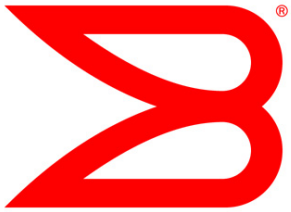

ENTERPRISE & MOBILITY

A Guide to Ensuring Wireless LAN Reliability

A reliable wireless LAN depends on smart planning, and preemptive troubleshooting but it also needs the ability to dynamically adjust to radio frequency issues as a result of unforeseen obstructions and changes in employee behavior.

BROCADE

INTRODUCTION

IT managers once relegated their network uptime concerns only to the wired network. Wireless LANs were viewed largely as ancillary luxuries, and if the wireless network went awry, well, so be it. With employee productivity tightly tied to employee mobility, most companies rely on their wireless networks for core business operations. Today's network users consider them less a luxury and more a necessity.

Every professional IT manager is familiar with the goal of "five nines," referring to a network that is up, running and available 99.999% of the time. It's a lofty but worthwhile goal, as the closer you come to meeting it, the more money you will save. Network downtime is not just frustrating; it's quantifiably expensive. A recent study of 80 large corporations, from Infonetics Research, showed that companies experience an average of 501 hours of network downtime annually, including both outages and service degradations. The average cost of this downtime equaled a whopping 3.6 percent of a company's annual revenue, the study found. And these days, when IT managers talk about network downtime, they're often referring to a company's wireless LAN.

It should be noted that in a wireless world, network downtime affects not only the office, but also all the mobile devices connected to the network—from the student laptops in classrooms to the networked infusion pumps in a hospital's emergency room to the dual-mode smartphone that is becoming key to user productivity.

In the nascent days of Wi-Fi, a corporate wireless LAN comprised a series of autonomous access points, scattered throughout the office and even branch offices around the globe. Garnering an effective radio signal was a matter of trial and error, and because there was no central management, the administrator wouldn't know there was a problem until someone inevitably complained. Today's Wi-Fi networks, managed from a central switch, can be even more reliable than a wired Ethernet network—but only if IT directors take the necessary steps to ensure reliability and promise superior quality of service in every aspect of the network.

ENSURING RELIABILITY MEANS PLANNING FOR EXPECTED CHALLENGES

It should go without saying that a reliable wireless LAN (WLAN) depends on smart planning and preemptive troubleshooting on the part of the IT manager—i.e. designing the network based on the specific needs of the company. Implementing a WLAN without conducting a thorough site survey, only creates coverage, bandwidth and other reliability issues.

Before investing in any WLAN hardware, you or your integrator should invest in **wireless LAN planning software** to plan the network while focusing on the following questions:

Who will be using the network, and when will they be using it? Obviously 2,000 employees require a more robust network than 20 employees. But beyond that, it's important to note whether there are certain times of day when a network—or even a single access point—is likely to experience a sudden flood of traffic. For example, is there a Monday morning meeting in which 60 employees and their laptops and smartphones squeeze into a single conference room?

What applications will the network serve? For example, will employees be using the network mainly for wireless e-mail and Internet access, or will the network also be used for virtual desktop, video and voice applications? The latter two likely will require more access points (AP). Video transfers require more bandwidth than other applications. And wireless voice calls are especially unforgiving when it comes to network glitches such as latency (a lag in data transfer time) and jitter (an unplanned fluctuation in signal transmission.)

Which workspaces require WLAN coverage? Are the company's wireless needs relegated to the so-called "carpeted" areas of the office, or will employees need the network in hallways, manufacturing floors, or the outdoor spaces on large campuses? And are there areas on the corporate campus that require the company to restrict network access to certain employees for security reasons?

