Choosing enterprise wireless LAN equipment

Every enterprise has its own unique blend of wireless applications, users and coverage areas. Learn how to map your needs to the right WLAN equipment for the job.

BY LISA PHIFER

IT DECISIONS

SearchNetworking.com

Choosing
ENTERPRISE WIRELESS LAN
equipment

BY LISA PHIFER

NOW THAT 802.11N has solidified and a new product generation has emerged, the time is right for enterprises to pursue broader WLAN deployment. Ideally, those purchases should be driven by technical requirements that map business needs onto product capabilities.

At a 30,000-foot level, 802.11n WLAN products may seem strikingly similar. After all, most adhere to IEEE standards and Wi-Fi Alliance profiles, implementing features widely expected by today's enterprise. But scratch beneath that spec-sheet surface and you will find a dizzying array of differences in architecture, design, configuration, maintenance and cost. For example:

■ Some 802.11n products are optimized for administrative simplicity, cutting total cost of operation for businesses short on IT staff and expertise. Other products maximize flexibility, so that the same access points (APs) can be used to support a diverse set of applications and environments. Finding both in a single product is rare; the right fit for your business may lie at either end of this spectrum.

■ Many companies deploy 802.11n to support demanding applications like video streaming and voice. But simply adding more of the same AP usually does not create a satisfactory environment for multimedia. 802.11n WLANs must be carefully designed to deliver service levels without undesirable side-effects. 802.11n

behaves differently from 802.11abg; good choices are less intuitive.

■ All 802.11n APs use multiple-input multiple-output (MIMO) antennas to improve throughput, range and reliability versus 802.11abg. However, some 802.11n APs deliver half as much throughput as others. Speeds maintained over distance also vary widely. These characteristics can seriously affect your cost of deployment and operation.

■ 802.11n price wars have begun, but don't be fooled by apparent bargains. An 802.11n AP that cannot simultaneously support old and new users or that cannot push new users toward less crowded spectrum will quickly grow obsolete. Furthermore, inexpensive 802.11n gear that cannot scale to higher densities or requires too much hand-holding will end up costing far more in the long run.

ESTABLISHING YOUR OWN REQUIREMENTS
Sorting out the differentiators between enterprise WLAN products can be tough. But a proven method is to start by defining business needs. Every enterprise has its own unique blend of wireless applications, users and coverage areas. Getting a handle on where you will need wireless coverage and for what purpose is absolutely essential.

Given that context, the next step is to map those business needs onto technical requirements. To help you complete that step, we have compiled a list of common enterprise WLAN requirements. Consider the following questions when drafting your own WLAN RFP and selecting products to fulfill them.

ARCHITECTURE
Enterprises deploy 802.11 for many reasons; identifying how each new WLAN is expected to fit into your network is critical.

■ **Physical:** Do you need wireless indoors, outdoors or both? Will APs be used to provide network access and/or backhaul to distribution layer APs or switches? Look for APs that can support access and backhaul simultaneously when deploying wireless in hard-to-cable areas. Specify AP and controller uplink number, type, data rate, and capacity requirements. For 802.11n APs, Gigabit Ethernet uplinks may be needed to carry up to ~600 Mbps per dual-radio AP.

■ **Radio frequency (RF):** Do you prefer micro-cell (multi-channel) or virtual-cell (single-channel) coverage? Most WLAN products use micro-cells with frequency planning to avoid co-channel interference. A few products tune all APs to the same channel to create large virtual cells.

The latter simplifies channel planning and reduces roaming latency but also shortens your list of possible vendors.

■ **Network:** Do you require wireless at one site or multiple sites? For multi-site WLANs, do remote APs need to operate autonomously when headquarters connectivity is lost? Will all wireless traffic transit a central point (such as a PBX or database), or must remote users communicate directly with others at their location? Beware of products that require central forwarding, filtering or authentication; choose a hybrid product if both central control and remote autonomy are needed.

■ **Management:** Do you want single-point firmware or configuration management for your entire WLAN? What (if any) management functions will remote sites need to perform (such as custom rules or user adds and deletes)? Some vendors connect APs to WLAN controllers; others connect APs directly to enterprise switches. But products in both camps can offer scalable, centralized management.

STANDARDS
Selecting products that implement standards and have passed certification tests will ensure baseline functionality and compatibility between access points and clients.

■ **Radio:** Today, enterprises should seek Wi-Fi Certified N products to protect investment while ensuring 802.11abg backwards compatibility. Certified N products support data rates up to 150 Mbps. If you need more throughput or capacity per radio, specify Certified Dual-N (300 Mbps) or Multi-N (450 Mbps).

