



Whitepaper

Secure Wireless Networking

Delivering Wireless Security Equal To or Better Than Wired Security

Introduction

Is Wi-Fi secure enough for your enterprise?

Wireless networks (WLAN) are common today in many security-conscious industries such as government, healthcare, and financial services. You might wonder how such organizations are able to deploy secure wireless networks given some of the well-publicized attacks on wireless security, like the one that affected TJ Maxx and Marshall's circa 2005.

Historically, the most significant Wi-Fi security breaches have been due to the failure of administrators to follow the latest best practices for security, and instead relying on outdated Wi-Fi security mechanisms such as WEP (Wired Equivalent Privacy). Unfortunately, the publicity of these breaches has tainted the perception of Wi-Fi security for many others.

Today, a wireless network designed with best practices is widely considered equal to or more secure than a wired network. By applying multiple layers of security through mechanisms such as encryption, authentication, firewalls, and IDS/IPS, the wireless network can be assuredly secured. This white paper will discuss each of these security layers and how they can be applied in production networks with Xirrus Wi-Fi solutions.

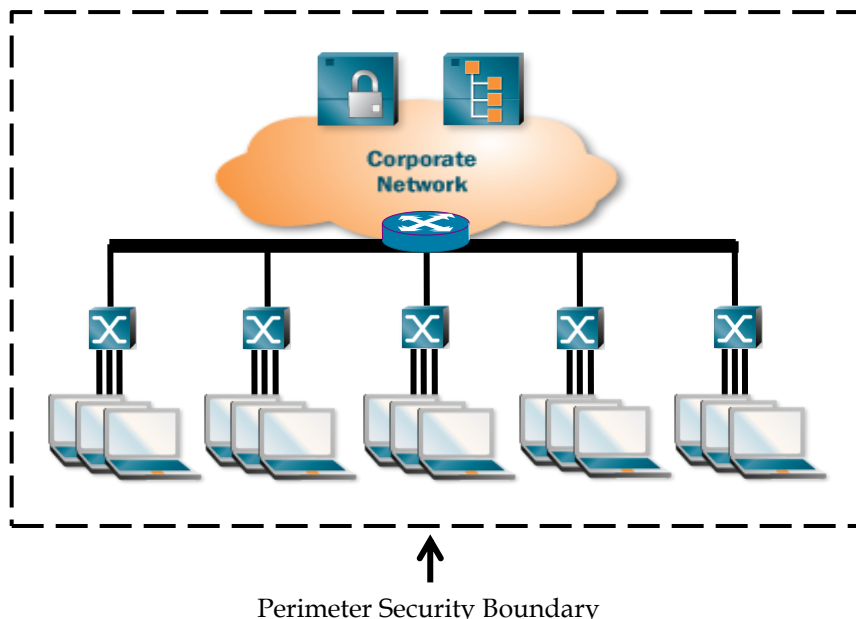
Wireless and Wired Security

The security considerations of operating wired local area networks (LANs) and clients are well known – the industry has worked them out over the last 25+ years since these networks first appeared. Whereas WLANs have been prevalent only for the last decade, so the aspects of operating these networks are newer to some IT administrators. Shortcomings in the Wi-Fi standards in 1999 tainted the initial perception of wireless security. However these limitations were solved with new standards put in place in 2004, paving the way for the broad adoption of wireless networks in all types of applications. In the end, both wired and wireless media are able to provide high levels of security if deployed correctly. The main difference between the two is how and where security features are implemented.

A primary aspect of wired network security is that it inherently provides a level of physical 'perimeter' security by limiting access to the network media (ports/cable) based on how and where it is deployed in the environment. Wireless on the other hand cannot be contained within a cable and RF signals will typically propagate beyond the physical boundaries of the organization. To address this, wireless security focuses on protecting the communication (data) itself in addition to the physical media (RF spectrum).

Perimeter Security (Wired)

Physical perimeter security in a wired network is based on the fact that communications are contained within the network (cables), and as long as only authorized users have access to that media, communications are secure. Physical protection for the wired infrastructure comes from fences, walls, doors, guards, receptionists, etc. Perimeter security is certainly not perfect and can be breached if a wired port is physically available to unauthorized users within the customer premises (i.e. from a printer port, open jack in a lobby or conference room, etc.).



Wired networks may also implement additional security provisions such as authentication, encryption, port activation, and network-monitoring tools. However, it is typical for wired networks not to employ most of these additional layers of security because of the perception that perimeter security provides a sufficient barrier.

Communication Security (Wireless)

The properties of wireless communication prevent physical perimeter security since RF signal propagation cannot be completely contained within a specific physical area. As a result, additional protection methods - most importantly securing the data itself - are required to secure the network. With this approach, even if the communication is observed/intercepted, the actual data is not compromised.



