Enabling Bring Your Own Device

Planning a Truly Connected Campus

Understanding Bring Your Own Device

The idea of bring your own device (BYOD) for connectivity has been well recognized in most networking environments. Yet some corporations are still struggling to understand its potential impacts. For them, the concept of users attaching privately owned and managed smartphones, tablets or laptops to their secure networks is a relatively new and worrisome concept. However, it is a challenge that customers in higher education have been dealing with for years as students have increasingly turned to easy-to-connect and affordable laptops as study aids.

While corporate and educational networks may share some similar concerns about BYOD, in the end the unique nature of academia (such as research, testing and the need for extensive mobility) create additional barriers that must be overcome. The very nature of higher education today requires that students have the ability to collaborate reliably and securely to empower the sharing of ideas. Combined with locations outside the classroom where BYOD might be utilized for learning, such as cafeterias, fitness centers, social events and sports venues, use of the technology is allowing students the capability to “live where they learn” in the truest sense.

To help improve understanding of BYOD and its impacts on modern network environments, this white paper will further explore the many differences that exist between corporate and educational approaches to the technology. We will also detail education-specific cases and take a deeper look at the evolving needs of wired and wireless network access by academia.

© 2015 Cisco and/or its affiliates. All rights reserved.

Introduction

Device Management

In corporate America, laptops are still usually pre-installed with standard software and operating systems (also known as the desktop image) before distribution to employees. This approach often limits what additional software can be added by the user, providing some perception of security for the corporation and its network. However, it usually also requires the hiring, staffing and training of a permanent Help Desk to provide support when things go wrong. Thankfully, due to the strict control and minimal deviation in device profiles among all users, this support can focus on just a few issues that may regularly arise.

For corporate BYOD users however, the desktop image is usually self managed. They might have to install device management software or access a virtual desktop where their corporate applications safely reside. This turns their device into a simple terminal, or window, to the corporate environment. These methods provide a certain amount of control for corporations in a BYOD environment. Even if a virtual desktop or device management software isn't used, there are usually a finite number of mandatory applications one is required to use in order to do their job. Corporations will usually limit their support to these officially-supported applications.

In the education space, dealing with non-standard, user-managed devices has been and still remains the norm. Unfortunately, the variety of devices means a multitude of operating systems and software are encountered, with many "standards" being defined. As a result there is little consistency in the device type or the software being installed. Since the device is owned by the student and is a personal resource, it is often difficult or impossible to enforce a policy that prevents users from installing software. In addition, due to the nature of learning as opposed to a corporate environment, it is also difficult to put a restriction on certain classes of software since all may provide a worthwhile educational purpose.

Administrative Issues

In schools that require students to purchase a particular device as part of their condition for enrollment, students generally have administrative access to the computer. This allows them the freedom to install software and reduces the "standard" nature of the device. As the number of non-standard devices increase, attempting to centrally provision each device may not scale due to strain on support desk resources.

In addition to students, faculty and staff, schools and universities have a wide variety of guest users in their facilities. This can include parents, visitors, alumni and conference attendees. For these users, access to the network allows them to be more productive and comfortable at the institution. But on-boarding can often be a difficult or frustrating process. That’s why it is critical for institutions to develop a simple and robust method that automatically facilitates on-boarding and configuration. Any such solution should be able to handle the large number of student and guest devices without overwhelming help desk resources.

Wireless vs. Wired

Wired connections are still being used today. However, the preferred method of connectivity has shifted dramatically to wireless. In the past, having a device with a wireless connection was a desirable option. Today, devices (especially mobile devices) may only support wireless connectivity. Wireless was once a “nice to have” technology available in select hot spots. But now Wi-Fi access is nearly universal, with people being able to connect at almost any public and private location.

Although wireless is important for end user connectivity, the wired network is still essential for delivering these wireless services. Wired devices typically have greater functionality with regard to advanced features for traffic management, switched network device access and troubleshooting. Having similar capabilities in the wireless environment is considered very beneficial. So providing a solution that unifies management and deployment polices across both wired and wireless devices is very desirable. By using a single approach, schools and universities increase operational efficiencies and reduce the overhead associated with managing two distinct networks.

