APRIL 2011 / VOL. 2 / NO. 2

NETWORK evolution

BUILDING THE INFRASTRUCTURE TO ENABLE THE CHANGING FACE OF IT

TWO COMPANIES, FOUR NETWORKS. WHY CAN'T THERE BE UNIFIED ARCHITECTURE?

PLUS:

IDEA LAB

THREE STRATEGIES FOR UNIFIED WIRELESS MANAGEMENT

WHY BOTHER COMBINING WIRED AND WIRELESS SECURITY?

TechTarget

idealab

Where evolving network concepts come together

Troubleshooting iPad and iPhone Wi-Fi Connection Problems

WHETHER OR NOT they like it, enterprise IT shops are increasingly forced to manage iPhone and iPad users and their plethora of iPhone Wi-Fi connectivity problems. If you're having iPhone or iPad wireless LAN problems, you can follow these iPhone operating system Wi-Fi connection debugging tips.

1. Start by rechecking your physical connections.

2. Next, verify that your iPad or iPhone Wi-Fi adapter is installed and working properly. Tap Settings/Wi-Fi. If Wi-Fi is OFF, tap the slider to set Wi-Fi ON. When Wi-Fi is ON, a Wi-Fi signal strength indicator will appear at the top left corner of your device's home screen.

3. Verify that your wireless router's LAN settings are correct.

4. Verify your client's TCP/IP settings to ensure iPhone Wi-Fi connectivity.

5. Once your iPhone OS client has a valid IP address within your router's LAN IP range, use "ping" to verify network connectivity. This step is different on an iPhone, iPad or iPod because Apple does not include a user-accessible "ping" app. However, you can still verify network connectivity.

6. If your iPhone OS wireless client still cannot connect, get a valid IP address or ping your router, it's time to look for wireless-specific problems. The router and client must use compatible 802.11 standards.

7. If a compatible wireless client and router can "hear" each other but still cannot connect or exchange traffic, look for a security mismatch.

8. Ensure RADIUS is working.

9. If RADIUS is working but the client's access requests are rejected, look for

an 802.1X Extensible Authentication Protocol (EAP) problem.

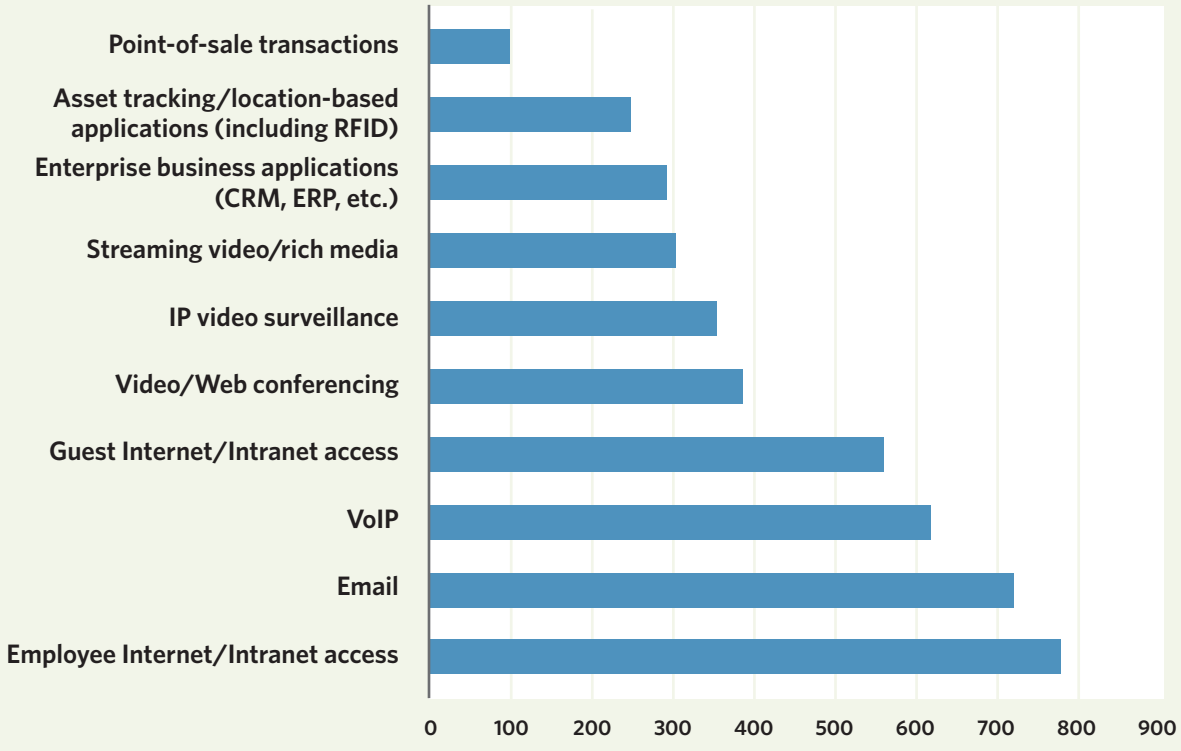
10. If your iPhone OS client still cannot seem to connect, seems very slow all the time or disconnects frequently, you may be experiencing lower-level wireless problems.

