Unified Wireless Switching

Enabling a Truly Converged Network

White Paper
March, 2007

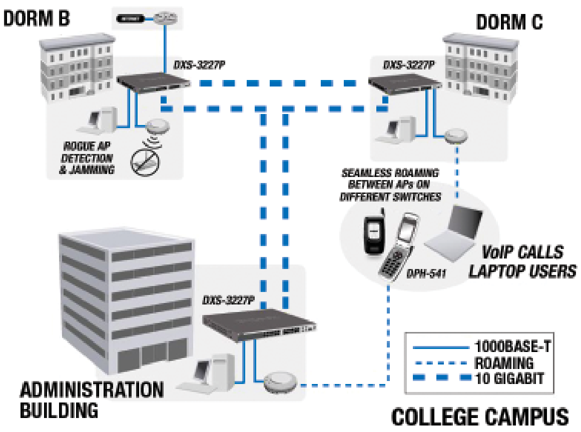
Abstract

As businesses scale, traditional wireless network deployments become more complex, more costly and less secure. Users expect the ability to roam between access points. New applications like Wi-Fi VoIP require the ability to roam seamlessly and securely, for example. Wireless switches provide a simple, centralized, iron-clad solution, with management tools, policy enforcement and built-in security. They make wireless LANs as secure as their wired counterparts. With today's technology, you can overlay WLAN switches without compromising the integrity of the original wired infrastructure. This white paper examines existing Wi-Fi challenges then explores the numerous security advances and manageability enhancements that wireless switch technologies provide.

D-Link®
Building Networks for People

Secure Mobility Challenges

More businesses are deploying wireless networks, giving users the ability to roam freely between access points and adopt new applications like Wireless-Fidelity Voice-Over-Internet Protocol (Wi-Fi VoIP). These wireless networks free users from the confines of their desks, offering them seamless access to company data from their notebook computers, whether it be in a conference room, lunch room, or presentation hall. Wireless networks can also be used to extend the corporate LAN between buildings. New applications for wireless LANs continue to be rolled out, including communication devices such as handsets and emerging Wi-Fi phones.



Centralized AP Management with Seamless Wi-Fi Roaming between Campus Buildings

The benefits of wireless are fairly obvious. However, the security risks often outweigh the benefits, because most wireless networks in use today know very little about the airwaves around them. APs are not smart enough to collect information about rogue users, rogue APs or general network traffic. On the other hand, they are just smart enough to be a security threat. Each AP hanging off of the wired network is a potential entry point for intruders using commonly available encryption cracking software (if encryption is enabled at all). APs placed by inexperienced employees or malicious network attackers present a severe security risk, since an unsecured AP potentially provides direct access to the corporate LAN. If the only thing between rogues and the internal network is an SSID and a weak WEP key, the network will eventually be compromised.

Without the proper security in place, rogue users can challenge the AP all day long without anyone being the wiser. Once a rogue gains access to the wireless network, there is no security intelligence that can recognize the rogue client, and the rogue has now bypassed the firewall. The AP says “here is a client with the right credentials” and then opens the door to the castle. This is of particular concern to government agencies and private corporations that house highly sensitive data. Once a rogue gains access to the wireless network, they have bypassed the company’s primary line of defense - the firewall.

Fat APs, Decentralized Risk

“Fat” APs that authenticate individually weaken access control and complicate management. Traditionally, “fat” APs listen to the RF spectrum to try to find a clear channel. They do not cooperate to optimize the use of the spectrum, however, because they operate individually. Coordination is difficult, and since there is no centralized coordination, the RF spectrum is often used inefficiently with multiple APs operating on overlapping channels. In addition, power levels of individual APs are not tuned to optimize coverage, and APs typically operate at their highest power setting, potentially causing unwanted interference.

Physical Access

Without centralized management and control, APs can be swapped out with illicit equipment. If there’s no security layer between the AP and the existing wired network, a new, illegal AP can be swapped in and compromise the rest of the network. In addition, when a “fat” AP needs to be replaced, configuring the replacement device can be very time-consuming and error prone.

Business Requirements

Secure and seamless roaming requires reliable mobile connections without multiple logins. This means that user-based policies and authentication, and centralized AP coordination are a practical necessity. With new technology like Wi-Fi Phones, seamless roaming is not just a “nice-to-have” feature. It’s a requirement for user satisfaction. In more complex settings, users may also need to roam between subnets and VLANs. If a wireless system forces users to manually re-authenticate as they “hand off” between multiple APs, then its value diminishes significantly.

