WI-FI: FAR AND WIDE

Secure and efficient network access while roaming requires an enterprise-class wireless infrastructure.

Executive Summary

For most organizations, limited wireless local area networks (WLANs) started out as a convenience — a simple way to let guests have an Internet connection while doing business onsite. That was then. Now, WLANs have become a critical resource for both staff and guest users.

Staff members are using an increasing number of wireless devices. In addition to notebooks, they are using smartphones and tablets as tools to read e-mail, manage contacts and calendars, and carry documents with them. What's more, organizations are developing their own line-of-business applications specifically for mobile devices.

BYOD is no longer just a hot buzzword; bring-your-own-device initiatives are a real trend. Everyone from the top down wants the ability to be productive, whether they're in the office or on another continent — and they want to be able to do it using their own notebook computer, smartphone or tablet.

TWEET THIS!

Table of Contents

In addition, staff and visitors working or attending meetings have a real business need for secure and effective Internet access. They must be able to connect to their own networks to retrieve and share information as well as to collaborate with the organization's users.

The Situation

Growth in the need – and demand – for wireless services has highlighted the often ad-hoc nature of how wireless networks have been deployed in buildings and on campuses. Network managers with meticulously designed and managed wired LANs are discovering that their wireless network's Quality of Service (QoS) doesn't match what users have come to expect from wired networks.

As increased usage puts stress on organizational wireless networks, staff members are discovering – and voicing concerns about – bandwidth bottlenecks, performance problems and coverage dead zones.

Security concerns are also driving technology and systems security managers to take a long, hard, look at both their wireless and wired infrastructures. In the current computing environment, users tend not to differentiate between wired and wireless access. Security policies and technologies, therefore, need to bolster protections at the point where users connect to the organization's systems and network infrastructure – no matter how they connect to it.

Benefits of an Enterprise-Class Wireless Infrastructure

Performance	With notebooks and tablets now capable of wireless speeds of 150 megabits per second to 300Mbps, an enterprise-class Wi-Fi network can offer users the same experience as its wired counterpart.
Agility	Wireless networks designed for near-LAN speeds can replace wired networks in some environments. This allows people to move into new permanent and temporary spaces quickly, both using time efficiently and reducing the expense of rewiring.
Flexibility	Wireless networks enable staff members, consultants and guests to be productive quickly in meetings, workshops and other collaborative spaces.
Mobility	Dependable wireless access is integral to any mobility strategy so that people can work when and where they choose. Users want the ability to collaborate and be productive without being tied to an office or desktop computer.
Security	Enterprise-class wireless networks offer a higher level of security than most wired networks.

Deploying an Enterprise-Class Infrastructure

To build an enterprise-class Wi-Fi network, an organization should follow a five-step process.

STEP 1: Identify requirements. Defining the needs of the organization's Wi-Fi networks begins with addressing two critical areas: coverage and security. Coverage defines where the wireless network will work and how fast it will operate. Security defines how users will connect to it and what access controls will apply to different types of users.

Setting the coverage parameters is not a simple matter, because different wireless uses require different types of coverage. For example, a wireless network that supports Voice over IP (VoIP) will need to cover more of a building space than one designed simply for use in offices and meeting rooms. Obviously, users will expect their phone calls to continue uninterrupted as they travel through hallways and staircases and between buildings.

Another coverage factor is speed. A wireless network designed to perform at speeds equivalent to wired connections will need a different layout of access points (APs) than one designed for more casual use or web-based applications. Defining what areas of each building will be covered and the expected performance at each point is a necessary starting point for developing any wireless strategy.

Meeting rooms and classrooms pose a special challenge for wireless networks because high densities – created when many users want to access Wi-Fi from the same location – require special engineering. As the number of wireless devices inhabiting a space increases, so does the difficulty of ensuring good service for everyone in that space. There are techniques that wireless engineers can employ to create the radio-frequency microclimates needed to sustain high densities, such as placing APs beneath the floor. Each room and building will require careful analysis.

Security for wireless networks, another hot topic, should be addressed early in the design phase. Although authentication and encryption capabilities of modern wireless equipment make Wi-Fi networks more secure than their wired equivalents, substantial misinformation about the security of wireless networks has made its way

around the Internet. Any network manager proposing deployment of a wireless network should be prepared to spend time educating peers and managers about the current status of wireless security.

