Upgrading to 802.11n

Enterprises can take advantage of broader WLAN deployments enabled by 802.11n's increased speed, throughput and coverage to create greater IT efficiencies. Although wireless LAN products may seem similar, if you scratch the surface, you will find an array of differences in architecture, design, configuration, maintenance and cost. This IT Decision Checklist explains the major differences in 802.11n products and what to look for when evaluating them.

BY LISA PHIFER

IT DECISIONS

INSIDE:

SearchNetworking.com

UPGRADING TO 802.11N

BY LISA PHIFER

WIRELESS LANS ARE now ubiquitous in the enterprise, with 802.11n triggering a new generation of ready-for-prime-time infrastructure products. As a result, enterprises can now pursue broader WLAN deployments that take advantage of 802.11n's greater speed, throughput and coverage to increase workforce mobility and IT efficiency.

Enterprise wireless LAN sales are projected to grow 49% by 2015, fueled by last year's explosion of 802.11n smartphones and other consumer electronic devices. According to Dell'Oro analyst Chris DePuy, "802.11n has helped to propel this market and is continuing to evolve, providing higher bandwidth connections and the ability to seamlessly roam from the cellular network to the WLAN."

But despite their standard foundation, today's wireless LAN products still harbor significant differences in architecture, configuration, operation, performance, security and cost. This IT Decision Checklist examines the capabilities and features offered by enterprise-class WLAN products, highlighting factors to consider when evaluating them. We'll identify important questions that enterprise customers should ask prospective vendors and provide a list of vendors that offer WLAN products.

THE CHANGING FACE OF ENTERPRISE WLANS

Before shopping for network infrastructure, it's essential to assess business needs. This is especially true for wireless equipment, which

has morphed from being an occasional convenience to the primary access method, elevating expectations for reliability, availability and integration with wired network products and IT processes.

Along the way, wireless populations and applications grew more diverse. In a March 2011 survey, Aberdeen Group found a broader and deeper-than-expected range of smart devices using business wireless LANs, led by smartphones, tablets and wireless video conferencing, surveillance and asset tracking systems. According to a July 2011 In-Stat report, consumer electronics now represent the majority of new Wi-Fi certified products, including not just smartphones and tablets, but also e-readers, cameras, TVs, media players, mobile hotspots, network attached storage, printers, projectors and displays.

Today's devices are not just physically diverse—they tend to use WLANs differently. Their radio implementations and behaviors are more varied. Their users are more mobile than nomadic. And devices are likely to run multiple streaming applications, reducing tolerance for coverage gaps, bottlenecks and over-subscription. Where laptops were bursty, new mobile Wi-Fi devices are relentlessly thirsty, constantly gulping bandwidth.

This evolution must be considered when upgrading to 802.11n. Faster data rates, wider channels and more efficient spectrum use can increase capacity, but wireless LANs must keep pace with escalating demand. Attention must be paid to product scalability and adaptability—desirable characteristics that are notoriously difficult to quantify.

THE IMPORTANCE OF WLAN ARCHITECTURE

Another critical step in selecting wireless LAN products is determining how each fits into your existing network. To do so, it can help to divvy functions into "planes" that can be performed in different places throughout a WLAN and may even be implemented by different products in each vendor's lineup.

- The **data plane** transmits, receives and relays traffic, using wireless access points (APs) distributed throughout coverage areas. Most wireless LAN vendors sell several AP models, which are differentiated by interfaces, capacity and environment (indoor/outdoor). Except when it is required to meet business needs—such as backhauling traffic to a wide area network uplink—avoid performing wireless data plane functions in upstream locations to minimize latency and bottlenecks.

