UNIT V:

Wireless Deployment Strategies: Implementing Wireless LAN's- Security Considerations Common Wireless Network Applications, Enterprise Campus Designs, Wireless IST Design, Retail and Manufacturing Design, Small Office/Home Office Design (SOHO)

Implementing wireless LAN's- Security Considerations:

To properly understand and counter the risks, the functional goals of the wireless network must be fully understood. We will explore the security considerations that should be applied to different layers of the wireless network— namely, the physical, network, and application layers. The physical section will cover radio frequency (RF) coverage, equipment placement, and building construction. The network section will cover the general network architecture, wireless local area network (LAN) medium access protections, and mobility and virtual private network (VPN) considerations. The application section will cover application communications tunnelling encryption.

Common Wireless Network Applications:

We examine the various common network configurations where wireless Ethernet is deployed. Many companies use wireless Ethernet as a drop-in replacement for Ethernet when mobility is needed or when wiring is difficult or impossible. Some historic buildings are very limited in wiring possibilities so wireless Ethernet is the only option for network connectivity. Another common way to bridge networks over short distances between buildings is to use a wireless bridge and directional antennae.

Wireless Internet service providers (ISPs) generally provide last-mile wireless access to fixed-point locations to either a home or business. This configuration is called point-to-multipoint, where the customers connect to the ISP upstream access point via a client adapter at the customer premises. Because the network is not designed with mobility in mind, it operates similarly to point-to-point configuration, differing only in that multiple clients can connect to one access point. The last two scenarios involve client roaming between access points. Roaming occurs because the wireless user moves out of range from the access point that was providing network services.

As the client moves out of range, the link deteriorates and is eventually lost because no other access point is in the vicinity. When the existing link begins to deteriorate, the client may also search for another access point to roam to. The roaming process drops the existing Transmission Control Protocol (TCP) connection and requires a new network connection upon association with the new access point. This leaves the wireless network designer with the problem of maintaining the TCP state during network disassociation and reassociation. Networks that permit roaming are often large and cover vast distances. When designed poorly, they can be a network administrator's nightmare.

However, if designed with security and performance in mind, the administrator will be rewarded with a high-performance, dynamic wireless environment that can also facilitate wireless network incident response.

Physical Security Considerations:

Good security engineering examines the problem from all angles, and when building a wireless network, you must begin at the physical layer. Control over the wireless coverage will reward the administrator with fewer headaches down the road. Understanding the boundaries of your network makes network incident response a less daunting task and can actually lead to better network performance. Key points on infrastructure placement also assist the designer and implementer in successfully deploying a wireless network that eliminates areas without coverage and focuses radio signals into needed areas.

Site Survey

A site survey is used to determine the physical environment in which a wireless LAN is installed. The site survey has two components: the physical walkthrough and the signal strength and access point placement evaluation. Having a site plan for the building or area that will be surveyed is recommended, but it is not always needed. During the physical walkthrough, the engineer takes note of the surrounding areas and the obstacles that need to be overcome. For example, dense vegetation, out buildings, large metal objects, large open distances, and building construction must all be noted. The buildings must be carefully evaluated. Outer- and inner-wall construction, window treatments, and window glass material must all be identified and considered when determining the placement of the access point and antenna.

The second component of the site survey is performed with access points and a roaming wireless client. An access point is installed in a potential service location and the wireless client is walked around while the user monitors the signal strength. Network coverage is evaluated and fine-tuned for optimal performance and security. A proper design for directional antennae occurs in this phase. After the general coverage is determined, the overall signal strength of the access point can be adjusted to contain wireless network exposure inside a controllable range.

Equipment Placement

You should follow several guidelines when deploying equipment in the field:

- Ensure that the access point is installed out of the normal reach of employees. Where possible, conceal the access point from sight.
- If the access point is installed outdoors, make sure the equipment is properly secured, discouraging tampering.
- When appropriate, sector network areas with directional antennae. This places RF where you intend it to be. It also quantifies areas where users are when connected to that cell. This is very useful when tracking down problems or running through incidence-response procedures.
- Name the access points so that they can be tracked down easily during frantic troubleshooting events.

Once the access points are in the best possible configuration, you should perform a perimeter sweep to ensure that excess radiation isn't bleeding into unintended areas. Most access points designed for corporate and enterprise use have an adjustable power output and can be trimmed down to remove excess bleeding.

RF Containment

The objective of RF containment is to attenuate or limit the scope of your network within the known boundaries. This is very important in large networks where roaming is necessary, but it also deprives would-be attackers from detecting the network or certain portions of the network, which lowers your drive-by profile. When combined with directional antennae, it also normally has a performance benefit.

In addition to attenuating the transmit power on the access point, you can also perform the following physical tasks to limit the amount of RF bleed out of buildings and rooms. When designing a new facility, specific rooms can be designed to prevent the leakage of excessive RF energy by installing metallic film or foil under the drywall. Metallic paint can also be applied to walls to add a layer of attenuation. Metallic window blinds provide better attenuation over cloth or plastic blinds. These simple details may result in the difference between a wireless perimeter extending tens of feet from the intended area to hundreds of feet.

Network Security Considerations:

The needs of the enterprise drive the majority of the network architecture, and security and performance must be considered from the onset of the project. In the following sections, we will discuss the major wireless network scenarios, provide best practices, and share some thoughts on how you would build a network to meet your goals in a secure manner.