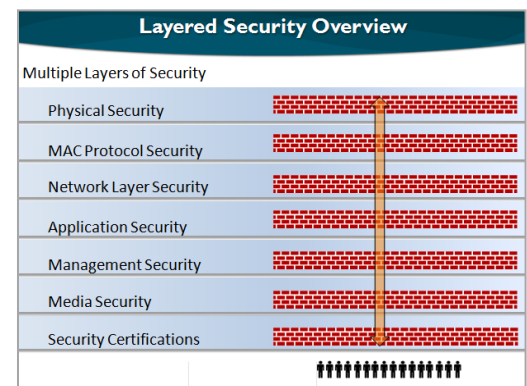
Layered Security

Network security encompasses a number of aspects – from the physical security of devices all the way up to the security of applications running on the network. Translating this to the commonly-used OSI model for networking, a full-security solution encompasses Layer 1 to Layer 7.

Layered security uses a suite of protection methods to protect the network resources. In this way, even if one layer is compromised, additional protection schemes will contain the breach and limit any damage. An example of this is an Internet firewall. It is a fundamental security tool for most organizations in protecting their networks from attacks via the Internet. However if an employee launches a malicious attack on the firewall from the inside, one level of security has already been breached and it is up to other layers to contain the attack.

Best Practices for securing both wired and wireless networks employs a layered security with the following components:

- Physical Protection of Network Elements
- MAC Layer Security
- Network Layer Security
- Application Layer Security
- Management Security
- Media Security
- Security Certifications and Verification



Often times it is not possible due to costs or other limitations to deploy all security layers. Actual deployment will depend upon the specific requirements for the network and the information to be protected. The following sections describe each layer of security and how it is addressed in both wired and wireless networks.

Physical Security

Physical security is about protecting access to the networking components and the media itself. Elements of physical security include building security, locked or disabled switch ports, protected passwords/keys, and a well understood employee security policy. Some of the common components of physical security are listed below and mapped to their applicability in wired and wireless networks.

Security Component	Wired	Wireless
Secured Network Closets	√	√
Secured Peripherals	√	√
Protected Keys	NA	√
Password Protected Devices	√	√

A key element of physical security is limiting access to network devices to only authorized IT staff by securing equipment in closets, data centers, etc. Networking equipment that must be distributed across the organization, such as printers, APs, scanners, etc. should be secured in such a way as to make it impractical for employees or guests to remove them from the facility.

Equipment must also be protected from unauthorized access. Immediately change all passwords when new equipment is used and use complex passwords if at all possible. For equipment with passwords and security keys, make sure this information is protected and inaccessible if the item were to be stolen. For wireless, most access points either do not store this information locally in the AP, or those that do use some form of EEPROM encryption.

MAC Layer Security

The MAC (Media Access Control) layer of security leverages functions built into the network technology itself (802.3 Ethernet, 802.11 Wi-Fi, etc.). Wi-Fi security is primarily defined by IEEE 802.11i, which was ratified in 2004. The IEEE 802.1x authentication protocol is also a key security element and is used by both wired and wireless technologies.

Security Component	Wired	Wireless
MAC Authentication	√	√
Segmentation (VLANs / SSIDs)	√	√
Data Encryption	NA	√
802.1x Authentication	√	√

For every IEEE 802 MAC layer protocol, tools have been created to aid in segregating and securing the communication channel. Examples include VLANs, SSIDs, encryption protocols, etc. The goal is to allow network access as required, but restrict access to specific resources.

For Wi-Fi, the MAC is the most important layer in implementing a secure network since it is where encryption of the communication occurs. The primary encryption methods are WEP, WPA and WPA2 with the latter being the implementation of the IEEE 802.11i standard.

WEP was the first wireless encryption standard but was cracked within a few years of its inception. Unfortunately, knowledge of this failure has remained in the minds of people today. To address the security holes with WEP, the Wi-Fi industry instituted WPA (Wi-Fi Protected Access). WPA came out in two different versions - WPA and WPA2 with different levels of encryption. WPA2 uses best-in-class Advanced Encryption Standard (AES) and is the recommended Wi-Fi security protocol for use today.

WPA and WPA2 can be implemented in two different ways: Personal and Enterprise. WPA/WPA2 Personal use pre-shared keys with the same key placed into both the AP and the station (e.g. laptop). The key is used to authenticate the station and encrypt its traffic. When using WPA/WPA2 Personal, keys at least 15

characters in length are recommended for best resistance to attacks. Unfortunately, the WPA/WPA2 Personal approach using pre-shared keys has vulnerability with offline dictionary attacks.

WPA/WPA2 Enterprise leverages the 802.1x authentication protocol and is implemented in conjunction with a digital certificate on a RADIUS server. Client-side credentials vary and can include username/password combinations, tokens, or digital certificates. The Wi-Fi security standards are summarized in the following table.