Refer to this SearchNetworking.com step-by-step iPad and iPhone troubleshooting guide for further instructions and illustrations. To facilitate debugging, you may also want to install a few free apps. For example:

- **Ookla SpeedTest:** Handy for measuring slow connections
- **Bitrino WifiTrak:** View current channel, signal/noise, and security settings
- **10base-t IP Scanner Lite:** Try to reach other clients on your own network. ■

APPLICATIONS DRIVING WLAN INVESTMENTS

In which of the following applications via wireless LAN do you expect your organization to invest in the next 12 months?



SOURCE: TECHTARGET NETWORKING PRIORITIES SURVEY, NOV. 2010

Tablet security: Best practices

COMPANIES THAT rely on corporate-standard phones to ensure security will have more trouble embracing tablets. Companies that are already securing employee-liable smartphones can start by applying smartphone mobile device security policies and practices to tablet security. The most important include:

1 **Device lock:** If a tablet is lost or stolen, enabling native device authentication can reduce risk of application, data or connection misuse. All contemporary tablets support this practice.

2 **Anti-theft measures:** Many tablets support remote lock or data wipe to stop missing tablets from being misused. While such measures are readily available for tablets, policies must be defined.

3 **Over-the-air encryption:** All contemporary tablets can secure Web and email with SSL/TLS, Wi-Fi with WPA2, and corporate data with mobile VPN clients. The primary challenge here for employers is proper configuration and enforcement, as well as protecting credentials and configs to prevent reuse on unauthorized devices.

4 **Stored data protection:** Hardware and mobile OS support for stored data encryption varies. However, self-protecting apps are readily available for tablets, such as email apps that store messages, contacts and calendars inside encrypted containers. Some employers find self-protecting apps preferable, because they insulate business data from personal data, making it easier to wipe the former without the latter.

5 **Mobile application controls:** Contemporary mobile operating systems employ code signing, data caging and feature restrictions to deter malware. Nonetheless, many downloaded apps require access to sensitive data and features, and employers may have little or no control over app installation. Centrally-enforced restrictions and blacklists are still emerging for tablets; consider this more of a stretch goal than best practice today.

6 **Anti-malware:** Tablets are not shipped with on-board anti-virus, anti-spam, intrusion detection or firewall apps. Although such apps are available, adoption has been slow. Instead, many users rely on corporate mail server or mobile operator SMS filters and a naïve hope that AppStore rules stop Trojans. The IT department has lots of room for improvement here.

7 **Device management:** For visibility, policy configuration, app provisioning and compliance reporting, employers can centrally manage tablets used for business, no matter who owns them. A minimum practice is Exchange ActiveSync policies. ■

802.11n Synopsis

802.11n Feature	Summary	Benefit
Multiple-Input Multiple-Output (MIMO)	Uses N transmit x M receive antennas to take advantage of previously destructive multipath reflections	MIMO antennas are used to enable many of 802.11n's features
Spatial Multiplexing	Splits data into multiple parallel streams, transmitted through different antennas to travel diverse paths	Two spatial streams double data rate and throughput; four streams quadruple them
Maximal Ratio Combining (MRC)	Merges signals received through more than one antenna to overcome errors and loss	Additional receive antennas can improve sensitivity and signal strength at distance (range)
Spatial Time Block Coding (STBC)	Transmits data redundantly via differently coded spatial streams, recombined by receiver	Additional transmit antennas can improve reliability and increase rate over range 1-3 dBm
Transmit Beamforming (TxBF)	Phase-shifts transmissions through two antennas to optimize reception at client's location (implicit or explicit)	Additional transmit antennas can improve reliability/range; mutually exclusive with STBC
Dual-Band Support	Operates on 2.4 and 5 GHz bands, either selectable or concurrently	Reduces interference, increases capacity for dense deployments
40 MHz Channel Bonding	Combines two adjacent 20 MHz-wide channels into one fatter channel	Doubles max data rate and application throughput
Short Guard Interval (SGI)	Reduces inter-symbol transmission gap from 800 to 400 milliseconds	Increases max data rate another 10%
Modulation and Coding Schemes (MCS)	Negotiates # spatial streams, channel width, guard interval, and coding to be used in each direction	Determines max rate, from 65 Mbps (1 stream, 20 MHz) to 600 Mbps (4 streams, 40 MHz, SGI)
20/40 Coexistence	Requires APs using bonded channels to shift to 20 MHz near legacy APs	Ensures "good neighbor" AP coexistence @ 2.4 GHz
Frame Aggregation	Bundles multiple frames (usually MPDUs) into each transmission	Reduces overhead up to 69%, increasing frame and bit rates—single biggest throughput boost
Block Acknowledgement	Sends one short ACK frame to confirm receipt of many data frames	Further reduces overhead, especially when streaming
Wi-Fi Multimedia (WMM) Power Save	Lets clients shut down unused radios and doze for longer periods	Extends battery life, especially with voice traffic

