XIRRUS WHITE PAPER

Tablets in the Enterprise

Considerations for Managed Device and BYOD Strategies

XIRRUS®

High Performance Wireless Networks

Tablets are Replacing the Laptop

The proliferation of tablets and other smart devices has increased dramatically in the past several years and use of these 'consumer class' products on enterprise networks is nearly ubiquitous. A recent study showed 90% of organizations polled allow some level of personally owned technology to be used on site — a phenomenon known as BYOD (Bring Your Own Device). Many organizations partially fund the purchase of employee-owned devices that are used as business tool. The Apple iPad in particular has driven significant changes, with its rapid market adoption followed by a myriad of other tablets entering the market.

Until recently, the enterprise has been hesitant to embrace the tablet seeing several false starts of similar products in the past. However with tighter corporate budgets and CFOs looking to leverage the cost benefits of personally owned devices, times have changed. Employees have fallen in love with their mobile devices and now commonly carry several of them to work or when travelling, extending the boundary of the office and where work can be accomplished.

Only a short time ago, standard corporate issue was a laptop and a business-focused smartphone such as a Blackberry. Today, it is a laptop, full-featured smartphone, and increasingly a tablet that is coming to work — in some cases tripling the number of wireless devices communicating on the network.

The New Corporate Reality

2009

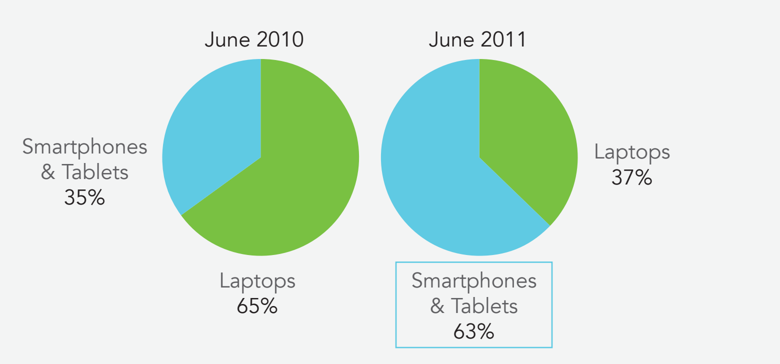
- Laptop + Blackberry
- Average of <2 devices
- ~100 Mbytes/Month mobile traffic

2012

- Laptop, iPad, Smartphone, etc.: Average of 3+ devices
- ~700 Mbytes/Month mobile traffic

Adoption of mobile devices in the enterprise means elimination of fixed work locations, improved collaboration, reduction in printing costs, and ultimately increased employee productivity. Many organizations are reducing or retiring wired network ports to save money.

US Wi-Fi Usage by Device Type



Source: Evercore Partners, Trends in Mobile Communications and Technology, March 2012

The shift in use to these smart devices has resulted in a dramatic shift of traffic to and emphasis on wireless networks since these devices do not have wired Ethernet ports. This shift is challenging IT staffs to engineer wireless networks that can support the demands of this new paradigm today and that are able to adapt to increased and changing requirements tomorrow. No longer does IT have the luxury of predictability in controlling the type and quantity of devices on their networks – they just need to support this new mobile revolution.

> Without Proper Planning, Enterprises Deploying iPads Will Need 300% More Wi-Fi
>
> Tim Zimmerman (Gartner), October 2011

Many existing wireless networks are encountering performance degradation and issues. As one IT administrator stated, **"I am getting complaints about poor wireless service in areas that have never been a problem in the past."** No longer is density and capacity contained based on a fixed number of Ethernet ports available. Now it based on how many employees, contractors, guests, and others show up with an indeterminate number of their own devices, in addition to existing corporate-owned wireless assets.

In granting personal mobile devices access to the enterprise network, security considerations around access control and data management are crucial to plan. While control of the device itself may have been given up, IT administrators must focus on the control of the network and data infrastructure in support of these devices.

Knowing not only who is on the network but visibility into what device they are using, what application they are using, and where they are located can feed into deciding what access policies to enforce for that session.