■ **Band:** Most enterprises buy dual-band access points to support older clients at 2.4 GHz and 802.11n clients and backhaul at 5 GHz. Require band-steering to automatically shift new clients to 5 GHz. Consider requiring each radio to concurrently support both bands. Ask whether 2.4 GHz radios can be disabled or upgraded to 5 GHz as needs change. Finally, require 802.11d and 802.11h if your WLAN must use non-U.S. channels or dynamic frequency selection (AP-automated channel change whenever interference is detected).

■ **802.11n options:** All Certified N products support core capabilities, but there are still many 802.11n options.
  If you must maximize throughput or capacity, require Short Guard Interval, A-MPDU (Aggregated MAC Protocol Data Unit), and 40 MHz-wide channels. If reliability is a key concern, look for extra spatial streams (MIMO antennas), space-time block coding, and perhaps transmit beamforming. If your 5 GHz airspace is

already congested, look for UNII-2e channel support.

■ **Security:** All Certified N products include WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) encryption. If you absolutely must support legacy clients, ask for WPA/TKIP (Wi-Fi Protected Access/ Temporal Key Integrity Protocol) as well, although those users will be limited to 54 Mbps. Require WPA2-

Good advance planning and design can make all the difference between disappointment and a successful wireless network deployment.

Enterprise (802.1X RADIUS user authentication) with EAP (Extensible Authentication Protocol) types that reflect your workforce's credentials (e.g., EAP-TLS for certificates/smart-cards, PEAP for passwords). To control access by embedded devices (e.g., VoIP handsets, scanners) and guests, use WPA2-Personal for configurable group passphrase authentication.

■ **Quality of service (QoS):** Unless you are deploying a best-effort, data-only WLAN, require 802.11e WMM (Wi-Fi Multimedia) for prioritizing airtime used by voice, video, data and background applications. Consider whether you need WMM Power Save to improve battery life for always-on mobile devices. Ask how traffic is prioritized and shaped inside APs and controllers and whether slow clients can be prevented from dominating airtime. Finally, specify QoS requirements for AP and controller uplinks like 802.1p, DSCP (Differentiated Services Code Point) and multicast.

■ **Power:** Enumerate your company's AC/DC requirements for Ethernet LAN devices, and when using 802.3af Power over Ethernet (PoE), specify a per-port power budget. Require vendors to detail AP features that must be disabled to fit your PoE budget or to propose solutions for operating at full capacity.

WLAN PLANNING AND DESIGN
When it comes to WLAN deployment, advance planning can make all the difference between successful rollout and disappointment.

■ **Application and user needs:** Define your wireless application, user and coverage requirements for each site so that vendors can propose access points that are appropriately

sized and featured. For example, you may have 50 voice users with minimum signal strength of 25 dB over a 30,000-square-foot area, or 100 people requiring 50 Mbps video streams at a minimum data rate of 100 Mbps over 20,000 square feet.

■ **Site survey:** Require each vendor to supply or recommend site survey tools or services for pre-deployment, in-situ RF measurement and post-deployment verification. The extent to which vendors encourage site surveys varies, but since 802.11n depends heavily upon multi-path, which in turn depends upon building layout and materials, beware of any vendor that does not consider your site's RF propagation characteristics when proposing a solution.

■ **Predictive planning:** When planning a large WLAN, ask each vendor to supply or recommend predictive planning tools or services to optimize design and installation costs. WLAN planners use floorplans, building characteristics, and application, user and redundancy needs to generate recommended AP layouts, work orders, and band, channel and power settings. For phased rollouts or upgrades, ask about planner support for "what if" analysis and including existing APs.

■ **Installation:** Ask vendors for detailed installation and set-up instructions, including mounting

brackets, any required manual initialization, and how to generate site-specific work orders. For large WLANs, require features that speed installa-

Beware of any vendor that does not consider your site's RF propagation characteristics.

tion, like AP and controller discovery and self-forming or self-healing backhaul links. For WLANs with many remote sites, ask about plug-and-play secure activation and remote configuration of factory-supplied APs.

WLAN CONFIGURATION
Purchasing Certified N APs is one thing, but make sure that you can also deploy them with desired configurations to meet business needs.

■ **Device administration:** Enterprises require scalable tools that can administer access points in groups, mapped onto topology maps and floorplans. Look for products that can push firmware and configuration updates to many APs at once while flagging errors before they cause outages. Audit tools that detect out-of-date and modified APs are helpful to keep your WLAN in sync.