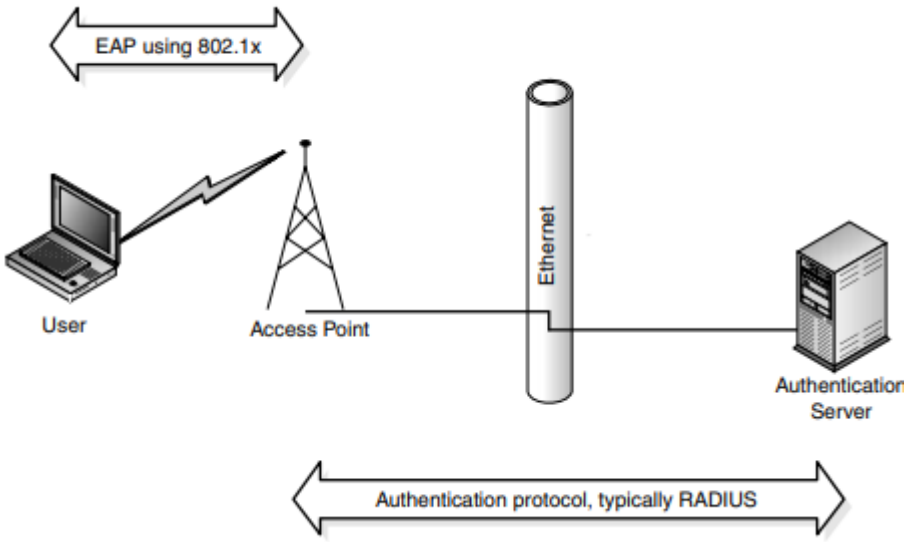
The general consensus is to treat all wireless networks as untrusted anonymous hosts just like the traffic originating on the Internet. Access is granted once the host successfully presents the qualifying credentials to an authentication server and all communications travel over an encrypted tunnel between the two systems. This still holds true to a point, but, when possible, you should segment the networks in order to minimize physical layer denial of service (DoS) attacks to shield critical networks from the external threats. As stated before, segmenting can also significantly assist in incident-response activities.

Segmenting off administrative communications channels is difficult with access points because the administrative interfaces are often limited to the Ethernet port. Some access points have out-of-band management through a serial port, but that can also be difficult to manage in large distributed networks; however, it is the only secure method. Most access points do not allow you to push configurations across many access points through the serial interface, but you can usually do it over the Ethernet or wireless interface. If possible, configuration capabilities over the wireless interface should be disabled to prevent attackers from tampering with the configuration. Management of the access point should be considered when choosing a brand of access point. Telnet, cleartext Hypertext Transfer Protocol (HTTP), and unencrypted Simple Network Management Protocol (SNMP) should be avoided. Instead, try using Secure Shell (SSH) or Secure Sockets Layer (SSL) for managing network devices. Some terminal servers with SSH capabilities can be configured to access the serial port on access points.

Physical and Data Link Layer Security Controls

The International Organization for Standardization (ISO) model as set forth in the earlier chapters by looking at the physical and data link layers. The 802.11 wireless Ethernet standard has minimal and flawed authentication and packet encryption methods defined within.

However, as mentioned previously, when used in conjunction with Wired Equivalent Privacy (WEP), 802.1x augments and corrects some of the standard's pitfalls.



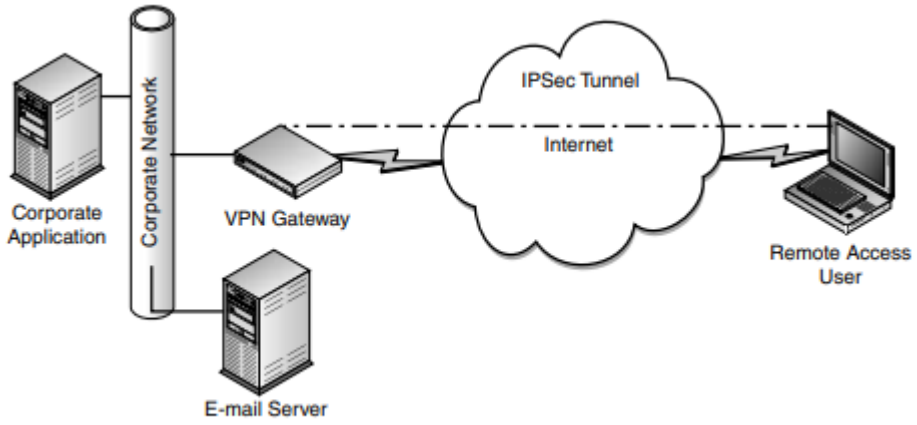
Using 802.1x with dynamic WEP keys eliminates most of the attacks against WEP, as defined in 802.11-1999 and 802.11b, as long as keys are rotated frequently. Shared authentication should never be used; always use an open system because the shared authentication scheme leaks WEP key information to attackers through known plaintext methods. One of the downfalls of 802.1x is that it requires more back-end equipment and a Remote Access Dial-In User Service (RADIUS) server with 802.1x capabilities. This additional management overhead should be considered.

Recently, many vendors have implemented WEP key hashing. Key hashing is the process of hashing the initialization vector (IV) and shared key before generating the RC4 stream. This is a highly effective way to prevent someone from recovering the WEP key by using passive attacks. At the time of this writing, all key-hashing features of wireless devices are vendor proprietary and not interoperable. Another common 802.11-based security mechanism is the use of Media Access Control (MAC) access control lists. A MAC access control list is a list of physical addresses that are allowed to access the wireless network. This security mechanism is found in almost all access points. It enables the network administrator to enter lists of valid MAC addresses into an access control list, limiting network access. With some access points, the list can then be pushed out to all participating access points. The downfall of this practice is that the MAC addresses of all wireless clients and access points are sent in the clear, even when WEP is enabled.

