white paper

How To Unify The Wireless Architecture in Education Without Limiting Performance or Flexibility

So much is happening today to give you a chance to rethink your wireless architecture. Indeed, you're almost forced to rethink and unify wireless into your overall network architecture. The good news is the payback from such changes in terms of lower IT management costs and increased productivity for a school district's increasingly mobile teachers, students and staff can more than pay for the effort.

"Unified wired and wireless offerings promise to reduce the time and effort required for network diagnostics, troubleshooting, and day-to-day network management and maintenance tasks," according to a recent report from the analyst firm IDC. Given that those ongoing tasks make up approximately 70% of the total cost of ownership of a network, unification is obviously worth considering.

Gartner essentially agrees while casting a slightly different light on the topic: "We are witnessing the 'growing up' of mobility, as it becomes increasingly controlled and managed as part of an organisation's architecture and strategy," says Gartner vice president and distinguished analyst Nick Jones.

However, it often requires a capital investment to save on operating costs. Can't you just maintain the status quo until budgets are less constrained? Perhaps, but the availability of higher bandwidth offered by the 802.11n standard and the explosion of applications that need it may provide another push towards a new architecture that can handle the increase from 802.11g's 54 Mbps to 300 Mbps for 11n.

Voice over IP, eLearning, video conferencing, IP Surveillance and the ubiquitous use of video in education demand 802.11n's higher bandwidth. Re-imagined video courseware that alters video

streams based on individual student responses similarly demand the new standard. Yet care must be taken lest you make the move to 11n and discover performance is problematic and management still too costly.

Here's what to look for in a wireless architecture that not only provides the mobility and performance today's applications need but also lowers your costs of operations while increasing wireless security.

Unifying Management

One guiding principle is to realise that wireless technology has moved from a convenience overlaid on wired infrastructure and managed in an ad hoc fashion to a mission-critical service that needs to be secure, seamless and flawless in coverage, and managed efficiently with as much automation as possible. This is particularly true in an educational setting where wireless is the only practical connectivity in crowded, 1:1 computing classrooms. In other words, wireless needs to be taken up to the standard of efficiency and reliability you've achieved on your wired networks.

If you are still living with an implementation of wireless that is layered on top of your wired infrastructure, you may find that you have to log into each access point (AP) to check its health and change configurations. As a first step, you need to move to an architecture that provides a single point of management control.

At a minimum, look for a solution that provides management of multiple access points across multiple subnets with these capabilities:

- Intuitive web UI for managing all APs on a WLAN
- Group management capabilities
    - Mass firmware upgrading by group
    - Mass configuration by group including QoS settings required for VoIP, video and other high bandwidth, low latency applications
- Fault management
- Real-time monitoring
- Real-time reporting

Stepping Up To A Wireless Switch

Given that much management of enterprise networks revolves around the switching infrastructure, it makes sense to roll up sets of access points into switches that are similar to ordinary managed switches with additional wireless controller capabilities.

Unified management of wireless switches and the APs connected to them is somewhat simpler than the master/slave AP hierarchies that lower the number of points you need to manage. The wireless switch similarly simplifies configuration and leverages the same centralised access security in place for the wired network. The wireless switch becomes your fulcrum point for reporting and troubleshooting including client association, security settings, AP utilisation, AP channel usage, and rogue AP detection and mitigation.

Control over RF (Radio Frequency). Another wireless switch capability to look for is control over

RF configuration, including channel selection and signal strength. Ideally, look for a wireless switch that automatically minimises interference between APs and maximises seamless coverage within a building or across a campus by selecting channels and setting signal strength, which in the past individually managing APs was a tedious and error-prone task. The best solutions can even detect the failure of an AP and automatically raise the signal levels of adjacent APs to fill in the resulting wireless hole.