SOURCE: LISA PHIFER, CORE COMPETENCE INC. 2010

Wired equipment upgrades for wireless network integration

BEFORE WIRELESS can stop being a nice-to-have luxury, wired network equipment must be readied to handle wireless demands. But few companies can afford to rip and replace network equipment in one fell swoop. Those upgrades must be budgeted and scheduled over time, resulting in an incremental network infrastructure migration.

Some Fast Ethernet switches may need to be replaced by Gigabit Ethernet switches to deliver sufficient backhaul bandwidth. Another possibility is to retire selected switches, replacing them with wireless backhaul. This "overlay" approach can be easier than upgrading actively used Fast Ethernet switches because installing new mesh APs need not disrupt existing cabling and port assignments. Over time, as wired access declines, older switches can be eliminated, transitioning any residual Ethernet clients to another wired or wireless port.

Finally, wired switches must be upgraded to deliver power to wireless APs via 802.3af or 802.3at Power over Ethernet (PoE). 802.11n APs use multiple-input multiple-output (MIMO) antennas and sophisticated signal processors that consume more electricity than legacy 802.11abg APs. In some cases, 802.11n APs exceed the 13 watts delivered by wired switch ports that implement 802.3af PoE. Fortunately, shortfalls are rapidly diminishing as vendors ship new, more power-efficient 802.11n APs. However, as 802.11n APs move from 2x2 to 3x3 and eventually 4x4 MIMO, power draw will increase. Over time, new wired LAN switches that implement 802.3at should be deployed to quench this growing thirst for power. ■

INVESTING IN WLAN PRODUCTS

In the next 12 months, organizations expect to invest in these WLAN products, listed by priority:

- **WLAN access points**
- **WLAN controllers**
- **VoIP-enabled WLAN handsets**
- **Wireless intrusion protection and/or monitoring**
- **WLAN-enabled Ethernet switches**
- **Wireless mesh systems (including outdoor wireless equipment)**
- **Third-party wireless management solutions**
- **WLAN spectrum analyzers**

SOURCE: TECHTARGET NETWORKING PRIORITIES SURVEY, NOV. 2010

Hybrid approach key to enterprise Wi-Fi success

Given broader Wi-Fi deployment, many enterprises are now rethinking use of both wired LAN and wireless cellular technology. But how can companies leverage their investment in increasing and improving enterprise Wi-Fi coverage with a strategy that leverages existing Wi-Fi investments, minimizes costs and improves coverage? Let's look at a few options for extending cellular coverage and how Wi-Fi can help.

Distributed antenna systems

Many workers and their employers would like to eliminate desk phones, shifting all business calls onto mobile handsets—especially dual-mode smartphones. This shift could greatly improve worker reachability and productivity while cutting costs by consolidating communications infrastructure, fees and maintenance.

However, one major challenge preventing this shift is poor indoor cellular penetration. In a mobile-only scenario, a high percentage of missed, dropped or poor quality cellular phone calls simply cannot be tolerated. One way to improve in-building cellular reception is by using a distributed antenna system (DAS).

Femtocells

Another way to improve indoor cellular reception is by backhauling cellular traffic across another network that already exists and is relatively ubiquitous: the Internet. This can be accomplished by deploying your own little indoor cell tower: a femtocell.

Fixed-mobile convergence

DAS and femtocell both improve indoor voice service by strengthening cellular signal. However, cellular isn't the only indoor wireless technology. Increasingly, homes, offices, large enterprises and even entire campuses are being blanketed by Wi-Fi, and a growing percentage of mobile handsets are now dual-mode (3G + Wi-Fi) phones. Combine these trends and you have a fantastic foundation for fixed-mobile convergence (FMC).