Changing the MAC address of a network card is a trivial task. Many times, it is a configuration option in the driver. An eavesdropper can easily compile a listing of valid MACs, detect when one disassociates, and attach to the network with that valid MAC address. Even with their limitations, MAC access controls are still useful in some circumstances. They can be powerful tools in preventing roaming clients from accidentally attaching to an open wireless network. However, the administrative overhead needs to be considered because keeping track of valid MACs and updating all access points with the valid address can be a time-consuming task.

VPN Tunnelling

As alluded to in the previous chapters, VPN tunnelling works extremely well in many environments. It is a proven technology and many companies are already equipped with a VPN gateway. Sometimes adding access to the VPN from the wireless network can be as simple as adding a network card to the VPN gateway or changing some firewall rules. When roaming is required, network designers need to take network subnetting into consideration. The IP address must remain the same for it to work seamlessly. In many cases, the VPN tunnel will drop when roaming and will reset TCP connections. This may require the user to renter authentication credentials.



MobileIP may be used for roaming. MobileIP may prevent the VPN connection from getting torn down when traversing between access points. MobileIP can also be used across different wireless network types. You can use MobileIP on cellular telephone data services, eliminating the enterprise's requirement of a separate infrastructure to support mobile tele□phony applications.

Intrusion Detection Systems (IDSs):

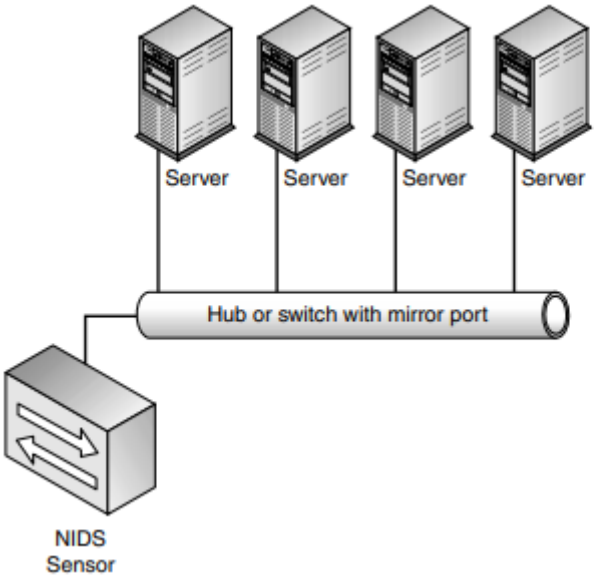
Your network will never be 100 percent secure. Not all attacks can be stopped and excessive security measures can sometimes be prohibitive to business. In other words, attempting to prevent all possible attacks is not only an exercise in futility, but it may not be worth the effort. Many people who want to secure their houses install alarms instead of bars on the windows to notify the police in the event of a break-in. The equivalent to home alarms in the digital arena is intrusion detection systems (IDSs). IDSs take many forms, but they normally break down into two categories: host based and network based.

A host-based IDS (HIDS) is normally a piece of software that monitors the system for suspicious activity. This involves monitoring system files for changes or the installation of new software, drivers, or kernel modifications. Sometimes an HIDS also monitors the network connections, looking for suspicious connections and new programs, listening for incoming connections, and initiating new outgoing connections. Some personal firewall software has an HIDS component.

A network-based IDS (NIDS) is based on a modified packet sniffer. It is installed on a network and has the capability to examine network traffic. The NIDS either monitors for

suspicious activity by comparing network traffic to signatures of known attacks or monitors for anomalies. Anomaly IDS systems have a learning mode in which they build rules based on the normal network traffic patterns. Then they monitor traffic with the created rules and alert any suspicious activity. Some systems are a hybrid of the two technologies. Many commercial IDS systems and some open-source systems are available.

One of the benefits of using NIDS over HIDS is that a single NIDS sensor can monitor a network containing many hosts, thus simplifying the installation and configuration of the IDS. Some HIDS can dramatically decrease the performance of the host operating system. Be sure to fully test the impact of different IDSs on your applications before deploying them to the entire network. Various forms of IDSs are included in the designs discussed in the following sections.



Due to the administrative overhead of monitoring IDS sensors and keeping IDS signatures up-to-date, many companies choose to outsource this service. An outsourced IDS service provides or sells sensors to be placed on the network and monitors them from the Internet or a dedicated telco link. The monitoring service is responsible for updating changes and alerting administrators of any suspicious activity. These services are expensive and are not for every enterprise. You should evaluate your in-house security and monitoring expertise before deciding to use an outsourced IDS provider.

Some people feel that an IDS can also involve reviewing logs for suspicious events. Regularly reviewing and archiving logs should be the standard practice on any network. Many intrusion-related events do not produce suspicious-looking logs during the event so the effectiveness of these systems as IDSs is limited.

Additional IDS resources include

www.snort.org

www.sourcefire.com

www.nfr.com

www.enterasys.com/ids/

Application Security Considerations

Wireless networks are often set up to offer a specific application. This may include roaming agents in airports, inventory tracking in warehouses, email, or service of the "killer app" to end users. Many times, these applications have already been hardened to work on a hostile network: the Internet. In these cases, wireless security precautions, such as WEP and IP Security (IPsec) may not be needed. Instead, SSL/Transport Layer Security (SSL/TLS) and SSH may be good ways to secure an existing application.

