WHITE PAPER: IRONSHIELD BEST PRACTICES SECURITY & WIRELESS LANS

Written By: Philip Kwan

July 2003

July 2003
Version 1.0.0

Introduction

The IronShield Best Practices: Security & Wireless LANs document is designed to help network and security administrators understand the security aspects of wireless LANs. The document illustrates the traditional weaknesses of 802.11b's WEP encryption scheme and presents the technology that helps to secure wireless LANs in the enterprise. Coupled with the many other network security features available with Foundry's switches and routers, enterprise can apply security in layers and achieve a "Defense-in-Depth" design with multiple levels of monitoring.

IronShield Security is not meant to replace Data Security infrastructures. With careful planning and implementation, IronShield Security features can help improve Network Security and enhance Data Security where it's needed.

Contents

IRONSHIELD SECURITY 3
AUDIENCE 3
THE WIRELESS EVOLUTION 4
BENEFITS OF WIRELESS LANS 4
BARRIERS TO IMPLEMENTATION 4
802.11X TECHNOLOGY IMPROVEMENTS 5
ENTERPRISE WIRELESS APPROACHES 6
STANDALONE APS (FULL FEATURED APS) 6
AP AGNOSTIC WIFI APPLIANCES 7
WIRELESS LAN SWITCH & AP SOLUTIONS 8
THE WIRELESS LAN SECURITY BARRIER 9
PROBLEMS OF EARLY 802.11B DEPLOYMENTS 9
WIRELESS SECURITY FOR ENTERPRISE 11
WIRELESS AUTHENTICATION 11
802.1X WiFi Authentication 11
Extensible Authentication Protocol (EAP) 12
WIRELESS ENCRYPTION 14
WEP With 802.1X 14
WPA With TKIP 14
AES & IEEE 802.11i 15
DESIGNING SECURE WIRELESS NETWORKS 16
AUTHENTICATION & DATA PRIVACY SOLUTIONS 16
CRITERIA FOR EAP SELECTION 17
WIRELESS NETWORK DESIGN STRATEGIES 18
Wireless Realms 19
Virtual LANs (VLAN) & ACLs 20
VPN Technology 20
802.1X Overhead Planning 21
Authentication Server Planning 21
Firewalls and Monitoring Device Placement 23
OTHER TIPS AND SUGGESTIONS 24
SUMMARY 26

Disclaimer

IronShield Security

Foundry's IronShield Security "Best Practices" papers serves as a guide to assist network and security designers in architecting and applying Foundry security features in their networks. Modern enterprise security is applied in layers – Defense in Depth. Consideration must be given to all the various layers with a full understanding of what threats are possible at each layer before implementing a defense strategy. By applying security in multiple layers, the defense is strengthened and vulnerabilities in one layer will not likely lead to successful attacks of corporate resources. The goal is to make it harder to attack your network by layering security chokepoints.

These practices should accompany your Security and Computer Usage Policies, not replace them. Applying the steps outlined in this "Best Practices" guide does not guarantee that attacks will not be successful against your security defenses and network resources. The best security design is dynamic. It must be coupled with a strong security policy, proactive network monitoring, diligent network and security staff that are working to stay on top of security alerts and system software upgrades and patches. Enterprise data security is always changing and growing with the advent of new security threats. Thorough, rigorous, and continuous inspection of all security components and processes will help you keep on top of the enterprise network.

IronShield Security documents are specifically written to work with Foundry products and work in conjunction with related Foundry documentation. Reference to other Foundry documentation is made with regards to command syntax and general feature information.

This Best Practices White Paper is designed to help network and security administrators understand how to design and implement secure wireless networks. It identifies the different authentication and data privacy features that are available in modern wireless components and describes how they can be part of your enterprise's wireless strategy.

Audience

IronShield Security "Best Practices" papers are designed to help the personnel responsible for designing and configuring the network and security components of an enterprise network. The topics discussed are at a beginner to intermediate level and assumes a good understanding of TCP/IP and related technologies.

The Wireless Evolution

Wireless networks have been available since 1999 with the introduction of 802.11b and have been widely accepted as a SOHO (Small Office Home Office) technology providing home user's with the convenience of wireless networking. With the many apparent benefits of wireless networks, users are asking their companies to install wireless technology for them to conduct business. Although wireless networking has been popular in the SOHO market place, enterprise network and IT managers have been slow to implement wireless LAN technology for business purposes. This is largely due to the vast amount of negative news surrounding early 802.11b wireless technology, where authentication and encryption was very weak and easily exploitable.

As popularity for wireless technology increases, additional standards will be developed by the IETF and IEEE to address the wireless security concerns and other short comings. Wireless vendors will continue to adopt the latest technology to help secure the wireless space and drive the cost of wireless implementation and ownership down. In turn, this will help the adoption of wireless technology in enterprise.

Benefits of Wireless LANs

As many early SOHO adopters have found, wireless networks provide many benefits. As enterprise enters the world of wireless networking, they are realizing the same benefits as the home user, but on a much larger scale. The benefits of wireless LANs include:

- Increased mobility by allowing employees to conduct business in all areas of the enterprise.
- Increased productivity by giving employees continuous access to information.
- Removes traditional cabling issues by eliminating the need for physical cable plants.
- Replaces cable plants in hostile networking environments - such as manufacturing and warehousing.
- Augments existing cable plants by allowing the addition of more network devices without the installation of new cable.
- Easy installation and rapid deployment.
- Broad OS support – Windows, MAC, Palm OS, etc.
- Lower long term costs.
- Rapid deployment

Barriers to Implementation

Wireless networks have garnished much press since its inception. With the many advantages also came the publicizing of the many weaknesses of early 802.11b's security features – causing enterprise to adopt a "wait and see" attitude towards the technology. Some the more common concerns of wireless LANs include:

- Wireless security - still the single largest concern of IT and Security managers
  - Static 40-bit and 104-bit WEP encryption keys can be compromised (based on RC4)
  - Short Initialization Vector (IV) allows encryption key to be reused
  - MAC Address filtering can be spoofed
  - 802.11x user authentication technology is not readily available or is a foreign technology
  - Any user can attempt to authenticate to the system – both employees and non-employees
  - Access Point (AP) units are not authenticated leading to rogue APs on the enterprise LAN
- Proprietary security features can force enterprises down a proprietary path – no interoperability
- No central AP management standard
- Unauthorized rogue APs brought in by employees are hard to detect and manage

- Limited wireless client management and reporting
- Limited Layer 3 roaming support
- Speed and capacity of 802.11x technology

802.11X Technology Improvements

To address the many downfalls of the early 802.11x implementations, the IETF and 802.11 IEEE Committee has proposed many new standards. Wireless vendors are converging on each standard with many new features which addresses each of the barriers.

802.1X Authentication	802.1X technology provides strong user authentication against an authentication server (mainly RAIDUS). 802.1X uses Extensible Authentication Protocol (EAP) to secure authentication transmissions – TLS, TTLS, LEAP, and PEAP. Authentication server can further enhance access control by providing user policy and VLAN information for the user.
WiFi Protected Access (WPA)	WPA is an interim technology that has been agreed upon by many wireless vendors until 802.11i is fully implemented. WPA uses 802.1X authentication and can use a RADIUS server with EAP or a preshared key to secure the data. With WPA, rekeying of encryption keys is required with the use of TKIP. WPA is trying to address interoperability issues as well.
Temporal Key Integrity Protocol (TKIP)	TKIP is used by WPA to rekey the unicast traffic's encryption key. Every data frame transmitted over the wireless space is rekeyed by TKIP. TKIP synchronizes the key change between the client and the AP. Global encryption keys are changed by an announcement to all connected clients by the WPA protocol.
Message Integrity Code (MIC/Michael)	MIC (also known as Michael) is a technology that is required by WPA to strengthen the integrity checks for each packet. With the older WEP encryption method, a 4 byte integrity check value (ICV) was appended to the end of the encrypted packet. Although the ICV was encrypted, it could still be manipulated without detection – allowing for replay attacks. Michael uses an 8 byte message integrity code (MIC) that is encrypted using MAC address information, the frame data, and the ICV and is place between the data payload portion of the 802.11 packet and the ICV. MIC uses a new frame counter in the 802.11 frame to prevent replay attacks.
802.11i WiFi Security	802.11i is an emerging standard that will replace the existing static WEP encryption technology. It uses strong AES encryption which is much lighter than traditional 3DES encryption standardized by Virtual Private Network (VPN) implementations. Will require existing users to upgrade older hardware that does not support 802.11i. The standard is expected to be fully ratified by the end of 2003.