The Internet of Everything (IoE) has spurred a revolution in mobility. Collaboration anywhere, anytime and with any device is quickly becoming the rule instead of the exception. As a result it is now common for students to bring mobile devices such as smartphones, tablets and e-readers into the academic environment to support their educational endeavors. For schools with residence halls there is an added dimension: the need for a network capable of handling literally hundreds of real-time connections to gaming systems, streaming players and smart televisions. This need will soon expand to include a multitude of wearable devices, all of which require a stable and secure network connection. For the successful delivery of education content in the classroom, we are finding that the requirements are quickly expanding beyond merely re-creating “home” in a single dormitory room. Home must now include the entire campus.

Application Usage by Students and Faculty

Over the past five years the number of mobile devices with only a wireless connection have increased astronomically. Much of this is being driven by the development of new and interactive applications, or “apps”. The abundance of these specialized, and often

© 2015 Cisco and/or its affiliates. All rights reserved.

custom made, apps is leading users to carry multiple devices with them instead of a single device. And they all have one thing in common: the capability to generate and consume an increased amount of bandwidth. Mobile devices are now regularly tasked with streaming audio and high definition video from the web. Video conferencing and teaching applications are quickly becoming critical components of the modern teaching methodology. Plus mobile devices are now capable of recording and uploading high definition video to users around the world via a variety of applications, both academic and social in nature.

Wireless deployments in support of BYOD originally focused on providing radio frequency (RF) coverage within an area using open, unsecure connections with networks being used to access both public and private resources. But that focus has shifted due to private resource security concerns. Users and devices at the network level can now be identified, authenticated and provided secure access to only the resources they require. This lets applications secure private resources but does require that the network be able to determine if and when sensitive information is being compromised.

The infrastructure supporting BYOD no longer has the sole purpose of providing a wireless radio signal within a given area. The focus is now about providing the appropriate bandwidth and quality to accommodate the ever-growing number of devices and ensure that an application provides a good end-user experience. In a sense, applications are now the major driving force behind the continuing evolution of BYOD. Because bandwidth is limited, one must ensure that users and devices are able to access the required resources with the appropriate priority in a given amount of time. For example, a teacher accessing video in the classroom for educational purposes during class hours should have greater priority than a student in the same area accessing a gaming site for recreation.

The world has witnessed a sea-change in how users connect, store and access applications themselves and the data created with them. Instead of applications running locally on a device, the are often leveraging resources in the cloud or in a remote data center. This is true for both recreational apps as well as those essential to education, such as learning management systems, as well as curriculum development and management.

© 2015 Cisco and/or its affiliates. All rights reserved.

A BYOD Approach for America's Campuses

The Classroom: Differentiated Access

The requirements for BYOD in education have changed significantly in just the last three years. A state-of-the-art BYOD infrastructure should now be capable of providing more than just generic, general-purpose wireless connectivity. In the classroom environment, the notion of "differentiated access" often resonates with faculty and staff. This means that not all applications and access to them should be treated the same. One should take into account several aspects when differentiating between types of access, including:

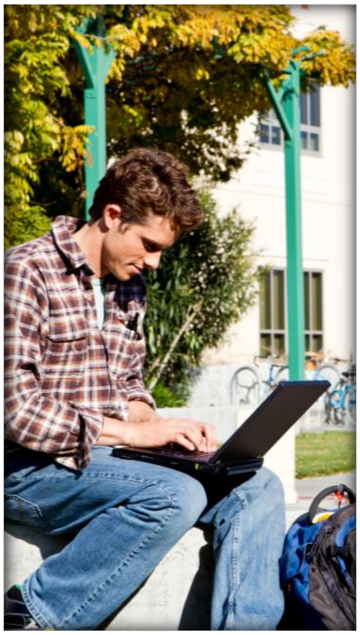
- Person accessing the information (professor, student, contractor or visitor)
- Type of device being used (laptop, mobile device, e-reader, etc)
- Owner of device (school or personal)
- Resource or application being used
- Location when accessing resources
- Time of network access
- Necessity of access to education.