Enterprise Campus Designs:

The following section deals with the security needs of the enterprise campus. Many applications are available for wireless networking on a campus. In some cases, these designs can be combined into a hybrid design to solve multiple business problems. Key design concepts are highlighted as best practices. Use these best practices when evaluating your current design or when creating a hybrid design for your application.

Enterprise Design 1

One of the most difficult challenges that wireless network designers face is the need to support many different platforms, operating systems, and hardware vendors with a single infrastructure. The following design was used in a campus that needed to support a large population of engineers and salespeople. Many of the engineers used different operating systems such as Windows, Linux, Berkeley Software Distribution (BSD), which is a Unix-like operating system, and Solaris. To make matters worse, many of the engineers used their personal laptops, which had a wide variety of wireless network cards. Due to the highly sensitive nature of the data being transmitted on the network and the network resources, security was a key concern. Because the users were not very technical, ease of use also played an important role.

The solution to the problem proved to be easier than first anticipated. The company already had an infrastructure for providing access from a hostile network (the Internet) with the corporate VPN. The network 200 Part 3 Wireless Deployment Strategies designers remembered the pain and agony that it took to meet the engineers' functional requirements with the VPN and did not want a repeat with the wireless network. The decision was made to build a completely separate wireless network that would not have Internet connectivity and the internal network would only be accessible through the corporate VPN.

The corporate VPN consisted of an IPsec appliance and an SSH gateway that was configured for port forwarding. Token-based one-time passwords (OTPs) were used on the IPSec appliance and the SSH gateway. The corporate VPN already had a requirement for using a company approved secure build or utilizing a personal firewall with a company standard rule set.

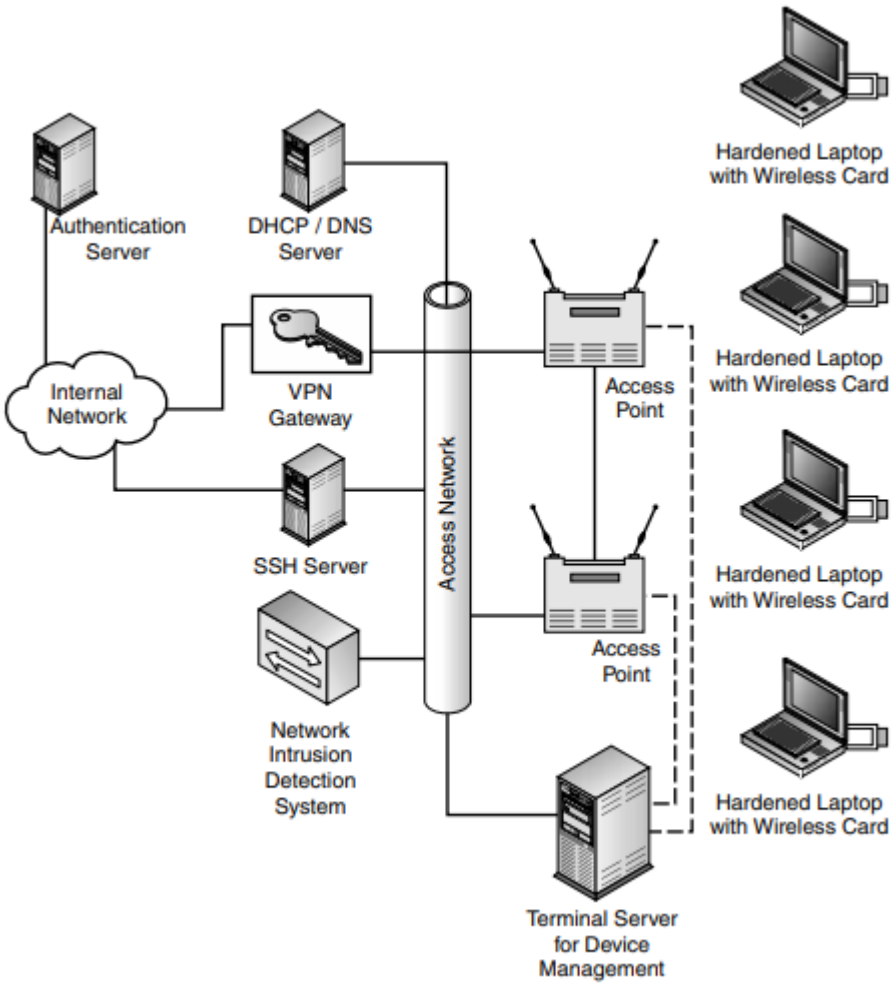
The installation proved to be easy. Additional network cards were added to the IPSec appliance and the SSH gateway for connectivity to the wireless network, as shown in Figure 8-4. Only a few more machines were needed to make the network fully functional. A server was added to provide Dynamic Host Configuration Protocol (DHCP) and Domain Name Server (DNS) services to the wireless users because the VPN and SSH clients were configured to connect to a hostname, not an IP address. Another server was added to the wireless segment as

a NIDS and a syslog server to capture logs from the access points and DHCP server. Finally, a terminal server was installed to manage the access points and Ethernet switches because the only network-based management options offered by the vendor were cleartext (telnet and HTTP). The best practices include the following:

- Segment the hostile wireless network from the rest of the internal network.
- Disable the management of access points with the wireless interface.
- Harden the DHCP/DNS server.