Hybrid approaches

Traditional DAS solutions have the benefit of being multi-operator, while femtocells have the advantage of being easily deployed. FMC appeals to those who want to use shared infrastructure to support multiple services. Vendors chasing the indoor cellular market have been searching for innovative approaches that combine these attributes.

The growing need for enterprise Wi-Fi coverage will prompt other new hybrid approaches to emerge, combining aspects of DAS, femtocell and FMC. By making your indoor network infrastructure investments do more, you may well be able to improve indoor coverage for many wireless services at a reduced total cost. ■

THE MYTH OF INTEGRATED WIRED-AND-WIRELESS LAN

COVENTRY UNIVERSITY AND alcoholic drink manufacturer C&C Group: two very different organizations with one similar networking problem.

Both have separate but equally necessary wireless and wired LANs. Each entity has separate (though effective) management tools for these networks, but both see the potential in at least integrating management across wired and wireless, if not going even further into combining architectures.

While lots of vendors talk integration, at this point few total solutions actually exist. Instead, users must take baby steps toward integration that likely won't totally occur until they face network refresh.

COVENTRY'S EXPANDING WIRELESS-WIRED NETWORK UNIVERSE

Just three years ago, Coventry University, a 33-acre campus with 18,000 students and staff, had a Wireless Local Area Network (WLAN) that consisted of 53 hotspots. Back then, students and staff weren't armed to the teeth with wireless devices so this network of convenience provided basic Wi-Fi Internet access.

While lots of vendors talk wireless and wired LAN integration, at this point few total solutions actually exist.

What may have been a convenience for wireless LAN users was a management headache for the school's IT department. Each access point (AP) required manual configuration and control. Clearly, the school had no vision for wireless.

But three years ago, the university's pro-vice-chancellor changed all that, announcing a vision for ubiquitous wireless across the Coventry campus.

Today, the campus has 703 APs serving 1,500 concurrent users, or about 5,000 users a day. The network provides access to internal campus services in addition to basic Internet depending on user role. Another 330 APs will go live when two new buildings, a student union and an engineering and computing teaching facility, are completed in 2011 and 2012, respectively.

Working with Cisco to deploy the vendor's Unified Wireless Network Architecture, the University today provides more robust wireless LAN access to more students and staff for a quarter of the cost of installing a wired network. It's also managing all 703 APs from one server. "It's simple and a huge improvement from when we were managing 53 WAPs manually," said Paul Brennan, head of network services at Coventry University.

Ubiquitous wireless LAN coverage at Coventry exemplifies what is perhaps the biggest trend in enterprise networking in years—giving users secure access to the network and applications regardless of device, media or location. That's especially important considering that the latest crop of tablets, most notably Apple's iPad, don't offer a wired Ethernet connection. And the iPad is making huge strides in the enterprise. According to Apple's quarterly earnings report in January, over 80% of Fortune 100 companies are deploying or piloting the iPad.

Still, Coventry's extensive wireless architecture, which includes a range of technology—from APs and centralized controllers to an automated network configuration application and Network Access Control—doesn't mean the university will move to total wired replacement. "Wireless isn't a panacea for wired. We want to see a mix of both," said Brennan.

"Wireless isn't a panacea for wired. We want to see a mix of both."

—PAUL BRENNAN

What's happening at Coventry is, in fact, what is occurring industry wide: a transition to unification that is about deploying and managing a network infrastructure where wired and wireless are recognized as equally mission-critical, complementing each other.

"Wired Ethernet will continue to play a significant role in network cores and data centers with many

enterprise networks going wireless at the edge, replacing virtually every Ethernet drop with wireless for network access," said Lisa Phifer, president of Core Competence Inc. "In between the edge and core, we'll see a mix of both, depending on logistics and load."

AS C&C EXPANDED, SO DID ITS WLAN

At Ireland and UK-based C&C, it was an executive edict that energized an enterprise wireless LAN deployment across the company's offices, brewery and warehouse.

"Our new leadership team was very mobile, on the go between Ireland and the UK, and they needed access to company data from wherever they were," said Kevin Minihane, IT manager at the C&C Group.

To add to that need, two corporate acquisitions in 2009 not only created a dispersed organization but also increased the number of employees from about 500 to 900.

