Chapter 8

Hardening Wireless LAN Connections

- Banning WLANs Without IT/Management Approval
- Hardening Wireless Access Points
- Hardening Wireless LAN Connections
- Hardening Windows XP Wireless Clients
Wireless LAN (WLAN) connections represent the classic struggle between security and usability. On one hand WLANs were created and are used to simplify the ability of users to connect to and access network resources. With a wireless NIC, a user can connect to a network anywhere on a campus, in an office, or at any neighborhood coffee shop. On the other hand, WLANs are by their very nature insecure. The data is sent over the airwaves, where anyone can potentially receive it. In addition, an illegitimate user can often connect to a WLAN with the same ease that a legitimate user can if the WLAN is left in the default mode. Indeed, no one in their right mind who has any kind of security focus would allow a WLAN in their environment. However, it is not a lost cause. As you will see, there are many things you can do to secure your WLANs.

At the same time, you may already have a WLAN or are planning one. Does this mean you aren’t concerned with security? Of course not. To the contrary, this illustrates how important it is to provide usability and functionality to your users. It also illustrates the simple reality that in the struggle between what users want and need and security, security frequently comes in second. This does not mean that we have to accept that we cannot secure our WLANs, though. Instead, it means that we need to take extra measures to ensure that we provide the access our users request while providing the security our network requires.

Banning WLANs Without IT/Management Approval

As mentioned in Chapter 1, wireless presents a unique problem to your networks. It is entirely too easy for someone to obtain a rogue WAP, connect it to your network (using DHCP to assign the WAP an IP address), and then allow anyone with a wireless client to be able to connect to your network, even though your wireless security policy should explicitly prohibit such actions.

Preventing Rogue APs

No good, bulletproof technical method exists to prevent a WAP from being connected to your network. By that I mean that if someone wants to bring a rogue AP onto your network, they are always going to have a chance of being successful. This doesn’t mean that you should pack up the tent and head home, however. There are a few things you can do to prevent or greatly reduce the odds of a rogue WAP being successfully connected to your network:

- Implement a wireless security policy. The first thing to do is to have a good wireless security policy. The problem of unauthorized WAPs is largely a people problem that requires a people solution in the form of enforceable security policies. Also, your wireless security policy is one that absolutely must have teeth. If
someone brings a rogue WAP online, they need to be subject to termination of employment. Your wireless security policy also needs to define what the response to a rogue AP is. For example, will the AP be confiscated, and, if so, who is responsible for that?

- Provide for physical security. A WAP has a limited range. You should implement physical security measures that prevent someone from being able to get within range of a WAP running in your organization. Unfortunately, oftentimes this is not a practical measure, and it’s useless in regard to people with unauthorized WAPs (they already aren’t paying attention to the security policy, so they probably don’t care about where they locate their WAP).

## WLAN Modes of Operation and Components

Another aspect of your wireless security policy should define the mode of operation permitted for your WLANs. WLANs have two modes of operation. The first mode of operation is infrastructure mode, and it’s the conventional WLAN configuration. Infrastructure mode entails the wireless clients being connected to the existing wired infrastructure by way of a WAP or wireless router. The second mode of operation is ad hoc mode, sometimes referred to as peer-to-peer mode. In ad hoc mode, multiple wireless clients are connected to each other in a peer-to-peer fashion, allowing small workgroups of computers to connect to each other without any other infrastructure. You should not allow ad hoc connections in your environment.

You also need to explicitly define the physical WLAN components you will allow in your network. This will assist you in detecting and identifying unauthorized wireless devices. The three primary WLAN components to define in your environment are the following:

- **Wireless access point (WAP)** A WAP (sometimes referred to as a base station) is the device that wireless clients connect to. A WAP can typically connect hundreds of wireless clients and effectively operates like a bridge, allowing the client access to the physical LAN segment the WAP is connected to. WAPs are typically used in enterprise environments to provide wireless access.

- **Wireless router** Wireless routers combine the functionality of a WAP with a router, allowing wireless clients to connect to the router and then be routed to other networks. Wireless routers often include firewall functionality and are typically used in small office/home office (SOHO) environments to provide wireless access.

