximately 20-30 Mbps, while an 11n AP can often deliver 75 Mbps or more. However, the average TCP throughput is much lower, depending on the number of clients on the AP.
Determining coverage area

Like a cellular base station, each AP defines coverage geography with a maximum radius determined by available signal power and signal attenuation from objects that block the communications path.

If the user population exceeds that in a given geography, the only way to increase the capacity is to add more APs into that geography. This must be done in such a way that each AP does not interfere with its neighbor.

A good way to accomplish this is to set a different operating frequency for each AP within an area. For 802.11b/g there are three non-overlapping frequencies, channels 1, 6 and 11. For 802.11n there are 23 non-overlapping frequencies.
Security integration

If you already support a centralized AAA (authentication, authorization and accounting) service, you’ll probably want to integrate it with your WLAN infrastructure.

If not, you may want to include AAA with your WLAN infrastructure.
Sighting for optimization and installation

It is always a good practice to walk through the planned deployment sites before installation.

- There can be variations in construction not specified on floor plans, variations in building materials, obstructed access to proposed AP locations and certainly concern for esthetics.
- Variation in building materials can affect the propagation of RF signals causing it to deviate from your planned coverage.
- For example, an AP designed to cover three or four rooms may work just fine through sheetrock walls.
- However, if those walls are made of concrete, the AP signals may not propagate beyond the walls on which the AP is mounted.

Lastly, building construction may prohibit AP placement where originally planned.
- Physically sighting AP placement will identify these issues before the installation to save time and money
Optimizing indoor AP placement

There are some placement guidelines you should follow to maximize AP performance.

- All APs should be mounted as high and as visible as possible.
- Try to avoid any obstructions, especially those in close proximity to the AP.
- An obstacle two to three feet from the AP will have a much more detrimental effect on performance than one located 20 feet away.
Outdoor coverage

If you need to provide Wi-Fi access outdoors, consider the possibility of extending the WLAN coverage from inside.

Many buildings enclose or adjoin outdoor areas of interest making this a viable option.

- Make sure to verify the type of window glass through which your signals will travel.
- Older buildings may have glass that contains lead which can affect signal propagation.
3rd party interference

Wi-Fi uses license-free RF spectrum. This means that any interference occurring within that spectrum must be tolerated.

You can’t control interference from other devices legally sharing your radio spectrum. Examples for such devices are:

◦ Cordless phones, microwaves, blue-tooth devices, adjacent APs, and Wi-Fi clients. During your walking tour, determine all potential sources of interference.

By adjusting AP placement you’ll likely eliminate much of the interference.
System operation, maintenance and growth

Experience has shown that checking the performance and availability of your WLAN from the clients’ perspectives gives the ultimate indicator of your system’s health.
Practice active management

Wi-Fi networks don’t stay in top condition on their own.
◦ The inevitable moves, additions and changes of people, furniture and everything else within an organization will cause the network to degrade over time and provide less-than-optimum service to users.

Wi-Fi networks are amazingly fault-tolerant.
◦ They can survive the loss of access points and the addition of interference without registering significantly perceptible effects.
◦ Problems might go unnoticed without active monitoring.

Good network management practices, including the regular scanning of logs and the active monitoring of devices and usage, will help identify problems before they affect performance.
Wi-Fi Scanners

InSSIDer for Windows (from Metageek)
- Create custom filters
- Log and export KML for Google Earth
- Channel View for determining Wi-Fi channel Overlap
- 2.4 and 5 GHz and network strength over time views

InSSIDer for Android
- Optimize your Wi-Fi network by choosing the best channel
- Shows how other networks interfere with your Wi-Fi network
- Runs on Gingerbread or newer versions of Android
- 2.4 and 5 GHz and network strength over time views

NetSpot (Mac OS only)
- the only professional app for wireless site survey, Wi-Fi analysis and troubleshooting on Mac OS X
Site Survey Tools

Heatmapper from Ekahau
- Wi-Fi coverage on a map
- Supports 2.4 and 5 GHz 802.11n
- Quickly locate Rogue Access Points
- 15 minute time limitation

