POINT OF VIEW

There’s More To Delivering a Good Wi-Fi Experience Than Sound RF

Executive Summary

There are endless articles describing how to figure out what’s going wrong with Wi-Fi. These typically focus on radio-frequency (RF) issues, such as interference from other devices. But for enterprise networks, running a good wireless network is about a lot more than just the RF. Several other factors come into play that impact how users view the network and whether they have a good or bad experience. Within the corporate setting, the security of the network, the network capacity (above the wireless layer), as well as the availability and reliability of key networking services need to also be taken into account.

Top Factors That Affect Wi-Fi Networks

There are four main elements that Wi-Fi networks rely on to work consistently and effectively. If any are not working smoothly, user experience and productivity will suffer.

The RF layer

Access point (AP) placement plays a large role in how good the eventual network will function at the RF layer, and a good plan can dramatically limit the amount of time spent after the fact chasing down dead spots and poor roaming areas. But a plan can’t account for everything. There’s also the issue of RF interference. Depending on the location, there can be necessary business equipment, Internet-of-Things (IoT) devices, or telephony systems that are using or emitting RF in the same bands that Wi-Fi operates. Sometimes this can be avoided, but in other cases it can only be mitigated by power adjustments or placement of additional APs.

Security of the network

Most employees are not going to call IT to complain about the security level of the network, but having a solid and reliable Wi-Fi network does depend on effective security. In addition to avoiding downtime caused by a breach, limiting access to only those devices that are authorized to use the network conserves bandwidth. It can be challenging to ensure all appropriate devices—and only those devices—get service when there are headless IoT devices within the network.

Network attack tools often cause overall network performance impacts, so having a well-secured network will improve overall performance both on the wireless and the wired corporate network that sits behind it.

Upstream networking

Most employees connect to the network via Wi-Fi, and think of the network as simply a "Wi-Fi network." Behind that, however, sits a switching network along with wide-area network (WAN) links (particularly at branch locations). Capacity constraints on the local-area network (LAN) and/or WAN can occur if links and equipment are not sized to support the amount of business traffic that occurs during the day. These bottlenecks show up to the user as a slow connection and deliver poor performance. While the issue may not be Wi-Fi, the user will perceive it as such and will likely complain that the wireless networking isn't working well or is too slow.

Uptime of key services (DHCP, DNS)

A complaint often heard in the IT space is how often IT tickets come in that the network is down when the network is doing just fine, but key network services are in fact down.[1] Most often the network services that impact users are Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and authentication. If any of these are not working, then the user believes the Wi-Fi isn't working. It's important to ensure that these key services are running and available to have a productive wireless network.

Conclusion

Enterprises today require a fast Wi-Fi network to enable productivity. Employees cannot get their work done if they are experiencing network slowdowns or outages. Perception of a good or bad network comes down to the experience of the end-user. In the case of business Wi-Fi users, there are factors beyond the RF layer that can cause performance issues. To ensure a "good" Wi-Fi network, elements from the RF, to security, wired network design, and key networking services all need to be taken into account.

[1] Jorge Diaz, "It's Not The WiFi, It's DHCP!" JDTech, August 21, 2021.

September 29, 2021 11:14 PM
1226605-0-0-EN