So, network administrators need to know and control the location and identity of all users on their LAN. They need to know how many users are on a particular AP, and they need the ability to examine the activity of each user when security concerns arise

Solution at the Switch
Secure, Seamless, Manageable, Flexible

Unlike traditional wireless networks, wireless switching offers a user-based approach to administration policy - as opposed to policy tied to ports, addresses or SSIDs. This puts the network administrator back in charge, with a centralized console for managing and troubleshooting any contingency. Network administrators centrally control authentication and encryption, manage VLAN groups, enforce roaming policies, and maintain tight control over Quality of Service (QoS) traffic. Each client is tracked by user identity, rather than by port, device or approximate location, making the environment more secure and intruders much more visible. Policies that govern who can do what (and where) while roaming wirelessly can be easily implemented. Centralized WLAN systems follow users and know who they are, so it is much easier to locate rogues when they appear on the scene.

In terms of mobility, users stay connected because Layer 2 and Layer 3 switching on the wireless switch allow them to move between Access Points (APs), VLANs and subnets. The wireless switch makes a transparent connection with the existing wired network, and the transition between APs is invisible to the user.

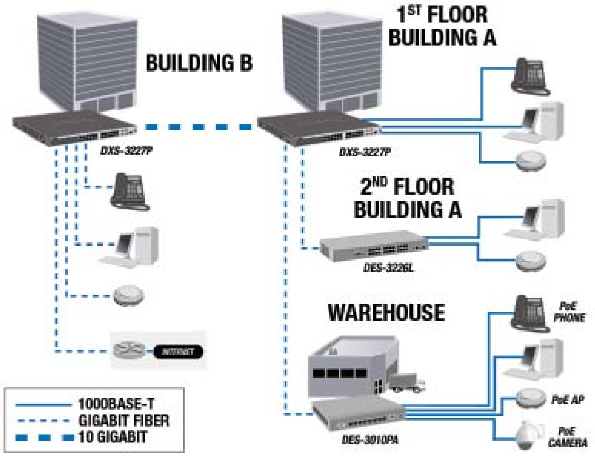
Organizations can opt for encryption at layer 2, layer 3, or both, and they can apply different encryption policies to different users and groups. This is different than the common VPN approach, which slows performance as it scales. The wireless switch centralizes encryption at the switch to maintain high performance levels, using “thin” APs. In “fat” AP scenarios, where the APs encrypt at each installation, performance, flexibility, manageability, and security suffer. The thin APs of the wireless switch model perform only transceiver and air monitoring functions. The WLAN switch sees the AP as an extended access port rather than another intelligent processing unit. The AP acts as a dumb terminal and a beacon that is smart enough to notify the switch when unauthorized users or rogue APs enter the scene.

Ultimately, businesses that provide wireless switching provide secure, reliable, seamless and flexible wireless connectivity without burdening users with numerous authentication exercises.

Centralized Management

With a WLAN switch, centralized management puts the network administrator in control of AP configuration, software images sent to each AP, and data flow throughout the wireless network. Most importantly, there are fewer devices (APs) to manage directly. Every security, support, and filtering function is managed from one console, on one secure device (the switch itself).

The administrator can provision each AP from one location, and manage the network. As a result, rogue users and APs are detected and eliminated, as are many DoS and man-in-the-middle attacks. All the common configuration items are downloaded from the wireless switch to each AP, so IT personnel can keep configuration policies consistent and easily update new switches. When an AP connected to the WLAN switch is booted up, the switch immediately sends the correct configuration settings. Any changes thereafter are updated centrally from the switch and uploaded to each AP.
If an AP fails, the plug-and-play model takes over. Network administrators plug in a new AP, and it is automatically discovered by the switch and configured accordingly. WLAN switches can also provide Power over Ethernet (PoE) to the APs. No one needs to touch the AP itself - ever (unless replacing a failed AP).



Centralized AP Management with PoE Deployment

D-Link Delivers Security, Mobility, Reliability and Control

Like the solution described above, D-Link’s wireless switching technologies offer a user-based (rather than port-based) design, providing a centralized security and management interface. The wireless network lies on top and is independent of the wired infrastructure. With D-Link wireless switching, security functions, such as encryption, authentication, and access control, follow users as they roam. Unauthorized wireless APs can be easily identified, whether they are placed by inexperienced employees or intentionally by malicious network attackers. D-Link solutions scan the airwaves to detect unauthorized APs (rogues) and allow network administrators to control AP power for optimum coverage. Network administrators can easily create virtual private groups to separate various user populations and filter their access based on security or activity. Group access can be managed by any number of attributes, including personal firewall filters, encryption types, QoS parameters, access schedules, and seamless or controlled roaming.