- The **control plane** makes real-time decisions governing wireless LAN operation, routing, security and quality of service. Functions include radio

THE CHANGING FACE OF ENTERPRISE WLANS

THE IMPORTANCE OF WLAN ARCHITECTURE

COMPARING WLAN CONTROL CAPABILITIES

BEYOND CAPABILITIES AND FEATURES

QUESTIONS TO ASK YOUR VENDORS

PROVIDERS AT A GLANCE

resource management, authentication, firewalling and prioritization. Products differ greatly in where they apply these functions. For example, users may be authenticated by autonomous APs, by a central WLAN controller or by either, depending upon reachability. Beware of centralized and remote control plane de-pendencies—especially those affecting service availability or total cost.

- The **management plane** supports administrative tasks such as provisioning, firmware update, fault surveillance and reporting. For scalability, enterprise wireless LAN products centralize most of these functions. But implementations range from controller-embedded to NOC appliances to "in the cloud" services; big differences exist in features and pricing. For example, guest management may be included, or an à la carte model may require an add-on license. Seek out features that enhance scalability, reduce total cost of operation and enable holistic (wireless + wired) management.

Don't be misled by product labels like "controller" or "cloud." Focus on whether a vendor can deliver the *functions* required by each site throughout your wireless LAN while assessing the consequences of each architecture on performance, availability and cost.

DRILLING INTO DATA

Small remote offices, larger branch offices and headquarter campuses often have different needs that drive product selection, especially at the data plane. 802.11n provides the essential foundation; steer clear of products that are not Wi-Fi Certified N APs. But Certified N APs can still vary quite a bit—even models within the same product line. **TABLE 1** on page 5 summarizes data plane capabilities and feature differences to consider.

Some of these capabilities are visible in certificates issued by the Wi-Fi Alliance; to search for Wi-Fi Certified N products, visit www.wi-fi.org. However, determining AP fit for each site requires drilling beyond spec sheets; on-site pilots are highly recommended.

COMPARING WLAN CONTROL CAPABILITIES

Control functions are often—but not always—performed by a wireless LAN controller. Controllers were created to simplify APs by consolidating control and management, making WLANs more scalable. But faster data rates, more demanding applications and geographic sprawl are pushing control functions back into 802.11n APs. Today, many vendors sell centrally-managed APs that can operate either with or without a controller.

Don't be misled by this pendulum

(Continued on page 6)