- **Wireless client** Wireless clients include any device that uses a wireless network card to communicate with a WAP or wireless router.
Hardening Network Infrastructure

- **Provide a supported WLAN infrastructure.** If people want a WLAN and they don’t have one, they might be tempted to implement one on their own. On the other hand, if you make sure you implement a WLAN that supports your users’ needs, they will be much less likely to decide to go about it on their own. The truth is, most rogue WLANs are implemented by nonmalicious users who simply think that a WLAN will make their lives easier.

- **Implement 802.1x port-based security on your switches.** As we will discuss in Chapter 9, you should implement 802.1x port-based security to prevent any unauthorized connections to your network by requiring all connections to be authenticated. This includes preventing an unauthorized WAP from being able to connect.

- **Limit the number of MAC addresses per port to only one.** This will prevent switches from passing packets from rogue WAPs because the WAP and the client both have different MAC addresses. This is also a good measure if you want to prevent the users from plugging in a “rogue” switch or hub as well. You can implement this on many IOS-based switches by running the following command at the CLI:

  ```
  switch02(config-if)# switchport port-security maximum <max addrs>
  ```

---

Rogue WAPs

I personally know of companies that have rogue WAPs that allow anyone on the freeway to access their internal production network, including potentially granting access to source code. A rogue WAP is a death blow to security because no matter how much you have hardened the perimeter, it has been instantly undermined by the WAP once it connects to your internal network.

Once you have undertaken procedures to prevent unauthorized WAPs, the next step is to implement procedures to detect unauthorized wireless connections.

**Implementing WLAN Discovery Procedures**

Just because we can’t really prevent unauthorized WAPs from being implemented on the network doesn’t mean we can’t detect and remove them. It just means that we need to get a little creative in how we approach the problem.
You have two primary methods of detecting unauthorized WAPs on your network. The first method attempts to detect them wirelessly. The second method attempts to detect them from the wired network.

**Detecting Unauthorized WAPs Wirelessly**

The most effective method of detecting unauthorized WAPs is by simply using a wireless client and locating the WAPs broadcasting in your environment. A few caveats must be considered when employing this method, however:

- You have to be within range of the WAP in order to detect it.
- It is very difficult to detect a WAP that does not broadcast its SSID.
- It can be difficult to survey remote sites.

The good news is that because most unauthorized WAPs are not implemented by malicious users (and oftentimes are implemented by nontechnical users), the odds are high that the SSID broadcast has not been disabled. This leaves us with the problems of needing to be within range of the WAP to detect it and trying to survey remote sites. It is often impractical for someone in IT to spend the day walking around trying to determine if they can detect access points. One of the best solutions I have seen for this is to take advantage of someone who on a daily basis must walk around the environment—the mail delivery person. You can outfit this person with a laptop or handheld carrying extra batteries and while they make their normal rounds delivering the mail, the laptop can sit in the bottom of the mail cart quietly detecting any WAPs. A number of wireless analyzers can be used to detect the presence of unauthorized WAPs, including the following:

- Airdefense (http://www.airdefense.net/)
- Airmagnet (http://www.airmagnet.com/)
- Boingo (http://www.boingo.com/)
- Netstumbler (http://www.netstumbler.com)
- Kismet (http://www.kismetwireless.net/)
- Wildpackets Airopeek NX (http://www.wildpackets.com/products/airopeek_nx)

Netstumbler provides one of the easiest methods for detecting a rogue AP over the wireless network. Once you install Netstumbler, the program automatically begins
scanning for WAPs with no configuration required on your part (other than providing the wireless NIC, of course). For example, the screen shown next depicts what I was able to capture while driving down a major freeway in the Houston area. I captured 175 WAPs, of which 113 were running no encryption whatsoever, and none of which were running WiFi Protected Access (WPA). Instead, they were all using WEP.

### Detecting Unauthorized WAPs from the Wired Network

Detecting unauthorized WAPs from the wired network is generally not as easy a process as it is to detect them wirelessly. After all, it doesn’t get much simpler than walking around with a laptop and a wireless card. At the same time, you can’t really do much about the biggest problem with trying to detect a WAP wirelessly—namely—detecting a WAP that is not broadcasting its SSID.

Using a wired detection process can alleviate some of the disadvantages to trying to detect an unauthorized WAP wirelessly. For example, a wired detection process is not susceptible to missing WAPs that do not broadcast their SSIDs. In addition, a wired detection process can be used to survey remote sites and can even be scheduled and scripted to increase ease of use.

