

The Great Divide

It's time to think differently about access and data center networks!

By Johna Till Johnson, President and Senior Founding Partner;
and Andreas M. Antonopoulos, SVP and Founding Partner,
Nemertes Research

Executive Summary

Although LANs have been around for over 30 years, they haven't stopped evolving. In particular, as data centers have consolidated and branch offices multiplied, the divergent user demands for data center and branch-office (access) networks are driving the need for IT professionals to design, build, and manage each network along fundamentally divergent principles.

Data center networks, which interconnect virtualized server farms and deliver applications to remote users, require massive scalability and performance. Access networks, which seamlessly link wired and wireless users, require a common set of management, configuration, and security policies to support an increasingly dynamic and mobile user population. And a key characteristic of these evolving access networks is the increased preponderance of wireless—a disruptive technology that's changing how organizations think about, and use, networking.

The Issue: The Changing Access Network

A few years back, servers and users shared the same campus network, had similar requirements, and therefore relied on the same networking technologies. These days, servers are increasingly virtualized and consolidated in data centers, which require high-capacity, highly-reliable switching. Users, in contrast, are distributed out across branches and administrative offices—and they require easy access and seamless, transparent security.

In other words, yesterday's one-size-fits all campus LAN has bifurcated into two LANs: a high-performance intra-data-center network, and a flexible, easy-to-manage network within branch and administrative offices that provides access to the core computing facilities. (Please see Figure 1: The Emerging Access Network).

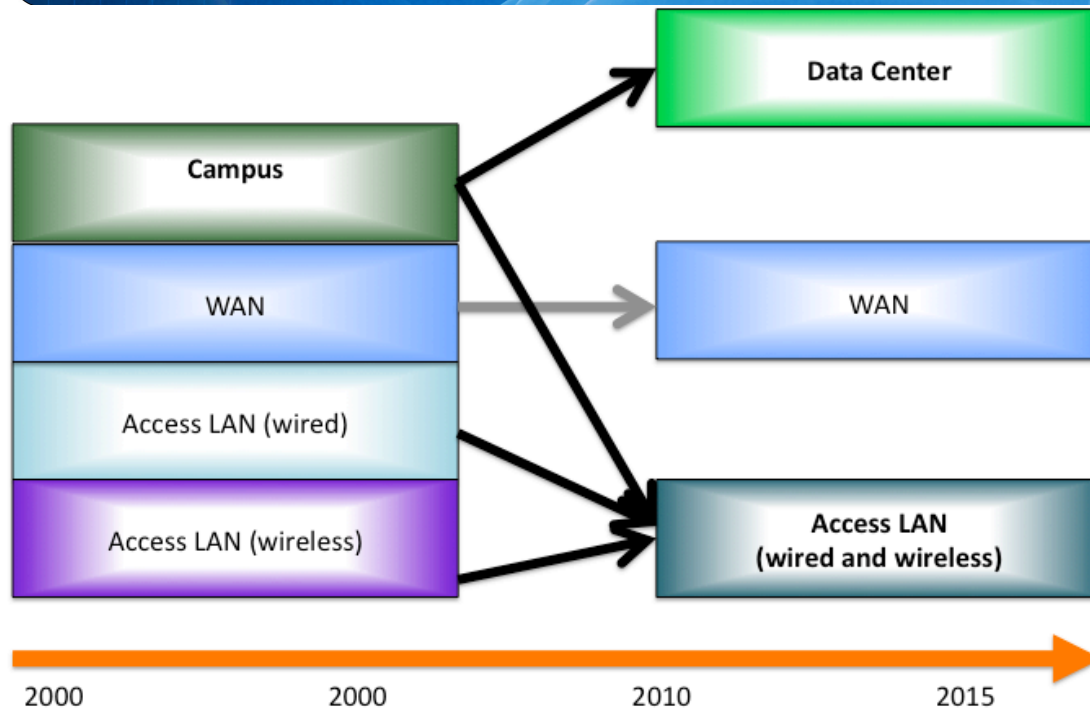


Figure 1: The Emerging Access Network

And that access network today increasingly consists of a mix of wireless and wired LANs—with the wired component becoming increasingly important. The challenge for IT professionals, then, is how best to implement, manage, and secure these access networks—regardless of physical medium.