Enterprise Design 2

Another option for implementing a secure wireless network is to use 802.1x. At the time of this writing, 802.1x is still in draft form and vendor interoperability is limited at best. However, 802.1x is a valid option for adding security to a wireless network. It is a new technology and still has not had the time in the market or been under public scrutiny to show what implementation-specific caveats and details need to be addressed.



However, 802.1x shows great promise and should be considered in a wireless network designer's toolkit.

This design does not suffer from the limitations of the previous design. In this case, the users were exclusively using Windows and all hardware was provided by the company, so using a vendor-specific implementation was not a problem. The vendor chosen was one that the network designers were very comfortable with: Cisco.

The 802.1x implementation used the existing corporate directory services. However, a new RADIUS server was necessary for the vendor's 202 Part 3 Wireless Deployment Strategies Access Network Access Point Access Point Terminal Server for Device Management Network Intrusion Detection System SSH Server VPN Gateway DHCP / DNS Server Authentication Server Hardened Laptop with Wireless Card Hardened Laptop with Wireless Card Hardened Laptop with Wireless Card Hardened Laptop with Wireless Card Internal Network Figure 8-4 Enterprise design 1 802.1x implementation of EAP over RADIUS, and additional features were required. 802.1x not only provided authentication services, but it was also used for dynamically creating WEP keys. RADIUS session timeouts of three hours were used to force the changing of WEP keys on a frequent basis. The implementation also used the key-hashing features mentioned earlier in this chapter.

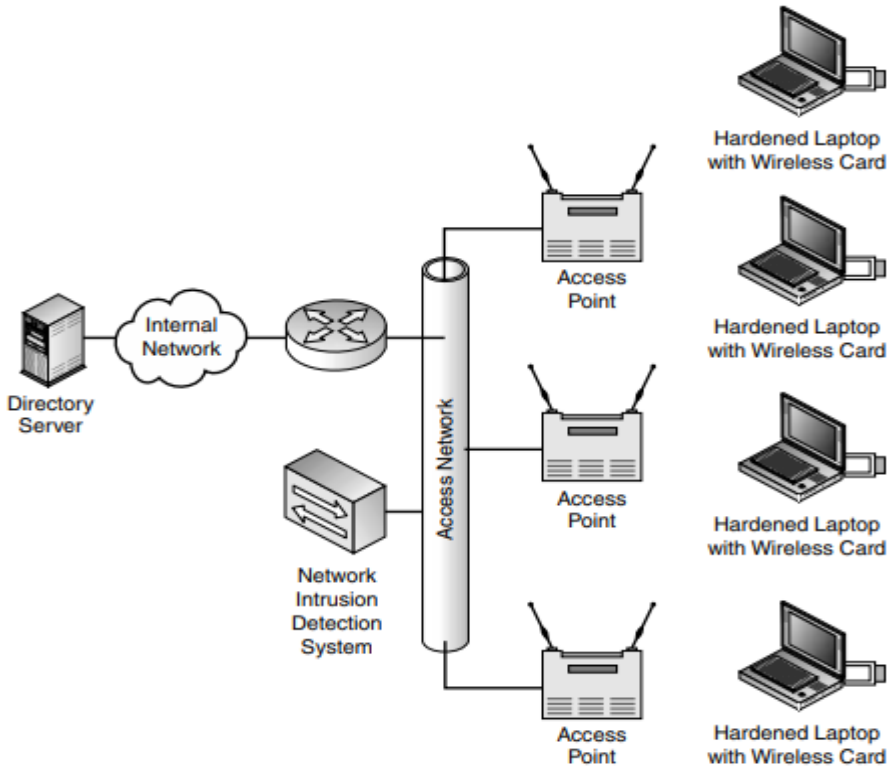
The best practices include the following:

■ Use 802.1x for authentication and encryption.

■ Change keys frequently; three-hour timeouts are used.

■ Use key-hashing features.

■ Advanced proprietary integrity checking features are used



■ The wireless network is kept segmented from the rest of the network to enable future network changes.

■ NIDS is used on the wireless network.

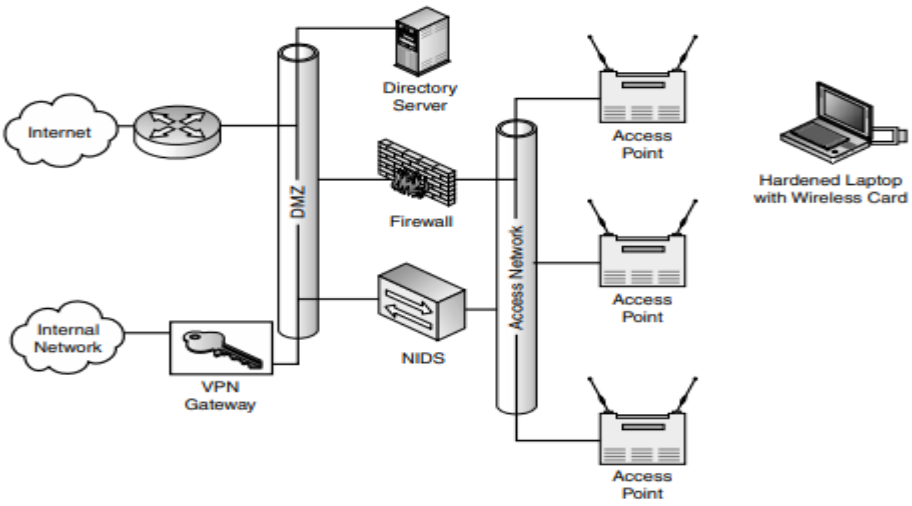
Enterprise Guest Network

Another application for a wireless network at an enterprise campus is for a guest network. A similar configuration can also be used at universities or training centers. At one corporation, contractors and vendors frequently needed access to the Internet. The information security team did not want people attaching to the network who had not signed the acceptable use policy so a guest network was set up. This was a separate network set up to protect the enterprise's intellectual property.