Inter Access Point Protocol (IAPP) 802.11f	IAPP registers APs in a wireless LAN to allow the rapid exchange of information between APs as users roam from AP to AP. The standard solves Layer 2 roaming issues in a multi-vendor environment. The standard is expected to be ratified by the end of 2003.
QoS 802.11e	The proposed IEEE 802.11e standard is designed to provide QoS services for wireless LANs to support voice, multimedia, and data applications. The proposal is backwards compatible with existing 802.11a and 802.11b technologies and will be implemented in the APs to support home users, enterprise, and hot spot implementations. The standard is expected to be ratified in mid to late 2004.
Dual Band APs	Multi-radio APs are now supporting 802.11a/b/g in a single unit. As radio technology is improved, speed and capacity will increase. Technologies that enable APs to automatically detect and correct for radio frequency interference, power levels, and capacity load balancing will be available for testing before the end of 2003. Wireless transmission speeds are continuing to improve: • 802.11b (11 Mbps) • 802.11a (54 Mbps) • 802.11g (54 Mbps with greater distance than 802.11a) • 802.11a Turbo Mode (108 Mbps)
Light Weight Access Point Protocol (LWAPP)	Several vendors are promoting a new technology called LWAPP to address how switches/routers communicate with APs. If ratified, this technology can standardize the protocol between network devices and APs to allow multi-vendor interoperability. Eliminating the need for vendor specific APs and allowing APs to be managed through standardized calls verses proprietary code. As of July 2003, this is currently an IETF draft.

Enterprise Wireless Approaches

As wireless vendors moved into the enterprise space, several topologies have been developed that has ranged from standalone APs with strong security to vendor agnostic wireless appliances to a combination of both.

Standalone APs (Full Featured APs)

Standalone or Full Featured APs are wireless access points that can function on their own. They provide the necessary authentication, security, management, and basic logging and reporting functions in a single contained unit. For enterprises that are only beginning to experiment with wireless networks, or have small to mid-sized wireless deployments, these APs can be a cost effective solution. Full Featured APs are generally managed individually on a one-to-one basis with either a Web interface or a CLI interface directly embedded in the access point.

Full-Featured APs are an evolution of SOHO technology with the latest features that provide enterprise class security. Security features will vary between manufacturers but most modern enterprise Full Featured APs will have:

- 802.1X authentication to a RADIUS server
- MAC address filtering
- WEP (40-bit to 104-bit)
- WPA with TKIP or Preshared Key
- Basic logging and reporting

The main disadvantage of Full Featured APs is the management aspect. There is no centralized management interface and reporting system to help coordinate access point inventory, provisioning, radio frequency coordination, radio power levels, capacity load balancing, and so forth. But the advantages are lower hardware costs, simplicity, and rapid deployment with the latest security enhancements.

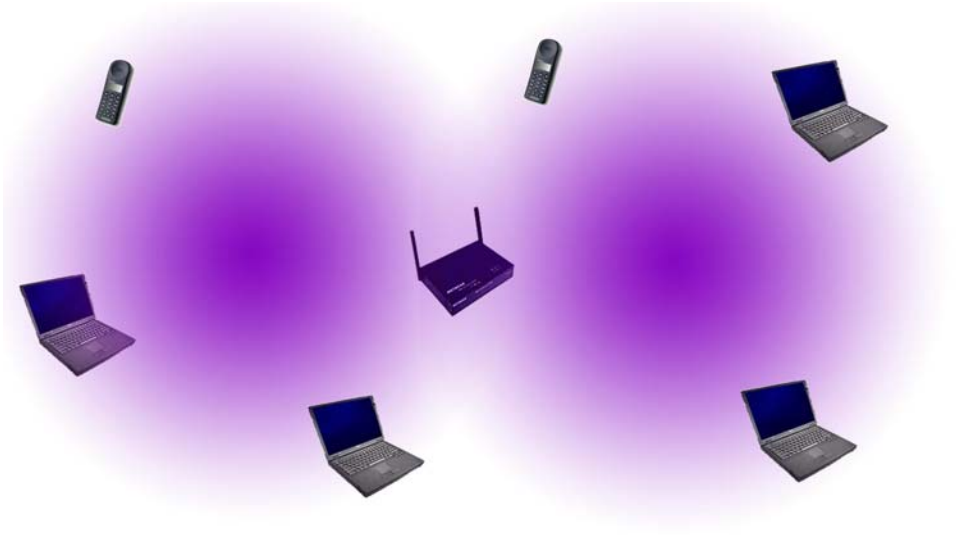

Figure 1. Full Featured AP

AP Agnostic WiFi Appliances

Some vendors have developed WiFi appliances that are AP agnostic – allowing any AP to be used with the WiFi appliance. These solutions are self contained appliances that are generally based on a hardened Unix operating system and have the following functions built into them:

- 802.1X authentication
- Local user database and group support
- Data encryption including WEP, WPA, 3DES, and AES
- VPN support may be available
- User policies to control access (static packet filters)
- Mobility for roaming between APs and WiFi appliances
- AP agnostic (can use any AP)
- Web based management, reporting, and logging
- Client software may be required on each wireless device

The WiFi appliance approach has many advantages over the Full Featured AP implementation, but has one major disadvantage. Performance is often fairly low as the WiFi appliance is performing the authentication, data privacy security, packet inspection, user policy, and packet forwarding functions. The cost of the WiFi appliance solution is much higher than the Full Featured AP solutions.

Wireless LAN Switch & AP Solutions

High-end, enterprise class wireless networking solutions have begun to emerge in 2003. These solutions are moving towards a combined topology that uses a WLan Switch (Wireless Switch) and Thin APs. This approach leverages the best of both networking components to deliver security, speed, and rich feature set.

With this "combined" topology, the Thin AP is designed to perform the following tasks:

- Real time 802.11 functions, such as packet translation from wireless to Ethernet
- Packet encryption and decryption – WEP, WPA/TKIP, AES
- Layer 2 AP to AP handoff
- VLAN tagging
- Quality of Service (QOS)

The WiFi Switch is designed to perform the following tasks:

- User authentication – 802.1X, Web
- User policy enforcement – packet filtering ACL's, MAC address filtering, VLANs
- Layer 3 mobility support
- AP management
- Reporting and logging functions

Figure 2. WLan Switch Solution

By splitting the functions between two devices, the WLan Switch and AP solution can support higher bandwidth applications and can support many more APs and wireless users. Additional features are possible by tightly integrating the APs to mature switch and router technology. The disadvantage is the higher cost of these solutions and the proprietary implementations from each vendor – making these solutions non-interoperable between wireless vendors and APs.

The Wireless LAN Security Barrier

As the popularity of wireless LANs grow, enterprise managers will have to address the implementation of this technology into their existing wired networks. Although there are many possible barriers to wireless technology, the single largest concern that enterprise managers have is wireless security. The challenge of how to implement wireless LANs with the traditional secured wired network will be the greatest barrier. With wired networks, the attacker must physically gain access to the network or host (through the wired network) before they can begin to attack or probe the system. With traditional network security and monitoring systems (such as firewalls, intrusion detection sensors, and various network monitoring applications), discovering and containing attacks on wired networks are well understood by network and security professionals.

Authentication and access control are well understood on wired networks, but wireless networks posed new challenges:

- How can you securely authenticate wireless users over the public airwaves?
- How can you prevent someone from listening in on the wireless sessions and authentication exchanges?
- How can you prevent well-known exploits such as session hijacking, identity spoofing, man-in-the middle attacks, replay attacks, and so forth?
- How can you prevent other users who are non-employees from associating with your wireless network?

With wireless networks, the attacker can be anywhere within radio range to perform their mischievous activities. Reports of attackers using modified antennas to receive wireless information from several miles away are not uncommon. In addition, monitoring and attack detection systems are still in their infancy in the wireless space – adding to the uneasiness of wide enterprise wireless adoption. Early implementations of 802.11b wireless technology that revolved around 40-bit WEP was a security disaster. Often being breached within hours or days with the methods clearly published on the Internet for others to try. With the reports of "war chalking" identifying non-secure or "open" wireless networks, the fear of wireless LANs was further increased.

Due to the publicity surrounding the security exploits of early 802.11b technology, many enterprise network managers and security professionals held off on wireless implementations. The methods used to break 802.11b's WEP encryption and the availability of the tools and methods used to perform these attacks were all too common. But this didn't stop wireless from entering the enterprise. Employees who wanted the wireless mobility advantages to conduct business often purchased their own APs and connected them to their corporate networks - without notifying their corporate IT or security departments. These rogue access points often forced companies to adopt very firm "non-acceptance" wireless policies and further restricted the wireless adoption in enterprise.