Even when an organization's IT staff and stakeholders share an accurate understanding of the capabilities of wireless security, decisions must be made about how users will get access and the type of access they will be granted. With wireless networks covering a broad spectrum of use cases, most organizations will want to differentiate user classes — these might include groupings such as guests, staff and VoIP phones — and apply broad access controls based on class.

The most common technique for differentiating users is by service set identifier (SSID), the wireless network name announced by each access point. In many wireless deployments, each AP will announce three or more SSIDs, and users self-select a group by the SSID they choose.

More secure SSIDs require authentication; less secure ones (such as guest access) might be completely open.

The use of multiple SSIDs isn't the only approach. Some wireless products have other capabilities to differentiate users, such as applying per-user firewall rules based on group information returned by a Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS) server when users authenticate.

Deciding the number of user classes needed and whether to make use of multiple SSIDs are important early choices. Such decisions will significantly affect an organization's product selection criteria.

STEP 2: Site survey. The site survey plays an important role in the design of a wireless network by identifying the necessary number and placement of APs.

Few organizations have the specialized knowledge required to do a good site survey themselves, so an external team with special tools and expertise in wireless deployments often handles this step.

Although the software and tools required to perform site surveys are widely available, their cost and the amount of training required are usually prohibitive for all but quite large organizations. For most wireless projects, an organization should budget for an external consultant to conduct the survey.

The main inputs are the requirements for coverage, along with maps of the buildings being included in the Wi-Fi network. The maps should identify user density for each area covered by the network. Ultimately, the Wi-Fi network should aim for between -67 and -72 decibels per milliwatt (dBm) of signal strength in 90 percent of the mapped coverage areas.

Site surveys should be designed around 5-gigahertz APs (the 802.11a band) rather than 2.4GHz (the 802.11b/g band) APs, because the 5GHz devices have a smaller working radius. If the APs are placed where they will be needed to provide good-quality service in the 5GHz band, they will naturally also cover the 2.4GHz band. Designing in the other direction will result in gaps in coverage for 5GHz users, the most important population in enterprise Wi-Fi.

It's a safe assumption that any enterprise wireless network will use dual-radio (2.4GHz and 5GHz bands) APs and support the 802.11n standard to achieve the highest speeds possible. But a site survey should also note any older active 802.11b devices that will not support 802.11g or 802.11n. These can be a significant drag on performance of the network if they are not removed or blocked.

The product of the site survey will be a set of maps showing where each AP should be located. It's important to remember that the site survey is just an educated best guess. After deployment, APs might need to be moved, added or removed. When budgeting for the site survey, it's wise to include a post-installation check of the new network to ascertain how well the initial predictions of coverage match reality.

A site survey also should include analysis of the bandwidth capacity of the LAN and the impact of adding wireless APs. Modern APs can transmit at speeds up to 300Mbps and require Gigabit Ethernet connections. An upgrade of distribution layer switches or an increase in the number of Gig-E ports in wiring closets could be required.

STEP 3: Product selection. Following the requirements definition and site survey phases, many technology chiefs express a preference for simplifying acquisition costs and reducing learning curves by working with the vendor of the existing wired network. There's nothing wrong with this kind of thinking. But there are also good reasons not to merge wireless and wired networks too tightly.

Some vendors offer wireless controllers integrated into their wired-switch chassis. This type of tie-in should be avoided because it links any upgrades in either one of the networks to the other, which often increases complexity and causes unnecessary expense. This doesn't mean that an organization must exclude wired vendors when implementing wireless solutions, but it would be wise to select products with the intention of maintaining a clear separation between the wireless and wired infrastructures.

With wireless standards continuing to evolve, asking a vendor for a nondisclosure briefing on future products is crucial before making any product selection. There's nothing worse than buying 200 access points in June only to discover that the vendor will release a replacement AP with better capabilities in September.

Unlike the differences in new versions of wired LAN hardware, many of which may be unimportant to most users, any wireless AP change could result in a significant increase in performance or capabilities. Spending extra time peering into vendor crystal balls is a good short-term investment that can help an organization avoid making a bad long-term one.

STEP 4: Installation. Installing wireless equipment generally involves running additional cabling, adding patch panels and Power over Ethernet (PoE) in the wiring closet as well as testing, labeling and verification.