THE CHANGING FACE OF ENTERPRISE WLANS

THE IMPORTANCE OF WLAN ARCHITECTURE

COMPARING WLAN CONTROL CAPABILITIES

BEYOND CAPABILITIES AND FEATURES

QUESTIONS TO ASK YOUR VENDORS

PROVIDERS AT A GLANCE

DATA PLANE CAPABILITIES AND FEATURES

Multiple-Input Multiple-Output (MIMO) Antennas1	Certified N APs have multiple transmit and receive antennas, but their number and design greatly impact coverage. Ask vendors to back claims by demonstrating results at your site(s).
Spatial Streams	Certified N AP radios transmit/receive data over NxM spatial streams, ranging from 2x2 to 4x4. Entry-level APs have fewer antennas and streams, reducing their cost, capacity and range.
Dual-Band Support	Certified N APs may use 2.4 or 5 GHz channels or both. Match band support to your device population, look for band-steering to nudge new devices onto 5 GHz, and beware that supported 5 GHz channel sets vary.
Number of Radios	Entry level APs may have one single-band or dual-band selectable radio, but many enterprise APs have two radios to support both bands concurrently. More radios add capacity and flexibility; ask if they can be used for access, backhaul or monitoring.
40 MHz Channel Bonding	Certified N APs may optionally combine adjacent 20 MHz channels into double-capacity 40 MHz channels. Look for bonding at 5 GHz in APs to be deployed to support high-throughput applications.
Short Guard Interval (SGI)	APs that support the SGI option can cut silence between transmissions in half, increasing max data rate approximately 10%.
Space Time Block Coding (STBC)	APs that support STBC can transmit redundantly over available spatial streams to improve reliability and rate-over-range. This is useful for APs deployed in challenging RF venues.
Frame Aggregation	APs that support TX A-MPDU can bundle multiple frames into each transmission. This is useful in APs deployed to support streaming applications.
Transmit Beam-Forming (TXBF)	APs that implement TXBF can use recent experience to optimize transmissions to each device. Implementations vary significantly; ask vendors to quantify expected improvements in each direction for each device type (11a/g/n).
Wi-Fi Multimedia (WMM) QoS	Certified N APs support WMM to prioritize airtime used by voice, video, data and background applications. Ask vendors about WMM Power Save, which extends battery life for mobile devices, and proprietary QoS features like airtime fairness.
Wi-Fi Protected Access (WPA2) Security	Certified N APs support WPA2 for data confidentiality and integrity. But not all support both passphrase and 802.1X authentication; EAP types also vary. Ask vendors to detail their support for your security policies and user/device credentials.
Network Connectivity	Enterprise APs usually have at least one 10/100 uplink for wired Ethernet. Popular options include GbE, dual Ethernet and integrated cellular uplinks.
Power over Ethernet	Many enterprise APs support at least 802.3af PoE; higher-end APs may require 802.3at PoE+ to operate at full capacity. Beware of proprietary PoE needs or AP features that require a PoE+ capable switch or power injector.
Wireless Mesh Networking	Enterprise AP support for wireless backhaul has grown, but radio use restrictions, mesh topologies and discovery/routing capabilities vary. When selecting APs to form an indoor or outdoor wireless mesh, consider capacity, latency and stability.

THE CHANGING FACE OF ENTERPRISE WLANS

THE IMPORTANCE OF WLAN ARCHITECTURE

COMPARING WLAN CONTROL CAPABILITIES

BEYOND CAPABILITIES AND FEATURES

QUESTIONS TO ASK YOUR VENDORS

PROVIDERS AT A GLANCE

(Continued from page 4)
swing, however. Control functions vary considerably among products; some are even lost when APs switch from controlled to autonomous operation. Don't make assumptions: Ask vendors to detail component dependencies, what happens when any component fails, and redundancy options to ensure availability.

For each area summarized below, assess reliability and scalability impacts for functions performed autonomously on APs, and availability and performance impacts of those performed centrally on controllers. Also ask vendors to specify features that require à la carte licenses or upscale hardware for apples-to-apples cost comparison.

PERFORMANCE, RELIABILITY AND SCALABILITY

Radio Resource Management	**Enterprise WLAN products can auto-assign channels and may also adjust transmit power. Most choose non-overlapping channels to create micro cells, but at least two products create one big virtual cell instead. Ask vendors how they manage RF settings to minimize interference and coverage gaps while ensuring stability for real-time applications. Consider AP-based spectrum analysis in offices plagued by transient RF interference.**
Authentication Services	**Enterprise WLAN products can assist in making authentication decisions. Common capabilities include MAC white/blacklisting, captive portal login and embedded RADIUS for 802.1X. Additional features may include guest management, device fingerprinting, PSK generation and NAC integration.**
Roaming Support	**Enterprise WLAN products often cache keys to speed Layer 2 roaming; some also support Layer 3 roaming across subnets by tunneling data between APs and/or controllers. Ask vendors what capabilities they offer to facilitate roaming, including any that might assist with WLAN / cellular roaming.**
Security Enforcement	**Enterprise WLAN products can usually firewall and tag intra/inter-LAN traffic to enforce security policies. Related features include dynamic VLAN (re)assignment, role-based policies, rogue detection and wired/wireless integration. You may choose to tunnel traffic to a central firewall, but beware of products that require it.**
QoS Enforcement	**Enterprise WLAN products can often enforce policies related to QoS prioritization and admission, 802.1p/DSCP mapping, traffic shaping, rate limits and load balancing. Ask about support for local forwarding and application-aware QoS optimizations such as voice call admission and video multicast conversion.**
Network Services	**Some WLAN products include on-board network services such as DNS, DHCP and VPN to create "branch in a box" solutions. Others offer hooks like DHCP relay to enable integration with existing services. Choose products that fit each venue.**

In deployments with dedicated controllers, also consider connectivity, capacity and redundancy requirements for that device. For example, controllers that aggregate traffic from 802.11n APs usually have Gigabit Ethernet (GbE), but the number of copper or fiber ports will vary along with backplane capacity and the number of APs—controlled or autonomous—that each model can support.