But not all wireless technology is negative. As the demand for wireless technology continues to surge, wireless manufacturers, the IETF, and the IEEE 802.11 standards committee are working hard to solve the security, mobility, and interoperability issues. By adopting some the most recent security enhancements found in modern enterprise class access points and wireless solutions, enterprises can now implement 802.11x wireless LANs with confidence. Strong authentication, encryption, packet integrity checks, and access control are available in many modern WiFi solutions today – making 2003 the year for enterprise wireless adoption.

Problems Of Early 802.11b Deployments

The early 802.11b wireless solutions relied on several security mechanisms to authenticate and encrypt data. MAC addresses were used as an authentication method to secure the network from unauthorized users. By programming the valid MAC addresses of the user's wireless NIC cards into the access points, simple authentication was achieved. The hackers soon found the weaknesses with MAC authentication and started

publicizing MAC spoofing methods to defeat the system. By sniffing the wireless 802.11b frequencies, hackers were able to see the MAC addresses of the clients and the APs – allowing them to assume the identity of either fairly easily.

Without central management tools for the access points, scaling MAC authentication solutions were also a challenge for early enterprise adopters. Trying to keep an accurate inventory of which user had which wireless NIC card and maintaining the correct MAC address list in each AP led to scaling problems very early on. Administrative mistakes could lead to blocked access for legitimate users or open access for unauthorized users.

To encrypt the data across the airwaves, Wired Equivalent Privacy (WEP) encryption was used. There are two flavors of WEP – 40-bit and 104-bit. WEP was supposed to provide adequate security to allow data to be transferred over open airwaves to resemble the level of security found on wired LANs. But this was soon proven wrong and shortly after its discovery, reports of how to breach WEP were publicized on the Internet. By capturing enough packets, hackers were able to use WEP cracking tools to discover the encryption keys used to secure the data.

Early 802.11b solutions used 40-bit WEP keys with a short initialization vector (IV) to generate the encryption algorithm. Later versions expanded the WEP encryption key to 104-bits but the IV was still left unchanged. The client and the AP had to have the same key, or shared secret, to have a successful exchange of information. The following WEP authentication and key exchange takes place between the client and the AP they're trying to attach to:

- When the client authenticates itself to the AP, it is issued a random challenge by the AP.
- The APs challenge is encrypted and secured with the static WEP key on the AP.
- The client sends an encrypted challenge response to the AP with the key (shared secret).
- The 24-bit initialization vector (IV) is used to scramble or randomize part of the key using the RC4 PRNG encryption algorithm.
- The AP receives the challenge response and decrypts the message.
- If the decrypted message matches the original message, the client is authenticated to the AP.

The primary weaknesses of WEP encryption include:

- Static WEP encryption keys that are programmed into the APs and the client's NIC driver. These keys are usually programmed once and never changed giving an attacker a chance to learn and crack the WEP keys.
- The short 24-bit initialization vector used to randomize the encryption key must be reused over time. With fast transmission speeds of 11 Mbps and high data volumes, the IV can theoretically be reused within 24 hours. An attacker sniffing the traffic can collect two packets encrypted with the same key and crack the WEP encryption key using common tools.

Reports of WEP keys being cracked within hours are becoming common and experiments performed by AT&T Labs have proven the ability to crack the 40-bit WEP keys in less than 15 minutes.[1]

[1] Stubblefield, A., Ioannidis, J., Rubin, A. D. "Using the Fluhrer, Martin, and Shamir Attack to Break WEP" AT&T Labs, August 21, 2001

Wireless Security For Enterprise

Security for wireless networks should be applied in layers, like any good security strategy that employs "Defense-in-Depth" methodologies. Authentication, encryption, and access control are the most common security practices employed in enterprise class wireless solutions.

Wireless Authentication

Traditional wired networks have been using "username and password" authentication for many years. CHAP, MS-CHAP, MS-CHAP V2, and EAP-MD5 Challenge are some popular examples of password challenge schemes used on wired and dial-up infrastructures. These authentication systems are based on a password hash with a random challenge from the authentication server. While password hash/challenge systems have been fairly robust on wired infrastructure, wireless deployments of the same authentication schemes have proven faulty. By capturing or sniffing the authentication packets from the airwaves, attackers can use common dictionary attack tools to try to discover passwords transmitted in the air, steal sessions with man-in-the-middle attacks, or attempt replay attacks.

Because authentication methods used in wired networks have weaknesses that can be exploited easily in wireless networks, the IETF and IEEE standard committees have worked with leading wireless vendors to create more robust authentication methods for wireless networks. IEEE 802.1X is the leading standard for wireless authentication.

802.1X WiFi Authentication

802.1X was enhanced and proposed by the IEEE WLAN committee as a way to strengthen user authentication in a wireless environment. It solves the common problems found in earlier implementations of 802.11b and allows for Extensible Authentication Protocol (EAP) subprotocols to add security and encryption to the authentication exchange between the client and the authentication server. 802.1X is an authentication framework that lays the groundwork of how a client is to authenticate with an authentication server. It is an open standard that is expandable with subprotocols and does not dictate which EAP authentication method should be used over another – making it expandable and scalable as newer authentication technologies are developed.

With 802.1X, an external authentication server (usually RADIUS) is used to authenticate the clients. In addition to performing simple user authentication, some wireless products have started using the authentication server for user policy or user control functions. These advanced features may include dynamic VLAN assignment and dynamic user policies.

The advantages of 802.1X over earlier 802.11b implementations include:

- The authentication is user-based, with each person accessing the wireless network having a unique user account on the RADIUS authentication server. It removes the device-based methods that relied on MAC address filtering and static WEP keys which were easily forged.
- The RADIUS server centralizes all user accounts and policies, eliminating the need for every AP to have a copy of the authentication database. To simplify management and coordination of account information.
- RADIUS has been widely accepted and deployed as a means of authenticating remote access for many years. It is well understood and mature.
- Companies can select the right EAP authentication protocol to best match their security needs - selecting bi-directional certificates where high security is desired or one-way certificates in other situations for faster implementation and lower maintenance. Popular EAP types include EAP-TLS, EAP-TTLS, and PEAP.
- Authentication servers can be tiered to provide scalability.

- 802.1X lowers total cost of ownership (TCO) when compared to individual AP management solutions where user accounts are stored on each AP.

Extensible Authentication Protocol (EAP)

There are several types of EAP. EAP is a subprotocol of 802.1X that is used to help secure the authentication transmission between the client and the authenticator. Depending on the EAP type used, data security can also be specified. Common EAP types include:

EAP-MD5
RFC 1994

EAP-MD5 is the base security requirement in the EAP standard and uses username and passwords as the authentication credentials. EAP-MD5 protects the message exchange by creating a unique "fingerprint" to digitally sign each packet to ensure that the EAP messages are authentic. EAP-MD5 is very "light weight" and performs its operations very quickly, making it easy to implement and configure. EAP-MD5 does not use any PKI certificates to validate the client or provide strong encryption to protect the authentication messages between the client and the authentication server. This makes the EAP-MD5 authentication protocol susceptible to session hijacking and man-in-the-middle attacks. EAP-MD5 is best suited for EAP message exchanges in wired networks where the EAP client is directly connected to the authenticator and the chances of eavesdropping or message interception is very low. For wireless 802.1X authentication, stronger EAP authentication protocols are used.

EAP-TLS
RFC 2716

EAP-TLS (Transport Level Security) provides strong security by requiring both client and authentication server to be identified and validated through the use of PKI certificates. EAP-TLS provides mutual authentication between the client and the authentication server and is very secure. EAP messages are protected from eavesdropping by a TLS tunnel between the client and the authentication server. The major drawback of EAP-TLS is requirement for PKI certificates on both the clients and the authentication servers - making roll out, maintenance, and scalability much more complex. EAP-TLS is best suited for installations with existing PKI certificate infrastructures. Wireless 802.1X authentication schemes will typically support EAP-TLS to protect the EAP message exchange. Unlike wired networks, wireless networks send their packets over open air, making it much easier to capture and intercept unprotected packets.