The first implementation of this guest network was adding data connections in strategic locations, such as conference rooms and visitor cubicles. After one visitor infected machines on the internal (nonguest) network with a virus by accidentally plugging into the wrong jack in a conference room, the network architects began searching for another solution. The decision was made to set up a wireless network that would be used by guests needing Internet access.

A process was followed to set up the guest network during its initial implementation without wireless, but the design evolved into a wireless network. Functional requirements were presented to the network architects. The guests needed the applications of web surfing and VPN access. The security group was concerned that an open network may give free Internet access to malicious attackers. After considering the functional requirements and the concerns of the security group, a design was proposed and approved.

The network was set up with a web proxy that required a username, password, and a packet filter that allowed VPN connections, as shown in Figure 8-6. The access points that were used offered DHCP services so a DHCP server was not needed. The proxy server was used to capture logs from the access points and provided DNS services. An NIDS was also added to the network. The help desk has a supply of wireless cards that can be checked out for guests and visitors. When a wireless card is checked out, a username and password are created on the proxy server and an instruction sheet with configuration instructions is provided. Each username and password expire after one week



The best practices include the following:

■ The guest network is segmented and firewalled from the rest of the network.

■ NIDS is installed on the hostile guest network.

■ Users must agree to an acceptable use policy in order to use the network.

■ Network uses 802.11 standards to give the maximum hardware support.

■ Corporate laptops are hardened before using the wireless network.

Enterprise Point-to-Point Configuration

The cost savings of replacing a traditional telco point-to-point connection with a wireless link can be tremendous; wireless links can also be set up much faster than traditional telco links. Existing wireless networking technologies can be used to create these point-to-point links. In many cases, ranges can be extended by using directional antennae and amplifiers. The security benefit of using a directional antenna is that it makes the link much more difficult to sniff or jam. This link is trivial to secure because both ends of the link are static and known.

In this commonly found scenario, you can easily use traditional IPsec based VPN-tunnelling software or appliances to protect all traffic flowing between one end of the bridge to the other. These VPNs can be set up using VPN appliances, routers, or software-based VPNs.

The best practices include the following:

■ Use directional antennae to eliminate signal loss and boost power.

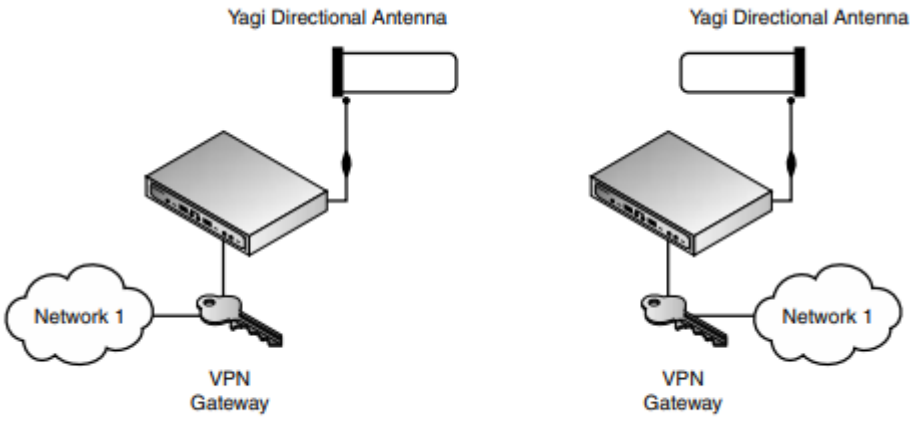
■ Configure access points to only connect to the other end of the connection; many times this is accomplished with entering a MAC address.

■ Use WEP.

■ Use IPsec tunnel mode.

■ Use a strong form of encryption, such as Advanced Encryption Standard (AES) or Triple Data Encryption Standard (TDES).

■ Rekey the VPN frequently.