Once this has been determined, a policy can be applied to the user and their activity on the network. Not only can we determine if a user should have access to a resource, we can also employ sophisticated ways of controlling that access. A good illustration of this capability is giving teachers that access video based curriculum material during designated classrom periods a greater priority than a student accessing recreational video. Another example would be guaranteeing higher priority for Internet cloud-based assessment applications over other applications.

In addition to categorizing priority, policies for managing bandwidth utilization can also be created. Quality of Service (QoS) rate limiting has been available for some time, but now there are newer QoS techniques available. Instead of arbitrarily saying that every user can only access a certain about of bandwidth, we can go further and define users within a particular group to access bandwidth in a fair way, such that those using more bandwidth will get rate-limited first, as new users within that group join the network. This ensures that everyone gets their "fair share" of the network resources, preventing users from consuming all of the bandwidth during times of congestion. This allows for the ability to restrict heavy uses during periods when the network is under high usage, and allows them to consume as much as they would like when overall usage is normally lower. The notion of doing this type of bandwidth shaping was previously only possible by deploying a device at the WAN edge, which would often become overloaded. But now this capability is available at the point where users first connect as well as throughout the network infrastructure.

© 2015 Cisco and/or its affiliates. All rights reserved.

Granular security can also be intelligently delivered. Traditionally, devices would be arbitrarily put in a network group based on the location in the network where they connect. They were able to see and access all resources within those network segments and security relied upon network segmentation to restrict access. Policies were written to allow one IP address or network to access another. But it is now possible to have more sophisticated policies based on identity. Once a user has been authenticated to the network, their traffic can now be tagged based on intelligent organizational groups; assigning policy classifications from the moment they connect to the network. It is possible to attach this tag at the point of entry to the network and independently of the IP address. Access policies can also be generated using organization-based labels instead of network abstracts. So instructors could have access to a particular resource that students do not. This same policy can be applied whether the individual is connecting with wired or wireless. These types of polices can also be designed to follow the user as they relocate, regardless of IP address changes.



Student Housing: Creating a Wireless "Home"

For student housing, the challenge is different. Students are accustomed to the type of connectivity that they have experienced at home. Typically, within their homes, their devices used simple security but could only be seen and accessed by people within the four walls of their home. In a dormitory environment or similar student housing, their "home" is the entire building and their "family" includes hundreds or perhaps thousands of the other residents. Because of the large number of users involved, services are often broken into a large groups consisting of a single wireless domain, which maps to a single dorm network on the wired side. Neighbors can easily see each other devices within this shared multi-tenant living space. At the same time, wireless traffic can be tunneled to a centralized controller. This means that devices that connect via a wired connection are often on a different network than those connecting wirelessly. This can prevent one student's device from communicating with another, even in the same room. For students this can be a frustrating and unfamiliar experience leading to support calls.

Many consumer devices and applications still rely on a "four walls of the home" concept for security. This often fails in dorm environments because consumer solutions do not take into account the typical dorm deployment model because they put ease of access and connectivity first. As a result, the four walls concept needs to extend to every resident in the dorm.

As with classrooms, bandwidth management for student housing needs to be considered. As the number of users and devices in dorms increases, the possibility of

© 2015 Cisco and/or its affiliates. All rights reserved.

network contention for the finite bandwidth available also increases. In the classroom example, having newer quality of service methods that ensures that everyone gets their “fair share” of bandwidth works better than imposing fixed rate limits per user. As more users connect to the system, those that are currently using more bandwidth get restricted more than those that are using fewer network resources. This helps ensure a good end user experience for all and is a workable model for student housing.

