CONNECT | MANAGE | PROTECT

WHITE PAPER:

Optimizing the Wi-Fi User Experience:

Tips and techniques for designing, implementing and managing high-performance wireless networks

Tulsa | Washington, D.C. | Atlanta | Chicago | Philadelphia
866.480.2263 | www.sagenet.com

Wi-FiWP091619

SageNet

CONNECT | MANAGE | PROTECT

EXECUTIVE SUMMARY

Employees are utilizing an average of three mobile devices to perform job functions. Those devices connect to the Wi-Fi network to access important business data and applications, including real-time collaboration tools such as voice and video conferencing. Customers are just as mobile and expect businesses to provide them with high-performance wireless connectivity.

Internet of Things (IoT) devices also rely on Wi-Fi and generate a mind-boggling amount of data. Cisco estimates that machine-generated IoT data transmissions will reach 600 zettabytes by the end of 2020 — 275 times the amount moving from data centers to end-users!

Cisco estimates that machine-generated IoT data transmissions will reach **600 zettabytes by the end of 2020** - 275 times the amount moving from data centers to end-users!

The design, architecture and management of the wireless network has never been more critical to business success. However, ensuring Wi-Fi performance and reliability involves a very different set of considerations than the traditional wired network. Administrators have to worry about radio frequency (RF) interference and ever-changing capacity requirements as devices move onto and off of the network. The experience of any given user depends upon a host of factors that are difficult to measure and control.

This whitepaper will explain the importance of upfront planning and assessment, as well as best practices for wireless LAN deployment. It also offers techniques for maximizing capacity and performance, and discusses tools administrators can use to troubleshoot issues and optimize the user experience.

DEVELOPING A PLAN

Planning is the critical first step toward ensuring a robust network infrastructure. In the past, coverage was a primary consideration, and it remains an important factor. Because signal strength drops as a device moves farther away from a wireless access point (AP), a wireless LAN that lacks adequate coverage will drop connections as users move about. Organizations should consider where mobile devices are likely to be used in order to determine whether to extend Wi-Fi coverage into break rooms, storage areas, warehouse facilities and loading docks.

COVERAGE ≥ CAPACITY

Today, however, capacity is at least as important as coverage. Organizations need to estimate how many smartphones, tablets, laptops and other mobile devices will be accessing the network today, and try to anticipate increasing numbers of devices and bandwidth-hungry applications. IoT initiatives should also be factored in, as a growing array of sensors and other devices can create wireless network congestion.

Organizations can begin to stratigically design a wireless network only when they have a thorough understanding of:

- Coverage and bandwidth needs
- Number of devices accessing the network today & estimate for tomorrow
- Future IoT initiatives
- Other requirements

It's important to recognize, however, that wireless LAN design can't be worked out on paper. This requires analysis of the physical space where the Wi-Fi network will be deployed.

EVALUATING THE ENVIRONMENT

Wireless LANS must be carefully engineered to account for:

- Stationary & mobile obstacles
- RF Interference
- Floor-to-floor signal bleed
- Other environmental issues

There are some rules of thumb regarding AP density and placement in an office building, but in practice these "rules" are of limited value. In the real world, it's impossible to remove every solid object between a transmitter and a receiver, so it's important to consider the impact that physical obstructions can have on Wi-Fi performance.

PHYSICAL OBSTRUCTION

Some facilities are particularly problematic when it comes to RF-blocking infrastructure:

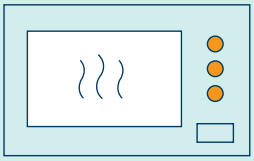
- School buildings (masonry or concrete walls)
- Warehouses (metal shelving)
- Medical facilities (shielded X-ray rooms, highly mobile metal objects such as medical equipment & beds/carts)

The potential for RF interference must also be evaluated. Given the explosion of wireless devices, RF signals are literally everywhere and can affect the performance and reliability of the wireless LAN. Co-channel interference occurs when two nearby APs are set to the same frequency — the culprit may even be part of a neighboring wireless LAN. In adjacent channel interference, an overlapping channel bleeds over into the frequencies used by Wi-Fi. Impulse noise from electrical devices can also interfere with Wi-Fi signals.

MEASURING COVERAGE

State-of-the-art tools can help with site surveys, coverage tests, and noise and interference detection. If an existing WLAN is in place, these tools can also identify areas of poor signal strength and quality and help determine whether the existing infrastructure can be modified to improve coverage. Still, multiple site visits may be required for an engineer to document the many obstacles, points of interference and areas in which AP placement may be restricted.

RF Interference is Everywhere



Many devices found in the typical office — wireless keyboards and mice, cordless phones, even microwave ovens — can cause RF interference in the 2.4GHz spectrum used by most Wi-Fi networks. Because these devices are only "on" at certain times, they can create phantom problems that are difficult to troubleshoot.

In fact, many Wi-Fi problems can be traced to the RF layer due to the inherently challenging and dynamic nature of the wireless environment. Moderate interference can cause sluggish performance while stronger signals can prevent users from accessing the wireless LAN at all.

ENGINEERING THE WIRELESS LAN

In addition to overcoming environmental challenges, WLANs must be able to support the user densities, escalating bandwidth requirements and seamless roaming associated with pervasive wireless. More wireless devices mean more wireless transmissions operating on similar frequencies, leading to interference.

While multiple users can communicate with the same AP, the AP only has a finite number of radios. In addition, Wi-Fi channels overlap, making it necessary to limit the number of channels used by a given AP. However, this also limits the number of devices that can connect with that AP.