Wireless ISP Design

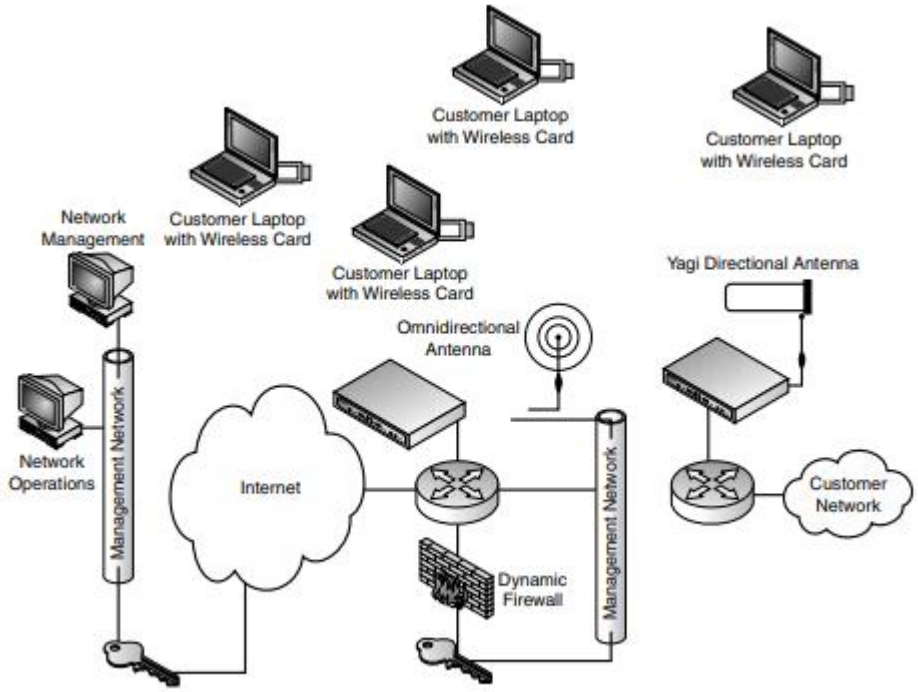
Metropolitan area networks (MANs) have seen a rebirth from almost certain doom with the adoption of wireless network technologies. Many regional and specialty ISPs are starting to offer wireless Internet access. This Internet access can be limited to a small area or can be offered in coffee shops, hotels, or airports. In order to prevent customer support calls and improve the customer experience, the network needs to be open. In this scenario, you don't know who is going to join the network. Therefore, network resources need to be well protected.

In order to meet customer requirements, an open design is required. The network administrators chose to implement a separate back-end network for management. During implementation, careful consideration was given to finding a vendor that had features for securing managing network devices, such as access points and routers. Unfortunately, no vendor was offering this during the buildout of the network so a separate management network was necessary. The management network had the added benefit of giving the network designers a lot of flexibility to roll out new applications.

The network was set up with a dynamic firewall that would open up holes for Internet access after users authenticated to the billing server. This was an off-the-shelf product that had some security holes, but building a custom solution would be cost-prohibitive. A VPN was used to access the management network for the network operation and management functions.

Retail and Manufacturing Designs

Wireless networking has proven to be a killer app for many network retail and manufacturing companies. The return on investment (ROI) for wireless applications has proven to be significant. Unlike the corporate campus, the common workstations for a retail or manufacturing wireless application are personal digital assistants (PDAs), bar-code scanners, and other thin clients. The following network designs were used in these environments.



Kiosk/Roaming Agent Design

Wireless applications can dramatically increase customer satisfaction. Customer-service applications are often wired to a desk or service point that may not be in the most convenient place for the customer, or a new application may need to be rapidly deployed into an existing store, or kiosk, and wiring constraints may prevent the adoption of the application.

This wireless design is for an application that has a very large user population that does not have much technical expertise, so the equipment and user experience needed to be simple. PDAs with bar-code scanners were chosen as the equipment for this application. The PDA had all the necessary functionality, but needed the capability to add a small printer. A quick proof-of-concept application was created using a wide-open wireless network and a modified web browser. All the functionality was there, but the security concerns needed to be addressed.

The application designers tried using off-the-shelf software modified for the particular environment, but after initial testing, the decision was made to customize an application. The application programmers were able to port the Mini browser application to IPsec using a cryptographic toolkit from a commercial vendor. The toolkit was designed to handle all the sophisticated cryptographic functions without the programmer needing to learn how to write IPsec software. Due to the highly public environment of the application, the designers chose to harden the application and use WEP and MAC access controls. A pair of VPN gateways and servers providing DHCP, DNS, and logging were set up for the entire network, serving hundreds of stores. An IDS system was also set up for network monitoring and detecting suspicious activity.

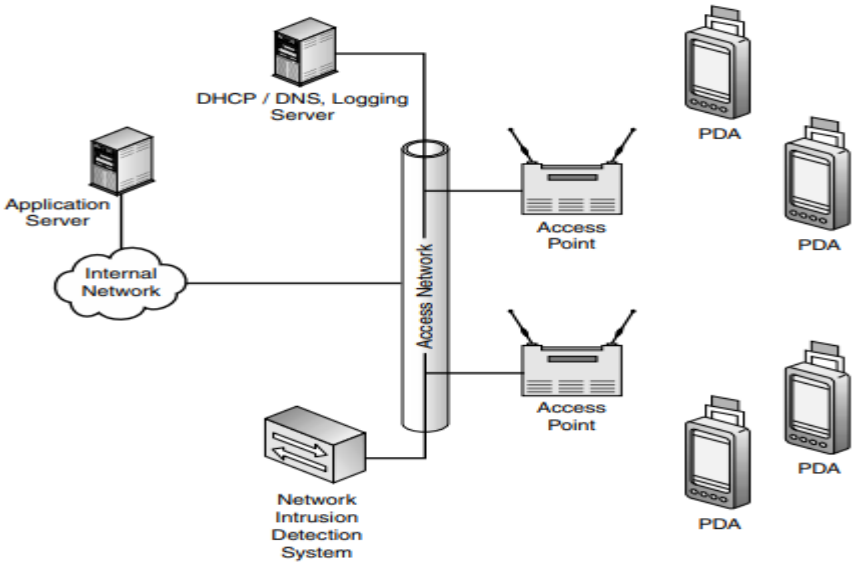
The best practices include the following:

■ All traffic is authenticated and encrypted.