Standard	First Certified	Encryption	Authentication	Relative Strength
WPA2 Enterprise	2004	AES	802.1X w/ EAP	Very High
WPA2 Personal	2004	AES	Pre-Shared Key	Moderate
WPA Enterprise	2003	RC4	802.1X w/ EAP	High
WPA Personal	2003	RC4	Pre-Shared Key	Moderately Low
WEP	1999	RC4	Shared Key / Open	Low

MAC layer security tools exist for wired as well as wireless networks, however authentication and encryption within the protocol are seldom used in wired networks which rely more on other protocols for authentication (e.g. Kerberos-based authentication used with Active Directory).

Network/Transport Layer Security

The network and transport layers (Layers 3 and 4) are where most people envision security to exist, as this is the domain of routers and firewalls. For wired or wireless at the network layer, there is little difference since the technologies function at Layers 1 and 2. In some cases, enterprise routers handle all wired and wireless communications; in other cases, separate controllers provide routing services for the wireless side.

Security Component	Wired	Wireless
Routing	√	√
Firewalls	√	√
Access Control Lists	√	√
Transport Layer Security (TLS)	√	√

While the MAC layer is useful for separating segments of the network and providing authentication and encryption services, the network layer is responsible for controlling individual users and segmenting communication paths per corporate policy. Via the use of routers, ACLs, and firewalls, very granular controls can be placed on communication paths, limiting segments, users, traffic types, etc. The network layer (Layer 3) sits above the wired or wireless network (Layers 1 and 2), allowing the same protocol to manage both.

Application Layer Security

Whether a wired or wireless network is being used is typically invisible to the application. This was one of the primary purposes of the layered OSI network model in the first place.

Security Component	Wired	Wireless
Active Directory Services	√	√
User Names/Passwords	√	√
Stateful Firewall	√	√
HTTPS	√	√

Applications operate for the most part independent of the Layer 2 protocol (MAC) being used. High bandwidth or time-sensitive applications may operate differently based on the type of network, however this is more of a vendor or product selection issue.

Management Security

Management security can be broken into two parts – device level management and enterprise network level management. Device security management entails using secure protocols and methods to configure and manage network systems. Enterprise security management is about monitoring the overall network for threats.

Security Component	Wired	Wireless
SSH/HTTPS	√	√
SNMPv2/v3	√	√
Management DOS Attacks	√	√
Detect Unauthorized Clients	√	√

Enterprise-class wired and wireless equipment can be securely managed via secured communication paths such as SSH, HTTPS, or SNMPv3. In addition, devices can be configured so that they will only respond to requests from specific management stations. Wireless offers additional capabilities for preventing management traffic over the air, thus protecting wireless components from wireless attacks. Both wired and wireless networks have the ability to detect unauthorized clients, however it is seldom used in wired networks.

Media Security

Media security involves identifying and restricting clients or other devices that are attempting to connect to the network or otherwise attacking the media, such as to hinder valid clients from connecting. Both wired and wireless technologies have developed tools to monitor the media and detect issues at this layer.

Security Component	Wired	Wireless
Spectrum Analysis	√	√
IDS/IPS	√	√
Location Tracking	N/A	√
Rogue Detection	N/A	√

An important piece of security on wired and wireless networks is intrusion detection and prevention systems (IDS/IPS). In wireless, these systems include capabilities to scan the RF environment for all types of

unauthorized devices and attacks. Radios are allocated to scan the air, periodically sweeping through each channel in a promiscuous receive mode.

Security Certifications

Any vendor can talk to the security capabilities of their product line, however it is key to verify that the products are certified by a 3rd party to offer the level of protection required by industry standards.

Security Component	Wired	Wireless
PCI	√	√
HIPPA	√	√
FIPS 140-2	√	√
Wi-Fi Alliance 802.11i	N/A	√

Payment Card Industry (PCI) certification applies to products used in point-of-sale environments where debit and credit cards are used. Health Insurance Privacy and Portability Act (HIPPA) establishes standards for electronic health care transactions. FIPS is the Federal Information Processing Standard and defines government level security. The Wi-Fi Alliance provides a certification program for 802.11 standards testing functionality and interoperability.

Summary

Properly designed wireless networks provide a very high level of security that goes beyond that of most of today's wired network implementations. The following summarizes best practices with regards to implementing enterprise-grade wireless security:

- Use a structured, multiple layer approach.
- Implement WPA2 Enterprise wherever possible – this is the most important single security mechanism. Using WPA2 Enterprise eliminates the impact of many attacks.
- If using WPA/WPA2 Personal, use long pass-phrases (a minimum of 15-20 characters) which are much more resistant to attacks.
- Segment users into different groups, through SSIDs and VLANs, and leverage firewall rule sets to give each group only the access they need.
- Don't overlook the basics, such as changing default values and end-user security awareness training.