Today, C&C maintains an existing wired Cisco network—consisting of a Catalyst 3560 POE switch in its plant in Dublin and two Catalyst 4500 series core switches at its Clonmel, Ireland, cider mill—as well

THE TRUTH ABOUT INTEGRATING WIRED AND WIRELESS LANS

MYTH	REALITY
▪ Wireless should be used everywhere.	▪ Wireless should be used where it provides advantage.
▪ Unified networking will only work if purchased from a single vendor.	▪ No single vendor offers a complete solution.
▪ Wireless is less secure than wired.	▪ Wired networks depend on limited physical access for security. Role-based access controls should be applied to both wired/wireless.
▪ Wireless (802.11n) is faster than wired Fast Ethernet.	▪ 802.11n MAX data rates range from 150-450 Mbps, which sounds faster than 100Mbps Ethernet, but wireless is not full duplex, and MAX rates decline with distance/load.

as a growing HP ProCurve wireless LAN based on dual M5M765 wireless LAN controllers, and the MSM310 and MSM320 APs.

"We use a number of tools to manage our current infrastructure. For our ProCurve switching environment, we use HP's ProCurve Manager (PCM), which we purchased when we purchased our HP switches, said Minihane.

For our WLAN infrastructure, we use the Web interface to the WLAN controllers, which allows us to make configuration changes to our WLAN environment and access points. We also use the PCM to manage our Cisco devices. For more ad hoc management, and for basic configuration changes, we use Kiwi CatTools to roll out configuration changes to multiple devices at a time."

For Minihane, all of these management tools work well individually, but there is also another bottom line: "So far I haven't discovered a solution that could do everything we need," he said.

WHY DOES UNIFIED MANAGEMENT MATTER?

If there is one common complaint among users, it's that lack of unified wired-and-wireless management. That's because total cost of ownership/return on investment (TCO/ROI) isn't quite as attainable until unified management is achieved.

Unified management should mean having one console that can handle common network functionality, such as planning, provisioning, configuring, monitoring (including performance, security and integrity), handling exceptions, logging and reporting. This console will also need the additional elements unique to wireless management, including connection reliability, spectrum management and monitoring, location and tracking functionality, as well as additional security concerns. Even then, some wireless experts believe that certain wireless functions will have to be maintained separately.

> "So far I haven't discovered a solution that could do everything we need."
> —KEVIN MINIHANE

"I think there may well be wireless-only edge/access devices that need to be deployed and managed differently than today's wired Ethernet switches. That doesn't mean that the network isn't integrated, it just means that some tasks will require unique tools," said Phifer, referring to those appliances that

handle deeper spectrum analysis, for example.

PLANNING THE TRANSITION TO AN INTEGRATED NETWORK

For IT organizations transitioning from a primary wired Ethernet infrastructure to a unified wired/wireless LAN, it can be difficult to determine where to start.

The answer is planning.

"Convergence and unification has to be addressed at the physical layer as well as management, security, policies and services," said Chris Kozup, director, mobility and borderless networks at Cisco.

Next, the roadmap toward unified wireless begins with an assessment and evaluation of the existing network infrastructure and how an organization wants to grow the network based on which applications need to be accessed by which users from which locations.

"Don't assume that the network architecture that you've had is the best architecture for the future," said Joel Vincent, director of product marketing at Meru Networks.

Once organizations look at the use case, they must assess capacity and ports, considering the allocation of bandwidth to build out the WLAN.

Vendor selection based on solution price/features and an RFP process follows. Industry experts recommend opting for 802.11n 5 GHz technology for greater throughput capacity and less interference.

The next steps are installation and tuning, followed by ongoing operations and network expansion. Unified management tools are largely a function of which vendor's equipment a company opts for. Third-party tools will still dominate security management and performance management of the wireless LAN. ■

The roadmap toward unified wireless begins with an assessment and evaluation of the existing network infrastructure.

LYNN HABER reports on business and technology from Norwell, Mass.

INTEGRATED WIRED AND WIRELESS LAN SECURITY? NOT SO FAST

MANY VENDORS PREACH integration of wired and wireless LAN security, but some network security pros say it's not worth the trouble. Ruairi Brennan, IT security analyst at The Electricity Supply Board (ESB) of Ireland, doesn't see the point.

"The best practice would be to keep the wired and wireless networks separate just for security," Brennan said. Isolating the two keeps vulnerabilities that are unique to wireless networks away from the wired network, he explained.

The ESB's wireless LAN serves between 8,000 and 10,000 users with 60 Aruba Networks access points (APs). It was built to provide wireless access in conference rooms and other areas that the existing wired LAN didn't serve well.

For security, the ESB turned to AirTight's SpectraGuard Enterprise Wireless IPS (a wireless intrusion prevention system product) and the SpectraGuard SAFE endpoint protection system. Deployed together, these products can stop "bridging" between wired and wireless networks.

