The Five “Ws” of Implementing a Wireless-N Network
Wireless-N (or 802.11n) networks have many advantages for mid-sized businesses, from simplified wireless mobility to increased performance. This paper looks at five questions or “Ws” you need to consider when planning Wireless-N networks, and contains insights and lessons learned from previous wireless deployments. The objective is to help maximize your success in designing and implementing a mission-critical wireless LAN (WLAN). The five Ws are:

- Why do you need wireless?
- Who gets to use the wireless network?
- Where do you need wireless network coverage?
- When should you care about radio frequency (RF) and traffic management?
- What can you do to simplify ongoing management?

Why Do You Need Wireless?

Connectivity is the lifeline of today’s dynamic business world. Mobility is a critical aspect IT administrators must consider when designing their networks. More and more mobile devices such as laptops, Smartphones, and IP cameras now support wireless connections.

Business applications and the amount and pattern of traffic on a network have a great deal of impact on your wireless network design and architecture. The WLAN may be the only network in the building, or it may complement existing LAN infrastructure. Your WLAN may need to accommodate time-sensitive applications such as voice or streaming video. There may be bandwidth-demanding applications present such as databases or file transfer mechanisms. There may be certain times of day or month that experience large amounts of data transfer. Proper sizing and planning based on your unique business needs will ensure your wireless network delivers maximum performance at minimal cost.

Many of today’s wireless access points (APs) and wireless controllers are designed to eliminate bottlenecks experienced in previous wireless architectures. In the past, a wireless network with several APs used to have all its traffic switched through the wireless controller, a centralized architecture that created bottlenecks. Today’s leading wireless APs and wireless controllers eliminate these bottlenecks. Once the controller authenticates a user and appropriate policies are enforced, traffic should be switched directly onto the network by the AP. If the user moves to another AP zone that is in the same subnet, the new AP should seamlessly pick up traffic without disruption (this is called Layer 2 or L2 switching or roaming.) If the user moves within range of a different subnet, the traffic should be switched through the wireless controller. This way, the users can maintain their current IP address without disruption (called Layer 3 or L3 switching or roaming). This mixed centralized/distributed architecture helps distribute traffic more evenly across the wireless network.

Who Gets to Use the Wireless Network?

Who will use the network and when they use it is a large factor in WLAN planning. Before you deploy, you’ll need to decide if all employees and contractors get access to the wireless network or if there are some departments that don’t require access. Whatever you decide, ideally a wireless network should look the same to your users as the wired network, with access to the same systems and no additional downloads or user logins required for security purposes. Business wireless solutions should integrate with existing centralized authentication, authorization, and accounting (AAA) services such as RADIUS or Active Directory (AD).

Beyond employees or contractors, you may want to plan for additional capacity for guests. The number of guests is widely dependent on your type of organization/business and how often those guests may require wireless network access. For example, public libraries have many guests requiring wireless network access, while manufacturing facilities have very few. In any case, guests must be restricted from accessing sensitive data or applications on the corporate network. A common mechanism used to provide secure access is a captive portal, which prompts guests to enter their usernames and passwords or other credentials. This allows you to grant WLAN privileges to only certain guests, for example, while locking down the network for casual visitors. Once a guest is granted access, they should be restricted to a virtual LAN subnet (VLAN) that lets them access the Internet without being able to access your data or applications.

Sometimes, people deliberately or unwittingly attempt to connect access points without the knowledge or permission from the organization. These are called rogue access points. Any wireless solution should automatically detect rogue APs that may try to camp on to a wireless network.

Finally, you may want to limit when users can access your wireless network. For example, you may want to restrict access late at night or on weekends when you want to conserve power or perform system backups. You could do this on a user-by-user basis in your AAA system, or use a wireless solution that can automatically power down APs at pre-configured times.
**Where Do You Need Wireless Network Coverage?**

Determining your wireless network coverage area is another important step in WLAN planning. Proper planning ensures seamless coverage with go-anywhere roaming as users move from room to room or floor to floor within a building. Not only do you need to decide what parts of the building need wireless access, you also need to decide how many APs are needed and where to physically place them. This used to be a very time-consuming task involving trial and error. Today, smart wireless controllers with sophisticated planning algorithms do the hard work (see Figure 1). You simply input information such as floor layout maps, building dimensions and number of users, and the controller automatically develops optimum wireless AP placements.

While today’s planning algorithms are sophisticated, they can’t take into account everything you’ll need to plan the placement of your APs. As a result, you may still need to adjust the placement of your APs to deal with obstacles within your building that are not captured on the floor maps that may interfere with wireless signal strength and distance. You may also need to adjust the AP placements simply to remove APs from areas of the building where you’ve determined wireless network access is not necessary.

![Figure 1: A wireless controller screenshot of auto-generated wireless AP placements](image)

Another consideration in planning where your wireless network needs to go is the physical building itself. Wireless networks are ideal for rooms or buildings where installing new LAN wiring would be expensive or esthetically displeasing, such as in old-construction or historical buildings.

Wireless networks are extremely flexible in their deployment, so much so that they can be deployed outdoors. This is one deployment consideration rarely considered in wired networks but if you have an outdoor seating area or a loading bay where it would be advantageous to have network access; leading vendors provide ruggedized wireless LAN antennas suitable for these outdoor uses.