Wi-Fi Security Frequently Asked Questions

The following is a collection of some of the most common questions concerning the ability of Wi-Fi to provide secure networking.

Q: What are the standards that define Wi-Fi security?

A: The IEEE 802.11i standard defines security policies for Wi-Fi.

Q: Does Wi-Fi support 802.1x and RADIUS standards for authentication?

A: Yes. IEEE 802.1x port security and RADIUS authentication works over both wired and wireless networks.

Q: With what security standards/policies does Wi-Fi comply?

A: The primary Wi-Fi security specification is defined by IEEE 802.11i. Additional wireless standards and certifications supported by Wi-Fi include:

- DoD 8100.2 – defines the security policies for the use of wireless by the Department of Defense
- FIPS 140-2 (Federal Information Processing Standard) – U.S. government-grade security certification
- HIPAA (Health Insurance Portability and Accountability Act) – U.S. national standards for electronic health care transactions
- GLBA (Gramm-Leach-Bliley Act) – personal financial information security in banking and finance
- PCI DSS (Payment Card Industry Data Security Standard) – information security standard for organizations handling cardholder information
- SOX (Sarbanes-Oxley) compliant – U.S. federal law that sets standards for public companies

Q: Can two secured Wi-Fi clients, connected on same SSID and radio, see each other's traffic?

A: No. Even though each may use the same shared key (in the case of WPA2/WPA Personal) and encryption protocol, each client negotiates its own set of encryption keys that are used to secure the specific communications. If data is captured from another client, it cannot be decrypted.

Q: What is the major difference between wired and wireless security?

A: Wired networks typically rely on perimeter security, which relies on the physical boundaries of the environment where the network operates. Since RF signals can propagate great distances, wireless security is focused on protecting the communication itself via strong authentication and encryption protocols.

Q: Can you use a private VPN over Wi-Fi?

Yes. In general, VPNs will work over wired, wireless, and WAN networks and provide end-to-end security in addition to what is provided by the network itself.

Q: Can you securely roam between access points?

A: Yes. When a client completes the association process to an access point, a master secure key is created. This is the Pairwise Master Key (PMK) from which additional keys are created to protect the actual communication. The Wi-Fi security standard 802.11i identifies how this key can be shared between access

devices to allow secure roaming without having to re-authenticate each time the client re-associates to a new AP.

Q: Is Wi-Fi subject to Denial of Service (DoS) attacks?

A: Yes. DoS attacks can occur at many layers in wired or wireless networks. Layer 1 DoS attacks can occur in Wi-Fi whereby radio transmitters are used to flood a channel with noise to thwart valid communication traffic. IDS/IPS systems are used to detect and mitigate most types of DoS attacks.

Q: What is a 'Rogue'?

A: The term rogue normally identifies an Access Point that is not approved to operate in a network. It could be a device deployed as a malicious threat to the network, an unauthorized device deployed by an employee, or an AP that belongs to a neighboring business.

Q: How do you detect Rogues?

A: There are many different tools that can be used to detect Rogue AP devices by scanning available Wi-Fi channels for activity by other devices. Free tools such as Netstumber or Xirrus Wi-Fi Inspector (<http://www.xirrus.com/library/wifitools.php>) can be used on laptops with a Wi-Fi card. Most APs support a mode whereby one of the radios will scan the RF environment for rogue devices. At the top end of the scale, IDS/IPS systems provide this function with dedicated threat sensor APs and include rogue mitigation functionality.

Q: What determines when a Rogue device is a threat?

A: This will vary by organization. Some organizations will consider any non-authorized AP as a threat while other organizations will set criteria based on signal level or encryption. Items to consider are:

- Is the rogue using strong security? If so, it may be unauthorized but is probably not a threat.
- What SSID is being broadcast? This may help to identify who owns the device (i.e. Starbucks). It is a more serious threat if the rogue is advertising your organization's SSID (spoofing).
- How strong is the signal? This will give an indication of where the device is located. A strong signal may indicate the device is within the physical boundaries of your organization.
- Note: Just because you see unknown APs, it does not necessarily mean they are a threat and that you should take action about them. Wi-Fi uses unlicensed frequencies and even though they may potentially interfere with your network, they may be operating legally.

Q: How do IDS/IPS services prevent rogue APs from interfering with the Wi-Fi network?

A: With respect to rogue APs, Intrusion Detection Systems (IDS) are used to detect and locate these devices. Intrusion Prevention Systems (IPS) are used to prevent rogue devices from interfering with the network, typically done by attracting your clients to their radios. Once a rogue device is detected, an alert is generated to inform administrators of the new device. Most systems also include the ability to provide location information. If it is determined to be a threat, staff should be dispatched to physically locate and remove the device if possible. In conjunction to this, IPS functions have the ability to interrupt communication between

the rogue AP and any associated client devices. The protocols and process used to actually disrupt the communication will vary by vendor.