"It's a massive security risk if you have someone on the LAN simultaneously accessing an outside wireless access point," Brennan said. "You could be bridging between a secure LAN and [what could be] an unknown AP on the wireless network." That only offers the rogue entry point access to secure data.

The SpectraGuard Enterprise package offers the basic necessities of wireless LAN security: It blocks unauthorized access to the wireless LAN by enforcing authentication policy. It also detects rogue APs and prevents them from connecting to the LAN, and it enables centralized management and policy enforcement. Meanwhile, SpectraGuard SAFE sits on endpoints and

stops them from connecting to the wireless LAN when they are plugged into the wired network and vice versa.

A MORE COMPLEX NETWORK WITH A ONE-VENDOR STRATEGY—AND NO INTEGRATION

Hospital chain Atlantic Health has broken up its wireless LAN, composed of 2,000 Cisco APs, into several segments with unique policies across its six hospitals. The wireless LAN supports free public Wi-Fi for patients, private wireless access for Neonatal Intensive Care Unit (NICU) rooms, remote access for ambulances and mobile caregivers, Vocera badges for mobile communications between medical staff in the hospital, telemetry reporting and other types of wireless communication.

Atlantic Health has chosen not to go to a third party for wireless LAN security, according to Pat Zinno, director of infrastructure support and services. Security mechanisms such as WPA2 encryption, authentication and RF monitoring for rogue AP detection are built into the APs and controllers, which are all centrally managed from a Cisco Wireless Location Appliance. The location appliance can enforce user policy, as well as RF capacity management on a location basis regardless of the connecting device.

Cisco offers integration of wireless network security with its wired network Intrusion Detection System (IDS), but for now, Atlantic's wired and wireless security strategies still remain separate.

Atlantic Health's wired LAN security requirements are not as complex or demanding as the wireless side. After all, computers connect directly into network ports that are firewall protected. The company also uses an Intrusion Detection System (IDS) product from Sourcefire that monitors all of the traffic as it traverses the network, Zinno said. He believes that this separation will "evolve over time."

"The more you can import all of that data [from monitoring across wired and wireless networks] into one, the better you will be," said Zinno.

WHERE SECURITY INTEGRATION STARTS IN THE ENTERPRISE

Network engineers who are charged with securing two separate and very large wired and wireless networks want unification for their security event information, not their security tools. They want a platform that collects and presents a unified view of information from differing reporting structures used to analyze logs from firewalls and servers.

"A security event management product correlates these events and helps the enterprise see when there's a security incident instead of a lot of noise. Certainly security

event management for the wireless LAN should be integrated into a wired security events management product," said John Pescatore, a distinguished analyst at Gartner Research.

Combining security strategies for extremely complex networks any further can be difficult because of differences in basic needs. Enterprises will set the same basic policies for both wired and wireless networks in terms of user access to certain applications. However, enterprises will have more divergent advanced security policies that are unique to either wired or wireless. Managers of wireless networks focus on RF interference, and their testing and troubleshooting techniques totally differ from those on the wired LAN, Zinno said.

PREPACKAGED SECURITY INTEGRATION: BUT FOR WHOM?

Smaller companies with less complex networks may find integration answers in prepackaged all-in-one systems that are marketed by security companies like SonicWALL and Fortinet. These security companies have extended their Unified Threat Management (UTM) systems—which include firewalls, content monitoring and intrusion prevention—to traffic coming in from wireless LANs.

SonicWALL says it offers a distributed wireless network with its own "dumb" APs that connect all wireless traffic to a centralized UTM appliance used for both wired and wireless.

Managers of wireless networks focus on RF interference, and their testing and troubleshooing techniques totally differ from those on the wired LAN.

"All traffic is backhauled to a UTM where we can make an intelligent decision," said Matthew Dieckman, SonicWALL's product line manager for secure remote access.

SonicWALL treats all wireless traffic as an "untrusted entity" until it is scanned by a UTM appliance. Then it can be subjected to all of the same access rules that apply to wired LAN traffic.

For smaller companies looking for the least expensive solution, a combined appliance might work, Pescatore said.

"Another scenario would be where the company has small branch offices. If I've got this branch office and they only need one access

point, and I could be sure I wouldn't screw it up, I wouldn't have a separate security solution in each of these branches," he said. But extending this into a more complex network wouldn't be easy, he added.

BIGGER SECURITY FISH TO FRY

Many enterprises are slow to adopt wired and wireless network security integration because they have more pressing wireless security problems.