Wireless networks are less expensive to build and maintain than wired networks, but they're not free. Upgrading an entire building or campus with wireless infrastructure can cause sticker shock. Every building and situation is different, but typical costs for installation can be equal to the cost of the APs.

If bandwidth to wiring closets must be upgraded too, the cost could be even higher because equipment and fiber upgrades can cascade back to the data center. It's important to be prepared for such potential costs when developing a wireless budget.

Most of the time and expense during this phase will go into physical installation of APs, but there are other integration issues that also require time to work through. Enterprise wireless services always link to enterprise directories (such as Active Directory), so the network team must set up and test this connection and analyze possible failover scenarios. When including endpoint security checks in the wireless project (wireless Network Access Control or NAC), project managers should plan for additional time, vendor support and testing before setting users loose.

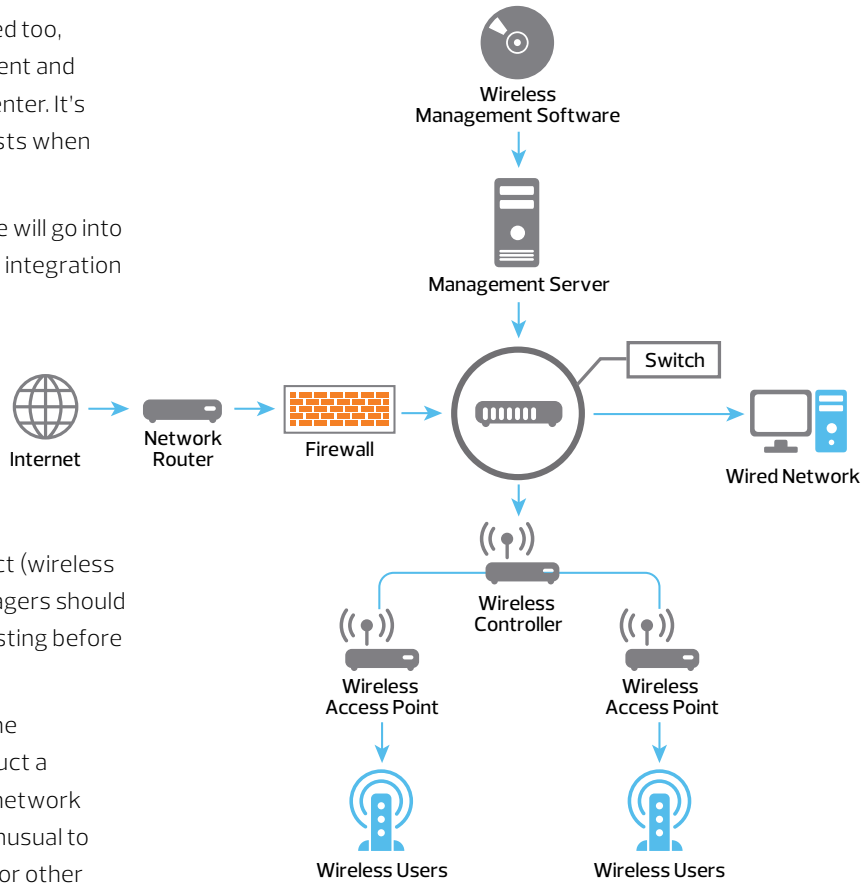
STEP 5: Management and Tuning. Once all of the APs have been installed, it's important to conduct a second site survey to verify that the wireless network performs according to requirements. It's not unusual to have to add or move APs to handle dead spots or other unanticipated issues.

The second survey provides an opportunity for the organization to train its network staff how to use a few wireless testing and debugging tools. No enterprise wireless manager should be without a spectrum analyzer and a Wi-Fi analyzer to help troubleshoot problems. Spectrum analyzers are inexpensive, starting at as little as $1,000 for professional-quality hardware and software. This tool will provide information that no built-in wireless card can offer.

Wi-Fi analyzer software can be used with standard built-in wireless cards on notebooks, although many vendors provide a custom wireless adapter, which offers greater debugging information, or a highly directional antenna to help location-specific devices. The Wi-Fi analyzer software can expose significant problems in wireless networks, such as excess retransmissions, corrupt packets and misbehaving clients.

The value of a good Wi-Fi analyzer is not just in its ability to sniff the airwaves — that can be done with a normal built-in

Components of an Enterprise Wireless Infrastructure



wireless adapter. Its strength is in its analysis of what is happening on the wireless network and its ability to boil down a lot of information into action items.