EAP-TTLS
Internet-Draft

Proposed by Funk and Certicom, EAP-TTLS (Tunneled TLS) is an extension of EAP-TLS and provides the benefits of strong encryption without the complexity of mutual certificates on both the client and authentication server. Like TLS, EAP-TTLS supports mutual authentication but only requires the authentication server to be validated to the client through a certificate exchange. EAP-TTLS allows the client to authenticate to the authentication server using usernames and passwords and only requires a certificate for the authentication servers. EAP-TTLS simplifies roll out and maintenance and retains strong security and authentication. A TLS tunnel can be used to protect EAP messages and existing user credential services such as Active Directory, RADIUS, and LDAP can be reused for 802.1X authentication. Backward compatibility for other authentication protocols such as PAP, CHAP, MS-CHAP, and MS-CHAP-V2 are also provided by EAP-TTLS. EAP-TTLS is not considered full proof and can be fooled into sending identity credentials if TLS tunnels are not used. EAP-TTLS is best suited for installations that require strong authentication without the use of mutual certificates. Wireless 802.1X authentication schemes will typically support EAP-TTLS.

PEAP
Internet-Draft

Protected EAP Protocol (PEAP) is an Internet-Draft that is similar to EAP-TTLS in terms of mutual authentication functionality and is currently being proposed by RSA Security, Cisco and Microsoft as an alternative to EAP-TTLS. PEAP addresses the weaknesses of EAP by:

- protecting user credentials
- securing EAP negotiation
- standardizing key exchanges
- supporting fragmentation and reassembly
- supporting fast reconnects

PEAP allows other EAP authentication protocols to be used and secures the transmission with a TLS encrypted tunnel. It relies on the mature TLS keying method for its key creation and exchange. The PEAP client authenticates directly with the backend authentication server and the authenticator acts as a pass-through device, which doesn't need to understand the specific EAP authentication protocols. Unlike EAP-TTLS, PEAP doesn't natively support username and password authentication against an existing user database such as LDAP. Vendors are answering this need by creating features to allow username and password authentication. PEAP is best suited for installations that require strong authentication without the use of mutual certificates. Wireless 802.1X authentication schemes will typically support PEAP.

Cisco LEAP

Cisco's Lightweight EAP Protocol (LEAP) was developed in November 2000 to address the security issues of wireless networks. LEAP is a form of EAP that requires mutual authentication between the client and the authenticator. The client first authenticates itself to the authenticator and then the authenticator authenticates itself to the client. If both authenticate successfully, a network connection is granted. Unlike EAP-TLS, LEAP is based on username and password schemes and not PKI certificates, simplifying roll out and maintenance. The drawback is that it is proprietary to Cisco and has not been widely adopted by other networking vendors. LEAP is best suited for wireless implementations that supports Cisco APs and LEAP compliant wireless NIC cards.

As the wireless security requirements push the development of 802.1X and secure data transport, newer EAP authentication protocols will be developed to answer the security issues. With IEEE 802.1X and the EAP standard, these new EAP security protocols should continue to work with existing hardware.

NOTE: To obtain more information on 802.1X, refer to Foundry's White Paper titled, "802.1X Authentication & Extensible Authentication Protocol (EAP)"

To obtain the IEEE 802.1X publication, visit: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

---

Wireless Encryption

Another concern of wireless networks that was not a big problem for wired networks is data privacy. With wired networks utilizing modern switches, eavesdropping is not a major concern as network switches forward unicast traffic only between the sender and receiver. However, data packets are transmitted over open airwaves in wireless networks and data privacy is a major concern. Encryption methods used to secure the wireless data packets must be robust and the key exchanges between the client and the access points must be authenticated and encrypted.

The IEEE 802.11i standard aims to solve the weaknesses associated with wireless data privacy. As of this writing, 802.11i is in draft form and is expected to be ratified by the IEEE by the end of 2003.

WEP With 802.1X

Traditional WEP that was implemented in early 802.11b technology was a fairly weak encryption system due to the short weak initialization vectors used to encrypt the key and the static nature of the keys themselves. Each user had to manually enter the static WEP key into their laptop and the static keys were often left unchanged due to the additional maintenance overhead. If the laptop was stolen or breached, the WEP keys could be stolen causing the wireless network to be compromised.

With 802.1X authentication and WEP, improvements have been made to solve the issues of traditional static WEP. Through the use of EAP and authentication to a RADIUS server, 802.1X solves the static WEP key issue by reissuing new keys each time the 802.1X authentication process is performed – creating dynamic WEP. The user no longer has to enter a static WEP key on the laptop as a new random key is generated each time the user is authenticated. Some implementations also allow the WEP encryption keys to be regenerated at specific times or enforce a re-authentication interval.

With 802.1X WEP encryption technology, WEP is still used as the encryption method but the dangers posed by the static keys and short weak initialization vectors are removed by the constant changing of the keys. Stolen laptops and handheld devices are now less of a concern as static encryption keys are no longer stored on the device.

WPA With TKIP

Until the full ratification of IEEE 802.11i (expected before the end of 2003), WiFi Protected Access (WPA) is the proposed interim solution to replace WEP based encryption. It is part of the WiFi Alliance and IEEE's effort to provide strong wireless security that is standards based and interoperable between wireless vendors. WPA is designed to be forward compatible with the 802.11i security standard and will be offered by many vendors as a software upgrade to their existing APs and wireless NIC cards.

WPA improves wireless security in several ways. It starts by adding authentication mechanisms which were largely lacking in traditional WEP implementations. WPA authentication can be achieved through 802.1X or preshared keys. 802.1X offers the ability to rekey but requires an 802.1X/EAP compliant RADIUS authentication server. The use of WPA with preshared keys does not require an 802.1X/EAP compliant RADIUS server but looses the strong user authentication capabilities.

The major differences of 802.1X verses Preshared Key includes:

Authentication Using 802.1X

- Uses 802.1X to authenticate the user against an authentication server (such as RADIUS)
- Unique encryption keys are generated automatically with each session
- Encryption keys can be rekeyed at specified intervals
- Encryption keys can be changed through re-authentication intervals
- Requires 802.1X and EAP compliant RADIUS server
- Requires a certificate server if EAP method chosen requires certificates
- Requires more setup and maintenance required if EAP-TLS is selected
- Can support RADIUS AV attributes for additional security features – such as VLAN and User Policy assignment

Authentication Using Preshared Keys

- Uses a static preshared key for authentication
- No enhanced security features such as VLAN and User Policy assignment
- Encryption keys can be rekeyed at specified intervals
- Can not perform rekeying by requiring re-authentication
- Does not need an 802.1X and EAP compliant RAIDUS server
- Simple to setup but not as scalable

Another area of wireless security that has been vastly improved by WPA is data privacy. Through the use of Temporal Key Integrity Protocol (TKIP also known as WEP2), the encryption key is continuously rekeyed during the wireless session - creating a unique key and integrity check on every wireless data packet. TKIP also includes improvements to repair WEP's weak initialization vector and integrity check values. A strong message integrity check (MIC or Michael) algorithm is incorporated to strengthen the packet integrity for each data packet – acting as a robust check sum. MIC's integrity check is created using several key pieces of information including: the source MAC address, the destination MAC address, and the plaintext data from each 802.11 frame. This new integrity check provided by MIC protects data packets from well-known forgery attacks.

To thwart well-known replay attacks, a new frame counter routine that uses a 48-bit initialization vector and an initialization vector sequence counter was also added back to MIC. To stop Denial of Service (DOS) attacks that rely on fragmentation, WPA, TKIP, and MIC improvements were made to drop all fragmented packets received out of order. With WPA, TKIP, and MIC, the security concerns of WEP have largely been addressed. TKIP still uses WEP's RC4 technology to encrypt the data (104-bit RC4 key and a 24-bit IV), but the issues with RC4 is no longer a real concern with the ability to rotate encryption keys and the use of strong message integrity checks.

To implement WPA technology, the client wireless driver and the AP, or wireless switch, must support WPA and TKIP standards. Many wireless vendors will offer WPA and TKIP improvements through software or firmware upgrades, but older hardware may not be upgradeable. WPA compliant products will begin shipping in the summer of 2003 and should be readily available by fall of 2003.

AES & IEEE 802.11i

IEEE 802.11i is a proposed standard for wireless security and is in draft form (as of July 2003). It is designed to address all aspects of wireless security: authentication, data privacy (AES), data integrity, secure fast handoff, secure de-authentication, secure disassociation, and secure IBSS. At the time of this writing, many of the ratified components of 802.11i have already been deployed or are in the process of being deployed by many wireless vendors. These include 802.1X and TKIP technology. Although WPA and TKIP are major improvements over

standard WEP encryption, its technology is still based on the RC4 stream cipher which has several known weaknesses.

A significant data privacy improvement that is included in 802.11i standard is the U.S. Commerce Department's NIST Advanced Encryption Standard (AES). AES is a Federal Information Processing Standard (FIPS Publication 197) that defines how the U.S Government should protect sensitive, unclassified information. AES can be used in different modes or algorithms and the IEEE 802.11i's implementation will be based on Counter Mode with CBC-MAC (CCM) - Counter Mode will be used for data privacy and CBC-MAC for data integrity.