■ **Radio configuration:** Do you need to control parameters like band, channel number, channel width and transmit power? Or do you prefer controllers or APs that adjust these to avoid interference, fill gaps and balance load? Even with automation, you may still want manual overrides. Look for protection options like the ability to deny 802.11b or operate in greenfield (pure 11n) mode.

■ **Service set identifier (SSID) configuration:** All enterprise APs now support multiple SSIDs per radio, but specify the number of SSIDs that you need and properties that must be configurable per SSID. Common per-SSID needs include VLAN and sub-net; authentication and encryption; default priority; max user throughput; Layers 2 and 3 packet filters; and authorized devices, users and groups.

■ **Security configuration:** Beyond 802.11i (WPA2/WPA), specify business needs for guest or portal authentication, VPN, and network access control (NAC) integration. For per-user access control, require RFC 3580 (802.1X/RADIUS virtual LAN tags). If you need to inspect traffic, require AP firewall features. For voice WLANs, request fast-roaming options like key caching and pre-authentication.

■ **QoS configuration:** Beyond 802.11e (WMM), specify business needs for per user, group and port traffic queues, rate limits, tagging, or SLA enforcement. Consider how QoS is applied at APs, controllers or next-hop APs (for backhaul and mesh links). Beware of architectural constraints that prevent local forwarding. For voice WLANs, ask about call admission control.

■ **High-availability configuration:** Specify any requirements for availability and fail-over, including redundant APs, controllers, uplinks and power. Ask vendors to detail what happens when any component fails. For example, is configuration synchronized with a hot-standby controller, how quickly is an outage detected, and are associations or sessions lost during fail-over?

WLAN MONITORING
After deployment, visibility into who is using your WLAN and how your network is actually performing is paramount.

■ **Event monitoring:** Enterprise WLANs should be required to meet common NOC monitoring needs, including (NTP-synchronized) syslog forwarding, SNMP traps, and perhaps email and SMS (Short Message Service) alerts. Look for configurable local logging to facilitate troubleshooting.

■ **Real-time dashboard:** Consider

staff expectations for real-time WLAN manager or controller dashboards. Do you need client and performance overviews? Must staff view only selected devices or sites? User interfaces and preferences vary greatly, so have staff evaluate each candidate's usability.

■ **Historical reporting:** Identify reporting needs for regulatory compliance, usage tracking and capacity planning. Many enterprises use third-party reporting systems and thus require event storage and export capabilities.

■ **Locationing:** Increasingly, enterprise WLAN products include location-awareness, like plotting clients or rogue APs on a floorplan or supplying their location to applications. If your business needs include location-awareness, specify required accuracy and methods used, such as Received Strength Signal Indicator (RSSI), triangulation or RF tags.

■ **Intrusion detection and prevention:** Most enterprise WLANs can scan for rogue access points. If you wish to do so, specify requirements like scan interval, channels and ability to relay RSSI to wireless intrusion detection/prevention systems (WIPS). Ask prospective vendors for details about WIPS integration—for example, whether APs can be converted to WIPS sensors on demand.

■ **Troubleshooting:** Most enterprises use third-party tools like WLAN and spectrum analyzers for troubleshooting, but WLAN infrastructure should provide basic troubleshooting tools, including real-time client (Layer 2 and Layer 3) status, reachability checks, and a way to disconnect a troubled client and watch it (try to) reassociate. On-AP packet captures can also be helpful. Ask vendors about help desk and trouble-reporting system integration and interfaces that might help your WLAN fit into unified, end-to-end workflows. ■

ABOUT THE AUTHOR:

Lisa Phifer is president and co-owner of Core Competence, a consulting firm focused on business use of emerging network and security technologies. At Core Competence, Lisa draws upon her 27 years of network design, implementation, and testing experience to provide a range of services, from vulnerability assessment and product evaluation to user education and white paper development. She has advised companies large and small regarding use of network technologies and security best practices to manage risk and meet business needs. Lisa teaches and writes extensively about a wide range of technologies, from wireless/mobile security and intrusion prevention to virtual private networking and network access control. She is also a site expert for SearchNetworking.com.

Wireless LAN equipment vendors at a glance

Click on the name of the vendor for additional information.