A BYOD system should be able to provide a network that can mimic the home-like environment so that a user can only see their particular devices or any device that is connected to their virtual room. Registration and security mechanisms should be developed that provide granular access to devices, allowing owners to regulate access by others. By limiting visibility by the entire network of users, the expsoure to outside threats is also reduced. This provides greter privacy and a more secure experience for students.

In a home environment a device is plugged directly into the home router or connected via wireless. Regardless of which method is used, performance usually remains the same and both devices are able to communicate with each other. For students experiencing dormitory living, this is also the expectation. To help students transition to their new home and gain the maximum benefits from their educational experience, this same expectation should, and can now, be delivered in student housing.

Around and Off Campus: Enabling True Connectivity

The student athlete must travel to away games and remote practice facilities. The time spent in transit could become more productive if access to campus resources were still available. Thanks to the Internet of Everything (IoE), athletic buses can now be equipped with network connectivity and provide campus Wi-Fi access to student athletes on buses. This network router can also provide a secure connection via 4G backhaul to campus, ensuring users a secure experience while traveling. In addition, the router can implement the same policies and access methods as the student would have on campus. This router and wireless network can be centrally managed with the same tools as those used for the devices located statically on campus. Plus, rather than each student having to create a secure VPN connection to access campus resources, the network on the bus can be a mobile remote extension of the campus network, while still providing the same security of the on-campus environment.

In K-12 environments, the application of such technology provides connectivity for learning with peace of mind by delivering a safer environment for students and greater sense of security for parents. The system can provide student-tracking services for parents based upon the location of their 1-to-1 device or a wearable device, such as a

© 2015 Cisco and/or its affiliates. All rights reserved.

student ID. School buses can also be outfitted with a fleet management system so that the location and status of the bus can be tracked. The telemetry and vehicle information can also relay information about the driver's behavior, such as length of time spent at each stop, abrupt braking or even speeding. In addition, a fleet vehicle's position can be tracked to indicate if it has deviated from its normal route or is subject to a traffic delay. From the time the student is within physical range of the school bus to the time they set foot inside the school building, the student's location can be tracked. This information can then be accessed by the students guardian via text alert on an app – even on a smartphone.

In addition to the location services, cameras can be deployed inside a bus to monitor student activity. This video could be securely streamed to the school in real time via the 4G WAN in order to help reduce incidents of bullying, harassment or other unsafe behavior in transit to and from school. By equiping buses with wireless video, drivers can be freed to focus on the road – and the safety of those they are transporting – rather than dangerous distractions caused by students that could end in a vehicle accident.

Use of Location-Based Services

In addition to general connectivity, an advanced BYOD solution should be able to provide various services based on location. Location-based services have a wide array of application in the education space.

In the college environment, visitors such as parents or prospective students are a common sight. Location-based services can provide their first interaction with the university. By delivering campus maps and directional information, location-enabled services can enhance the experience of these visitors and provide a positive image to them as well. As a visitor enters a particular building location, information could automatically be provided. In the case of a visiting student, information about the history of a building, departments contained within the building, or other resources could be presented to enhance a guided tour, or provide the perspective student the ability to have a self-directed tour of the campus facilities.

For the K-12 environment, in addition to providing the visitor information, these location-based services can improve security be tracking them as well. Once a visitor has registered and been issued a Wi-Fi enabled visitor ID, their location can be tracked throughout the school. They can also be tracked via their personal device.

By issuing visitors, students and faculty a Wi-Fi enabled badge system, their safety and security can be increased tremendouly. In an emergency situation the badge can be

© 2015 Cisco and/or its affiliates. All rights reserved.

activated to alert security. This feature can be as simple as seperating the badge from its lanyard to instantly send the location of the incident to appropriate personnel. An alert can also be sent if the wearer is not in an upright position. With Wi-Fi enabled badges there is no need to dial a phone, find a security officer with a radio or yell for help. The result is increased response time and a more positive outcome for those involved.

Location-based services also extend beyond security to information. The approach also allows students to receive information about specials in the dining hall, special offers at the campus bookstore or upcoming events. For alumni returning to campus, location-based services can enable rapid re-integration by providing the information, news and mapping they need to feel right at home. And BYOD can be used to push information to users. This creates tremendous opportunity to build a sense of community in a secure and very affordable way.