AES is a symmetric iterated block cipher technology and uses the same encryption key for both encryption and decryption. The encryption process uses multiple passes over the data portion of the 802.11 packet and the clear text data is encrypted in discrete fixed length blocks. AES encrypts data using 128 bit blocks with 128 bit encryption keys. AES builds on the advancements made by TKIP and MIC and uses many similar algorithms to achieve the high level of data protection.

With the additional processing overhead required by AES, new client and AP, or WLan switch, hardware will need to be purchased to support the enhanced data privacy feature of 802.11i. 802.11i is expected to be approved by the end of 2003 and 802.11i compliant products should be available in limited quantities starting in Q1 2004. Enterprises with earlier hardware will need to determine if the increased security is worth the cost of 802.11i compliant hardware.

Designing Secure Wireless Networks

There are many security choices when deploying wireless networks and care must be taken to evaluate each type of security feature with the needs of your enterprise. You must weight the benefits of the security feature against the implementation and maintenance overhead and risk of not having the desired level of security.

Authentication & Data Privacy Solutions

There are several authentication mechanisms that can be mixed and matched with various encryption methods that are available in nearly all modern wireless solutions. Each mechanism has benefits, implementation requirements, and ongoing maintenance costs.

WEP With MAC Filtering	Static WEP encryption keys with MAC address filtering is simple and easy to deploy, but is very weak in security and not very scalable.
WEB Authentication	WEB authentication redirects the wireless user to an HTTPS authentication server and usually requires username and password credentials. This can be used with or without encryption and is considered a better mechanism than MAC address filters for authentication. WEB authentication is not considered strong authentication for wireless networks and should be used for Guest Wireless LANs only. WEP encryption can be combined with WEB authentication if data privacy is a concern.
802.1X With WEP	Authentication by user credentials is much better than authentication by MAC address. 802.1X implementations of WEP eliminate static WEP keys and can offer rekeying of WEP keys at specific intervals. 802.1X requires an authentication server such as RADIUS and implementation of EAP.

	Depending on the EAP method selected, implementation and ongoing support efforts will vary.
802.1X With WPA	802.1X combined with WPA offers strong user-based authentication and good data privacy. WPA implements TKIP and MIC which strengthens data privacy and encryption keys. It eliminates many of the well-known weaknesses of WEP and guards against many known attacks: packet forging, session hi-jacking, man-in-the-middle attack, replay attack, fragmentation attack, and some DoS attacks. It requires the use of an authentication server such as RADIUS and implementation of EAP. Depending on the EAP method selected, implementation and ongoing support efforts will vary.
Preshared Key And WPA	Using a preshared key for authentication purposes will make rollout and support much easier as a RADIUS server and EAP is not required. The solution is not very scalable and the preshared key may be compromised as employees leave the company or if it is accidentally given out. The advantages of WPA, TKIP and MIC for data privacy are still present with this solution, but the authentication strength is sacrificed for easy deployment.
IPSec VPNs	Virtual Private Networks (VPN) are proven technology that utilizes strong authentication and encryption to secure remote transmissions across the public Internet. Many early wireless LAN adopters have implemented IPSec VPNs to help secure the open airwaves for their employees. VPN clients are installed on each wireless device and the VPN server sits between APs and wired network. For companies that are using VPNs, this strategy is a common one as end users are already familiar with the client software and the hardware investment has already been made. For companies that have not deployed VPNs, this strategy will create additional hardware costs, implementation overhead to install the clients, and ongoing maintenance costs. VPN on wireless LANs will most likely be replaced with modern wireless security features such as 802.1X and WPA.

Criteria for EAP Selection

As with most IT projects, the total cost of wireless ownership is not just the initial cost of purchasing the wireless hardware and the cost of implementation. Ongoing maintenance can be a very large part of wireless networks depending on the EAP method selected and the type of wireless solution purchased.

If 802.1X is used, EAP must be present. By answering the following questions in light of your company's security requirements, budget, and human resources, you can select the best authentication and encryption methods that are right for your wireless implementation.

1. **Do you need to authenticate the user as well as the wireless network (APs)?** By authenticating both users and networks, the ultimate authentication scheme between employees and corporate wireless networks is achieved. This protects the network from unauthorized users as well as users from unauthorized wireless networks. If this is the case, EAP-TLS is the best choice.

2. **Do you need to provide strong authentication security?** The level of security used for the exchange of user credentials and passwords between the client and authentication server must be considered. Strong authentication is good, but often requires more implementation overhead, ongoing maintenance, and user knowledge. If strong authentication is required, EAP-TLS, EAP-TTLS, or PEAP are good choices. EAP-TTLS and PEAP are easier to implement than EAP-TLS as client certificates are not required.

3. **Does it require a lot of ongoing maintenance?** As more users adopt wireless technology, setup time and ongoing maintenance for each additional user will also become a deciding factor on which EAP type to use. EAP-TLS is the most secure, but requires the use of client certificates – increasing the amount of setup, maintenance, and tracking efforts.

4. **Is a unique session key for each user important?** By requiring a unique session encryption key for each user, data privacy is greatly increased over static WEP. This can be achieved through the use of clients and authentication servers that support 802.1X wireless authentication. Most EAP types can be used to support 802.1X with Dynamic WEP keys but existing RADIUS servers may need to be upgraded or front ended with 802.1X and EAP compliant RADIUS servers.

5. **Is encryption key rekeying important?** By requiring user sessions to rekey at specific intervals, wireless data privacy becomes very secure. 802.1X with WPA and TKIP will accomplish this. Most EAP types can be used to support 802.1X with WPA and TKIP but existing RADIUS servers may need to be upgraded or front ended with 802.1X and EAP compliant RADIUS servers.

6. **Can your existing user directory services be used?** Rollout time can be greatly reduced if the 802.1X RADIUS servers can leverage existing LDAP or Windows Active Directory databases. Users will benefit by being able to use their existing account information and using the wireless network will become more seamless.

7. **Will there be Guest access or access with little security requirements?** For wireless connections which value "ease of use" and simplicity over security (such as Guest access or wireless Hot Spots), WEB authentication with no WEP key or a simplified WEP key may be sufficient. Low security or no security wireless LANs must be separated from normal enterprise data traffic through the use of VLANs or separate connections to your extranet or DMZ. Firewalls should also be considered along with some form of monitoring and intrusion detection system (IDS).

Wireless Network Design Strategies

Modern enterprise wireless networks will require strong authentication and security. There are several ways to achieve this and several common strategies will be presented in this white paper to illustrate the concepts. Weaker authentication and encryption methods such as traditional 802.11b static WEP will not be discussed as it is does not offer an enterprise class security solution.

As with all other security designs, "Defense-in-Depth" is the ultimate goal and wireless security features must be incorporated with existing network security features to achieve a strong security stance. After selecting the right authentication mechanism, EAP type, and encryption scheme for your wireless network, successfully integrating it into the wired network will require planning and thorough testing.

Wireless Realms

Most enterprise wireless implementations will consist of one or more APs per wireless realm, also known as a wireless network. A wireless realm is one continuous wireless service area with the same SSID or ESSID. Wireless users will see wireless realms advertised on their wireless devices and the wireless device's network card will automatically associate with the best AP in the wireless realm. Depending on the wireless network strategy for your enterprise, you may decide to create wireless realms by building, floor, department, or some other differentiator.

If your company's internal LAN strategy is to allow full access to all areas of the internal network, one wireless realm per building or Layer 2 subnet is a good starting strategy. If your company's internal LAN strategy is to separate, monitor, and control network traffic by department (or some other means), you may need to create a separate wireless realm for each department or traffic segment. As you design the wireless network, try to adopt the same divisional and management strategy that is used on the wired LAN to keep security policies consistent.

The advantages of a single wireless realm per building or floor, is easy planning and simplicity for the users. This strategy sacrifices access control for each wireless client since each wireless realm can be only assigned to one VLAN ID. If multiple departments are using the same wireless realm, there is no way to granularly control the access of each user with VLANs. Some modern wireless solutions offer dynamic VLAN and User Policies to compensate and allow VLAN settings and User Policy settings to be specified by the RADIUS server – based on the user's credentials.

Another strategy is to create one wireless realm for each security requirement that your company has for wireless users. A good example of this strategy is creating a very secure wireless realm for your regular employees and a low security wireless realm for guest users. The wireless realm servicing the company's regular employees can be advertised using some descriptive SSID name (such as "Building-A Floor 1") and secured with 802.1X and WPA. The guest wireless realm can be advertised using an obvious SSID name (such as "Visitors") and secured with a simple WEP key and WEB authentication with a generic username and password.