Q: Can unauthorized clients be detected in a Wi-Fi network?

A: Yes. Any transmitting Wi-Fi device can be detected, identified and/or located.

Q: Can you detect Wi-Fi devices that are just listening and not transmitting?

A: No. If a device is not generating a signal and not connected on the wired network, it is not possible to detect the device via traditional means. Such devices listen promiscuously and intercept data. Standard encryption methods will prevent the data being compromised.

Q: How does location-tracking work and how accurate is it?

A: There is no standard method for location tracking, however the two most common ways are using either dedicated tracking sensors or multiple AP radios to locate the device. The sensor method requires the deployment of sensors to define the network boundaries. Then devices can be located based on their relation to known network points. The second method uses multiple radios to 'triangulate' the location of the device based on how the signal is received. The more radios 'seeing' the device, the more accurate the location can be. Typical Wi-Fi location services provide a three to five-meter resolution.

Q: Can I use the same authentication and directory services with wired and Wi-Fi networks?

A: Yes. Wi-Fi operates at a lower level (Layer 2 in the OSI stack), so all standard AAA and directory services (AD, LDAP, RADIUS, etc.) run transparently over both wired and wireless networks.

The Xirrus Wi-Fi Security Implementation

Today's Wi-Fi networks face a number of potential security threats in the form of rogue access points, ad-hoc clients, unauthorized clients, wireless-based attacks, eavesdropping, etc. As 802.11n continues its increased adoption in enterprise networks, the importance of defending against these threats is becoming more critical. The Xirrus Wi-Fi Array was engineered to deliver the primary network connection for the enterprise over wireless. To that end, the highest level of security protection has been integrated into each Array.

Xirrus' approach of implementing all security elements at the edge of the network, instead of dividing the functions between the edge and a centralized controller in the closet, delivers the best RF view of the environment as well as the highest level of security performance. The Array performs all encryption in hardware and at line rate in each Array, thereby avoiding the oversubscription choke point created when traffic is backhauled to a central encryption engine in a centralized controller.

Every Array supports a comprehensive suite of security features from Layer 1 to Layer 7, plus mechanical security elements, to provide a complete multi-layer security solution. Key among these are:

- WPA2 Enterprise (AES encryption with 802.1x authentication) for the most secure data transport. WPA2 uses government-grade 128-bit AES encryption. 802.1x authentications ensure unique encryption keys per user, per session, and per data packet.
- Dedicated threat sensor radio allocated in each Array, (or every other depending on network design) for complete 24x7 IDS/IPS coverage of the RF environment. Rogue APs and Wi-Fi attacks are detected and mitigated via this threat sensor radio. This is distinct from time-sliced functionality on traditional 2-radio APs, which share radio resources between servicing users and detecting threats. This method significantly compromises security coverage by limiting the time the RF environment is being monitored.
- Integrated firewall in each Array for restricting traffic and thwarting threats at the network edge as opposed to allowing such traffic to traverse the network.
- Guest access management to identify, authenticate, and isolate guest users on the network to ensure security of corporate resources.
- Security compliance auditing to enforce appropriate configuration for compliance with the security requirements of the network. The Xirrus Wi-Fi Array includes optional PCI and FIPS140-2 audit modes to monitor compliance.

Xirrus Array security components are packaged in the RF Security Manager (RSM) option. The RSM provides complete wireless network security and minimizes the risk in deploying 802.11n wireless networks. The RSM includes:

- Intrusion Detection and Prevention - rogue scanning, blocking, alerts, and logging
- Stateful Firewall
- Web Page Redirect
- User Group Policies
- PCI Compliance Enforcement

- SSID/Group Time of Day access control
- ACLs
- NAC Integration via re-authentication timer
- Internal RADIUS server

Leveraging the integrated 24/7 threat sensor radio and hardware-based encryption/decryption in each Array, the RSM secures the Wi-Fi network from multiple types of threats. The result delivers uncompromised overall network security with greater flexibility and performance compared to traditional centralized Wi-Fi networks.

The following sections describe the Xirrus wireless security solution in greater detail.

Array Physical/Mechanical Security

Security is not just for the communication channel; it must start at layer 1 and includes a full set of physical as well as mechanical security components to protect the Array. Physical layer security features built in the Wi-Fi Array include:

- A Kensington locking device, which makes removal difficult without specific knowledge of the mechanism.
- An indoor locking enclosure compatible with all Wi-Fi Array products. This 2ft x 2ft enclosure replaces a standard drop-ceiling tile and can be secured via lock and key. An optional tamper detect mechanism for the enclosure is available which will send an alert via SNMP trap if the enclosure door is opened.
- Tamper detection seals that clearly identify if an Array was physically opened.
- Protected power connection to prevent malicious/accidental power down.
- Full configuration information is stored on the Wi-Fi Array, including SSID, VLAN, IP addresses, admin login, pre-shared keys, external RADIUS server addresses, etc. No information is at risk of being compromised as the data is stored in a secure EEPROM encrypted with MD5 hash 128-bit encryption.