MANAGING YOUR WLAN

Most enterprise wireless LAN vendors sell products to manage their own controllers and APs. Smaller WLANs may do without a dedicated manager, but large distributed WLANs cannot be managed efficiently without centralized administration and monitoring. Usually, WLAN managers are delivered as on-premises appliances, but vendors have started to offer multi-tenant pay-as-you-go cloud management services.

Both approaches can meet enterprise wireless LAN management requirements. Management functions rarely require real-time execution and are usually carried out through consoles remote from the devices being managed anyway. Wireless LAN managers must communicate with those devices—often reaching APs through controllers—but can easily tolerate brief outages without impacting network service delivery. Ultimately, this choice boils down to ownership/control versus simplicity/ cost.

In both cases, enterprises should demand the same wireless LAN management capabilities and features summarized in the following table. Expect to pay more for advanced management options. However, good management tools can leverage automation and visibility to cut total cost of operation, preempt outages and reduce time-to-repair.

GOOD MANAGEMENT TOOLS CAN LEVERAGE AUTOMATION AND VISIBILITY TO CUT TCO, PREEMPT OUTAGES AND REDUCE TIME-TO-REPAIR.

BEYOND CAPABILITIES AND FEATURES

A thorough examination of available capabilities and features can determine how well a vendor's wireless LAN product line meets your functional requirements, as well as identifying the products and models to best fit each venue.

At the end of the day, however, many purchasing decisions are strongly influenced by other criteria. For example, in an informal survey

(Continued on page 9)

THE CHANGING FACE OF ENTERPRISE WLANS

THE IMPORTANCE OF WLAN ARCHITECTURE

COMPARING WLAN CONTROL CAPABILITIES

BEYOND CAPABILITIES AND FEATURES

QUESTIONS TO ASK YOUR VENDORS

PROVIDERS AT A GLANCE

WLAN MANAGEMENT CAPABILITIES

WLAN Planning	Before enterprise WLANs can be deployed, AP number and placement must be determined for each venue. Planning tools use floorplans and RF characteristics to predict coverage areas, data rates and signal strength. After deployment, site survey tools measure in-situ results. Ask about free planning tools and services; online planners or site surveys for new customers are increasingly common.
Discovery and Provisioning	Enterprise APs often use discovery protocols to find a controller or manager. Upon joining a WLAN, APs can be auto-provisioned with firmware and settings. Look for batch deployment aids and avoid APs that require hands-on initialization.
Firmware Maintenance	Enterprise APs and controllers must be maintained by applying software and firmware updates when appropriate. Look for update notifications and options to minimize disruption.
Configuration Management	Enterprise APs are commonly configured by pushing centrally-defined settings and updates. Look for templates, version management, auto-retry and verification.
Live Monitoring	Enterprise WLAN managers can display operational status of all APs in near-real-time. Look for customizable dashboards, analysis aids and mobile access.
Historical Reporting	Enterprise WLAN managers collect and log past AP events and admin actions for later use in historical reports. Look for both flexible custom and canned compliance reports.
Fault Surveillance	Enterprise WLAN managers can generate error and threshold alarms to warn operators about impending faults—preferably before service impact. Look for features that focus on major faults, as well as integration with other systems.
Intrusion Detection and Prevention	Enterprise WLAN managers usually report on rogue APs detected by authorized APs using periodic or background scans. But some vendors offer Wireless Intrusion Prevention Systems (WIPS) that do much more, analyzing data from APs or dedicated sensors to alert, diagnose and react to attacks and policy violations. Ask vendors to detail their WIPS approach and threat coverage.
Performance Monitoring	Enterprise WLAN managers can usually present graphs and charts depicting key performance metrics. However, some vendors offer Service Assurance (SA) products that do more, analyzing performance versus SLAs or identifying per-application usage. Look for actionable insights and automated responses that help make a WLAN self-tuning.
Trouble-shooting	Enterprise WLAN managers often present basic troubleshooting tools such as the ability to eyeball a user's status or forcibly disconnect them. Advanced options can include helpdesk integration, end to end (wireless + wired) diagnostic tools and AP-based troubleshooting.
Locationing	WLAN managers have grown more location-aware. Many can plot APs or connected devices on floorplans. Advanced locationing engines may integrate other data sources (RFID) and supply results to applications.