Are there any obstacles that might interfere with Wi-Fi radio signals? Most businesses and buildings are rife with possible interferences, including:

- **Microwave ovens:** Unfortunately, microwaves can interfere with the 2.4GHZ 802.11b/g Wi-Fi signals. An AP placed too close to a microwave oven could experience degradation in performance every time it is used. Older cordless phones and Bluetooth devices also interfere with WLANs.
- **Metal:** Many types of metal, especially steel and lead, can block Wi-Fi signals. File cabinets, sculptures, benches, large chairs, and steel doors are obvious problems, but IT managers also must be mindful of hidden obstacles —such as metal studs in plaster walls, wire mesh in windows, and steel beams in ceilings—and place access points accordingly.
- **Concrete:** Concrete floors and walls tend to block Wi-Fi signals. This is a boon in terms of blocking signals from neighboring businesses, but a detriment when it comes to blocking signals from your own network.
- **Nature:** Especially with regard to networks that span between two buildings, IT managers must plan for interference from trees, bodies of water, and other gifts of nature that most likely existed before Wi-Fi ever did.
- **Someone else's Wi-Fi network:** Just as microwave signals can interfere with your Wi-Fi signals, so can the Wi-Fi signals from neighboring networks—especially if they are operating on the same or neighboring channels.

Who will be running the network? Will wireless network operations be under the charge of one or two IT employees in a single location, or will there be network operators in remote locations who oversee subsidiary WLANs of their own?

What are the likely security challenges? Security breaches can lead to network downtime and stolen data. Does the building's location make it especially susceptible to war-driving hackers? Are the signals from your network likely to leak into a neighboring office? Is there classified data on the network?

Again, before investing in any wireless LAN hardware, invest in **wireless LAN planning software** that simulates possible scenarios and helps plan and map a new WLAN network.

What's it going to cost if it's not working? While the costs to IT typically include helpdesk and field engineering, the lost opportunity or productivity costs can be damaging for companies that depend heavily on the wireless network for mission-critical operations.

ENSURING RELIABILITY MEANS PLANNING FOR "UNEXPECTED CHALLENGES"

Of course, the best-laid plans will go awry if they don't account for unforeseen obstructions and changes in employee behavior. Chances are that your business is a dynamic, ever-changing environment. To that end, a reliable wireless network requires the ability to dynamically adjust to radio frequency issues such as:

- **Radio interference from new networks or microwave ovens:** In a simple scenario, a new microwave in the corporate kitchen will cause unexpected WLAN interference every time it's used. Or the business in the office next door might install a new WLAN with strong signals that bleed through the walls and interfere with your own WLAN.
- **Sudden changes in usage patterns:** A new account or project might mean that employees are suddenly holding large, all-hands meetings and wireless video presentations, in a single conference room, overloading an AP previously used for nothing but wireless voice applications. A reliable WLAN will address such an event by increasing the signal on the overloaded AP and moving some of the traffic to neighboring APs.

- **Ever-changing cubicle patterns:** Especially in an uncertain economic environment, it's pretty common for a business to consolidate both its workforce and its workspace—which often means reorganizing an office's cubicles overnight. Even if the cubicles themselves don't pose an obstacle to wireless signals, changing the pattern of the cubicles will change the usage pattern of the WLAN, meaning that it will require some adjusting in order to work at full capacity.
- **Sudden changes in inventory, equipment, or customer behavior that leads to RF interference:** This is an issue especially prevalent in today's fast-changing enterprises. Empty classrooms suddenly fill up with students; or 20 new wireless infusion pumps are installed on a floor. An IT manager in a convention center might have to deal with major changes in the RF environment on a daily basis—a room filled with gourmet food booths one day might be replaced with giant metal structures the next.

Network administrators can best handle such scenarios with dynamic or intelligent RF management capabilities built into the infrastructure that automatically tune the network to ensure an optimal user experience at all times. It's important to note that these intelligent RF management capabilities will not completely compensate for or fix poor network design. Good network design in conjunction with intelligent RF should provide optimal user connectivity with far less support from IT.