MAC Layer Security

The Xirrus Array is fully 802.3/802.11 compliant supporting all standard security features defined within these protocols, including but not limited to:

SSIDs and Security Policies

The Wi-Fi Array supports up to 16 SSIDs across the 2.4GHz and 5GHz bands and each can be defined with independent association policies, security settings, QoS, and forwarding policies to meet varying requirements. Each can be defined and maintain individual security policies with the following:

- Broadcast - On/Off
- QoS Priority - 4 levels (queues)
- VLAN ID - Number and/or name
- Band Association 802.11a, 802.11bg or Both
- DHCP Pool - for internal DHCP
- Traffic Limit - None/SSID/Client
- Operational times - Day/Time
- Security Type - Open, WEP, WPA, WPA2 or WPA-Both
- Security Settings - Global for Array or SSID specific
- Per User Packet Throttling
- Each SSID can be bound to separate VLAN

Authentication

Authentication ensures users are who they say they are, and occurs when users attempt to join the wireless network and periodically after that. The following authentication methods are available:

RADIUS 802.1x - 802.1x uses a remote RADIUS server to authenticate large numbers of clients, and can handle different authentication methods (EAP-TLS, EAP-TTLS, or EAP-PEAP).

Internal RADIUS server - Includes all the core functionality of a full RADIUS server built into the Array.

Pre-Shared Key (PSK) - Uses a pass-phrase or key that is manually distributed to all authorized users. The same pass-phrase is given to client devices and entered in each Array.

MAC Access Control Lists (ACLs) - MAC access control lists provide a list of client adapter MAC addresses that allowed or denied access to the wireless network, and can be used in addition to any of the above authentication methods. ACLs are good for embedded devices, like printers and bar-code scanners (though MAC addresses can be spoofed). ACLs can be assigned at the Array or SSID level. The Array supports 512 ACL entries.

Web Page Redirect (Captive Portal):

- Web based authentication against an internal or external RADIUS server
- Local host or remotely hosted web page redirect (log-in/splash screen)
- Configure splash screen time out
- Array can limit users on physical site, time of day, day of week, and amount of traffic

The Wi-Fi Array fully supports 802.1x authentication servers. Xirrus has performed extensive verification testing with NPS, IAS, ACS, Odyssey, OSX, Free RADIUS, Radiator, and other AAA servers. Xirrus interoperates with external RADIUS servers to authenticate users to Microsoft Active Directory. RADIUS failover capability is supported by allowing the specification of primary and secondary servers and timeout values. All Wi-Fi Arrays also include an integrated RADIUS server that may be used for authentication of wireless clients.

Extensible Authentication Protocol (EAP) is the authentication framework used by 802.1x and defines different methods for negotiating authentication. Those methods supported by the Wi-Fi Array and certified by the Wi-Fi Alliance are:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM
- EAP-AKA
- EAP-FAST

In addition, the Array supports pass through of Lightweight EAP (LEAP), a proprietary method developed by Cisco.

Encryption

Encryption ensures that no user can decipher another user's data transmitted over the air. Encryption is performed in hardware in the Array at line rate. There are three encryption options available:

- WPA2 with AES – Advanced Encryption Standard (AES) is government-grade encryption and is available on most of today's client adapters. The IEEE 802.11i standard specified use of 128-bit AES. Its use is strongly recommended in any enterprise wireless networks.
- WPA with TKIP – Temporal Key Integrity Protocol (TKIP) provides good encryption for Wi-Fi networks. It was designed as a solution to replace the original Wi-Fi security standard of WEP using the same client hardware (AES required new hardware). TKIP solves the security issues of WEP by using more sophisticated key mixing and sequencing to create unique keys per user and per packet. In addition, TKIP provides a Message Integrity Check (MIC).
- WEP – Wired Equivalent Privacy (WEP) was the original security mechanism standardized for Wi-Fi in 1999. It comes in two versions – WEP-40 and WEP-104 – which use 40-bit and 104-bit keys respectively. WEP was found to be vulnerable to cracks less than 2 years of its standardization. It is still commonly used, especially on legacy clients, however we recommend it is deployed only when absolutely necessary.
- The Xirrus Array supports AES and TKIP simultaneously on the same SSID. This allows different types of clients access to the same SSID with different encryption types. In general, it is best practice to minimize the number of different SSIDs operating in a given environment.