Trends and Business Drivers: The Virtual Workplace

If three words could describe today’s workplace, they would be *dynamic*, *mobile*, and *virtualized*. More than ever before, employees are accustomed to “anytime, anywhere” computing—and they’re relying on a range of devices and services from smartphones and tablets to VOIP and virtualized desktops.

That means wireless is increasingly important as a networking technology. Wireless deployment is virtually universal, with 97% of participants in Nemertes’ most recent benchmark deploying wireless LANs (WLANs) in 2010. A full 11% of organizations say that wireless is the only form of network connectivity for some of their users. As the IT manager for a large university says, “Our incoming freshmen don’t know, and don’t want to know, what an Ethernet cable is.”

And laptops aren’t the only mobile devices. By next year, over 70% of organizations will have deployed a range of mobile devices, including not only BlackBerrys, iPhones, Android and Windows 7 mobile phones, but also tablets (iPads, Playbooks, Galaxys, and the like). (See Figure 2: The Mobile Device Explosion).

Moreover, it's not just that devices are increasingly wireless—there's an explosion in the number of them. Before 2003, the ratio of devices to people was below 1:1 (more people than devices). That ratio has flipped: These days, many organizations report device-to-person ratios of 3:1, 5:1, or even higher.

This is for two main reasons. First is the obvious one: People are carrying more than one mobile-enabled device. Your typical office worker might carry a smartphone (or two) and a tablet (or two) in addition to his or her laptop. And this trend is accelerating with the influx of under-30 workers, who are conditioned almost from birth to be multiply-connected, carrying smart phones, tablets, laptops, and other devices.

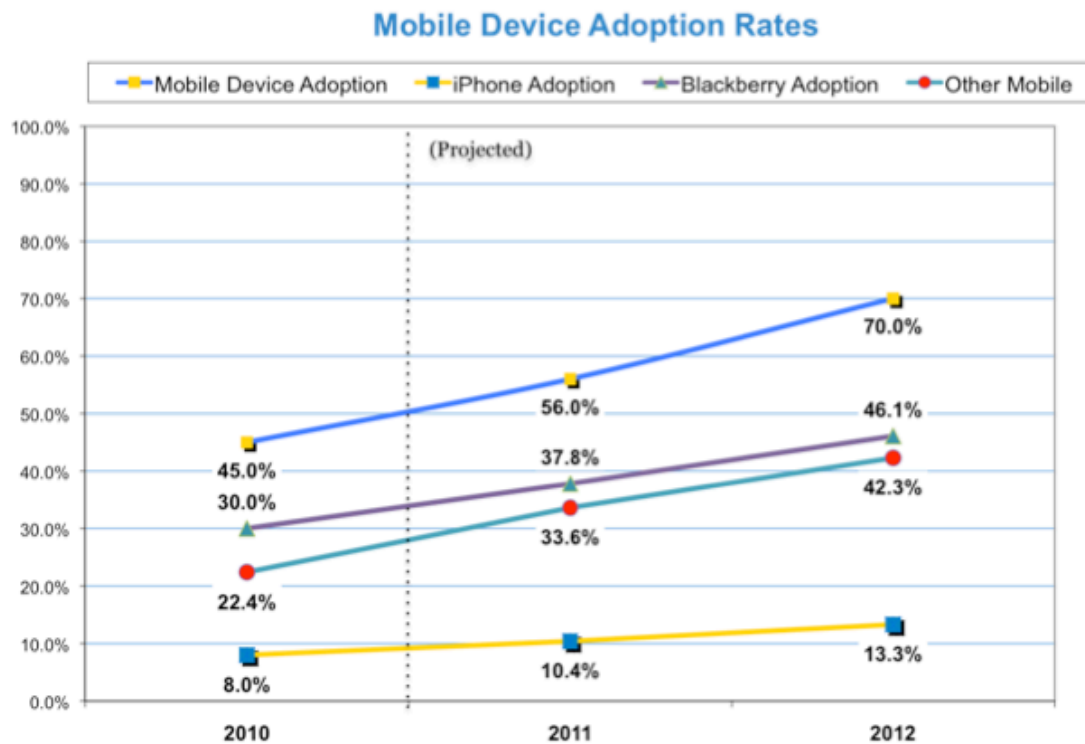


Figure 2: The Mobile Device Explosion

The second reason is a growth in non-human wireless devices. Many organizations are building out sophisticated machine-to-machine networks, in which wireless devices include including security, monitoring, and control networks. For example, many companies are implementing wireless power-monitoring sensors. These devices need the same level of integrated management, control, and security that (human) users do.