Cellular Connectivity

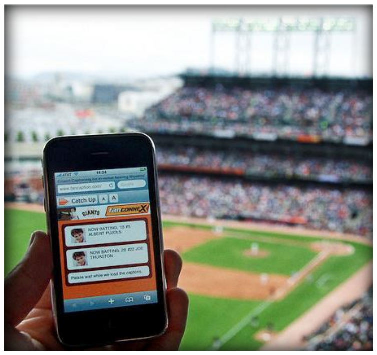
The delivery of voice communication services within the school environment is experiencing great change. In the past, coin-operated pay phones at the end of the hall were the primary method for students to call home. These gave way to college-provided room phones. Today students control the technology themselves - with mobile cellular devices.

Traditionally there are systems for providing Wi-Fi coverage and separate systems that act as a cellular repeater. In today’s academic environment however, that is becoming less viable. Deploying these systems independently brings a whole set of challenges. There is often duplicate physical cabling required, separate modifications to accommodate internal cellular antennas and labor to install separate mounting brackets. Plus there is the need for separate power and management systems. But a single wireless system with the capability to simultaneously provide both cellular and Wi-Fi coverage removes these obstacles.

It is important to understand that today’s students prefer to use their own mobile phones, rather than school or privately owned landlines, for communication. Mobile phones have become a reflection of the owner’s mindset and an extension of their personality. Due to the convenience of having a single mobile device that gives them instant connectivity with family and people on campus, students have helped drive traditional landlines to near extinction. Schools are taking note and are adjusting appropriately. Most schools no longer provide residential dorm room phones unless specifically requested. As this trend continues, the concept of a desk phone will likely end like that of pay phones.

© 2015 Cisco and/or its affiliates. All rights reserved.

Although these devices can use Wi-Fi for a variety of applications, such as video chat and messaging services, they still provide traditional voice calls and SMS (text) services using cellular signals. As the shift towards the cell phone as the primary means of communication solidifies, the delivery of reliable cellular coverage with the bandwidth to handle the density of users in a dorm environment is becoming more critical. For students, being able to receive a strong and reliable cellular signal from within the walls of student housing is no longer an option – it is a necessity.


14:24
www.fancaption.com/
Catch Up
A
A
GIANTS
FANCONNEX
NOW BATTING, 1S #5 ALBERT PUJOLS
NOW BATTING, 2B #22 JOE THURSTON
Please wait while we load the captions.

At Major Venues: Connecting Stadiums, Auditoriums and Student Unions

In addition to the campus and dorm environment, schools often have areas where large numbers of users congregate. Large common meeting rooms in student unions are heavily used on the nation’s campuses and it is not uncommon for lecture halls to accommodate several hundred students throughout the day. In a campus BYOD environment, a system needs to be able to address these and other high density locations by providing connectivity for large numbers of users and effectively managing utilization to ensure everyone connected has a high quality end user experience.

Stadiums provide an additional set of challenges and opportunities. Due to their massive capacity, high ceilings, multiple gathering spaces and mix of construction materials, stadiums are some of the most challenging environments to implement a BYOD solution. As more stadiums and concert venues are providing an enhanced customer experience, expectations are changing. It is no longer sufficient to merely provide connectivity. Attendees are now becoming more accustomed to an interactive experience within the venue. Electronic ticketing, real time access to video and audio simulcasts, wayfinding and information distribution are being incorporated into the fan experience.

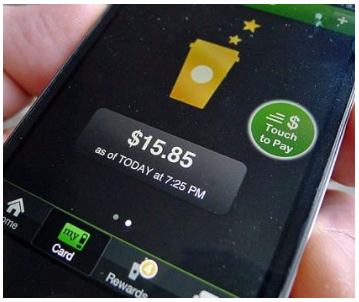
These enhanced BYOD deployments not only improve the experience for attendees but also provide increased capabilities to the venue. Venues can now push promotional information, gift shop offers, special deals at the concession stands and opportunities to purchase or upgrade tickets directly to the fan. By providing this enhanced fan experience, venues now also have the opportunity to pursue new avenues to push content plus create new sources for revenue.