Understanding Tablet Wi-Fi Capabilities

Any discussion about designing a wireless network to support tablets must begin by understanding the Wi-Fi capabilities of these devices. The tablets of today do not have the same wireless capabilities as the traditional laptop. Understanding their limitations is a key part of planning for success.

There are several important characteristics of tablets to understand:

1. Lower Transmit Power – Due to hardware space and power consumption limitations, tablets typically have lower Wi-Fi transmit power compared with laptops. This difference can range from 3-9dBm depending on model and Wi-Fi band. This means the transmit power of a tablet can be from 1/2 to 1/10 that of a laptop. These power and antenna limitations reduce signal sensitivity in the receive direction as well, and ultimately lower the device's wireless performance compared to other more robust wireless clients.

2. Lower Data Rates – While 802.11n today supports data rates up to 450Mbps, achieving this rate depends on the client. With typically just one antenna (compared to 3 required for fully capable 802.11n), tablets are limited in the ability to achieve higher data rates relative to laptops that can house multiple, larger antennas. Most tablets support only one 802.11n spatial stream and no channel bonding, resulting in a maximum data rate of 65Mbps. Typical laptops can achieve 300Mbps and some up to 450Mbps.

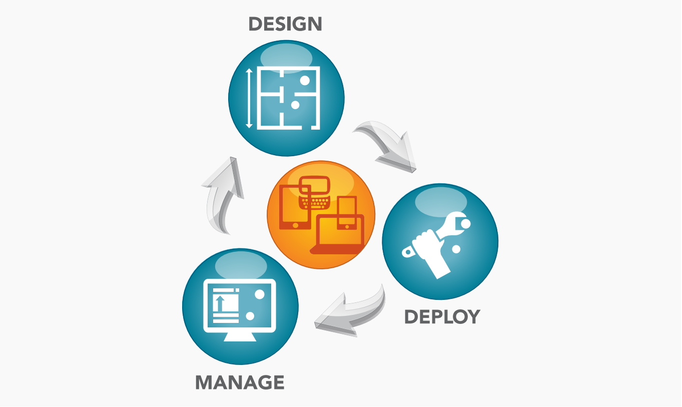
3. Dual Band Support – Tablets vary in their ability to operate in both the 2.4GHz and 5GHz bands available with Wi-Fi today, however most mid to higher tablets support both, including the iPad. Smartphones typically support 2.4GHz only. The ability to operate in the 5GHz band is key to achieving best wireless performance since that spectrum has much more available bandwidth and typically much less interference from non-Wi-Fi devices. 5GHz support should always be looked for when selecting a tablet.

4. Sticky Roaming – When moving around a physical location, iPads and other tablets tend to remain connected to the same AP even when a much stronger signal is available from another AP. This can be due to design constraints in the device or how the Wi-Fi drivers are written. This restricted roaming ability can lead to significantly reduced performance while the device is hanging on to a poor wireless connection.

5. Limited Device Discovery – Apple iOS applications such as AirPlay and AirPrint use a multicast protocol called Bonjour for automatic naming and discovery of devices and services on a network. This scheme was designed for home or small networks with a single network segment and without a DNS server. Enterprise networks typically extend across multiple Layer 3 network segments and use dynamic DNS for device naming and discovery. Since Bonjour traffic does not natively pass through routers, it does not scale well for use in the enterprise. The network infrastructure must be aware of Bonjour traffic and appropriately handle it to ensure iOS devices and applications will work properly.

Building the NEW Wireless Network

The days of wireless being deployed as an 'overlay' service on top of and in addition to a primary wired network infrastructure are over. Today's mobile clients do not have Ethernet ports and their use fundamentally requires a reliable, high performance wireless network. Many of the principles and practices for network design perfected in the wired world apply to wireless as well. The lifecycle of the network must be viewed as an ongoing and iterative process of Design, Deploy and Manage that ensures a network capable of meeting current requirements with the ability to evolve to changing business demands over time.



The Wireless Network Lifecycle

Design

The influx of tablets and other smart mobile devices has altered the RF landscape and fundamentally changed the way wireless networks must be designed. These devices do not operate on the wireless network in the same way as laptops, netbooks, printers, and other wireless devices. And with the sheer number of devices on the network increasing, the Wi-Fi spectrum is frequently becoming saturated in wireless networks everywhere, decreasing performance. Supporting tablets and BYOD in the enterprise starts with a solid foundation in the wireless infrastructure that is able to deliver the client density and capacity necessary to allow these devices to be operated as they were intended.