Centralised Security. One of the important considerations in Gartner's 2010 magic quadrant for wireless LANs was to tie into the security infrastructure and processes already in place for your wired infrastructure. Among the things to look for:

- Built in Access Control Lists (ACLs)
- Network and 802.1x authentication for WLAN clients
- Rogue AP mitigation
- Support for encryption
    - WPA and WPA2 security utilising Advanced Encryption Standard (AES)
- Portal support
    - Web-based authentication process to capture initial HTTP/HTTPS traffic and redirect the client to authentication provided by a switch or a RADIUS server
    - Tunneling to isolate guest traffic across the corporate network

Seamless Roaming. In addition, look for a wireless switching solution to provide seamless wireless roaming across all the APs connected to it if it's operating at Layer 2 of the network. A Layer 3 stack of wireless switches adds the ability to roam among APs connected to a logical grouping of switches. From the end user point of view, not having to re-authenticate while you take your notebook or testing clicker or smart phone through a campus of seamless wireless connectivity is ideal.

Centralised Management Without The Bottleneck

Be careful, however, if your wireless infrastructure architecture is heading towards what is essentially a centralised WLAN controller. While you get the benefits of central management, security, and the ability to roam across APs, your design comes with a built-in bottleneck and single point of failure. Why force wireless traffic through a central switch on its way to the application server? The unnecessary latency can play havoc with real-time applications like voice or video, adding video stuttering and even inserting white noise into remote learning conversations your users are attempting.

Just as important, you're sending each wireless packet back and forth through the wired core of your network. While that might have worked with the older 802.11g standard, the potential for bottlenecking is greatly magnified with the 6-fold increase in bandwidth provided by 802.11n. Moving to the higher speed APs reduces the number of APs you can support without a fork-lift upgrade of the WLAN controller. You can also find yourself in a situation where the double whammy of back-and-forth 802.11n wireless packets overwhelms the bandwidth of your wired network core.
Instead of a centralised WLAN approach, look for Wireless Switching at the edge of the network.

In addition, the most flexible approach distributes traffic forwarding to the APs to optimise traffic flow for latency-sensitive applications such as voice.

A Middle Ground In The Cloud

Some Education IT organisations may find the cost of a Wireless Switch is too high, particularly in smaller districts.. As we mentioned, some vendors provide the benefits of centralised management across a groups of APs using a master/slave approach to handle similar groups of APs. But another alternative to consider is AP management from the cloud.

Overtaxed Education IT groups that do not have the time or skills to implement the complexities of WLANs, or simply prefer to outsource it for their smaller outputs, can work with wireless vendors who provide equipment manageable by wireless controller capability in the cloud. The best of them include built-in security that handles CIPA compliance.

D-Link's Unified Wireless Approach

Our wireless management capabilities allow you to control, configure and monitor all D-Link Switches and Wireless APs from the same single pane of glass, significantly reducing operation overhead and total cost of ownership. D-Link's unified management pulls wireless into the automated end-to-end security, configuration, monitoring, reporting and group firmware upgrades that distinguish D-Link's overall network solutions.

Scalability. As many as 256 D-Link access points supporting as many as 2000 WLAN clients can be connected by 8 logically stacked Wireless Switches to support seamless roaming throughout the largest of campuses, or even whole districts that use 10G Fiber links to bridge the distance between campuses. D-Link's Wireless Switches deploy at the edge and can be matched with APs that manage traffic forwarding for applications like voice and video streaming that are sensitive to the latency added by traversing a Switch.

Ease of installation and operation. D-Link's solutions adjust each AP's wireless signal and channel to mitigate interference. If an AP drops, the wireless "hole" is closed by raising the signals of adjacent APs.

In addition, the wireless and PoE compatibility of D-Link's APs can eliminate the need to run Ethernet cable or electrical power, and D-Link's plenum-rated business-class APs can be placed in air ducts without violating stringent fire regulations. Finally, a variety of access points for indoor and outdoor deployment feature modes that bridge the gaps including Wireless Distribution System (WDS) with access point, WDS/Bridge (No AP Broadcasting), and Wireless Client.

Green. As with all D-Link solutions, state-of-the art green design helps reduce power consumption resulting in lower operating temperatures that extend product life. D-Link WLAN installations also simplify power saving automation including turning off Wi-Fi radios after buildings and areas close according to a flexible schedule, cutting power use 80% during link-off mode.

Visit the web address below for more information on the complete line of business products:

www.dlink.com

D-Link® Building Networks for People