Organizations that have never had an enterprise wireless network also should invest some time in learning the management requirements of the new infrastructure. A training class or onsite consulting can help reduce the steepness of the learning curve.

Finally, it's important to remember that the network team must monitor the wireless network for performance and reachability just as it does its wired network. This may require adding the new devices to existing monitoring tools or setting up a dedicated system to watch over the wireless network.

It's also a good idea to schedule periodic site surveys every year or so to check on overall performance. Any environmental changes — repositioned furniture or replaced window coverings, for instance — could affect a wireless network significantly, and tweaks may be needed to assure continued high availability. Repeating the site survey yearly can identify changes to the network so that solutions can be implemented — hopefully before users notice any trouble.

Best Practices in Implementing Wireless Networks

Building wireless networks requires blending systems engineering — properly tuning radio frequency, for instance — with hard-earned knowledge. Although there are many ways to configure and use Wi-Fi, best-in-class organizations should apply these strategies to get the most out of their networks:

Practice active management: Wi-Fi networks don't stay in top condition on their own. The inevitable moves, additions and changes of people, furniture and everything else within an organization will cause the network to degrade over time and provide less-than-optimum service to users.

Wi-Fi networks are amazingly fault-tolerant. They can survive the loss of access points and the addition of interference without registering significantly perceptible effects. Problems might go unnoticed without active monitoring. Good network management practices, including the regular scanning of logs and the active monitoring of devices and usage, will help identify problems before they affect performance.

Use managed wireless products: The world of wireless changed dramatically in 2003, when Airespace (later acquired by Cisco Systems), Aruba Networks and Trapeze Networks (later acquired by Juniper Networks) developed wireless controller technology.

Before that, it was necessary to manage and configure each wireless access point separately. More important, any tuning of the wireless configuration — such as power levels, channel assignments or enabling hot-spare APs — had to be done manually. In addition to being difficult to learn and error-prone, wireless tuning is a continuous process that varies depending on the number of people in a room, the usage of the network and even the humidity level in the building.

But Airespace, Aruba and Trapeze developed technology that treated the entire wireless network as a single entity, rather than as a series of individual APs. Thus was born the fully managed wireless solution.

Since then, other vendors have entered this market with similar products. The technology today can handle issues such as mobility, keeping an IP address and connection alive while a user on a VoIP call walks between rooms, floors and even buildings.

When considering wireless management, the network team should be careful to distinguish between fully managed solutions and those that only offer configuration control and log collection. Simply capturing the configurations of each AP and pushing changes to them uniformly is not true wireless management. Although that is a useful function in some environments (such as branch offices with one or two APs), any deployment with more than eight APs will need a fully managed solution.

Prioritize usage: In the first few days after a network is turned on, the smartphones of at least 10 to 20 percent of the people in the building will connect automatically. These devices will consume bandwidth even when no one is using them. If the building is on a high school or college campus, that figure will be closer to 80 to 90 percent. In other words, a wireless network can reach near capacity even when no one is actively using it.

The solution isn't to prohibit casual use, but simply to make sure that mission-critical applications, such as VoIP (unified communications) or transaction processing, and business uses get priority over nonbusiness and casual usage. By using management configuration, firewalls or Wi-Fi Multimedia (WMM), it's possible to throttle bandwidth.

Develop a guest policy carefully: Accommodating guest access to wireless networks is generally considered a requirement for enterprise wireless installations. Guests commonly have a legitimate need to connect to the Internet while visiting an organization. Although some road

warriors may use alternative technologies, such as 3G or 4G wireless, to bypass local Wi-Fi networks, it is important to plan how other guests will connect to the organization's WLAN.

Of course, these guests shouldn't require much access to anything inside the normal enterprise network — printing, perhaps, being the occasional exception. Therefore, securing connections to ensure that guest users do not gain elevated privileges is important.

Any guest policy must balance its requirements for accountability and prevention of "drive-by" connections with the goal of making guest connections simple and quick. Many vendors offer specific guest services, such as captive portals and automated guest provisioning systems, that can ease the task of offering guests wireless connectivity.