Unfortunately, there are some drawbacks to this method. It can be difficult to locate all the unauthorized access points. This is largely due to the lack of mature or specialized products for this task. Currently, most techniques rely on using MAC addresses (because
all vendors are assigned a MAC address range) or OS fingerprinting to identify the WAP, both of which are an imprecise science. Here are two tools that can assist you in identifying an unauthorized AP by monitoring MAC addresses:

- **AP Tools** ([http://winfingerprint.sourceforge.net/aptools.php](http://winfingerprint.sourceforge.net/aptools.php)) AP Tools not only can discover an access point based on the MAC address, it can also attempt to check to verify that the access point is a WAP.

- **Arpwatch** ([http://www-nrg.ee.lbl.gov/](http://www-nrg.ee.lbl.gov/)) Arpwatch can monitor the network and maintain a database of MAC address and IP address pairings.

Here are some tools that can assist you in OS fingerprinting:

- **Nmap** ([http://www.insecure.org/nmap/index.html](http://www.insecure.org/nmap/index.html)) Nmap can be used to identify the OS that a scanned host is running. For more information on using Nmap see Chapter 13.

- **Xprobe** ([http://www.sys-security.com/html/projects/X.html](http://www.sys-security.com/html/projects/X.html)) Xprobe is similar to Nmap in its ability to identify the OS through the use of fingerprinting.

- **Nessus** ([http://www.nessus.org](http://www.nessus.org)) Nessus is discussed in detail in Chapter 13. However, you can find an excellent whitepaper that details the process of using Nessus to detect rogue WAPs at [http://www.tenablesecurity.com/wap-id-nessus.pdf](http://www.tenablesecurity.com/wap-id-nessus.pdf).

Both of these methods share the common problem of generating false positives. For example, Nmap recognizes a Linksys WAP54G as a Linux device because it actually runs Linux for the OS. This can make it difficult to determine whether the device is indeed a WAP or just a Linux host running on your network. MAC address tools rely on identifying a device due to it having a MAC address that has been assigned to a wireless vendor. That can make it difficult to distinguish between a Cisco AP and a Cisco switch if the database of MAC addresses has not been accurately updated.

### Detecting WAPs from the Wired Network

While I was writing this, I got into a discussion with a colleague about the inconsistencies and difficulties of detecting a rogue wireless AP on the network. He mentioned that he was testing an alpha version of Network Associates ePolicy Orchestrator (EPO; [http://www.nai.com/us/products/mcafee/mgmt_solutions/epo.htm](http://www.nai.com/us/products/mcafee/mgmt_solutions/epo.htm)) that has the ability to detect rogue wireless APs. When I asked him how well it worked, he mentioned that he had tested EPO with a number of different wireless APs and that it detected all of them within 5–8 minutes of being brought online. The technology is definitely improving, and the accuracy of the detection algorithms is getting much better.
Removing Rogue WAPs

Once you have detected a rogue WAP, you have a couple of methods you can use to shut it down. One option is to attempt to physically locate and disconnect the WAP from the network. However, this can be both time consuming and prone to failure. The obvious difficulty in this method is that it can be very difficult to locate the WAP, usually through a trial-and-error process. (Is the WAP here? No. Is it here? No.)

Another option is to locate the switch port that the MAC address is connected to and shut that switch port down. Similarly, you can determine the IP address of the WAP and attempt to block the IP address. Personally, I recommend shutting down the switch port. In many cases, this will cause the person to seek you out, saving you the time and effort of trying to find them.

User: Uh, yes, I can’t access anything on the network anymore. I don’t know what happened.

You: No problem. We know exactly what is going on. What office are you in?

Hardening Wireless Access Points

Although all wireless access points have unique interfaces, they share common functions and processes that can be hardened. This section focuses on what you can do to harden the WAP itself. We will look at the following hardening steps:

- Hardening remote administration
- Configuring the Service Set Identifier (SSID)
- Configuring logging
- Configuring services
- Configuring wireless mode

It would be impossible to detail the procedures for hardening every type of wireless access point manufactured; therefore, I will illustrate the specific hardening steps for the following WAPs:

- Cisco Aironet 1200 running IOS version 12.2(13)JA2
- Linksys WAP54G running firmware version 2.06
- Dell TrueMobile 2300 running firmware version 3.0.0.8 in access point mode
Chapter 8: Hardening Wireless LAN Connections

HEADS UP!