Enabling the Digital Smart ID

The smartphone has become the quintessential multipurpose device. It is no longer used solely for audio communication. It is a small portable computing device that can be used for a variety of other purposes and is limited only by the device’s hardware capabilities and those of the applications installed.

© 2015 Cisco and/or its affiliates. All rights reserved.

In addition to being a source of communication and entertainment, the smartphone is beginning to replace credit cards for payment and badges for identification and access. This evolution is also being driven by applications that can serve as virtual storefronts and can consolidate rewards cards virtually as well. This trend has continued with airlines, insurance companies and a variety of other entities that are replacing traditional paper or plastic ID cards with smartphone based apps.



In addition to identification, apps on the smartphone are also changing the way we pay for purchase and access physical spaces. With Google Wallet and Apple Pay, mobile users can pay for purchases without the need to carry cash or traditional credit cards. Even door lock manufactures are producing smartphone based entry options that work alongside traditional physical keys or keypads. This race to mobile ID is extending to automobiles as well, as manufacturers have begun developing and distributing smartphone apps to unlock car doors when your hands are full, lower windows to cool interiors on a blazing hot summer day or start the ignition and begin heating the car interior in the dead of winter.

Though smartphone based campus ID, one payment and physical entry systems are not yet widely deployed, there are many early adopter schools that have begun to deploy these capabilities. As the trend in the consumer world moves further in this direction, schools must be prepared to support similar applications within the campus environment. To do so, institutions must begin to lay the groundwork now that will ensure a stable and secure wire and wireless infrastructure for decades to come.

Empowering Flexibility for the Future

Minimizing Upgrade Impacts

The ability to perform major network upgrades is quite challenging in the educational environment. Educational institutions are operating under very tight budgets. Often funds are unavailable to make frequent major investments to upgrade network equipment. In many cases, the IT staff is stretched thin, trying to do more with less, and doesn't have time to implement major changes. While there are limits due to budgets and personnel, there are often also very tight time constraints. Schools have a very limited window of time each year to perform network upgrade tasks. Often the only times are when classes are not in session. Though there are breaks for holidays, many schools have summer or winter sessions that minimize these opportunities to upgrade; creating a situation where the network needs to be "always on". For these reasons any BYOD solution being considered needs the flexibility to address future requirements in an incremental fashion, minimizing the cost and disruption to the network.

© 2015 Cisco and/or its affiliates. All rights reserved.

802.11ac Technology

Although 802.11ac Wave 1 is currently in use, it is just a step in the continued evolution of wireless and BYOD. As it evolves it will deliver data rates greater than 1Gbps to each wireless client. This increased throughput will naturally result in new applications, capabilities - and questions. For example, will the access point 1Gbps uplink become a bottleneck? Should installs include additional cabling to accommodate future requirements? Or will current access points and switching infrastructure need to be replaced? A well thought-out approach to BYOD should have the ability to adapt to these and other emerging concerns. If possible, this should be planned in such a way that will avoid major investment in rewiring or wholesale replacement of materials and equipment.

Software Defined Networking

Software Defined Networking (SDN) is another networking trend that promises great flexibility for users. It is already beginning to see early adopters. Various applications have always traversed the network so SDN offers the capability for these applications to be used to dynamically modify the network configuration. SDN promises a wide variety of possibilities in the future. Though it is still early, a strategy for BYOD should be able to address these requirements as they arise.

Device Life Span

The consumer driven nature of the bring your own device boom is serving as a catalyst for change and an opportunity for future flexibility. Many consumers want to have the latest offering on the market. Nowhere is this better exemplified in the BYOD environment than with the mobile device; in particular the smartphone.