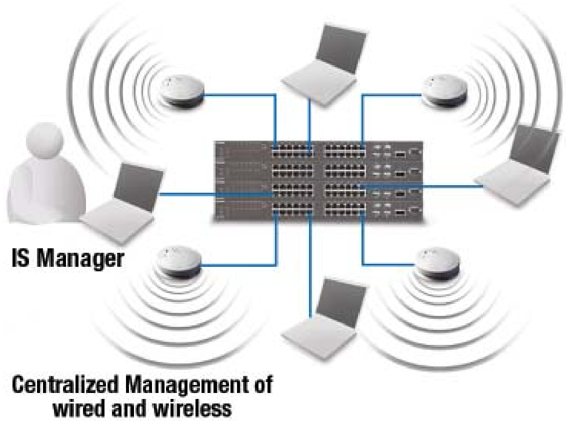
More specifically, the D-Link xStack 3200 series of wireless switches provide the rich feature set of the xStack managed layer two switches along with the ability to control up to 50 APs per switch/stack.

D-Link xStack 3200 Series

The xStack 3200 series is a unified wired and wireless switching solution that provides powerful wireless security, easy deployment, the ability to detect rogue access points, and centralized management for all compatible WLAN components. These switches enable secure, seamless roaming between access points ensuring clear, uninterrupted data and voice communication throughout your wireless network infrastructure.

Centralized Management

xStack 3200 switches centrally manage compatible wireless access points. Access points no longer need to be configured independently, and your entire wireless network can be managed through a single interface. The switches include support for automatic discovery, configuration and monitoring of APs so you can gain real-time visibility into utilization and performance of WLAN users and devices.



xStack 3200 Series Centralized Management of Wired and Wireless Functionality

Wireless Security

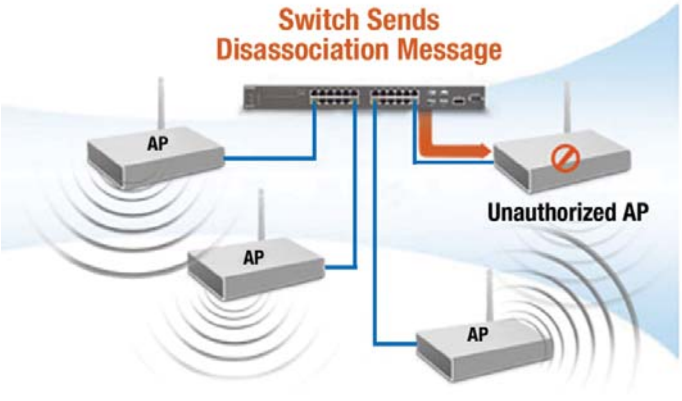
The D-Link xStack 3200 series switches include WEP, WPA™ and WPA2™ encryption to guarantee the privacy of your network data, and 802.1x authentication for secure network logins. Rogue AP detection and containment ensure only the APs you install are able to function on your network.

xStack 3200 Series Wireless Encryption Protects Network from Website Attack

The xStack 3200 series supports legacy WEP (Wireless Equivalent Privacy) encryption with static and shared keys of lengths of 64 and 128 bits. WEP encryption/decryption is useful for compatibility with legacy scanners, PDAs, clients and VoIP phones. The xStack 3200 series also supports newer WPA™ and WPA2™ encryption methods. WPA™ (Wi-Fi protected access) is more secure than WEP. It provides improved data encryption and user authentication over legacy WEP encrypted networks. The xStack 3200 series supports WPA™/WPA2™-Enterprise and WPA™/WPA2™-PSK. WPA™-Enterprise uses 802.1x key management and WPA™-PSK uses pass phrases for key generation.

In addition to encryption/decryption methods, the xStack 3200 series supports primary and backup RADIUS server for WPA™ and WPA2™ user authentication. To further improve security, the xStack 3200 services can only be administered from hosts residing in the wired network. Wireless stations are blocked from access to management interfaces of the switch.