Many of the configuration changes you make to the Dell TrueMobile 2300 require a restart before they take effect. This can make it difficult to make changes during production hours or while clients are connected to the WAP.

The instructions in this chapter assume that you have configured the device with an IP address that is relevant for your network and that you have already connected to the respective web-based management GUI and successfully logged on. In addition, the screen references refer to the menus you would need to click to access the given screen. For example, “go to the Security | Admin Access screen” means that you must click the Security menu and then the Admin Access menu to be presented with the screen in question.

Hardening Remote Administration

Like all our network devices, we should secure our WAPs against unauthorized remote administration. Unfortunately, unlike many network devices, virtually all WAPs fail miserably at providing secure remote administration. This is due to most of them providing only an unencrypted management protocol such as Telnet or HTTP for connecting to the device. Even with that gross oversight in security, certain steps can be taken to harden remote administration. The most important task is to change the default administrative username and to implement passwords that conform to your password security policy.

Changing the Default Administrator Name and Password

The Cisco Aironet 1200 implements a full IOS feature set. Consequently, it can be hardened for remote access by requiring all CLI connections to use SSH, as you do for your Cisco routers (refer to Chapter 6). In addition, out of the box the Cisco Aironet 1200 uses the default authentication mechanism of a global password (enable secret). You can change the password at the Security | Admin Access screen, as shown next. I recommend that you use an authentication server, where possible, and individual local users if an authentication server is not an option. By default, the WAP ships with a default username of Cisco and a default global password of Cisco. You should change both of these as well. Click Apply in each section when you are finished.
If you want to use an authentication server, you must first configure the WAP to use a RADIUS or TACACS+ server at the Security | Server Manager screen in the Corporate Servers section, as shown next. Make sure you scroll down to the Default Server Priorities section and select the newly added authentication server for the Admin Authentication setting. When you are finished, click Apply.
The Linksys WAP54G does not implement username and password security. Instead, it uses a password only. You can configure the password at the Setup Password screen, as shown here. When you are finished, click Save Settings.

The Dell TrueMobile 2300 utilizes both a username and password. By default, the username is admin. You should change both the username and password according to your security policy. This can be done at the Advanced Settings Administration Settings screen, as shown next. When you are finished, click Submit.
The system administration section shown here is used when the WAP is operating in router mode. The settings allow you to permit an external host (that is, across the Internet) to be able to make remote administration connections to the WAP. You should never enable this functionality because Dell does not support HTTPS for remote administration connections.

**Securely Configuring the Service Set Identifier (SSID)**

The service set identifier (SSID) is a unique identifier used in the packet header of wireless packets as a password for authenticating the client. The SSID is also known as the *network name*. By default, most WAPs will broadcast the SSID so that wireless clients can identify the WAP to which they should connect. This creates an obvious security vulnerability, however, because anyone with a wireless client can immediately determine a WAP is in the area by using a tool such as NetStumbler.

To address this issue, it is recommended that you disable the SSID broadcast.

**HEADS UP!**

In my experience, I have found that some wireless clients will not connect to a WAP that is not broadcasting the SSID. This is particularly true of Microsoft PocketPC 2003 devices using the SanDisk SDIO WiFi NIC (or any other NIC based on the Socket chipset and driver). I have, as of yet, been unable to determine why this is, though my suspicion is that it’s due primarily to the immaturity of the SDIO cards and drivers.

Another problem with the SSID is that many people configure it with a value that makes it easy to locate where the WAP is physically located. This is both good and bad. It is good in the sense that it allows you to quickly identify where a WAP is. It is bad, however, in that it can let hackers know that they have connected to a WAP at their target company. As a result, when you configure the SSID, you should never include any information that might identify your company, location, or brand of WAP.

The last aspect of SSID hardening you should configure is the *beacon interval*, which is the amount of time that transpires before the WAP advertises the SSID via broadcast. By setting the beacon interval to its maximum setting, you increase the difficulty of performing passive scanning. It is important to understand that disabling SSID broadcast or increasing the SSID beacon interval is not an end-all security solution. In fact, Microsoft claims that this is not a security measure at all. This is due to the fact that even if the SSID is not broadcast, it can still be determined if someone is using a sniffer in the area where a WAP is in operation. Changing these settings is still an effective method of obscuring your WAP from casual threats, however. All these SSID settings can be configured as follows.