Smartphone manufacturers typically design a product toward a 4-year product life cycle. The Apple iPhone 4 was first released in June 2010, running iOS 4. The phone was discontinued for sale in September of 2013. Then the final release of software for this platform, iOS 7.12, was released in June of 2014. As of November 2014, the current release of iOS is 8.1. This version of iOS does not run on iPhone 4 and requires the iPhone 4S as the minimum hardware. Though an individual may continue to use the iPhone 4, they will not have the ability to upgrade the software to gain features available on newer models or to conditionally receive any future bug or security updates.

Although manufacturers plan a 4-year lifecycle, the average user will probably refresh their device before this time. Some industry groups estimate the average actual life cycle of a smartphone may be as short as 2 years. End users, especially students, clamor for the newest cool device with the latest features. Older smartphone devices

© 2015 Cisco and/or its affiliates. All rights reserved.

are usually unable to run newer operating systems with these enhanced features. Even if they can, it will not work as effeciently and merely frustrate the user. As a result, the ongoing desire by users for new fully functioning features is and will likely continue to reduce the time between user-determined device upgrades.

Consumer driven demand has a tremendous impact on the market for mobile devices. Providers have even changed their contract models to adjust for this. In the past, providers would lock users into owning a single device for the majority of their contract term and then provide the phone at a reduced cost or for free. In return, the consumer would agree to be locked into a contract for some length of time. This would leave the consumer unable to upgrade their mobile device until the end of the contract. It would also leave them with outdated technology they could not rid themselves of.

However, due to increased competition among providers, phone number portability and consumer demand, many of these restrictions have changed. Providers now have contract models that allow customers to upgrade at an earlier time without penalty. This is being done to keep customers from breaking their contracts and fleeing to a better device at a better price.

These new buying patterns mean that newer devices, with increased capabilities, are being adopted even more quickly. This is happening at a rate that easily surpasses the rate at which schools and universities perform major upgrades to their network infrastructure. While smartphones are greatly impacted by this due to their salience, this trend holds true for any consumer device that could be brought into the academic environment (i.e. tablets, gaming consoles, etc.). Any major investment in BYOD must take this into account and provide a way to adapt and meet the needs of the next wave of consumer desired technologies.

The Next Big Thing?

The next big thing in BYOD is not limited to hardware. Software and apps used on the smartphone also have a great affect. With many apps available for free, or at very low cost, there is very little preventing users from exploring new applications. In addition, with the cloud centric nature of apps, new network traffic patterns and bandwidth requirements are occuring. Several years ago, very few would have predicted the proliferation of streaming audio and video services that exist today so BYOD infrastructure deployed should be planned in such a way as to anticipate a similar evolution in the years to come.

Based on past purchasing trends it is likely device manufacturers and end users will adopt newer technologies, such as 802.11ac, at a faster rate. Though one cannot

© 2015 Cisco and/or its affiliates. All rights reserved.

purchase future technology, whichever systems are decided upon today should be flexible enough to adapt to the ever-increasing rate of change in the BYOD landscape.

Conclusion

Having access to wireless connectivity in today’s world is almost a given. Wi-Fi is nearing the point of being universal. It is not uncommon for most homes to have their own wireless network. If one has a home cable modem service, they can also usually connect to Wi-Fi via the same provider anywhere throughout their community, if they desire. Railroads, commuter trains and buses are even providing wireless connectivity for their passengers. And airlines are actively marketing wireless connectivity, including with pay-per-view on demand movies, in-flight.

The fact that wireless availability has become so common has instilled certain expectations in the minds of consumers and users of educational networks. Whether student, faculty, visitor or alumni, they expect connectivity equal to or greater than that experienced in their homes. Merely providing connectivity is no longer good enough. A well-designed BYOD solution should exceed the expectation of the users. It should address the business needs of educational institutions and not just be a replacement for wired connections. Wireless and the next generation of BYOD should be the enabler that provides new applications and enhanced capabilities to improve the overall academic environment and opportunities for America’s students.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco and/or its affiliates. All rights reserved.