Client Security

Additional Array features available to protect clients include:

- Station-to-Station traffic blocking
- SSID to VLAN mapping
- Traffic limiting per SSID or client
- Time of day, day of week access

- ACLs by individual MAC or client type (including wildcards)

Network/Transport Layer Security

Stateful Firewall

The Wi-Fi Array provides an integrated firewall with stateful traffic inspection to allow or deny traffic directly at the network edge. Non-stateful filter rules can also be defined for blocking or forwarding traffic. The firewall blocks packets from traversing one network interface to another, including from wireless to wired and wireless to wireless. Firewall rules can be set to block by protocols, MAC addresses, VLANs, SSIDS, and ports, including sources and destinations.

With stateful traffic inspection, once a user flow is established through the Array, it is recognized and passed through without application of all defined filtering rules.

The Array also offers administrators the ability to create Filter Lists. These are groups of individual filters that may be applied to SSIDs or User Groups. This feature provides a quick way to apply a large number of filters at one time.

MAC Access Control List

MAC Access Control Lists (ACLs) specify client MAC addresses that are allowed or denied access to the wireless network, and can be used in addition to any of the above authentication methods. ACLs are good for embedded devices, like printers and bar-code scanners, however MAC addresses can be spoofed. ACLs can be assigned at the Array or SSID level.

Secure Roaming

The Xirrus Wi-Fi Array design allows users to seamlessly roam between IAPs (integrated access points) and between Arrays whether or not they are on the same VLAN or IP subnet (Layer 2 and Layer 3 roaming). Normal RF design of an Array network provides some coverage overlap (nominally 10-15%) between adjacent Arrays to accommodate this.

Roaming times between the IAPs in an Array are very quick (sub-10 msec) and between Arrays sub-50 msec. Xirrus Arrays support the 802.11i provision, which allows the optional use of PMK (Pairwise Master Key) Caching. This feature was designed to allow wireless access points to store authentication information in order to reduce roaming times when stations move between access points. Without this capability, authenticated clients who roam would need to re-authenticate with the new access point. Depending on the authentication method and location of authentication server (RADIUS) the delay could be substantial.

Application Layer Security

Active Directory Integration

The Xirrus Wi-Fi Array integrates with Windows Active Directory (AD) environments for authentication and application of user policies. The interface to an AD environment is provided via a RADIUS server. Xirrus has performed extensive interoperability testing with 3rd party RADIUS servers, including NPS, IAS, ACS, Odyssey, OSX, Free RADIUS, Radiator, and others. In addition, all Wi-Fi Arrays contain an integrated Free RADIUS server.

The Array provides RADIUS server failover capability by allowing the specification of primary and secondary RADIUS servers and timeout values.

Stateful Firewall

The integrated stateful firewall in the Xirrus Wi-Fi Array provides application-level traffic filtering via the specification of application port numbers (ranging from 1 to 65534). A pre-built list of more than 50 application traffic types can be chosen from when creating firewall rules.

Management Security

Secure Device Management

Device management involves secure protocols and methods for configuring and managing network devices. The Xirrus Wi-Fi Array provides a number of functions related to secure device management, including:

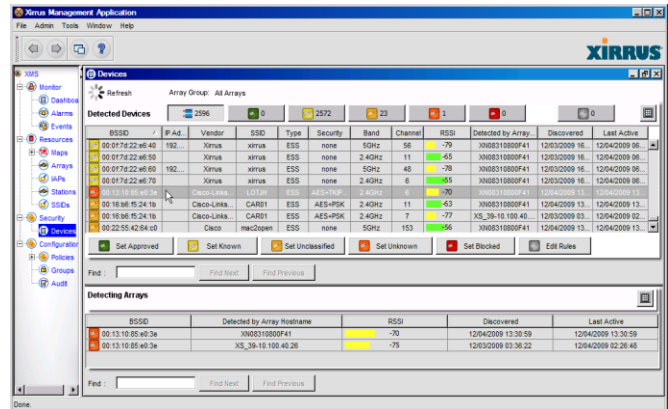
- Ability to block management traffic on any or all methods and interfaces. Methods include SSH, Telnet, serial console, HTTPS, and SNMP while interfaces includes both wired and wireless access to the Array.
- Secure web management access via HTTPS
- Secure command line management via SSHv2
- Dedicated out of band management via separate 10/100 port (XN8, XN12, and XN16 model Arrays)
- Secure network management via SNMPv3
- Granular administrator accounts with up to 7 privilege levels
- 802.1x authenticated administrator accounts
- Internal/external syslog support
- Idle session timeout
- Administrator change logs

Secure System Management

The Xirrus Management System (XMS) uses the SNMP and streaming interfaces to provide central management of a Xirrus Wi-Fi Array network. The XMS automatically discovers, configures, and monitors an Array network, and can scale from single-site to large-scale, multi-site deployments.