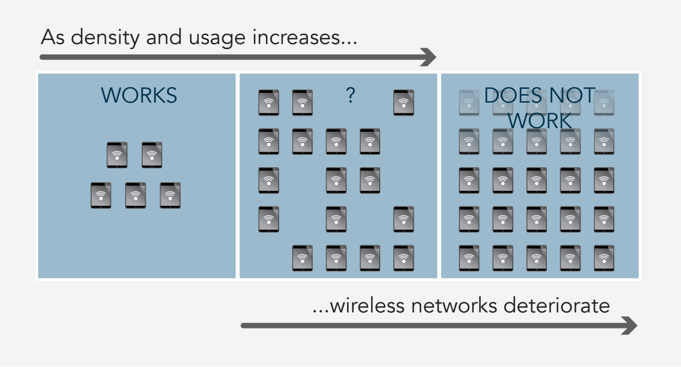
> By 2015, 80% of newly installed wireless networks will be obsolete because of a lack of proper planning
>
> Paul DeBeasi (Gartner), October 2011

Designing for Density and Performance

The design of any wireless network must be matched to the business requirements of the organization for which it will operate. The influx of tablets and other smart devices has expanded the requirements for device density and capacity in these networks. Properly designing the wireless network for the appropriate level of performance and reliability is critical to lay the foundation for the successful operation of the services and applications which will operate over it. Without this appropriate foundation, the wireless network will fail.

Many variables can impact wireless performance, including the total number of wireless clients, the total number active at one time, the applications in use, non-Wi-Fi interference in the area, the connected data rates of the clients, the use of 2.4GHz and 5GHz spectrum, etc. All must be considered in the design. However handling client density and planning for density growth are by far the biggest challenges.

Wi-Fi is a shared communication technology with multiple users sharing the same communication channel. Even in the most pristine RF environment, only so many users can be supported on a given wireless network before performance deteriorates and users will begin to complain.


As density and usage increases...
WORKS
?
DOES NOT WORK
...wireless networks deteriorate

Consequences of under-scoping wireless network design in high-density environments

As the graphic demonstrates, the more users on a given wireless network, the more the performance and user experience will degrade since they are sharing a fixed number of radio resources. It is never a cut and dry threshold where the network will tip over. Design considerations must be made to accommodate worse case scenarios – and beyond.

The traditional approach to handling increasing device densities is to add more APs. This will work to a certain extent, but at some point, you run into the spectrum limitations of Wi-Fi. In particular, the 2.4GHz band provides only 3 separate channels for communications. The 5GHz band between 8 and 21 (depending on country). Since the majority of tablets and laptops support 5GHz, it is critical to design your network to provide the bandwidth and performance available in this band.

Most traditional APs are designed in a fixed band configuration with one 2.4GHz and one 5GHz radio. This 50/50 mix of radio types severely limits the ability to access a large portion of wireless spectrum in 5GHz that is necessary to scale. As more APs are added to increase capacity, the number of 2.4GHz radios will increase to the point where they significantly interfere with each other. The result is that some 2.4GHz radios will need to be disabled else become a significant source of interference. When this point is reached, no additional bandwidth benefit is realized in 2.4GHz by adding APs and radio resources are thus wasted. Meeting the demands of high density requires more intelligent solutions that can adapt as requirements change. Multi-state radios that can be operated in either Wi-Fi band are key to enable dynamic adjustments to the client environments.

Design Recommendations

Based on the device characteristics of tablets and the Wi-Fi design fundamentals we have discussed, the following best practices should be applied when designing a wireless network for supporting tablets.

Maximize Use of 5GHz

With up to eight times as much bandwidth in 5GHz as in 2.4GHz and typically much less non-Wi-Fi interference, optimizing use of 5GHz is a fundamental requirement for best performance. As many Wi-Fi radios as possible should be set to operate in 5GHz. Typically some radios will need to be set to 2.4GHz to support certain clients (smartphones and legacy clients).