Rogue AP Detection and Containment

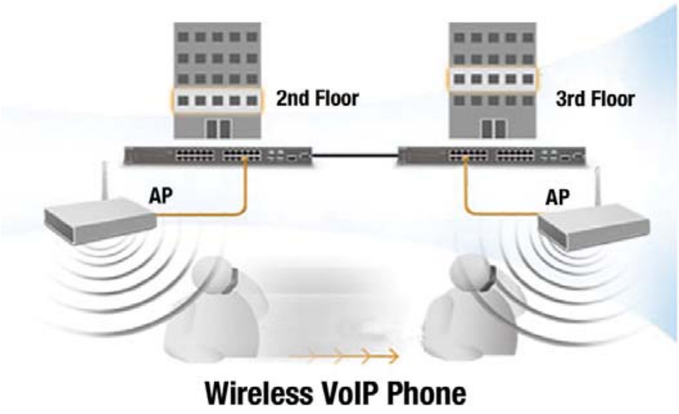


Rogue AP Detection Prevents Unauthorized Authentication to Non-network Access Points

The xStack 3200 Series supports Rogue AP detection and containment for enhanced wireless security and protection against attack. Radio-based rogue AP detection institutes continuous scanning of radio channels in an attempt to identify transmissions of unauthorized WLAN nodes. The xStack 3200 series switch scans and collects information about wireless nodes in their neighborhood and transfers this information to the central control point where it is analyzed, possibly triggering corrective actions. Possible actions can be notification of the network administrator, tracing and blocking of the physical port where the rogue AP is connected, and manual or automatic jamming of the unauthorized wireless network. If configured to do so, the switch will initiate jamming by periodically sending broadcast de-authenticate frames to the offending network mimicking the BSSID of the rogue AP.

Seamless Roaming

The 802.11 protocol supports mobility of wireless stations with Extended Service Set (ESS). ESS is a collection of 802.11 APs connected to the same broadcast domain of a wired network. Access Points announce their ESS membership by what is known as an SSID.



xStack 3200 Series Seamless Wi-Fi VoIP Inter-building Roaming

When a user roams between APs connected to different broadcast domains, the users IP address is no longer valid after the move to the new AP. This means the user's device (laptop, PDA, VoIP phone) will need to change its IP address, thus breaking the active session. With "always connected" devices such as VoIP phones and PDAs this can create a huge problem. The need for a solution to provide seamless roaming between APs on different subnets becomes essential to maintaining active sessions and VoIP calls.

The xStack 3200 series of switches address this problem by bringing AP configurations and support directly into the switch itself. This allows the user to move between access points (within a single stack of up to 16 switches) with seamless mobility. To the users PDA or VoIP phone, the move appears as if it were between APs on a single broadcast domain. This means the users device will retain its VLAN membership and IP address guaranteeing uninterrupted communication.

Supported Roaming Mechanisms

The xStack 3200 series offers a wide range of roaming mechanisms. The switches support roaming of wireless stations between APs connected to the same xStack 3200 series switch. Station VLAN membership and QoS are retained during roaming. The xStack 3200 series also supports roaming of wireless stations between wireless interfaces of the same AP – for example, roaming between 802.11g and 802.11a bands within the same AP.

In addition, the xStack 3200 series supports roaming of wireless stations between access points attached to different switches, even third party solutions. The seamless inter-switch roaming procedure allows a station's VLAN membership, IP subnet, and QoS parameters to be retained upon roaming between APs connected to multiple switches throughout the network. Inter-Switch roaming is an extremely beneficial feature when creating a large WLAN environment such as a campus or multi-floor office. Inter-Switch roaming allows the user complete freedom to roam between switches located in different buildings or on different floors without disconnection or need for re-authentication.

Interoperability

While the unified wireless features of the xStack 3200 series switch are intended for use with supported D-Link APs, customers may still have legacy stand-alone APs they want to use with the switch. The xStack 3200 series will support third-party stand-alone APs, however the wireless switch functionality will be limited when using third party APs.

WLAN Capacity and Performance

The xStack 3200 series provides support for up to 50 simultaneously connected access points (DS-750 license key required). Each of the up to 50 supported APs are capable of supporting 30 WLAN users. In addition, if using a dual-band access point supporting both 802.11a and 802.11g, a maximum of up to 600 WLAN users per switch/stack can access the WLAN network simultaneously.

The xStack 3200 series supports up to 256 wireless VLANs with flexible distribution of stations across different APs. VLAN operation is somewhat different in a WLAN environment than in a traditional wired LAN. Due to the mobility of wireless stations, assignment to a VLAN cannot be port-based. In a wireless network, a station is assigned a VLAN. This can be performed on an individual station or group of stations. Once assigned, the client may then roam between switches while retaining VLAN membership. In addition, wireless stations can be assigned to a dedicated VLAN devoted to wireless stations. This is useful for relatively small deployments, where it is desirable to separate wireless and wired traffic for security or traffic planning reasons.