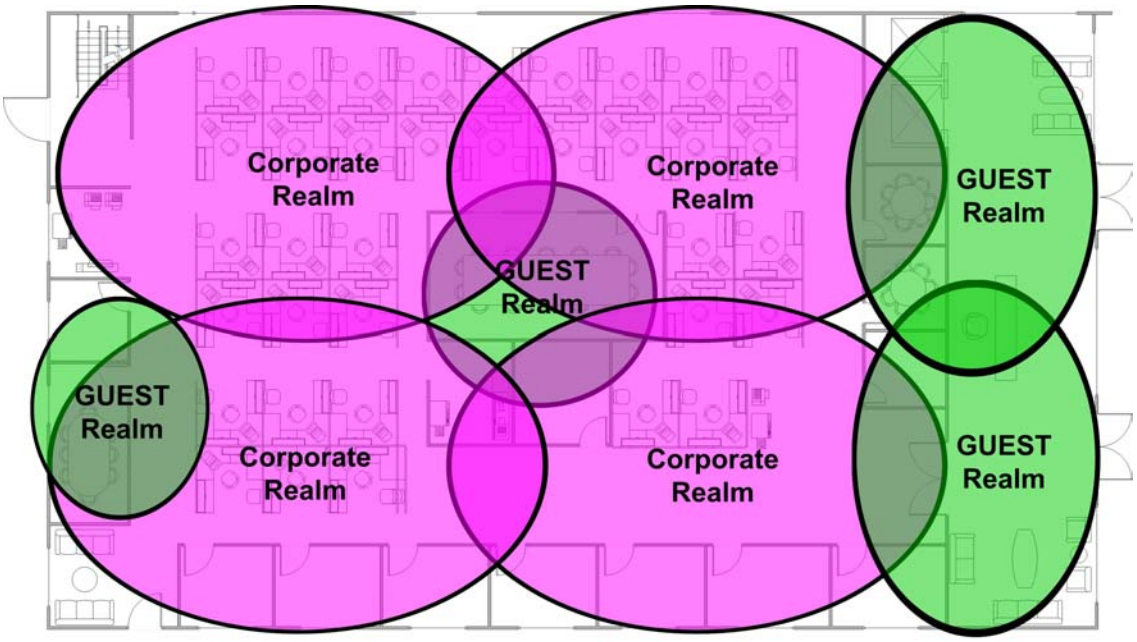

Figure 3. Wireless Realms

Virtual LANs (VLAN) & ACLs

If your design calls for multiple wireless realms, leverage your network device's abilities to further secure the wireless traffic. VLANs are a great tool that can be used to separate the different wireless realms. Additional security controls such as Access Control Lists (ACLs) can be applied to each VLAN to control access to various locations in the internal network. By implementing specific IP address ranges for each wireless realm, further control decisions are possible through the use of Layer 3 and Layer 4 ACLs.

For example, the corporate employee wireless realms can be given access to the entire internal LAN while guest wireless realms are only given access to the public Internet through a tagged uplink port or through a dedicated up link port terminating in the DMZ or Extranet. ACLs can be used to further restrict guest wireless access in the DMZ or Extranet. If your company's security policy prohibits wireless clients from accessing specific subnets or hosts, ACLs can be used to control access based on the wireless client's IP addresses.

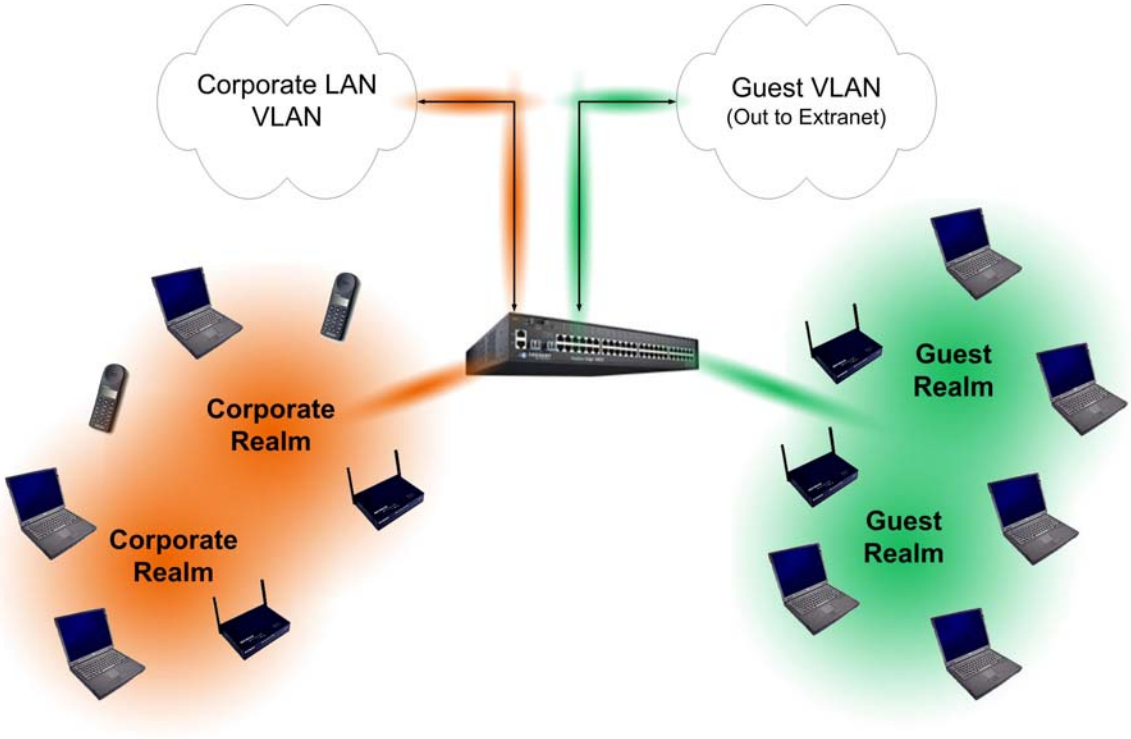

Figure 4. VLAN Realm Topology

VPN Technology

If your company already has a VPN solution or your wireless components do not support strong authentication or encryption such as 802.1X and WPA, an IPSec solution on top of the wireless infrastructure is a good alternative to rolling out a new secure wireless infrastructure. VPN technology is well understood and fairly easy to use, but requires more deployment work up front and ongoing maintenance as the company scales its wireless infrastructure.

Depending on the VPN selected, there are many different authentication and encryption options. Local user databases are supported as well as popular LDAP and Windows directory services. PKI certificates and two factor token cards are also supported by many VPN solutions giving the IT staff great flexibility in designing its authentication schemes. Encryption is usually very strong with 3DES and AES support and strong packet integrity checks.

Client software will generally be required for each wireless mobile device and the VPN server will be placed between the access points and the wired network. Each wireless user will have to authenticate to the VPN server before gaining access. With most modern VPN servers, firewall technology is available to control traffic based on stateful inspection and many provide the ability to limit access based on the user and group credentials.

802.1X Overhead Planning

When using 802.1X authentication with EAP-TLS, TTLS, or PEAP, consideration must be given to performance of the RADUS server. The cryptographic routines used by 802.1X and the various EAP types to create the secure authentication tunnels and 128-bit unique keys can cause heavy loads on RADIUS servers - especially if rekeying is turned on for short intervals. Careful monitoring of the RADIUS server's CPU and resources should be performed on a regular basis to determine if additional RADIUS servers are needed throughout the enterprise to support the number of users accessing the wireless network.

If your environment requires multiple RADIUS servers, consider implementing a hierarchical topology or a topology where wireless APs and switches authenticate to specific RADIUS servers deployed throughout the enterprise. Another way to increase RADIUS server performance is by separating the 802.1X and EAP functions from the authentication functions. For example, the 802.1X and EAP computationally intensive functions can be performed by a RADIUS server closest to the wireless user while user credential information is performed on a backend RADIUS server.

Consult with your RADIUS server vendor for more information on using multiple RADIUS servers for increasing 802.1X authentication capacity.

Authentication Server Planning

In addition to the number of realms that are required or the performance of each RADIUS server, the hierarchy and placement of RADIUS servers is very important. The number of authentication servers required will generally depend on the number of wireless users authenticating to the server, the number of remote sites, and the desired level of redundancy. Authentication server strategies can revolve around a central authentication database, distributed authentication databases, or a mixture of both models. The following four case studies illustrate some of designs that can be used to accomplish authentication requirements.