THE CHANGING FACE OF ENTERPRISE WLANS

THE IMPORTANCE OF WLAN ARCHITECTURE

COMPARING WLAN CONTROL CAPABILITIES

BEYOND CAPABILITIES AND FEATURES

QUESTIONS TO ASK YOUR VENDORS

PROVIDERS AT A GLANCE

(Continued from page 7)
conducted by Revolution Wi-Fi, respondents identified product quality and stability, vendor technical expertise, solution scalability, support response time, and availability of product documentation as the most important factors when selecting a wireless LAN vendor.

In short, a feature-rich product line that is buggy, hard to decipher or difficult to support may be passed over in favor of one that meets needs more simply while garnering higher confidence. Take advantage of the product assessment and selection process to

WLAN QUESTIONS TO ASK YOUR VENDOR

- **Does your product offer indoor, outdoor and/or mesh products? Please describe.**
- **What is your product's WLAN architectural model? Explain the function of controllers versus access points.**
- **What wireless standards are supported, and is the product backward-compatible with previous standards?**
- **What is the upgrade path for customers who have older equipment and for future standards development?**
- **How much bandwidth and how many users does each device provide?**
- **What type of security is integrated into the product?**
- **What type of RF management does the product provide?**
- **Do you provide a site survey to predict coverage and identify potential interference and/or security issues?**
- **How is the system managed, patched and updated?**
- **What are the wired network and power requirements for the product?**

—Complied by **Susan Fogerty**, *Editorial Director*

get to know each wireless LAN vendor, but don't limit yourself to hand-holding demos. Run in-situ tests on your own, going through normal support channels and documentation to resolve questions and problems. Every enterprise WLAN product poses some learning curve, but even small pilots can deliver very valuable insight into total cost of ownership. ■

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.

PROVIDERS AT A GLANCE

THE FOLLOWING IS a list of WLAN infrastructure providers. Click on the vendor name for more information.

- Aerohive
- AirTight Networks
- Alcatel-Lucent
- Aruba Networks
- Avaya
- BlueSocket
- Brocade
- Cisco
- D-Link
- Enterasys/Siemens
- Extreme Networks
- Extricom
- HP Networking
- Juniper Networks
- Meraki
- Meru Networks
- Motorola
- NEC
- Netgear
- Proxim
- Ruckus Wireless
- SonicWall
- Xirrus

—Complied by **Susan Fogarty**, *Editorial Director*

NETGEAR®
Connect with Innovation™

- E-Guide: Benchmarking Core Switches: Modeling Techniques for Switch Testing
- 10 Things to Know Before Deploying 10 Gigabit Ethernet
- 5 Steps to Secure the Wireless Network

- HP Mobility Solutions: Unifying wired and wireless access best-in-class architecture, performance, and TCO
- HP intelligent wireless networking solutions
- HP Wireless Portfolio

- Technology Behind the Solution
- Extending Your Enterprise
- The HiveMind Blog

- Xirrus TV
- Xirrus Twitter