Design for Appropriate Signal Strength

The Wi-Fi signal level design criteria typically used for laptops (nominally -70dBm RSSI) is not sufficient for tablets, especially when they will be deployed in dense numbers. Since tablets transmit at lower signal levels and have inferior antennas compared to laptops, networks must be designed with stronger signal to ensure maximum data rates. Wi-Fi networks for tablet support should be designed with a minimum -65dBm signal strength in both the 5GHz and 2.4GHz bands in all locations.

Provide Sufficient Radio Bandwidth

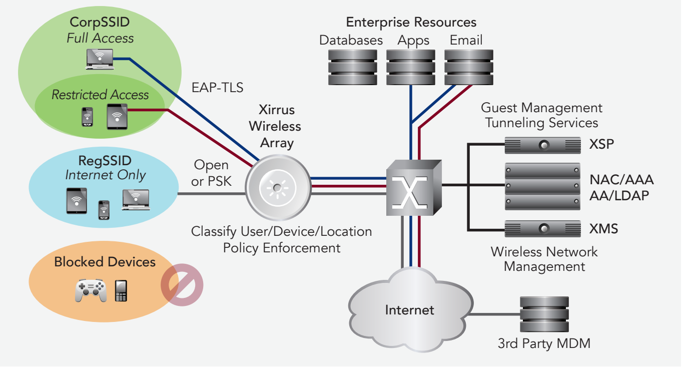
Because of lower transmit power and limited 802.11n data rate support, tablets will typically achieve much lower traffic throughput performance compared with laptops. More Wi-Fi radios are therefore required to support tablets in a wireless environment than for an equivalent number of laptops. A general rule of thumb is to design the wireless network with enough radios to handle the expected number of tablets at a ratio of 15 per 5GHz radio and 8 per 2.4GHz radio.

Deploy

Building upon the design of the wireless infrastructure, the next phase in the wireless lifecycle is deploying the network components and services that match with the unique requirements of the organization. There is no one-size fits approach, however there are principles on which all tablet and smart device deployments should be based.

Enterprise-class mobility deployments should integrate with the primary corporate network and not be deployed as an overlay technology. The wireless network should connect seamlessly to the existing wired infrastructure to provide access to corporate and external resources.

In BYOD deployments, access control is a key component. Policies must be established as to what resources a given user and device will have access to once connected to the wireless network. Devices such as tablets and smartphones should not necessarily be able to access to all corporate resources, regardless of who is using it. Mobile devices are commonly lost or stolen and along with them, the threat of valuable corporate information being compromised. Organizations must enforce access policies on mobile devices and monitor them once they are on the network. Policy management components include Active Directory (AD), NAC (Network Access Control), and RADIUS servers for user authentication and security policy enforcement. A new class of Mobile Device Management (MDM) tools provides additional management control specifically for mobile devices such as tablets on the network.



Deploying an End-to-End Mobility Solution

Mobile Device Management (MDM)

MDM is an emerging product category for solutions that provide functions related to managing smart mobile devices in an enterprise environment. In general, MDM communicates with client devices to determine posture, OS, security settings, add/remove/patch applications, location tracking, and remote wipe of content in cases the device is lost or stolen.

MDM has become important for controlling company owned as well as personally owned tablets, smartphones, etc. that may contain corporate sensitive information. They help manage configuration profiles and posture control for these devices prior to allowing them network access.

Network Access Control (NAC)

NAC allows IT administrators to define policies controlling how users and/or the devices they are using gain access to network resources. It is typically common to both the wired and wired infrastructures of a given organization.

One of biggest drivers for NAC is the ability to control guest access to a network. Most networks have a variety of user classes requiring various levels of access, such as employees, contractors and visitors. All require access, but at various levels to corporate-owned resources.

NAC services discover, classify and assign endpoints as they access the network. Users attempting to access the network are classified based on who they are, what client they are using, and where they are located. Based on this information, access policies can then be applied.

Active Directory (AD)

Active Directory (AD) is Microsoft's directory service and is the most commonly deployed in the industry. Directory services provide a central directory for managing and controlling access of users and their devices.