The bottom line? Users and applications have become increasingly dynamic—and infrastructure needs to follow suit.

Access vs. Core: Requirements

As noted earlier, the notion of a “one-size-fits-all” campus LAN is now obsolete. With wildly different requirements for the data center and branch offices, IT organizations are increasingly deploying two separate and very distinct types of LANS: Data center networks and access networks. And even though they’re both LANs, these networks are different in almost every respect, from the most critical characteristics they require to the types of workloads they support. (See Figure 3: Diverging Access and Data Center Characteristics).

Specifically:

- Critical characteristics. Although characteristics like performance, scalability, consistent management and ease of use are important for both types of LANS, the priorities (and definitions) are different for each. Specifically, data center LANs need to scale to the transport of terabit/s traffic, with nanosecond latencies; access LANs need centralized management, policy, and provisioning for a high density of (relatively) low-bandwidth users.
- Convergence. The driving trend within data centers is the convergence of Ethernet and Fibre Channel into a common infrastructure. Within access networks, it’s the convergence of wireless and wireline.
- Device Characteristics. As noted, data center LANs interconnect hardware such as servers and storage subsystems. Access LANs interconnect users (and connect those users to data center resources).
- Access control. When it comes to protecting resources, access control in the data center focuses on ensuring that users have access to the right suite of applications. In the access network, the challenge is about ensuring that the right users are permitted on the network.
- Physical media. The predominant physical media in the data center are 10 Gbit/s (and in future, 100 Gbit/s) Ethernet and Fibre Channel. In the access network, they’re WiFi (increasingly, 802.11n) and wired Ethernet.
- Density and dynamism. Both data center and access LANs need to handle density and dynamic load. The difference, again, is in the definitions. Data center LANs have to support an increased density of virtual workloads, which migrate dynamically across servers. Access LANs, in contrast, have to handle user density and dynamism—particularly in a wireless environment.

Technology Issue	Data Center LAN	Access LAN
Critical Characteristics	Performance, scalability	Consistent manageability, ease of use
Convergence of...	Ethernet and Fibre Channel	Wired and Wireless
Device Characteristics	Fixed (Hardware)	Mobile (Users)
Connecting...	Servers and storage	Users
Access Control	By Application	By User
Physical Medium	10/100 G Ethernet	WiFi and Wired Ethernet
Density of...	Virtual Workloads	People
Dynamism of...	Virtual Workloads	People

Figure 3: Diverging Access and Data Center Characteristics

Wireless Now Sets The Bar

As noted, one of the key characteristics of access networks is that they increasingly combine both wired and wireless technology. Many IT professionals mistakenly think that means making wireless technology “as good as” the wired kind.

That mindset is outdated. The tables have now turned: It’s no longer about making wireless networks as good as wired ones—it’s about bringing wired networks up to speed with wireless ones.

WLANs are a classic example of what noted author Clayton Christensen calls a disruptive technology. Disruptive technologies initially inspire skepticism, because they appear to be pale imitations of established technologies, often because they have poorer performance characteristics. Christensen’s original example was the 5.25-inch floppy disk drive introduced in the early 1980s, which was less reliable than the prevailing 8-inch drives. A more modern example is VOIP.

Over time, disruptive technologies create new markets by offering novel capabilities, a unique form factor, or a price point that’s not available with established technologies, thereby disrupting market dynamics. That’s what happened with VOIP. Initially ridiculed as unreliable and not suited for “real” applications (such as business phone calls), VOIP has become the standard form of communication. Many new office (and residential) buildings don’t even bother wiring rooms with telephone cable these days—the assumption is that voice will be carried over the data infrastructure. In business hotels, guests get unlimited local and national phone calls bundled into the Internet connectivity fee, but have to pay separately (and quite a lot) if they want to use traditional telephony.

In other words, if you want plain old telephone service (POTS), you have to pay more and get less: VOIP has gone from being “not as good as” to “substantially better than”, the technology it’s replaced.

WLANs have followed the same trajectory. Initially, WLANs were perceived as (and were) far less reliable and secure than their wired counterparts. In fact, the first wireless encryption protocol, Wired Equivalent Privacy (WEP) was explicitly designed to make wireless LANs as secure as wired ones.

