WIRELESS SOLUTIONS FOR

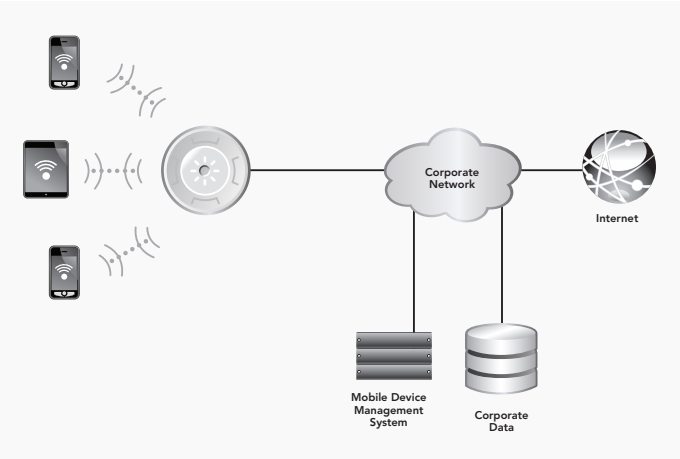
Tablets and Smartphones

XIRRUS®

High Performance Wireless Networks

Tablets and smartphones. Challenge or opportunity?

The proliferation of smartphones and tablets in the consumer space is quickly working its way into enterprise networks. Users are falling in love with their mobile devices and are pushing to bring the convenience and productivity these devices provide into the work place. Laptop shipments have surpassed desktop shipments, smartphone shipments have surpassed laptop shipments, and the number of tablet shipments is expected to grow 1,100% over the next three years. In short, users want mobile devices.



Supporting the influx of mobile devices presents a challenge for IT — but also a huge opportunity. Despite some of the challenges with supporting tablets and smartphones, most companies are looking at how to support the growing requests from their end users. Seventy-five percent of enterprises already have a "bring your own device" policy in place (many include tablets) according to Aberdeen Group and Gartner predicted that "by 2014 90% of organizations will support corporate applications on personal devices."

There are some challenges with supporting tablets and smartphones, but if the steps outlined in this document are followed, IT personnel can lower capital expenditures and have happier, more productive end users.

Tablet and smartphone challenges for IT:

The influx of new devices creates three main challenges for network administrators:

1. Maintaining and growing your high-performance wireless network
2. Creating a secure environment for mobile, non-corporate devices
3. Providing appropriate resource access

Maintaining high performance

Most wireless networks were designed as an overlay network to the wired infrastructure and were not designed to support large numbers of users (i.e., high user density). Wi-Fi is a shared medium, so the more devices on the network, the higher performing the network needs to be. Before allowing additional devices onto the wireless, networks need to be upgraded to ensure sufficient bandwidth and network processing power to handle the increase in traffic loads.

Creating secure environments

With mobile devices, two main aspects of security need to be addressed. The first goal is to ensure that only the people and devices that need to be on the network are allowed on the network — user authorization and authentication. The second goal is to be sure that devices getting on the network comply with corporate policies — network access control.

Providing appropriate access

Just because a user/device can have access to a network doesn't mean that that user/device should have access to all of the elements of the network. Proper classification and segmentation of the network must be implemented.

"Enterprise IT departments can save between 10% to 40% in capex by allowing employees to bring their own devices to work."

GARTNER

Key benefits:

- Higher performing networks
- Happier employees
- Lower capital expenditure

Key features:

- Multi-radio access points
- Device identification
- Per-user policy enforcement
- Easy network integration

Recommended actions:

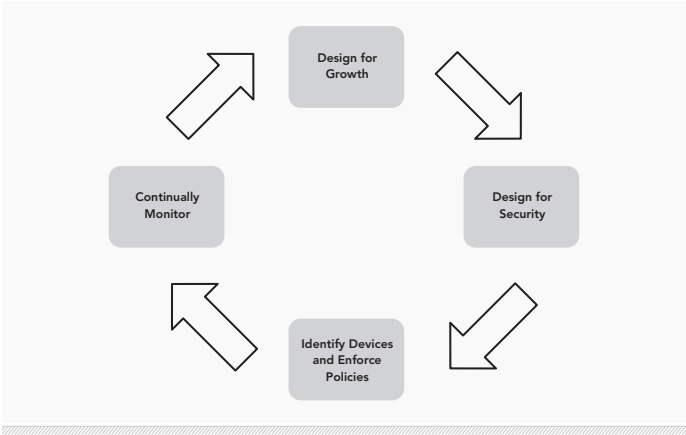
- Design for growth
- Design for security
- Identify devices and enforce policies
- Monitor and adjust network provisioning

Design and manage better wireless.

To handle more end-user devices properly, and to support bring your own device (BYOD) policies on a wireless network, four key steps must be followed. Those steps include the following:

1. Design for growth
2. Design for security
3. Identify devices for policy enforcement
4. Monitor and adjust network provisioning

As with any network design, these steps should be reviewed and redone on a periodic basis if necessary.