For one thing, network managers are more concerned with monitoring and troubleshooting across various types of wireless spectra as smartphones, tablets and other wireless-enabled devices like vending machines that flood their networks.

"If there was one tool we could have, it would be one that picked up all of the wireless spectrums out there," said Zinno.

Atlantic Health's network is facing interference from microwave ovens and Bluetooth devices, among others. If somebody mistakenly moves a Bluetooth-enabled scanner into an area where it will interfere with Wi-Fi transmittance, Zinno's team needs to be able to track the problem—and that's not always possible with existing tools. Zinno is currently testing out Cisco's CleanAir spectrum analysis technology, which Cisco claims can find radio interference, map it to the source and automatically troubleshoot the issue.

Engineers also want to use wireless IPS appliances to go beyond detecting rogue APs and into determining where there is unwanted 3G or 4G activity on an enterprise network. This will especially be the case in government agencies and healthcare settings that must meet deep compliance requirements.

While integrated wired and wireless network security might seem like an easier management proposition, wireless network engineers will always demand functionality that is different from what enterprises need on a wired network. Unless those security paradigms can be incorporated into an integrated system, enterprises are likely to stick to managing two separate security systems. ■

Many enterprises are slow to adopt wired and wireless network security integration because they have more pressing wireless security problems.

RIVKA GEWIRTZ LITTLE, senior site editor, TechTarget Networking Media.

EXPLORING THREE PATHS FOR UNIFIED WIRED-AND-WIRELESS NETWORK MANAGMENT

SINCE ITS INCEPTION, enterprise wireless LAN has functioned as an overlay network on top of wired networks. As a result, the management platforms for wireless and wired network solutions have evolved separately, usually with separate teams working in each environment.

Now enterprises are deploying wireless networks more widely and adopting them as the primary access layer. Wireless ubiquity is forcing enterprise networking teams to find ways to consolidate capital expenditures and simplify operations by treating the Ethernet and wireless LAN networks as a single unified infrastructure with an integrated management platform. Enterprises have several options for unifying their wired and wireless management. The path they choose will depend on the network infrastructure they already have, how users connect to the network and IT's willingness to embrace new paradigms such as cloud computing.

ABSORBING WIRELESS NETWORK MANAGEMENT INTO WIRED NETWORK MANAGEMENT

Some enterprises unify wired and wireless network management by installing add-ons for the wireless LAN infrastructure to their existing wired network management platforms. In most cases, the networking vendors have mature network management software for their routers and switches that can serve as a solid framework for added wireless management capabilities. However, this approach favors enterpris-

es that use a single vendor for both their wired and wireless networking infrastructure.

Grove City College standardizes on HP Networking for its network infrastructure, and the network team at the Pennsylvania school manages the wired components with HP's ProCurve Manager Plus (PCM+) solution. When the college started to build out campus-wide wireless network access, CIO Vincent DiStasi decided to standardize on HP wireless LAN products, not only because they met his requirements, but because they allowed him to have an integrated wired and wireless network management approach with PCM+.

The college has three generations of HP's wireless LAN products deployed on campus, ranging from legacy standalone access points to some of the latest 802.11n controller-based products. PCM+ integrates all of them into a centralized network management system.

"HP ProCurve does not make a product available for sale without having a way to plug it in to PCM+, even the product lines from the Colubris and 3Com acquisitions." DiStasi said.

DiStasi's network engineers use PCM+ to view the school's switches, routers, controllers and wireless access points by model, enabling the networking team to maintain consistency in firmware versions and configuration changes.

The networking team can also use the PCM+ Identity Manager add-on to apply bandwidth and security policies across both wired and wireless infrastructure to users based on integration with the school's Active Directory server. "As a college, we basically rotate 25% of our users every year. To keep support calls to a minimum, we strive to make it easy for all of our users to connect to the network, wherever and however they need to," DiStasi said. "The value of network management cannot be overstated. Without PCM+, our days would be very long."

MANAGING WIRED DEVICES THROUGH YOUR WIRELESS NETWORK MANAGEMENT PLATFORM

Many wireless network management products are expanding to support wired devices.

Using a native wireless network management platform will appeal to companies that are striving to become an all-wireless enterprise. These organizations have forgone cabling Ethernet ports to the desktop and are deploying wired network ports only to wireless access points. A wireless network management system that includes support for the primary wireless access, as well as support for the switches that connect the wireless LAN elements,

might be all that an all-wireless enterprise needs.