In most cases, AD, NAC and MDM work together to allow the different device management applications to leverage a single database and apply rules based on information defined in the Active Directory policies. These systems integrate with the wireless (or wired) infrastructure to identify and classify the different user categories.

The associated deployment diagram shows all the components for an end-to-end mobility solution. The following example set of use cases depicts how different access policies are applied based on both user and device:

USER	CLIENT DEVICE	ACCESS POLICY
Employee	Corporate Provided Device	Full Access
Employee	Approved BYOD Device	Limited Access
Contractor	Approved BYOD Device	Limited Access
Guest	Approved BYOD Device	Internet Access Only
Employee/ Contractor/Guest	Non-Approved BYOD Device	Blocked
Unknown/Rogue*	Any Device	Blocked

Mobile Device Management tools allow administrators to create policies to balance "security" and "access" in a BYOD environment, achieving greater productivity without increasing risk in the network.

Manage

Wireless networks require continuous and robust management and monitoring functionality as part of ongoing operation. This includes management of the infrastructure, the clients, and in addition with wireless, the RF environment.

Infrastructure Management

Centralized management systems provide network administrators single console access for managing and maintaining the entire wireless network configuration, including policies that can be applied across the entire network. Commonality is important with mobile devices since they move between locations and should interact the same with the network, whether at corporate headquarters or in a remote office.

Administrators must continuously monitor the wireless network in support of mobile device deployments. Security policy compliance is critical on ongoing basis.

Network performance must be monitored to ensure new roll outs are not adversely affecting users. Enabling BYOD on a network will most certainly increase network activity and often will necessitate an upgrade of the wired infrastructure to support it.

Network architects can use reporting tools and analytics to provide actionable insight to plan upgrades and improvements to the wireless and wired networks to meet business needs. This is a continual process that ultimately points back to the design phase.

Client Management

A critical component of mobile device deployment in an enterprise is a level of visibility and control of the devices on the network. Since tablets and smartphones are often personally owned, the level of control afforded to IT administration may vary based on corporate policy. Mobile device management systems provide a number of key functions in support the ongoing operation of these devices on the network, including the ability to distribute applications, execute software upgrades, configure settings, manage corporate data, and remotely wipe lost devices.

RF Management

Based on the very nature of RF, wireless networks have potential of being affected by interference – from both Wi-Fi and non-Wi-Fi sources – as well as nonconforming or malicious devices. As a result, enterprise-class RF monitoring systems are an important element of wireless network management for monitoring the spectrum, wireless activity, and all RF transmitters. Wireless management solutions should integrate IDS/IPS services that include at a minimum:

- Dedicated threat sensors
- Rogue AP detection, classification and mitigation
- Wi-Fi attack detection and mitigation
- Spectrum analysis
- Wireless packet capture and analysis

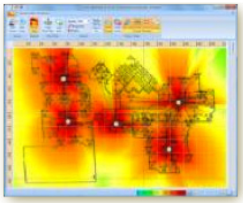
The Xirrus Wireless Solution

From its inception, Xirrus has understood that traditional enterprise Wi-Fi solutions are not built to effectively scale to handle expanding wireless performance requirements. The recent explosion in use of tablets and BYOD initiatives requires a different approach to scale than just adding more equipment. It requires building an intelligent, high performance wireless foundation upon which reliable and mission-critical services can be delivered. The reality is that foundation is not in place in many enterprise networks today.

Xirrus delivers a comprehensive solution that addresses today's needs and can flexibly adapt to meet new requirements as devices change and network usage increases.

High Performance Infrastructure

Any successful wireless deployment starts with the appropriate RF design. This entails producing plans for the right number and placement of access points to deliver the coverage, performance, and user capacity required.



To design and verify the Wi-Fi network design, Xirrus offers the Wi-Fi Designer application. Wi-Fi Designer is specifically architected for wireless network design using the multi-radio Xirrus Wireless Array. It is used for both active and predictive site survey designs to create the best-fit wireless network strategy for an environment. After installation, Wi-Fi Designer is used to verify the results of the implementation to ensure design criteria are met.