Design for growth.

As more devices use the corporate wireless network, the network needs to be able to handle the increased utilization of network resources. This can be accomplished by providing more bandwidth and/or by limiting the bandwidth utilized by each device. Xirrus allows enterprises to add more bandwidth by providing multiple radio access points (i.e. Arrays). Xirrus also allows maximum utilization of Wi-Fi bandwidth by using multi-state radio. All radios in the Xirrus Array can be moved from 2.4GHz to 5GHz to utilize fully the additional spectrum available in the 5GHz space.

It is ideal to provide more bandwidth for end users, but if that is not an option, it may be desirable to restrict user bandwidth to prevent some devices from monopolizing the network. Xirrus allows bandwidth limits and time-of-day access restrictions to be placed on particular users or particular device types (see device identification section below). Xirrus Arrays also allow network administrators to set QoS parameters for different traffic types.

Design for security.

As different types of devices access the network, it must be ensured that the devices and the network are secure. First, network access should be restricted by using proper network authentication and authorization (e.g., 802.1x). Second, the network traffic should be encrypted using the latest network security (e.g., WPA and AES). Finally, client devices should be checked to confirm they are running the latest antivirus software and patches (e.g., Network Access Control). Xirrus' unique wireless architecture seamlessly integrates with standard network infrastructure to allow the same firewall, NAC, and RADIUS to be used for both wireless and wired users to simplify management and administration.

Identify devices and enforce policies.

Just because a user has the credentials to access the network, that does not mean that user should get access to all of the corporate resources. For instance, a corporate employee on his company-provided laptop may get access all of the corporate resources. However that same employee, using his own iPad, may only be provided access to corporate email and the web. A guest may only need access to the Internet. Xirrus Arrays allow different user groups to be created with each group being mapped to specific VLANs, access control list, and QoS parameters. By assigning devices and users to a specific group IT administrators can easily control who has access to which information from what devices.

Xirrus' Device Fingerprinting identifies the devices operating systems such as iOS®, Microsoft® Windows®, BlackBerry®, or Android™ and can then classify the device type such as tablet, laptop, or smartphone. Once the device has been identified, a policy can be applied to control a device's reach and behavior. The device ID, along with the user ID, can be used together to map that instance to a specific user group.

CONSIDERATIONS FOR IPAD DEPLOYMENTS

There can't be a discussion of tablets without an emphasis on Apple iPads. iPads still account for over 75% of the tablet market, and while some lower cost devices (Amazon's Kindle Fire) are gaining ground in the consumer space, the iPad is still king for in the Enterprise.

When designing wireless networks for the iPad there are three critical elements to understand and account for:

1. Lower transmit power – in order to make the iPad lighter and more energy efficient, the maximum transmission power is set to 10dBm. Typical laptops have a transmit power of between 15 – 17dBm.
2. Single Spatial Stream – with 802.11n, the iPad only uses a single spatial stream and are not able to do channel bonding, limiting their link rate to a maximum of 65Mbps. Typical laptops can use two or three spatial streams and can do channel bonding, giving them the possibilty of a link rate of up to 450Mbps.
3. Dual Band Support – iPads are able to operate in both the 2.4GHz and 5GHz frequency, and actually default to the 5GHz when available. With these elements in mind the following sections outline some network designs considerations that should be considered when deploying iPads.

Signal Strength

In the past, best practices for designing wireless networks suggested having a -72dBm signal strength everywhere. With -72dBm signal, most laptops would be able to achieve the maximum possible throughput anywhere in the network. However, since iPads transmit at between 5 – 7dBm lower signal strength networks need to be designed with stronger signal strength everywhere to be sure the iPads can transmit at maximum data rate. In general networks should be designed to have -67dBm or stronger everywhere.

Maximize 5GHz usage

In Wi-Fi there are two main frequencies – 2.4GHz and 5GHz. 5GHz has eight times the number of channels than 2.4GHz, has much less interference, and typically offers much faster performance. When designing for iPads as many Wi-Fi radios should be set to 5GHz to maximize the network throughput and performance.

Wireless Performance

Because of the lower transmit power and the fact that iPads can only operate with a single spatial stream, iPads will typically have lower throughput than traditional laptops. In order to achieve faster performance more Wi-Fi radios need to be available for the iPads to achieve the same throughput as enterprise laptops. In fact, Gartner says that when using traditional Wi-Fi Access Points Enterprises would need to deploy 300% more Access Points for iPads to achieve the same wireless performance as industry laptops..

- iPad policy enforcement with device identification
- Connect more iPads with 75% less equipment
- Easily add more capacity as use density increases

Xirrus Advantages

Due to the popularity of the Apple iPad, Xirrus has put a lot of emphasis testing with iPads and optimizing wireless network performance for iPads. As part of the normal quality testing process , each release of the Xirrus Array is tested with 100 iPads streaming live video. In fact, a demo of this test was shown at Interop New York in 2010.