VENDOR	ACCESS POINTS	CONTROLLERS/ SWITCHES	TRAFFIC MANAGEMENT	WIRELESS INTRUSION PREVENTION
3Com (HP)	●	●	●	●
Aerohive	●		●	●
AirMagnet (a Fluke Networks company)			●	●
AirTight Networks			●	●
AirWave (a division of Aruba Networks)			●	●
Alcatel-Lucent	●	●		●
Aruba Networks	●	●	●	●
BlueSocket	●	●	●	●
Brocade	●	●		
Cisco	●	●	●	●
D-Link	●			
Extreme Networks	●	●	●	●
Extricom	●	●	●	●
HP ProCurve	●	●	●	●
Juniper Networks	●		●	●
Meru Networks	●	●	●	●
Motorola	●	●	●	●
NEC	●	●	●	●
Netgear	●	●		
Nortel (Avaya)	●	●	●	●
Proxim	●		●	
Ruckus Wireless	●	●	●	●
Siemens (Enterasys)	●	●	●	●
SonicWall	●			●
Trapeze Networks (a Belden brand)	●	●		●
Xirrus	●		●	●

CHART COMPILED BY SUSAN FOGARTY

Reliable. Affordable. Simple.

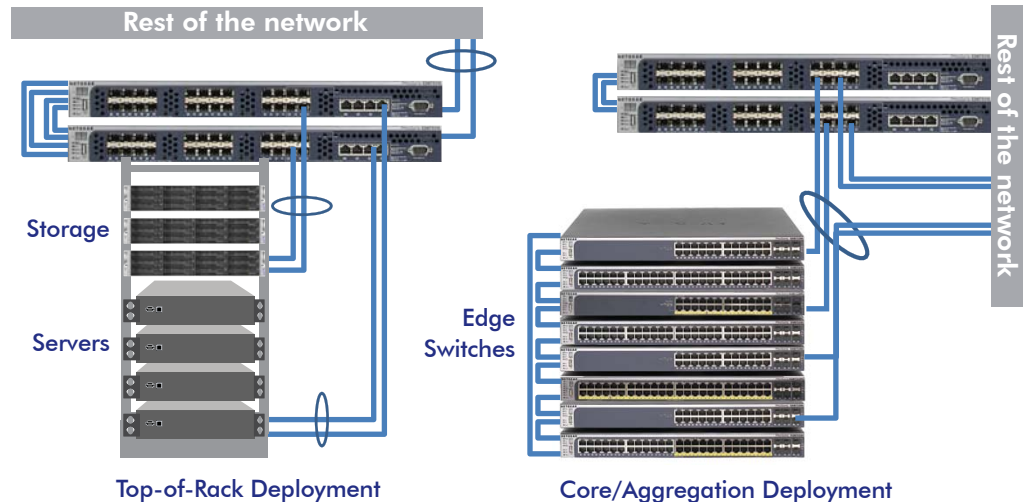## 10GB Ethernet for top-of-rack, server virtualization and core deployments

XSM7224S ProSafe® 24-port 10 Gigabit Stackable L2+ Managed Switch

KEY FEATURES

- Top-of-Rack Switch with 24-port 10 Gigabit Ethernet
- Stacking technology for easy deployment of resilient virtualization
- Distributed LACP allows for active-active server teaming for more throughput
- Versatile SFP+ and RJ45 ports, with 10 Gigabit and 1 Gigabit compatibility on all ports
- Enterprise-class L2+ with VLAN routing
- L3 License scalability for core/aggregation deployments, including IPv6, VRRP, OSPF, and Multicast

WHY 10 GIGABIT?
10 times the performance to meet the needs of Virtualization, and aggregating Gigabit Ethernet edge switches

Rest of the network

Storage

Servers

Top-of-Rack Deployment

Edge Switches

Rest of the network

Core/Aggregation Deployment

Learn more:
- **Speak with a Switching Specialist at 877-703-0385**
- **Visit our Managed Switching product page**

NETGEAR®
Connect with Innovation™

- **5 Steps to Secure the Wireless Network**

- **Building Mobility into Your Network**

- **IP Networking and Its Impact on Video Surveillance**

About NETGEAR:
NETGEAR is a global networking company that makes business class networking, storage and security solutions without cost and complexity of traditional monolithic vendors. Over 18 million businesses worldwide have deployed NETGEAR business solutions, in large part because these solutions have been designed from the ground up specifically for business use. For over a decade, we have delivered more than 800,000 TB of storage, 120M Ethernet ports and 2 million firewalls to businesses worldwide. NETGEAR offers industry-leading warranties, 24x7 technical support in 16 languages and works with 39,000 partners worldwide.