Common alternatives, such as requiring guests to preregister Media Access Control (MAC) addresses or obtain a temporary user name and password, tend to be cumbersome and should be avoided. One bad result of a guest policy that is poorly developed or difficult to follow is that staff members might spend valuable time trying to get their visitors logged on to the wireless network. Or, even worse, a staff member might encourage a guest to connect directly to the internal wired network to bypass issues with the wireless infrastructure.

Build security from the start: Security managers tend to be fairly suspicious of wireless networks. If user credentials are all that is required to connect, then a stolen set of credentials could provide an easy pathway into the network via wireless or virtual private network (VPN) connections.

Many techniques exist to increase overall security for wireless users, but it pays to have the organization's security teams involved from the beginning. Doing so will make it possible to incorporate their requirements into the architecture design and product selection phases of the project.

For example, many enterprise network managers build wireless networks with separate firewall rules and inline intrusion prevention systems. Some wireless products include these features in their solution sets, while others require external devices. Depending on the organization's security architecture, one method might be more desirable — but discerning that requires collaboration with the IT security staff.

Network access control meshes well with wireless deployments because the wireless authentication standard — known as Wi-Fi Protected Access 2 (WPA2) — uses 802.1X, which is a convenient method for passing NAC information between clients and servers. Although NAC can add complexity to the wireless deployment, having a good solution in place as part of the network can be a first step toward eventual enterprisewide NAC deployment.

Thick Versus Thin APs

There's been confusion in the marketplace about whether "thin access points" are somehow better than "thick APs." Vendors have suggested that thin APs are less expensive, although they are about the same price — or even more expensive — after factoring in the cost of the controller. There's also a misperception that thin APs are a prerequisite to a fully managed solution, which is not true.

From an enterprise perspective, whether the APs are thin, thick or something in between is essentially irrelevant. What's critical is that the infrastructure is fully manageable, provides mobility services and optimizes the wireless radio-frequency network continuously.

There are important differences between vendors' fully managed wireless solutions. For example, wireless products do not integrate with the enterprise network in the same way. One major difference is the amount of traffic backhauled to the management controller. For some networks, bandwidth between wiring closets and data centers is essentially unlimited; but in other environments, there may be bottlenecks that require a different architectural solution.

Ultimately, evaluating what will and won't work for a particular network will prove much more important than gauging relative thickness of the access points.

Optimizing Network Performance with 802.11n

The publication of the IEEE 802.11n specifications was a turning point in wireless networking. It allowed enterprise managers to deploy wireless networks at speeds far above the old 54Mbps limit. Anyone currently considering creation of an enterprise-class wireless infrastructure should focus on 802.11n and eliminate any pre-802.11n equipment from the network.

The following strategies can be used to optimize performance of networks based on 802.11n:

Use 2.4GHz (802.11b/g) and 5GHz (802.11a) bands, but focus on 5GHz: Legacy wireless equipment often uses the 802.11b/g band, but it can be difficult to get good network performance in that band when 802.11n is deployed. The small number of channels available (three) in the 2.4GHz band means that the 802.11n high-performance 40MHz channels cannot be used.

For best performance, devices should employ the 5GHz band whenever possible. This assures that the higher capacity 40MHz channels can be used and that more devices can share the radio-frequency space in a smaller physical area. Those factors are critical for successful Wi-Fi deployments that involve crowded classrooms, conference rooms and the like.

Use 802.11n 3x3:3 access points whenever possible: Because 802.11n is a multiple-antenna, multiple-stream standard, user devices and APs can have from one to four streams.

Today, most devices supporting 802.11n have two streams and two antennas (2x2:2) or two streams and three antennas (2x3:2 or 3x2:2). These are limited to a top speed of about 13Mbps, or 270Mbps if double-wide channels are used in the 5GHz band. Newer devices coming on the market have three streams across three antennas (3x3:3). These have a top speed of 195Mbps, or 405 Mbps with double-wide channels.

The longevity required of APs makes it worthwhile to purchase devices that support three antennas and three data streams. This will extend an organization's refresh cycle.

Turn the power down: The most commonly ignored wireless advice is to keep power levels as low as possible. Wireless devices must share the same radio-frequency space. Therefore, additional power simply creates noise and performance slowdowns for adjacent devices and APs. Although wireless APs generally can support power of up to 100 megawatts, setting a maximum power level of 50MW or lower will yield better network performance.