**PoE**

PoE is a technology supported on some IP network devices—such as certain switches and wireless access points—whereby they safely receive electrical power through the same standard cable that transmits IP data. Power can come from a PoE-enabled device like an Ethernet switch, or a special-purpose power supply device such as a midspan. PoE makes it simpler to install APs where power is not available. Instead of hiring an electrician to install power outlets, a device with PoE support only needs to plug into an Ethernet cable. It is relatively easy and inexpensive for any network installer to run Ethernet cabling to new locations in a building.

**When Should You Care about Radio Frequency and Traffic Management?**

Wireless signals travel in radio waves all around us. The blessing and curse of 802.11 networks is that they use a license-free spectrum. Unlike cellular phone carriers, you do not have to pay a license to use certain frequencies, which keeps the cost of wireless networking low. Unfortunately, it also means your wireless network is susceptible to interference from other APs and wireless clients, or other devices using the same RF spectrum such as microwave ovens, cordless phones, and Bluetooth devices (see Table 1). This interference can lower throughput speeds or disrupt connections entirely. Radio Frequency (RF) management is critical in ensuring that your wireless network is running interference free. Many of today’s wireless APs operate in both the 2.4 GHz and 5 GHz band. The newer 5 GHz band avoids interference from many older network devices. However, that does not solve the problem of newer network devices interfering with one another.
<table>
<thead>
<tr>
<th>Wireless LAN frequency</th>
<th>Wireless LAN protocol</th>
<th>Other devices that may cause interference</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 GHz</td>
<td>802.11 b, g, n</td>
<td>Bluetooth, microwave ovens, cordless phones, fixed wireless systems, electricity meters, video cameras, baby monitors, video game controllers</td>
</tr>
<tr>
<td>5 GHz</td>
<td>802.11 a, n</td>
<td>Cordless phones, fixed wireless systems</td>
</tr>
</tbody>
</table>

Table 1: Devices using wireless LAN frequencies

In the past, operations staff would manually tune APs to different frequencies so they would not interfere with one another. Now, the newer wireless controllers optimize channel allocations for neighboring APs, so your own APs do not interfere with one another. In addition, some wireless controllers are self-healing; they can automatically detect third-party interference and switch APs to another channel, thereby avoiding the interference altogether. They may also detect holes in coverage due to outages, and boost the signal strength of surrounding APs to close the hole and ensure network coverage.

Traffic management can be tricky in wireless networks. Wireless network usage tends to be bursty and uneven, because users often congregate together around one access point, perhaps in a meeting room. This can create congestion for some APs, while others are practically unutilized. Load balancing features in wireless controllers direct APs with overlapping coverage to share the load, ensuring users experience adequate service even in crowded conference rooms.

If some users are using more than their fair share of bandwidth, rate-limiting features contained in some wireless controllers can allocate bandwidth more evenly.

**What You Can Do to Simplify Ongoing Management?**

Like any network, WLANs are not static. Wireless networks can experience interference from other APs, or infiltration by rogue APs, i.e., one not authorized to be on the network. Roaming users or traffic loads may create bottlenecks, affecting response times for applications. Wireless networks must adapt to changing user and business demands.

Choosing the appropriate wireless solution is the one of the biggest factors in determining the ease of network installation and ongoing management. Wireless controllers with Graphical User Interfaces (GUIs) and features such as RF planning tools help simplify planning and deploying wireless networks. Once your network is in place, network management features like automatic access point detection, rouge AP detection, quality of service, and wireless interference detection and recovery ensure that your wireless network remains operational with a minimum amount of management effort. Visual management tools like real-time data traffic and signal strength views make it simple to check on the health of your network.

With the appropriate tools in place, much of ongoing wireless management can be simplified and automated—saving time and resources.

**Summary**

Wireless-N networks offer high performance and extended range. They are an affordable, convenient, and quality solution for mid-sized businesses looking to extend their wired LAN or upgrade their existing wireless network. Following the five “W’s” of wireless planning will help you simplify planning, deployment, and ongoing operation of your new WLAN network.

**About NETGEAR ProSafe Wireless Management Solutions**

NETGEAR® ProSafe® Wireless Management Solutions solve the quandary of individually configuring, deploying, and managing multiple standalone wireless access points. Supporting from one to 150 APs, they provide a single location to configure and manage your wireless network. NETGEAR® ProSafe® Wireless Controllers are designed for medium-sized businesses, but deliver all the features needed for large wireless networks.

The NETGEAR ProSafe WC7520 Wireless Controller’s user interface is designed to reduce time and effort for installation and ongoing management of WLANs. It includes a GUI with RF planning tools and allows you to easily add, move, and make changes to your wireless network. It automatically maps and detects new APs, allowing you to accept or reject them from the network. The WC7520 continually monitors their traffic load, RF interference, number of clients, and displays them as metrics per AP, per floor, and for the entire wireless network. The WC7520 supports seamless L2/L3 fast roaming, maintaining voice over IP wireless calls as users roam the building. The WC7520 enforces comprehensive security measures, including existing authentication and authorization mechanisms, captive portal, and guest access management.

NETGEAR®, the NETGEAR logo, Connect with Innovation, ProSafe, ProSecure and ReadyNAS are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Information is subject to change without notice. © 2010 NETGEAR, Inc. All rights reserved.