The primary use cases for Wi-Fi Designer include:

- Predictive surveys for remote planning of an optimal Wireless Array solution
- Active surveys for designing a Wireless Array network by taking live measurements at the deployment site
- Validation of a deployment post-installation to ensure meeting all design criteria

Based on an appropriate design, a scalable and reliable infrastructure can be created from the Xirrus Wireless Array portfolio as a foundation for a high performance wireless network. Xirrus Wireless Arrays provide a number of key advantages that are ideal for delivering flexible, scalable wireless networks to meet expanding wireless network requirements. These include:

- Complete product range – Xirrus Arrays support from 2 to 16 modular APs in a single element compared to only 2 radios in most enterprise APs. This range provides flexibility to deliver wireless capacity as needed to meet performance requirements, from areas requiring basic coverage up to those with 1000’s of users in one area. With 4 to 8 times the number of radios per element, a single Xirrus Array replaces 4 to 8 traditional 2 radio APs – and subsequently reduces cable and wired infrastructure costs significantly.
- Fully upgradeable – Xirrus Arrays utilize a fully modular architecture. Each Array chassis includes a set of modular AP slots, from 2 to 16 per chassis. Modular APs can be added, moved, or upgraded within a chassis, enabling future capacity upgrades, technology upgrades, and custom coverage design.
- Directional antennas – Xirrus Arrays utilize directional antennas that transmit and receive approximately twice as far as the omni-directional antennas on traditional APs. The ability to “talk” and “listen” at greater distances provides performance advantages working with the lower transmit power and smaller antennas on tablets. Directionality also helps provide isolation from interference to which omni-directional antennas are more susceptible.
- Dual band radios – Traditional APs are fixed with one 2.4GHz radio and one 5GHz radio, resulting in a static 50%/50% radio mix. However most tablets support the much higher performance 5GHz. With the Array, each modular AP can be set to either 5GHz or 2.4GHz, greatly increasing the flexibility to design the wireless network for optimal performance for tablets.

Integrated Network Services

Building upon a reliable, high performance wireless foundation, Xirrus provides a suite of integrated network services that operate in conjunction with the Array platform to optimize wireless deployments based on business requirements.

Delivering the right set of network services is critical to the success of an enterprise wireless network – to keep it secure, performing efficiently, and providing value add functions that can benefit business. Xirrus provides an adaptive and flexible set of services that can be customized per user, device, and application. The complete network services offering is as follows:

SERVICES COORDINATION

SECURITY SERVICES	GUEST SERVICES	VOICE AND VIDEO SERVICES	LOCATION SERVICES	PERFORMANCE SERVICES	MONITORING AND ANALYSIS SERVICES
WPS/WDS	Captive Portal	Video Streaming	Asset Tracking	Application Performance	Pkt/Traffic Capture
AAA/NAC	Directory Integration	Voice	Client/Rogue Location	User Performance	Spectrum Analysis
Mobile Device Policy Enforcement	Policy Management	Large File Transfer	Mapping	Network Performance	Event/Log Management
			Surveying	RF Performance	Resource Assurance
			Planning		

Mobile device policy enforcement is a key services component to deploying tablets and smart devices in an enterprise network. The Xirrus wireless network will identify users, devices, and locations, then apply and enforce policies specific to those attributes in each Array. These policies ultimately control the device’s reach and behavior on the network based on each organization’s unique requirements.

The Xirrus Array solution is based on a distributed paradigm that places the intelligence and processing power in each Array. This is in contrast to traditional enterprise wireless architectures which rely on central controllers to coordinate many of the functions across APs. The distributed architecture enables policy enforcement that is controlled directly at the network edge. Security policies can be enforced and extraneous traffic filtered before the traffic hits the corporate wired network. With a high performance architecture coupled with a robust policy engine in every device, Xirrus has the proven capability to deliver enterprise-grade Wi-Fi service across the complete range of environments from basic to extreme density.

Smart Device Management

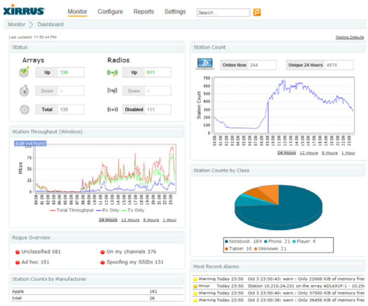
Tablets, smartphones, and similar smart mobile devices present a unique set of challenges when operating on enterprise wireless networks. Their limited size and power restrict their wireless capabilities. But their extreme mobility and hunger for rich-media content makes them uncompromised in their demands on the wireless network.