If users report poor signal strength, the first solution should be to add another access point. It's rarely wise to turn up wireless power. A low power setting will increase the battery life of all wireless devices, especially smartphones and tablets.

Block low-speed access: When a device on the edge of the wireless network connects, the network will attempt to accommodate the user by reducing the device's speed. This impacts performance in two ways: The user has a slow connection, and this slow user could block wireless access for all other users for an extended period.

Enterprise networks should block clients from connecting at low data rates by increasing the data rate use for beacon frames (the 10-times-a-second frame that every AP emits to announce its capabilities) as well as the minimum connection speed allowed. The default should be raised above not only the commonly used 1Mbps and 2Mbps, but also over the old 802.11b rate of 11Mbps. This adjustment will have the desired effect of blocking old 802.11b devices from connecting to the network and causing performance problems.

Networks that have multicast applications, such as multicast video, should have their minimum data rates increased as well, although this requires more sensitive tuning that will depend on the capabilities of the wireless product selected.

Mobile Device Management

Mobile device management isn't tied specifically to organizational Wi-Fi, but many network managers consider it a required first step before letting mobile devices (including users' personal devices) connect to the enterprise network.

MDM tools provide the network team with configuration and security controls to manage mobile devices, such as smartphones, tablets and notebooks. The organization can then define policies and profiles for every device allowed on its networks. For example, a typical MDM policy could require that users establish passwords or personal identification number (PIN) locks that must be entered every time a device connects to the network. MDM software also provides the ability for the security team to remotely wipe or lock devices reported as lost or stolen.

MDM products have particular appeal within enterprise wireless programs, because their capabilities can extend far beyond security to include features such as software updates, data backup and restoration, application installation and controls as well as help-desk tools.

CDW: A Wireless Partner That Gets IT

Wireless infrastructure allows users to take the office with them wherever they go. The wireless network provides employees and guest workers with untethered access to voice, video, data and applications regardless of their physical location.

A well-designed wireless infrastructure can provide multiple benefits including:

- Reduced setup time and amount of cable required to outfit a location
- Greater flexibility that allows new and temporary users quick access to the network
- Improved collaboration and productivity
- Easier deployment and relocation
- Increased security

When considering the implementation of a wireless network, it is important to:

Perform a site survey – The site survey can provide a roadmap for designing the optimal wireless network, identify potential interference and coverage issues, and propose solutions to remediate any difficulties.

Address security concerns – Wireless networks authenticate users and encrypt transmitted data, making it more secure than a wired line.

Your CDW Account Manager and certified solution architects are ready to assist you with every phase of choosing and leveraging the right wireless network solution for your IT environment. Our approach includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed vendor evaluations, recommendations, future design and proof of concept
- Procurement, configuration and deployment of the final solution
- Ongoing product lifecycle support

To learn more about CDW's wireless infrastructure solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/wireless-infrastructure.

Cisco Gold Partner

Cisco wireless controllers help reduce the overall operational expenses of Cisco Unified Wireless Networks by simplifying network deployment, operations and management – extending the same Cisco Borderless Network policy and security from the wired network core to the wireless edge.

Cisco wireless controllers provide the visibility, scalability and reliability your organization needs to build highly secure, enterprise-scale wireless networks.

CDW.com/cisco

Cisco Gold Partner

Cisco wireless controllers offer more visibility and control. Features and capabilities include:

- High-quality mobile experience with efficient roaming capabilities
- Reliability with secure access
- Software license flexibility to add APs as needed
- Versatility to support advanced services

CDW.com/cisco

LANDesk SOFTWARE

The perfect balance between user flexibility and enterprise readiness, LANDesk Management Suite gives you all the control you need – no matter how big or diverse your environment – to address IT concerns in the 21st century. It enables you to discover devices in your network and store information on its configurations, OS, processor speed, installed memory, hard drive capacity, loaded applications and more in a central database. That information helps you optimize the systems under your umbrella.

CDW.com/landesk

Cisco Gold Partner

Cisco Ethernet switches securely deliver Layer 2 and 3 connectivity for voice, video and data networking. The offerings include:

- Modular and stackable models
- Power over Ethernet (PoE) switches in a variety of port densities
- 10/100 and 10/100/1000 access ports
- 1-Gigabit Ethernet and 10-Gigabit Ethernet uplink capabilities

CDW.com/cisco

TWEET THIS!

CDW PEOPLE WHO GET IT