Case Study One
For small or simple implementations that only have a single site, a centralized authentication model is usually best. All users are located in one site and authenticates against one RADIUS server which contains all user credential information. As the wireless network grows, simply add more access points and RADIUS servers to replicate the central database.

Case Study Two

For companies that have multiple sites that are managed locally by each site's IT staff, a distributed authentication model may work best. This topology requires one or more RADIUS server at each site with a copy of the authentication database loaded on each RADIUS server. Users authenticate locally to each RADIUS server on the site and accounts are managed by local IT staff. If users travel between sites regularly, database replication is performed between the sites. WAN connectivity is not an issue with each RADIUS server performing local authentications.

Case Study Three

Companies with multiple sites may decide to centralize and route all authentication functions back to a single controlled location. In this topology, wireless LAN users are required to perform authentication over the WAN or network back to the centralized RADIUS server. RADIUS server(s) is only required at the central site and cost can be reduced. The user's ability to authenticate against the central RADIUS server will depend on the condition of the network or WAN links connecting the user to the central site. With only a centralized RADIUS server, performance may be an issue as the number of users increase and the demand for cryptographic resources increase.

Case Study Four

Companies with multiple sites may also decide to run a centralized authentication site with distributed RADIUS servers at each remote location. This is a combination of case study two and three. It offers the benefits of centralized authentication with a single managed database with the ability to split the 802.1X and EAP computational functions to the local site's RADIUS servers. By using this hierarchical approach, the heavy computational requirements are performed by the RADIUS servers closest to the wireless users, preserving WAN and network bandwidth. The remote site's RADIUS server(s) calls on the central RADIUS server for all user authentication requests. The conditions of the WAN and network links are still a factor in this model, but the scalability and performance is improved.

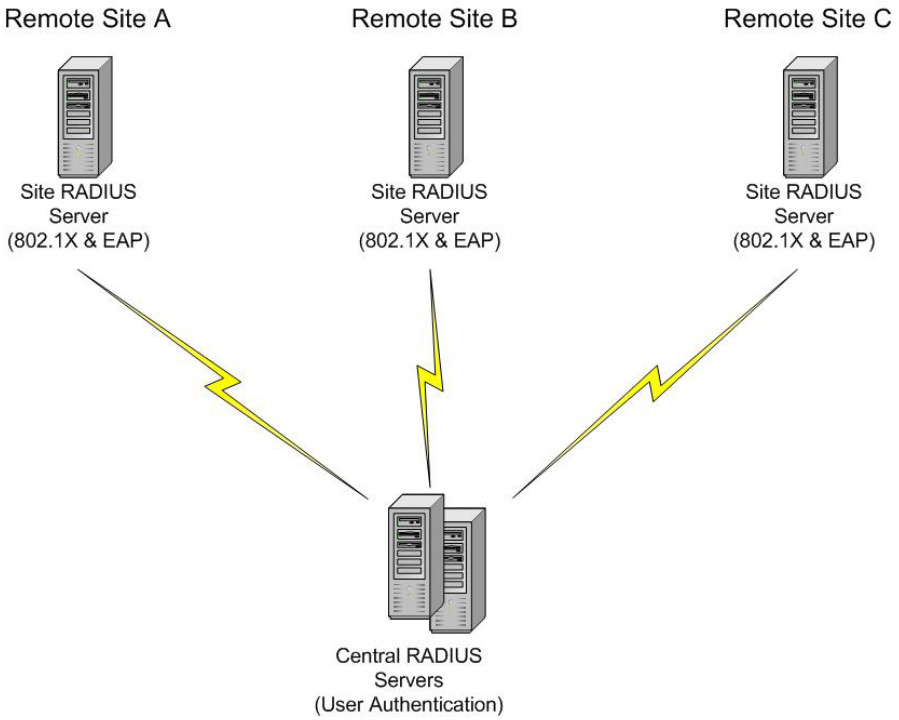

Figure 5. Distributed RADIUS Topology

Firewalls and Monitoring Device Placement

The largest concern for enterprise adoption of wireless technology is security. With wireless access, intruders do not have to be in your buildings physically to pry and hack at your corporate network resources. For this reason, many security managers have designed extra precautions around wireless LANs.

Some of the additional security considerations include:

- Wireless networks are terminated outside of the firewall. Either in the DMZ or another dedicated external subnet controlled by the firewall.
- The firewall provides stateful inspection of all wireless sessions into the network verses implementations of user policies that rely on stateless packet filtering.
- Intrusion Detection Sensors (IDS) and Intrusion Prevention Sensors (IPS) are used between the wireless network and the wired network to monitor activity.
- IDS and IPS systems are tuned to look for IP bridges – rouge APs.
- MAC Address filtering is used to control client wireless NICs that can associate with the wireless APs (not extremely secure, but stops casual association by neighboring company employees).
- Regular site monitoring with wireless sniffers to detect rogue APs – unauthorized APs that employees have installed on the internal LAN.
- Corporate security policies are appended with new wireless usage policies and acceptance guidelines.

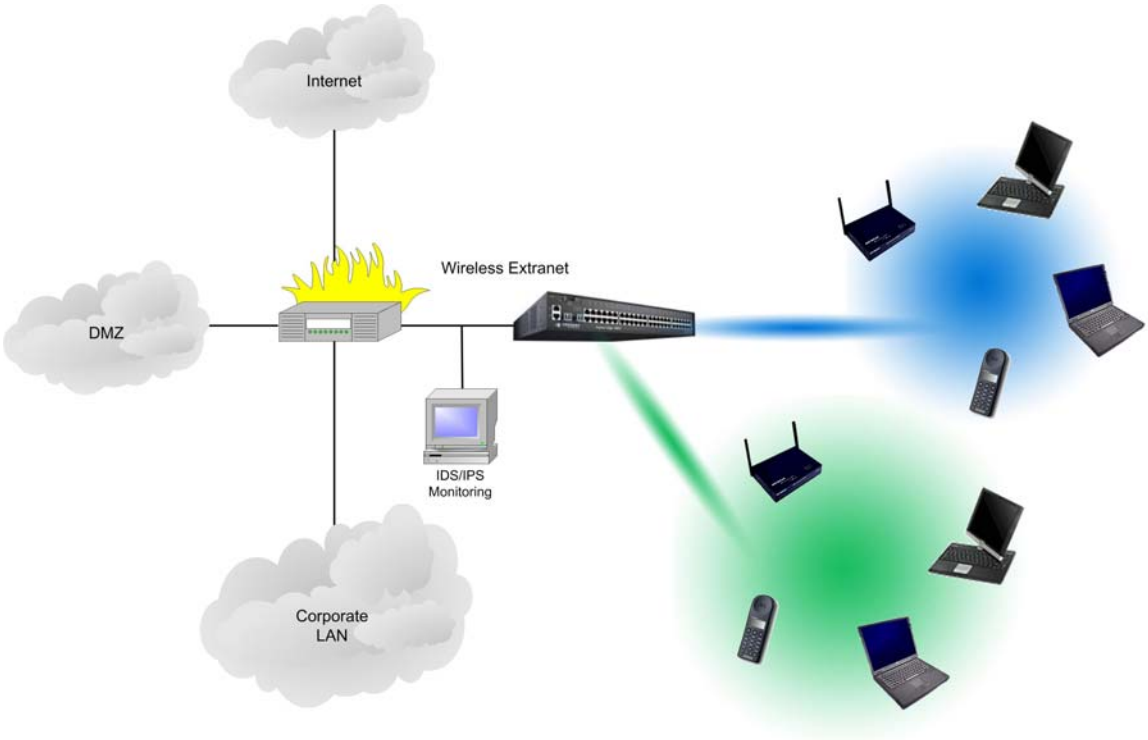

Figure 6. Wireless Extranet Topology

Regular and vigilant monitoring is part of any good security strategy and should be planned as part of any wireless deployment. Review your AP and WLan switch logs to look for intrusion attempts, failed authentications, and irregular pattern usage. Perform regular site surveys to look for unauthorized APs on your internal LAN that are not secure and educate users as to the "do's and don'ts" of wireless networking.

Other Tips and Suggestions

In additional to all the of the security features and options mentioned thus far, the following are other critical configuration points to keep in mind as you deploy wireless LANs.