To address the challenges of incorporating smart mobile devices into the workplace, Xirrus has developed a set of optimizations and services to ensure successful operation of these devices on Xirrus wireless infrastructure. Some of these optimizations include:

- Roaming Assist – Roaming between APs on a wireless network can be compromised on devices such as tablets due to their smaller size and low power requirements. Xirrus has developed specialized roaming assist functionality for iPads and similar 'sticky' clients. Roaming is coordinated between Arrays in a wireless network to move tablets from Array to Array at optimized times instead of waiting for the device to make the roaming decision.
- Device Discovery – The Xirrus Array's integrated intelligence (as compared to a central controller) enables optimized handling of Bonjour multicast traffic for Apple devices at the network edge by only forwarding traffic as required. Extraneous traffic is pruned from the network to minimize its impact on network performance.
- Performance Optimization – Given their wireless performance limitations, Xirrus has made a number of specific enhancements to ensure tablets and other smart mobile devices are operating at maximum performance. Rating algorithm enhancements ensure tablets operate as close to their 65Mbps maximum transmit rate as possible. Band steering and load balancing ensure radio and spectrum resources are allocated appropriately to maximize performance.

Management

For monitoring and management of a Xirrus wireless network, Xirrus provides the Xirrus Management System (XMS). The XMS is a wireless network management platform enabling network administrators to automatically and efficiently discover, configure, and maintain a Xirrus Array network from a central location.



Last updated: 11:50:44 PM

Arrays		Radios	
Up	136	Up	611
Down	0	Down	0
Total	136	Disabled	111

Online Now 244
Unique 24 Hours 4574

● Notebook: 184 ● Phone: 21 ● Player: 6
● Tablet: 16 ● Unknown: 21

● Unclassified 581 ● On my channels 376
● Ad hoc 151 ● Spoofing my SSIDs 131

Apple	161
Intel	26

```
Warning Today 23:50   Oct 3 23:50:43: warn : Only 22668 KiB of memory free
Minor   Today 23:50   Station 10.210.24.231 on the array ADLeX1F-1 - 10.25
Warning Today 23:50   Oct 3 23:50:40: warn : Only 37500 KiB of memory free
Warning Today 23:50   Oct 3 23:50:36: warn : Only 36456 KiB of memory free
```

The XMS scales from single site to large scale, multi-site deployments. Network administrators choose from a range of installation options including on-premise software and pre-configured appliances, providing the flexibility needed for fast implementation and the lowest costs to best fit operating requirements.

Key functions include:

- Centrally define and manage configurations/policies
- Monitor wireless network performance
- Drill down reporting and analytics
- Security monitoring & alerting
- Centralized troubleshooting and maintenance

Summary

The requirements being placed on wireless networks today differ significantly from what they were just a few years ago. Wireless networks have morphed from an overlay technology that supported primarily higher performance clients such as laptops to becoming the primary connection technology for all types of devices. Key to supporting the influx of tablets and other smart devices on wireless networks is to understand their unique requirements and to design and adapt the wireless network implementation accordingly.

Key Benefits of the Xirrus Solution

High Performance Infrastructure:

- Performance and reliability to deliver mission-critical applications over wireless
- Ability to adapt and scale to handle unpredictable device growth
- Increased employee productivity by delivering uncompromised mobility

Integrated Network Services:

- Seamlessly scale as the network grows without imposing stair step costs
- Increased efficiency and scalability with edge, not central, policy enforcement
- Superior resiliency by distributing functionality and no single points of failure

Smart Device Management:

- Maximize user productivity for devices designed for consistent connectivity

About Xirrus

Organizations depend on high-bandwidth voice, video, and data going to and from mobile devices. Business is done in the cloud. Today, you need highperformance wireless. Xirrus delivers it. Our wireless solutions provide wired-like reliability, superior security, and they perform under the most demanding conditions. Xirrus is a privately held company headquartered in Thousand Oaks, CA.

High Performance Wireless Networks

1.800.947.78.71 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