Pat Wren, managing director of operations for Edmonton-based ATB Financial chose Aruba Networks' AirWave Wireless Management Suite as his unified network

A wireless network management system that includes support for the primary wireless access, and the switches that connect the wireless LAN elements, might be all that an all-wireless enterprise needs.

management platform, partly due to its support of third-party wired networking products like Cisco switches and routers. AirWave gives his network engineers an easy-to-use, visual representation of the wired and wireless networks across multiple ATB locations around Alberta, Canada. "Our network administrators... get a view of our locations throughout the entire province and can quickly zoom in to the trouble spots on our overall network," Wren said.

He said that maps of the company's offices are overlaid with the locations of all network devices within the AirWave interface.

ATB deployed AirWave when it rolled out an Aruba-based wireless LAN, but the company's engineers use the product to monitor and manage Cisco Integrated Services Routers (ISRs) at ATB's 165 branches. The combination of the AirWave product and the new wireless network has reduced the number of physical switch ports needed at remote branches, while giving engineers full visibility and control of the branch networks.

MOVING WIRED AND WIRELESS NETWORK MANAGEMENT INTO THE CLOUD

Some enterprises view the cloud as the ideal point for unifying wired and wireless network management. New cloud-based network management platforms offer many of the benefits of other cloud computing services, including reduced capital expenditures and simplified software maintenance. A number of wireless LAN vendors, including Aerohive and Meraki Networks, now offer management products in a subscription-based cloud platform. Both Aerohive and Meraki also offer cloud-based routers that can be managed through the same cloud. Aerohive's routers are part of

a recent acquisition of Pareto Networks, and Aerohive plans to integrate the products into its existing management platform.

Ty Puckett had traditionally struggled with managing his legacy wireless LAN at Greenway Medical in Georgia. The IT director had to move back and forth among command line interfaces and complicated licensing schemes for every new feature he wanted to deploy.

When the electronic health record software company upgraded its wireless network, Puckett and his team replaced the legacy network with new wireless LAN infrastructure from Aerohive. The deployment included a subscription to HiveManager Online, Aerohive's cloud-based network management platform.

"We have been moving a lot of the systems our company depends on into the cloud, so we were pretty open to a cloud-based WLAN management," Puckett said.

The cloud-based HiveManager manages all configuration, management and monitoring of the company's wireless access points through an encrypted Web link. Puckett and his team can log in from anywhere with Internet access to add new access points to the network, change network settings or troubleshoot issues on network. Puckett said he is able to push software updates to his access points from home, rather than logging on to a console in the office.

"I typically log in on a Sunday evening from home and push the new firmware to groups of radios. And we never have to upgrade the software in our cloud controller," said Puckett, adding that he has seen a continuous stream of updates and new functionality that literally just appears when Aerohive revises the HiveManager Online management software.

"We have been moving a lot of the systems our company depends on into the cloud, so we were pretty open to a cloud-based WLAN management."
—TY PUCKETT

For Puckett, the power of cloud-based management was realized during Greenway Medical's annual user conference. Puckett's team was tasked with providing wireless access for both Greenway's employees and conference attendees who were miles away at the chosen off-site venue.

"In the past, I certainly would have spent the week at the hotel ensuring

that everything stayed up. With cloud management, I was able to tweak and optimize both the corporate and guest wireless networks to deal with demand while sitting at my desk," said Puckett.

The remote access capabilities, an easy to use Web interface and lower costs when compared to hardware wireless LAN controller-based solutions were the key points that Puckett cited for switching to a cloud-based management product.

> "Cloud-based management will definitely factor in to future infrastructure purchasing decisions."
> —TY PUCKETT

"HiveManager Online has made me rethink how to manage my network going forward. Cloud-based management will definitely factor in to future infrastructure purchasing decisions. If Aerohive started selling switches and routers this way, sign me up," Puckett said. ■

BY MICHAEL BRANDENBURG, technical editor, TechTarget Networking Media

TechTarget
Where Serious Technology Buyers Decide

Network Evolution Ezine is produced by TechTarget Networking Media.

Rivka Gewirtz Little
Senior Site Editor
rlittle@techtarget.com

Shamus McGillicuddy
Director of News and Features
smcgillicuddy@techtarget.com

Michael Brandenburg
Technical Editor
mbrandenburg@techtarget.com

Kara Gattine
Senior Managing Editor
kgattine@techtarget.com

Linda Koury
Director of Online Design
lkoury@techtarget.com

Susan Fogarty
Editorial Director
sfogarty@techtarget.com

FOR SALES INQUIRIES, PLEASE CONTACT:

Tom Click
Senior Director of Sales
tclick@techtarget.com
617-431-9491

Cover photograph by Simon Potter/plainpicture