The XMS provides network-wide security monitoring by providing a centralized view and command center for the security information of all the Arrays on the network:

- Centralized wireless intrusion detection and prevention system (IDS/IPS) to detect and mitigate rogues and attacks
- Information per rogue device includes:
 - Type of encryption, SSID, MAC address, product vendor, device type, band used, channel used, RSSI value, discovery time, last active time, and detecting Array(s)
- Automated alerting upon discovery of new, potential rogue devices



Media Security

The Wi-Fi Array has a dedicated threat sensor radio that constantly scans the local wireless environment for rogue access points, unencrypted transmissions and other security issues. Administrators can then classify each rogue access point and ensure that these devices do not interrupt or interfere with the network. Other solutions use a shared radio model that causes users and scanning to share time on the radio, effecting performance and security.

The threat sensor is a default component of the Array; it will automatically detect report and mitigate threats from rogue APs (IPS).

Xirrus integrates an IDS/IPS service in all Wi-Fi Arrays that uses the RF threat sensor to provide proactive monitoring of the Arrays' environments and will report on all Rogue APs and unauthorized clients detected. When unknown APs are detected they can be classified as rogues and blocking enabled to prevent users from inadvertently connecting to these devices. Additionally unauthorized clients can be identified and prevented from accessing the Array.

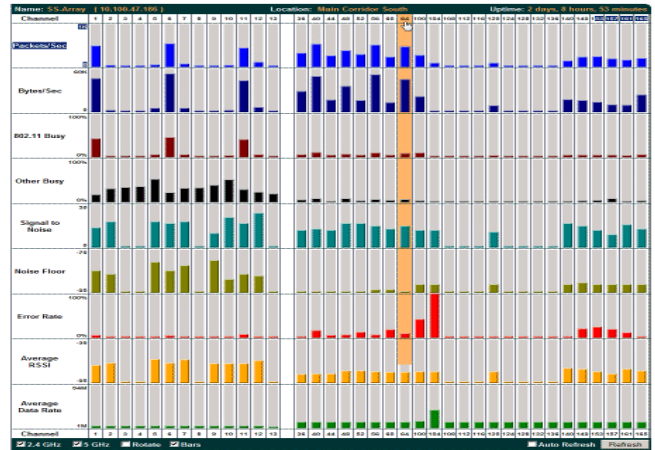
Key threat sensor features include:

- 24x7 monitoring of the wireless RF environment without "time-sharing" radios with Wi-Fi client stations
- Leverages embedded RF threat sensor built into each Wi-Fi Array for threat/attack detection and prevention
- Detection of potential rogue or malicious APs, ad hoc, and stations
- Rogue device classification
- Automatic alerts, alarms, and logging of rogue devices
- Key rogue device information such as first seen, last seen, manufacturer, SSID, channel
- Triangulation from multiple Arrays to accurately locate unauthorized device to within approximately 5 meters
- Automated shielding of rogue devices by Array radios to contain threatening devices when detected, while still scanning for new threats

- Ensures compliance with wireless security policies and regulations through automated reporting
- Blocking of access by time of day, day of week and traffic thresholds

Integrated Spectrum Analyzer

The Wi-Fi Array provides a distributed spectrum analysis capability that covers the entire Wi-Fi network. The spectrum analyzer uses the Array's threat sensor radio to monitor the RF environment and analyze interference in the network. This provides 24/7 and network-wide coverage in contrast to traditional spectrum analyzers that require the user to be in the right place at the right time to analyze interference sources or threats. The Array monitors all 802.11 channels in 2.4GHz and 5GHz, not just those currently used for data transmission.



The RF Spectrum Analyzer displays traffic and RF statistics in real-time for all channels as measured by the Array's threat sensor radio as well as values measured by each user servicing radio on its current channel. When enabled, the spectrum analyzer will scan across all Wi-Fi channels with the analyzer window presenting the data in a graphical display of bar graphs or numerical statistics for all RF measurements.

Security Certifications

The Wi-Fi Array is fully certified by Wi-Fi Alliance for: 802.11a/b/g/n, WPA, WPA2, and Extended EAP (Extensible Authentication Protocol) types including:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

In addition to the standard EAP types, the Array also supports Cisco LEAP pass-through.

Additional security certifications and compliances include:

- DoD 8100.2 – defines the security policies for the use of wireless by the Department of Defense
- FIPS 140-2 (Federal Information Processing Standard) – U.S. government-grade security certification
- HIPAA (Health Insurance Portability and Accountability Act) – U.S. national standards for electronic health care transactions
- GLBA (Gramm-Leach-Bliley Act) – personal financial information security in banking and finance
- PCI DSS (Payment Card Industry Data Security Standard) – information security standard for organizations handling cardholder information
- SOX (Sarbanes-Oxley) compliant – U.S. federal law that sets standards for public companies