ENSURING RELIABILITY MEANS PLANNING FOR POTENTIAL EQUIPMENT OR SIGNAL FAILURES

For every potential failure, network administrators need to ensure that there is a failover plan for every piece of the corporate wireless LAN, regardless of how reliable each individual piece of equipment is in the first place.

If an access point fails: In a reliable wireless network, the central switch will detect an AP failure and automatically increase the signaling power to the neighboring APs, so they can handle additional network traffic until the troublesome AP is repaired or replaced.

If the central switch/controller fails: The central switch/controller is the heart of the WLAN. In the unlikely event of a controller failure, network administrators can ensure network uptime by clustering two or more controllers together—so that if one fails, all operations automatically failover to the neighboring controller. Note, the controllers can be clustered to operate as one intelligent and resilient system, yet geographically distributed to ensure no single point of network failure.

If the WAN connection fails: WLAN reliability can extend beyond the usual functions of a Wi-Fi network. For instance, if a company's main WAN link goes down, a company can provide back-up support by creating a wireless 3G or wireless broadband backhaul link that attaches directly to the wireless controller or AP.

If a wired Ethernet link fails: A WLAN can make up for a wired Ethernet failure if its APs include wireless mesh capabilities. In a wireless mesh network, the network dynamically routes packets from AP to AP. So if the WAN fails, all APs in the mesh can route traffic to one or more APs with a 3G or wireless broadband backhaul. A few nodes have to be connected directly to the wired network, but the rest share a connection with one another over the air. Initially designed specifically for outdoor networks, mesh APs provide a way for the WLAN to operate even if an Ethernet link loses power. And with 802.11n, there is enough bandwidth to make mesh networking a robust and high-capacity distribution mechanism in case of wired Layer 2 failure.

If the whole central office loses power: Large corporations often comprise a main central office and several remote offices, which are connected to the main network. But network administrators should make sure to set up operations in such a way that if headquarters loses power, the employees in remote offices still maintain wireless network access. Conversely, the network administrator must have remote access to branch offices that may not have IT staffs of their own.

ENSURING RELIABILITY MEANS ENSURING WIRELESS NETWORK SECURITY

Security is a top concern for network administrators. And it really should be, because an unsecured network is clearly unreliable, especially as far as your customers are concerned. Wireless hackers can infiltrate corporate networks and steal important data from insufficiently-secured wireless networks. Furthermore, certain attacks—especially denial-of-service attacks in which hackers flood the network with useless but bandwidth-heavy data—have the potential to degrade wireless network performance or even bring it down entirely.

To that end, a reliable wireless network requires superior encryption mechanisms; 24x7 intrusion detection and protection at both the edge and core of the network; a centralized management and troubleshooting; consistent policies for network clients; audit logging of all network activity; and a firewall that detects all wired/wireless activity.

ENSURING RELIABILITY MEANS PLANNING FOR FUTURE TECHNOLOGIES

To stay competitive and ensure the highest possible level of performance, companies should use the latest Wi-Fi standards and expand the network to include other wireless technologies when necessary. For example, a company might upgrade from an 802.11b/g network to an 802.11n network because the latter promises faster data throughput rates and QoS for voice and video over an adaptive mesh network. The company might also want to add support for RFID, RTLS (real-time location system), and 3G WAN backhaul. Companies also want to stay current with security mechanisms and software updates for the WLAN, both at headquarters and in remote offices. To that end, companies need to make sure that their WLAN is relatively simple to upgrade and that they can make positive changes to the network with a minimum of downtime. Scheduled downtime is still a detriment to operations, so ideally such updates can happen dynamically, with a company's employees noticing nothing about the network other than improvements.

INVESTING IN A BROCADE WIRELESS LAN MEANS ENSURING RELIABILITY

Fortunately, Brocade® offers the tools necessary for a multi-faceted approach to deliver a network that dependably provides optimal network service and superior quality of experience. Compared with other leading wireless network equipment providers, Brocade has the most resilient, reliable portfolio on the market—from conception to future-proofing, and every step in between.