Security Tips

- Change the default WEP keys on all new APs.
- Use the longest WEP key that is supported by the APs and the clients. Use hard to guess WEP keys.
- Select tough to guess preshared keys (if used).
- Change the default password of all APs and WLan switches. Use strong password selection techniques.
- Centralize AP and WLAN switch passwords. Use AAA authentication if supported.
- Use SSL, SNMP v3, and SSH to manage all wireless APs and WLan switches.
- Restrict all AP and WLan switch management to the internal LAN. Do not allow management from the wireless network.
- Be careful when selecting ESSID and SSID names. Do not use company names, use unique names, and don't attract attention.
- Turn off all functions and features on APs and WLan switches that are not absolutely necessary.
- Do not let users run wireless devices in "adhoc mode" or "peer-to-peer" mode. Make them attach to an authorized AP for wireless services.
- Use separate APs for Guest wireless realms and VLAN or connect directly to DMZ or Extranet.
- If AP supports port filtering, use it to pre-screen unwanted traffic.
- Filter out unnecessary broadcast traffic on APs or WLan switch.
- Synchronize time with an NTP server on all APs (if supported) and WLan Switches to help coordinate logs.
- Export all AP and WLan Switch logs to an external Syslog server.
- Wireless laptops running Windows XP should turn on built-in firewall. Consider installing personal firewalls on other wireless laptops.
- If the client's wireless NIC driver allows password protection, enable it to protect wireless driver settings.
- Educate wireless users on "best practices" for using wireless technology.
- Modify corporate security policies to include wireless use and acceptable practices.

AP Radio Tips

- Position the APs where the wireless users are located. Try to select unobtrusive areas to place the APs (ceiling mount is usually best).
- Tune AP power down for APs that are close to outside walls to prevent signal leakage outside of the building.
- If the AP supports omni-directional antennas with diversity settings, tune the radio patterns to avoid sending signal to the outside of buildings.
- Perform site surveys with wireless sniffer to test leakage patterns outside of building and retune if necessary.
- Select AP channels that are far apart to prevent interference.
- Place more APs where there are more users to share the load. Tune the power levels down if APs are close together to reduce interference. Always use the lowest power level needed to provide adequate coverage.

- If 802.11g APs are used, remove 802.11b NIC cards and replace with 802.11g NIC cards. Although 802.11g is backwardly compatible to 802.11b's 11 Mbps standard, the maximum speed of an 802.11g AP is determined by the user with the lowest speed NIC card associated to that AP. If there is a mixture of 802.11g users and 802.11b users on the AP, all users will resort to the 802.11b 11 Mbps transmission rate.
- For each building, try to keep all APs on the same subnet or VLAN for faster, seamless roaming and less re-authentication.

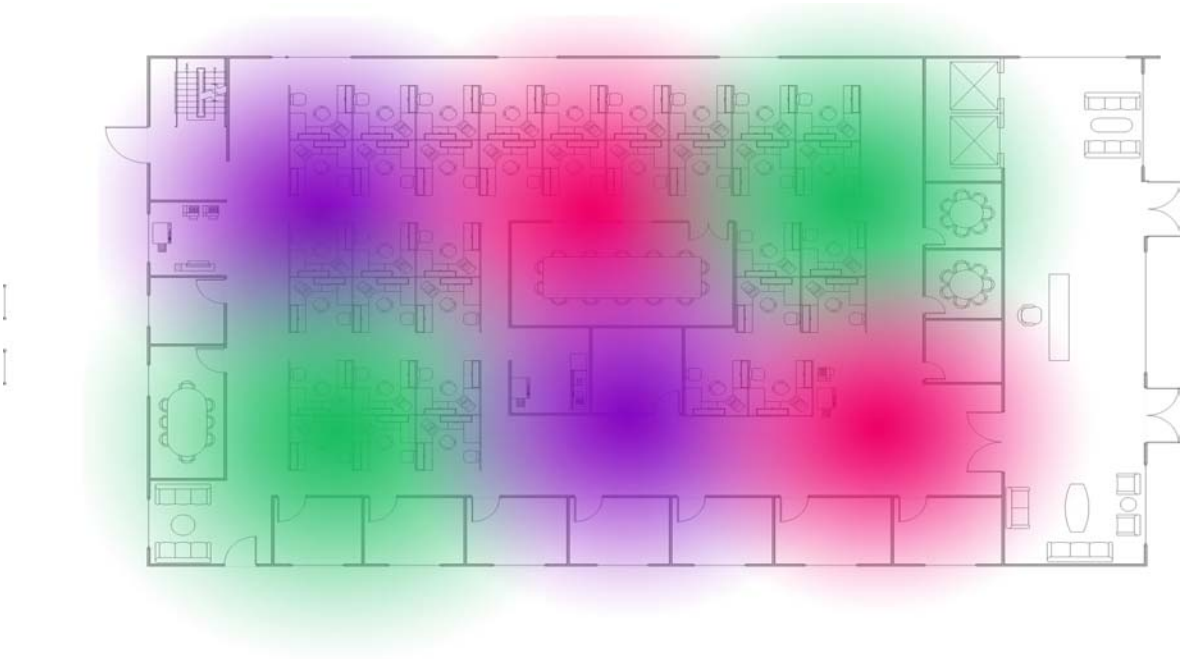

Figure 1. Frequency Coverage

Figure 1 shows how even coverage can be achieved by placing APs throughout the building. Alternating the AP frequencies and adjusting the APs power settings will help tune coverage while minimizing leakage to the building's exterior. User density and load is not taken into consideration in this model.

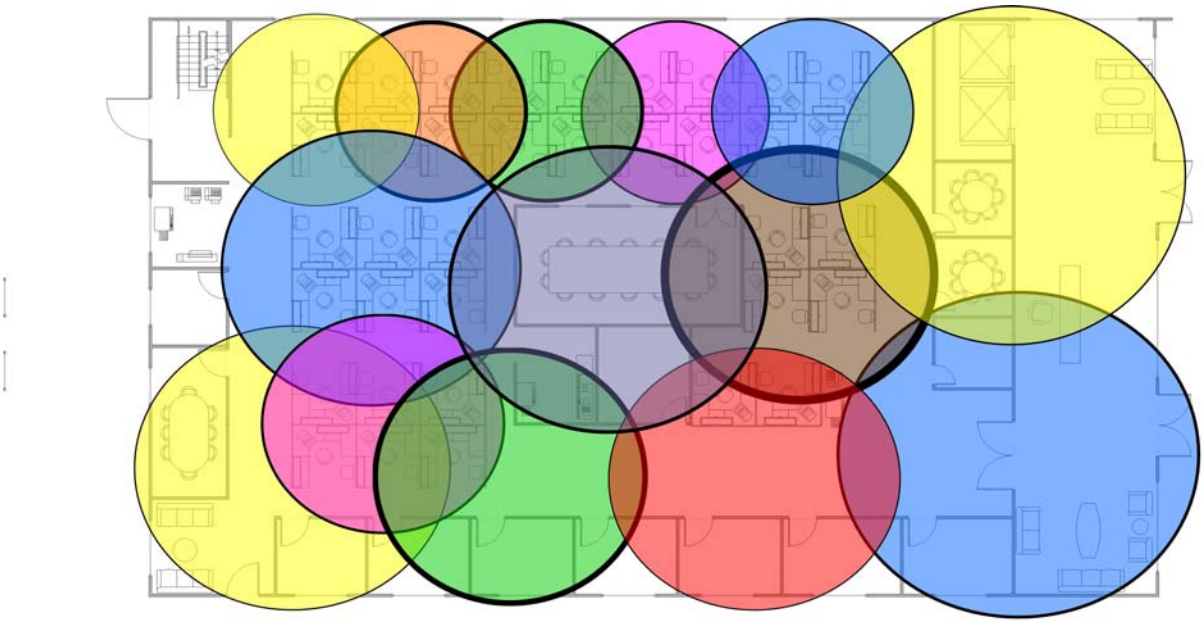

Figure 2. Density Coverage

Figure 2 shows how additional APs can help scale and increase load. As more APs are added, more wireless devices can be supported. AP power and frequency must be adjusted accordingly to avoid interference.

Summary

Wireless LANs offer enterprise users many benefits and productivity improvements, but have adorned much negative press due to the initial offering's weak authentication and encryption methods. With the advancements made by the IETF and the IEEE 802.11i committee, many wireless vendors have addressed the weaknesses of WEP. 802.1X, WPA, TKIP, MIC, and AES technology are new standards that provide strong authentication and encryption for wireless networks – reducing the risk and exposure.

With careful planning and layering of security features from both the wireless and wired environments, wireless networks can be securely integrated into corporate networks to extend its functionality. For more information on Foundry Networks wireless products, please visit our corporate Web site at: www.foundrynet.com

Foundry Networks, Inc.
Headquarters
2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100

U.S. and Canada Toll-free: (888) TURBOLAN
Direct telephone: +1 408.586.1700
Fax: 1-408-586-1900
Email: info@foundrynet.com
Web: http://www.foundrynet.com