The Xirrus Array has several unique advantages that make it ideal for iPads deployments.

Directional Antennas – Xirrus Arrays use directional antennas that transmit and receive signal strength twice as far as the omni-directional antennas. With the directional antennas the Arrays can "talk" and "listen" at greater distances, making them ideal for the lower transmit power of iPads.

Multiple Radios – Xirrus Arrays can have up to 16 radios in a single device. With up 8x the radios of a traditional access point the Arrays have up to 8x the throughput. With an 8-radio Array an Enterprise can replace four traditional access points, so rather than having to deploy 300% more access points with a traditional access points as Gartner suggest, an enterprise can actually achieve the same performance for iPads using 25% fewer Arrays!

Configurable Radio Frequency – Most traditional access points have one 2.4Ghz radio and one 5GHz radio forcing the network mixt to be 50% 2.4Ghz and 50% 5GHz. However, iPads can support and prefer 5GHz networks. With the Array, each modular AP can be set to 5Ghz, greatly increasing the network performance and taking advantage of the natural benefits of 5Ghz (more channels and less interference).

Full line rate encryption – the iPad has put a lot of focus on encryption, however many traditional access points cannot perform line rate encryption. In fact the throughput of many Wi-Fi networks drops 50% when encryption is turned on. With the Xirrus solution, each Array has its own embedded encryption engine that performs full-line rate encryption. Ensuring high-performance, secure networks.

Thanks to these and many other advanced features, the Xirrus Array is the ideal solution for iPad deployments.

CASE STUDY — MILLIS PUBLIC SCHOOLS

One institution that has fully leveraged the benefit of tablets is Millis Public Schools. Millis Public Schools is in Millis, Massachusetts, located approximately 19 miles southwest of downtown Boston. Millis earned the Silver Medal status in 2010 as one of America's Best High Schools, placing it in the top 3% in the United States. Millis has been a leader in technology-driven learning programs to improve learning and communications for its students and faculty. Millis was looking to embrace a personalized learning initiative by giving Apple iPads to all of its incoming students. By deploying Xirrus W i-Fi Arrays, Millis Public Schools has been able to further expand on its personalized learning initiative, providing solid and reliable wireless connections for its computer-based applications and 1:1 Apple® iPad initiative.

Requirements

- Support all students and faculty on the wireless network
- Prepare for true 1:1 initiative
- Save cost on installation and maintenance
- Provide a reliable solution to support the increasing density
- Support up to 30 devices per class without putting an AP in every classroom

Solution

- A full-scale Xirrus 802.11n deployment
- 1:4 ratio of wireless Array to APs
- Elimination of 15 APs per school
- Elimination of 15 cable runs per school
- Elimination of 15 GigE switch ports per school

"We have always used technology in our district to help leverage teaching and learning programs."

GRACE MAGLEY — Director of Educational Technology for Millis Public Schools

Monitor continuously.

As more devices are brought onto the network, the network should be constantly monitored to verify that all resources are being efficiently utilized. Network traffic should also be analyzed to be sure there are no issues or network bottlenecks. The centralized Xirrus Management System analyzes network resources and then provide easy-to-read reports to help identify growth in network usage or potential problem issues. Xirrus Station Assurance feature monitors client connectivity to quickly identify network issues.

As monitoring continues, changes should be made and future growth planned for. As new devices are introduced to the network and new security threats are identified, the cycle should be constantly tweaked to maintain a secure, high-performing mobile network.

Tablets and smartphones: it's good for business and IT.

More and more users are expecting to be able to use their mobile devices at work. Business is working wireless into operations objectives to help increase productivity. IT administrators must be able to support this influx of devices or run the risk of alienating employees and stymieing that productivity. Tablets and smartphones can present a challenge for network administrators, but by following the steps outlined above and by utilizing the right wireless infrastructure, tablets and other "non-standard" devices can be easily handled. This allows IT staff to raise employee satisfaction — and ultimately focus on other IT issues.

Discover more.

For more details about how Xirrus can help you solve the pending influx of Wi-Fi devices, visit us at www.xirrus.com or send us an email at info@xirrus.com

About Xirrus

Xirrus provides unique, high-performance, array-based wireless solutions that perform under the most demanding conditions, while delivering wired-like reliability, superior security, and less infrastructure requirements. Xirrus is a privately held company headquartered in Thousand Oaks, CA.

XIRRUS®
High Performance Wireless Networks

1.800.947.7871 Toll Free in the US
+1.805.262.1600 Sales
+1.805.262.1601 Fax
2101 Corporate Center Drive
Thousand Oaks, CA 91320, USA

To learn more visit:
xirrus.com or
email info@xirrus.com