Most WLAN solutions are now equipped out of the box with features and capabilities like built-in encryption to the distribution layer, zero-configuration deployment, centralized control and policy management, network access control, traffic shaping, and QoS to the distribution layer. Wired LANs can of course be configured to support these capabilities—typically with “overlay” products and technologies—but they’re not inherent in the architecture. (See Figure 4: Comparison of Wireless and Wired LANs).

Feature	WLAN	Wired LAN
Encryption to distribution layer	✓	Overlay
Zero-configuration deployment	✓	✓
Centralized control	✓	✓
Centralized policy management	✓	✓
Network access control	✓	Overlay
Traffic shaping & prioritization	✓	✓
QoS services to distribution layer	✓	Overlay

Figure 4: Comparison of Wireless and Wired LANs

WLANs incorporate these characteristics either as part of the standards, or as nonstandard but widespread implementations. Wired LANs support these characteristics via overlay technology. Specifically, WLANs provide encryption to the distribution layer via the 802.11i specification (part of WPA2, required for WiFi certification). Zero-configuration deployment and centralized policy management are implemented by most major wireless vendors. Network access control results from conformance with 802.1X, which is also part of WPA2). Centralized control results from the access-point/controller-based architecture of wireless networks, and traffic shaping, prioritization, and QoS are defined by the wireless multimedia (WMM) specification 802.11e, which is a required part of 802.11n.

Wireless Business Benefits and Use Cases

Clearly, then, wireless plays an increasingly important role in the evolving access network—so companies should consider taking an integrated approach to access LAN management. Such an approach offers more than just engineering elegance (however satisfying that might be!). It also offers concrete benefits to companies that deploy it, specifically:

- **Lower cost of operations.** By eliminating redundant management, an integrated approach reduces the staff sizes needed to configure, manage, and maintain the access network.
- **Increased security.** Implementing encryption and access control end-to-end across wired as well as wireless networks minimizes risks. Consistent policy and management increases security by making sure the same standards can be enforced for a user no matter how they try to get in, and by making sure that standards are consistently deployed (eg users can't count on finding a switch or access point somewhere that hasn't yet been updated to block them out).
- **Rapid deployment.** Requiring minimal to no configuration enables sites to get up and running quickly.
- **Seamless transition between wired and wireless.** As noted earlier, a majority of workers require both wireless and wired access. An integrated approach means that shifting between the two is virtually transparent: users gain the mobility they need from wireless, and plug into the wired LAN when it's available.

Campus Zero-Configuration Deployment

A system administrator at a college campus typically needs to deploy a mix of wired and wireless networks: Hotspots in common areas (dorm lounges, classrooms) and wired connectivity—including dozens of switches—to individual dorm rooms and suites, offices, and laboratories. With centralized configuration management, the network managers can roll out the entire campus infrastructure, with both wireless access points and wired access switches autoconfiguring instantly. That reduces the cost of deployment and ensures consistent policies regardless of medium.

Mobile Knowledge Workers

People think of knowledge workers as either “at their desks” (ie presumably connected via wired networks) or “mobile” (outside the office on a wireless network). The reality is that even during the course of an ordinary workday at the office, a knowledge worker typically travels between offices and into and out of conference rooms. He or she may bring a laptop, smartphone, or (increasingly) a tablet device—and expects to receive identical access to applications regardless of how he or she is connected.

Hospital Dual-Use

Physicians often capture data at the patient's bedside using a mobile tablet or other device. When they return to their desks, they may use that information to complete forms, issue prescriptions, or perform diagnoses. The information needs to be stored, protected, and managed identically whether it's travelling over a wired or wireless network—meaning encryption policies should be identical. And if a physician requires access to specific applications, access policies should be identical regardless of the network medium.

Conclusions and Recommendations

Yesterday's one-size-fits all campus networks have bifurcated into specialized access and data center networks. IT managers need to rethink how they purchase and implement access networks. Instead of buying, configuring, and managing separate wireless and wired LANs, they should seek to implement integrated wired/wireless access networks that support seamless security and management policies. Such an approach reduces costs, improves responsiveness, and above all keeps the infrastructure aligned with the needs of today's dynamic, mobile, and virtualized workers.

About Nemertes Research: Nemertes Research is a research-advisory firm that specializes in analyzing and quantifying the business value of emerging technologies. You can learn more about Nemertes Research at our Website, www.nemertes.com, or contact us directly at research@nemertes.com.