Wi-Fi Mapper from Meraki
- Wi-Fi coverage on google maps or floor plan,
- No installation
- Quickly locate Rogue Access Points
- Estimated throughput results

NetSpot (Mac OS only)
- The visual Wi-Fi map
- Tee all dead zones without coverage and optimize hotspots' placements; you can see channels' load and decide how to use them ideally.
Heat Mapper Image
Site Planning

Free Wi-Fi Planner from Aerohive
- Upload a floor plan.
- Auto placement for quick and easy planning.
- Must register for Hive Manager Account
- Works With: Aerohive APs only

NetSpot is also an amazing wireless survey tool for Wi-Fi planning.
- Load a map,
- Collect some wireless site survey data,
- Build a comprehensive heatmap of your network.
Third Party tools for identifying sources of interference and rogue APs

For example, there are two outstanding open source offerings known as AirSnort (based on the popular Snort package) and Kismet.

◦ **AirMagnet** offers tools for debugging RF problems in the field as well as tracking down offending rogue APs or wireless clients.

◦ **WildPackets** and **Cognio** offer a line of Wi-Fi analyzers that monitor RF spectrum plus capture and analyze individual wireless packets or protocol dialogs.

◦ Other excellent free tools are **NetStumbler** and **Wi-Spy**.
Use managed wireless products

When considering wireless management, the network team should be careful to distinguish between fully managed solutions and those that only offer configuration control and log collection.

Simply capturing the configurations of each AP and pushing changes to them uniformly is not true wireless management.

Although that is a useful function in some environments (such as branch offices with one or two APs), any deployment with more than eight APs will need a fully managed solution.
Prioritize usage

In the first few days after a network is turned on, the smartphones of at least 10 to 20 percent of the people in the building will connect automatically.

- These devices will consume bandwidth even when no one is using them.
- If the building is on a high school or college campus, that figure will be closer to 80 to 90 percent.
- In other words, a wireless network can reach near capacity even when no one is actively using it.

The solution isn’t to prohibit casual use, but simply to make sure that mission-critical applications, such as VoIP (unified communications) or transaction processing, and business uses get priority over nonbusiness and casual usage.

- By using management configuration, firewalls or Wi-Fi Multimedia (WMM), it’s possible to throttle bandwidth.
Develop a guest policy carefully

Accommodating guest access to wireless networks is generally considered a requirement for enterprise wireless installations. Guests commonly have a legitimate need to connect to the Internet while visiting an organization. Although some road warriors may use alternative technologies, such as 3G or 4G wireless, to bypass local Wi-Fi networks, it is important to plan how other guests will connect to the organization’s WLAN.

Of course, these guests shouldn’t require much access to anything inside the normal enterprise network — printing, perhaps, being the occasional exception. Therefore, securing connections to ensure that guest users do not gain elevated privileges is important.
Balance

Any guest policy must balance its requirements for accountability and prevention of “drive-by” connections with the goal of making guest connections simple and quick. Many vendors offer specific guest services, such as captive portals and automated guest provisioning systems that can ease the task of offering guests wireless connectivity.

Common alternatives, such as requiring guests to preregister Media Access Control (MAC) addresses or obtain a temporary user name and password, tend to be cumbersome and should be avoided. One bad result of a guest policy that is poorly developed or difficult to follow is that staff members might spend valuable time trying to get their visitors logged on to the wireless network. Or, even worse, a staff member might encourage a guest to connect directly to the internal wired network to bypass issues with the wireless infrastructure.
Build security from the start

Many techniques exist to increase overall security for wireless users, but it pays to have the organization’s security teams involved from the beginning. Doing so will make it possible to incorporate their requirements into the architecture design and product selection phases of the project.
MDE Field Engineers - Ciber

Donnie Cummins
- dcummins@mde.k12.ms.us
- 601.946.0839

Glen Popiel
- gpopiel@mde.k12.ms.us
- 601.209.9866

Tim Rutland
- trutland@mde.k12.ms.us
- 601.942.9932