■ An IDS system is used for watching the network.

■ Standard-based 802.11 security features are used, but are not relied on.

■ A hardened server provides network services (DHCP and DNS).



Warehouse Design

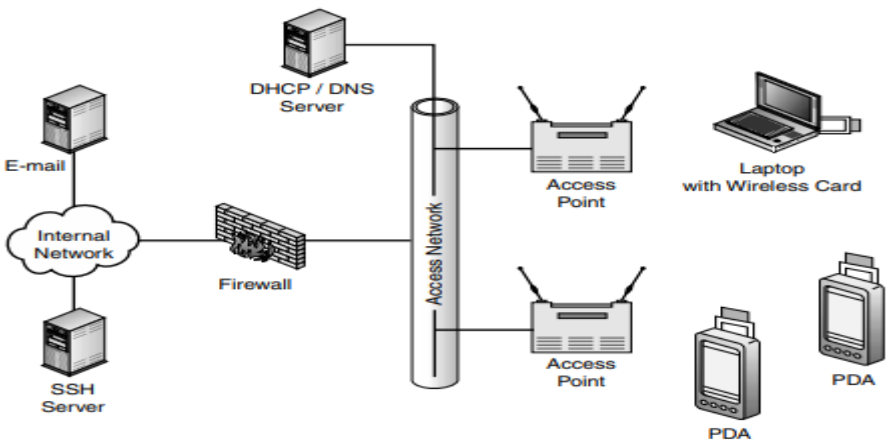
The early adopters of wireless technology included the manufacturing and warehousing industries. Wireless was adopted mainly for the mobility that it provides and to prevent significant wiring changes that are frequently needed in a warehouse. Internet and e-mail are not common applications in the industry. The most common are inventory tracking and shipping applications. Many times, these run off a PDA or connect to a thin client or terminal. Many of these early implementations used telnet or a simple browser for user input in conjunction with a bar-code scanner or magnetic-strip reader. WEP was used to secure these applications because cleartext protocols were being used. After the shortfalls of WEP were publicized, a network redesign was needed.

Once the wireless network was installed, there was no going back, but security was still needed. The network was redesigned to keep the functionality and ease of use while adding security. If a malicious attacker were to attack the network, downtime could be very expensive. Troubleshooting wireless networks is also expensive because in many cases the staff is not immediately available and often must travel to the site. Many warehouses and manufacturing companies lose money if products cannot be delivered on time. During the network redesign, using a technology that uses licensed frequencies was considered, but it was cost prohibitive and not available in all locations.

The existing network was used with a few modifications. Shared key authentication was replaced with an open system. WEP keys were rotated on a monthly basis. MACs were utilized when the feature was not previously enabled. Then an IDS was added to the network. SSH was used to replace the telnet application and port forwarding to the e-mail server that was added for the program. The network was also designed to allow the addition of thin clients using an encrypted protocol.

The best practices include the following:

- Use encrypted protocols.
- Use a firewall or packet filter to limit network exposure.
- Monitor for potential failure conditions or attacks.
- Regularly change WEP keys.
- Use MAC access controls.



Small Office/Home Office Design (SOHO)

One of the biggest challenges in securing a Small Office/Home Office (SOHO) wireless network is deciding how much security to use. You would not buy a million-dollar safe to protect a thousand-dollar diamond. To make matters more difficult, SOHO configurations are often implemented with inexpensive hardware that does not offer many security features. However, achieving adequate security for your SOHO is still possible. The decision about security should be made before purchasing hardware to ensure that the hardware has the necessary features.

The primary question that needs to be answered is how will adding wireless to your SOHO change the current threats? Some SOHO networks are connected directly to the Internet through a broadband connection. If this is the case, then adding a wireless connection to the network does not significantly change the threat to the already Internet-connected machine. However, a new threat to the network bandwidth is being introduced. A malicious user could attach to the wireless connection for free Internet access.

To make matters worse, this malicious user may attack other sites or use your Internet connectivity to introduce a new virus on the Internet with your connection. Therefore, steps must be taken to secure the wireless connection. Very destructive viruses, such as the Melissa virus, have been introduced to the Internet using stolen Internet access accounts. Although the authorities were eventually able to track down the writer, the person with the stolen AOL account went through much heartache. Tracking down a wireless user who attached to someone's unprotected access point could be very difficult, if not impossible, and may leave the negligent owner liable. By the way, make sure that your desktop computer has a virus-scanning program and it is kept up-to-date.

Now let's take a step back and examine the threats toward the SOHO machines. As stated before, many times these machines are directly connected to the Internet. In some cases, these may be protected by a firewall or router, which provide a level of protection. In either case, if you add a wireless connection to a SOHO network, the machines on the network must be hardened. Hardening hosts may involve many different processes, but this normally involves disabling unnecessary services, using strong passwords, deleting unused accounts, or adding firewall software.

Reasonable steps should be taken to secure a SOHO wireless network. Use the security features of the access point, which may include WEP and MAC access controls. Consider purchasing a high-end access point with advanced security features. Cisco produces access points with very advanced security features (such as LEAP, an 802.1x implementation) that cost just a little bit more than most access points and will give you much better performance and radio coverage. It is money well spent.

The best practices include the following:

■ Access point—use WEP and MAC access controls. This will significantly increase the level of complexity of an attack.

■ Network hosts—add personal firewall software to machines and add strong passwords to the printer and router.

■ Turn off the equipment when it is not in use.