65% of hotel guests are using Wi-fi within 7 minutes of checking-in.

MU-MIMO PRODUCTS

802.11ac Wave 2 products support a higher user density with multiuser, multiple input, multiple output (MU-MIMO) capabilities. With the previous standard, each spatial stream could support only one user transmission (single-user MIMO). MU-MIMO allows up to four simultaneous user transmissions on a single spatial stream.

The 802.11ax standard, also known as Wi-Fi 6, takes this even further by supporting eight simultaneous streams and using beamforming technology to accurately aim those streams at the receiver's antennas. 802.11ax also has a 160MHz spectrum channel, four times wider than those used by 802.11ac, and uses a technology called orthogonal frequency division multiple access (OFDMA) to break the channel down into hundreds or even thousands of subchannels. This allows up to 18 clients to send data simultaneously without creating signal contention or congestion.

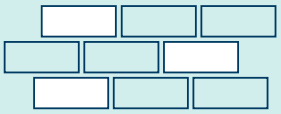
BANDWIDTH MANAGEMENT

Still, Wi-Fi remains a shared medium. More users, devices and applications mean more wireless traffic and less bandwidth to share, which can slow response times. Bandwidth management is essential.

One option is to simply place limits on how much bandwidth an individual device is permitted to use. This technique, called policing, drops traffic that exceeds this limit. However, policing doesn't take into account varying bandwidth requirements. Traffic shaping enables administrators to allocate more bandwidth to certain types of devices, applications and functions, and even to specific areas of a facility during certain times of day.

Quality of Service (QoS) policies are designed to ensure high performance levels during periods of heavy traffic. QoS prioritizes certain types of traffic, allocating more bandwidth to latency-sensitive traffic such as voice and video and less bandwidth to lower-priority traffic.

Overcoming Capacity Challenges in Open Spaces



There are two competing design factors in Wi-Fi deployment: nearby APs improve capacity, but having too many APs can degrade it. Ironically, RF-blocking physical infrastructure, such as masonry walls, facilitate high-density Wi-Fi. In older schools, for example, it's possible to place an AP in every classroom and run it at reduced power. The masonry walls attenuate the signals of APs in adjacent rooms.

Wi-Fi signals propagate very well through the air, making it difficult to get adequate capacity in open spaces. However, beamforming combined with intelligent client steering, high minimum bit rates and low power settings, can improve capacity in an open space.

THE IMPORTANCE OF MANAGEMENT TOOLS

In the past, management of the wireless infrastructure was often an afterthought, with organizations implementing point solutions to address specific problems. Given the mission-critical nature of today's wireless LAN, organizations should invest in the tools they need to ensure optimal performance, security and control.

A centralized, multivendor wireless LAN management solution provides visibility and control of the entire Wi-Fi environment from a single, intuitive interface. Multiple dashboard views make it possible to diagnose potential issues with coverage, bandwidth usage and application performance. Clustering simplifies the management of thousands of users, devices, access points (APs) and controllers across any number of remote locations.

Leading management solutions take a user-centric approach to identifying causes of service-quality issues through real-time monitoring and proactive alerts. Maps display the real-time health and performance of individual devices and applications as well as the network as a whole.

Network performance is assessed based upon the infrastructure, user location and signal coverage using data gathered from APs, controllers and devices. RF scanning pinpoints sources of interference, while deep packet inspection provides IT with greater control of applications based upon quality of service requirements and bandwidth usage policies. This information enables better service quality and faster problem resolution.

U.S. Broadband Households now have an average of **9.1 Connected DEVICES**

CONCLUSION

Wireless connectivity is critical to operations today. Organizations need a wireless LAN with the capacity, reliability and performance to support growing numbers of users and applications. However, the increasingly mobile workforce and explosion of employee-owned devices has made it difficult for enterprises to deliver an optimal user experience. Network administrators often struggle to troubleshoot problems and respond to support requests.

The best way to avoid performance-draining issues is through careful assessment and planning of the wireless LAN design. Organizations must consider environmental factors that can impact Wi-Fi performance, including physical obstacles and RF interference. They must also strategically place APs to maximize both coverage and capacity, and employ bandwidth management and QoS techniques to optimize performance.

Manageability is also important. In many organizations, small IT staffs are already spread thin managing existing IT operations and often lack specific expertise in Wi-Fi. It is important to integrate management tools that enable non-specialists to support wired and wireless LANs and mobile devices from a “single pane of glass.” These tools can help ensure high availability by speeding the discovery, diagnosis and troubleshooting of problems that surface in the highly dynamic environment.

ABOUT SAGENET

SageNet is passionate about trusted connections. The company believes that by creating, discovering and nurturing trusted connections with its customers, associates and community, SageNet enhances the world that connects us all.

As a leader in managed network and cybersecurity services, SageNet connects, manages and protects technologies and devices across the enterprise. SageNet’s collaborative approach provides peace of mind and systems-confidence that empowers an organization to focus on its core mission.

The company offers world-class service and support via its three US-based 24/7 Network Operations Centers (NOCs) and Security Operations Centers (SOCs), geographically-diverse teleports, a central National Logistics Center, multiple data centers, and a nationwide field service organization.

With a three-decade track record in managed services, SageNet boasts a long-term customer base that includes the nation’s largest retail, healthcare, financial, utilities and energy organizations. SageNet manages communications at more than 220,000 endpoints. Headquartered in Tulsa, SageNet has regional offices in Washington, D.C., Atlanta, Chicago and Philadelphia.