With the xStack 3200 series switch, wireless stations can be assigned to a VLAN based on a number of criteria. This gives the administrator extreme flexibility in building the WLAN infrastructure. Such options include the ability to assign stations based on the SSID the station is associated to, the security suite supported by the station (such as WPA™ stations assigned to VLAN 1 and WPA2™ stations to VLAN 2), and user information such as user RADIUS authentication.

Support for Multiple SSIDs (Virtual AP)

Diverse populations of wireless stations characterize many WLAN deployments. Wireless adapters may come from different vendors, be different product generations, and certain stations may consist of dedicated devices with limited functionality, such as Wi-Fi phones or wireless cameras. In addition, some stations may belong to visitors, who can be provided with guest access to the Internet, but blocked from access to private network resources.

Different types of wireless stations and applications will have different security requirements and use different security schemes, while using the same physical WLAN network. Support for multiple SSIDs allows logical separation of different classes of wireless stations on the same physical wireless network. Station classes can be mapped to different VLANs for further logical separation of station classes in the wired network.

The xStack 3200 series supports up to 16 concurrent SSIDs (virtual APs) per access point. Each SSID can be configured independently with RF and security parameters, and different APs may have different SSID sets. For example, access points in the finance department may have configured different SSIDs than the access points in a public area. Multiple SSIDs also allow different classes of devices to be assigned different relative priority for access to the wireless medium. For example, SSIDs hosting Wi-Fi phones will be assigned highest priority, while SSIDs hosting guest users will have lowest priority, only consuming network resources when there is available bandwidth.

WLAN Management

With the xStack 3200 series switch, WLAN is supported on all management interfaces. WLAN management information is accessible and configurable through a variety of options including HTTP, HTTPS, Telnet, SSH2.0, and SNMP. This provides the user extreme flexibility in monitoring and configuring the WLAN network. In addition, all configurable parameters in the access point are accessible from the switch. There is no longer a need to manually configure each access point individually.

WLAN Monitoring / Logging

Status information collected for wireless stations is useful in providing visibility into a station's performance and help in troubleshooting of connection and performance issues. The xStack 3200 series provides a wide range of WLAN status information to assist the network administrator. Some of the supported information include:

- MAC address
- Connection status (authenticated, associated, failed authentication, WPA™ authenticated)
- Supported rates
- Rx and Tx frame counts
- Time from last roaming and the AP that previously served the station
- VLAN information
- Station's IP address

To further assist in troubleshooting, the xStack 3200 series maintains logs using the SYSLOG mechanism on WLAN events such as: user connection success or failure, station roaming, AP connection, error rates above threshold, and encryption errors. In addition, logging filters can be created to assist the administrator and reduce an over abundance of log events. Filters can be created for such things as: errors only, all events, per station, and per AP.

Radio Resource Management

System administrators deploying WLANs expect similar levels of reliability, availability and performance as wired Ethernet LANs. However, wireless environments present unique challenges related to the shared nature of the wireless medium. The xStack 3200 series incorporates a robust set of Radio Resource Management features intended to improve functionality of the wireless network.

The xStack 3200 series supports automatic channel assignment and can be configured to perform automatic selection of frequency channels for the connected access points. On a per access point basis, the channel can be assigned manually or automatically. If the AP is configured to have its channel assigned automatically, a channel is selected during the bring-up sequence. First the access point scans the different channels for other access points and noise sources. Second, the access point selects the channel that has the lowest noise level. Similarly, the xStack 3200 series also supports dynamic load balancing. Dynamic load balancing refers to the mechanism of distributing wireless stations and traffic load across APs with overlapping coverage. Load balancing decisions will depend on individual utilization of APs in the coverage area, stations proximity to the AP, and station location relative to other APs in the overlapping coverage area.

Conclusion

With support for centralized AP management, seamless roaming between APs, rogue AP detection and containment, and enhanced radio resource management, the xStack 3200 line of switches from D-Link eclipses the competition with the most advanced, feature rich, high-capacity product line in its class. Regardless of existing network design, the xStack 3200 series compliments even the most demanding network with support for a variety of applications from Wireless LAN switching to powering IP phones and cameras.

For more information about D-Link wireless switching solutions and related equipment, please call 1-800-326-1688 or visit www.dlink.com.