A reliable Wi-Fi network starts with a plan. LANPlanner includes all the tools necessary to create design plans, simulate network traffic, and perform site surveys for centrally managed 802.11a/b/g/n networks. The software analyzes the expected number of users who will be using the wireless LAN, the deployment environment (including physical obstacles), and the types of applications that users will employ as AP location and density requirements are distinctly different for data-only applications versus voice/data/video requirements. Armed with that information, LANPlanner makes educated recommendations about the placement and density of each piece of equipment in the wireless LAN, so as to ensure superior QoS.

Once the network is up and running, Brocade's intelligent operating system quickly and automatically adjusts to interruptions and interference, adjusting power and channels to handle unforeseen challenges in the RF environment. Brocade Mobility APs include RF monitoring capability—keeping track of neighboring APs while still maintaining the ability to send data. If an AP detects that a nearby AP has failed—or has been suddenly blocked by an obstruction such as a large metal object, the mobile users associated with that AP will seamlessly fail-over to a neighboring AP which will adjust its power to assure optimal quality. All mesh traffic will be automatically rerouted around the failed AP while an alarm is sent to the NOC to troubleshoot and repair the problem.

On Brocade dual-band, dual radio APs (AP-650 and AP-7131), one radio can be dedicated to network access and mesh and the other can act as a sensor that monitors the airwaves for intrusions and rogue devices 24 hours a day, versus the commonly used time-slicing technique that monitors for mere minutes per day. Additionally, Brocade's security monitoring is not band-locked like all others so a single radio can monitor both 2.4 and 5.0 GHz frequencies so you'll get twice the security coverage of any other wireless intrusion protection product.

With Brocade's RFS6000 and RFS4000 WLAN controllers and the AP-7131 access point, you can directly add 3G backhaul or access to a Brocade wireless broadband backhaul (with speeds up to 300 Mbps) so the WLAN always have greater network connectivity.

The Brocade RFS4000, RFS6000 and RFS7000 WLAN controllers also come equipped with SMART RF technology, which automatically assigns channels and adjusts power to the radios on each AP, based on unexpected RF interference, changes in usage patterns, or failure of neighboring APs, in addition to unforeseen coverage holes that degrade data rates. This mitigates possible RF interference issues such as attenuation, fade and jitter that hampers or destroys call quality. SMART RF ensures superior QoS across the WLAN. Brocade's RF management software also allows network administrators to troubleshoot problems in remote offices, diagnosing the problem in order to make it easier to solve it from afar.

The Brocade SMART RF can work on a single WLAN controller or across a cluster of WLAN controllers for scalability, ease of management and reliability. Brocade offers a cost-effective licensing plan; there is no license fee for fail-over ports so the cost of redundancy is far less with Brocade. This is especially important for operations that must have a reliable WLAN but need to be frugal with expenditures.

Brocade also makes it easy to stay up to date with the latest wireless technologies and prepare for the future. Brocade WLAN controllers are designed from the ground up to support 802.11a/b/g/n Wi-Fi networks, Radio Frequency Identification (RFID) technology, and real-time location technologies.

Brocade's unique clustering technology allows WLAN controllers to be configured in a single cluster and distributed across the enterprise. The WLAN controllers have the intelligence to operate as a single virtual operation and load balance the AP load across the cluster. This also enables high availability as the load for any WLAN controller failure will be immediately assumed by the cluster. Brocade's zero-port licensing means users don't have to pay for stand-by ports so the cost of maintaining a reliable WLAN controller operation is significantly reduced.

As companies increase their reliance on wireless technologies the reliability value of Brocade networks will be more critical. From planning to managing to adjusting to failover and to anticipating the future, Brocade offers the most reliable WLAN portfolio on the market. Whether a network is concentrated in a campus or distributed globally across theaters, Brocade offers unparalleled multi-level resiliency with the best return on investment.