The Cisco Aironet 1200 uses a default SSID of “tsunami” in what is called *guest mode*, which means the SSID is broadcast in the beacon. The default SSID should be removed and replaced with a new one for your environment. This can be done at the
Security | SSID Manager screen shown next. If you want to make sure the SSID is not broadcast, ensure that no SSID is configured in the Guest Mode field in the “Global Radio0-802.11B SSID Properties” section of the SSID Manager screen. When you are finished, click Apply.

For the Linksys WAP54G, you can configure the SSID at the Setup | Basic Setup screen, shown next. When you are finished, click Save Settings.
The beacon interval can be configured at the Advanced | Advanced Wireless screen, shown next. When you are finished, click Save Settings.

For the Dell TrueMobile 2300, you can configure the SSID and the beacon interval at the Advanced Setting | Advanced Wireless screen, as shown next. To turn off the SSID broadcast, check the box labeled Hide My Wireless Network. When you are finished, click Submit.
Chapter 8: Hardening Wireless LAN Connections

Configuring Logging

Like with your firewalls, it can be extremely beneficial to configure your WAP for logging. The objective is for the logging to show you what is going on with the WAP, particularly in regard to unauthorized access attempts. Cisco and Linksys support conventional syslog. Dell does not support any logging facility.

For the Cisco Aironet 1200, you can configure logging to a syslog server at the Event Log | Notification Options screen, shown next.

For the Linksys WAP54G, you can configure logging at the Setup | Log screen, shown next. Simple enable logging and enter the syslog server to which events should be sent. When you are finished, click Save Settings.

Hardening Services

Not many services need to be hardened for most WAPs, with the notable exception of Cisco. The most common services you might run across are as follows:

- Simple Network Management Protocol (SNMP)
- Network Time Protocol (NTP)
- Dynamic Host Configuration Protocol (DHCP)

Configuring SNMP

Cisco and Linksys support using SNMP for management of the WAP; however, neither supports using SNMPv3. Also, both SNMPv1 and SNMPv2 have no security features. Therefore, if you do not need SNMP, you should disable it.

By default, the Cisco Aironet 1200 ships with SNMP disabled. However, you can enable this service at the Services | SNMP screen.

You can configure SNMP support for the Linksys WAP54G at the Advanced | SNMP screen, shown next. Simply enable SNMP, specify a read-only and a read-write
HARDENING NETWORK INFRASTRUCTURE

community string, and enter the appropriate information in the identification fields. When you are finished, click Save Settings.

**HEADS UP!**

Because the Linksys WAP54G displays the SNMP community strings in clear text, you should ensure that no one is looking over your shoulder while you are at this screen.

**Configuring NTP**

The Cisco Aironet 1200 supports the use of NTP primarily to facilitate accurate timestamps for the syslog facility. You can configure NTP at the Services | NTP screen, shown next.
Chapter 8: Hardening Wireless LAN Connections

Disabling the DHCP Server
Because the Dell TrueMobile 2300 is sold as a SOHO wireless access router, it is shipped with a DHCP server configured and active by default. You should disable DHCP at the Advanced Settings | DHCP Server Settings screen by unchecking Enable DHCP Server Functions and then clicking Submit.

Configuring Miscellaneous Services on the Cisco Aironet 1200
In addition to the previously mentioned services, the Cisco Aironet 1200 ships with a whole slew of additional services you need to be aware of. They can all be accessed at the Services screen, as shown next (in this case, the screen shows the default status of all the services after I disabled Telnet and permitted only SSH access, as previously recommended).

<table>
<thead>
<tr>
<th>Services Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet/SSH: Disabled/Enabled</td>
</tr>
<tr>
<td>CDP: Enabled/Disabled</td>
</tr>
<tr>
<td>HTTP: Enabled/Disabled</td>
</tr>
<tr>
<td>Workgroup: Disabled/Enabled</td>
</tr>
<tr>
<td>SNMP: Disabled/Enabled</td>
</tr>
<tr>
<td>VLAN: Disabled/Enabled</td>
</tr>
</tbody>
</table>

As you can see, many of the services are disabled by default. In general, you should disable any service you do not need. The Cisco Discovery Protocol (CDP) and Domain Name Service (DNS) are two specific services you should consider configuring.

Cisco Discovery Protocol  As previously discussed, CDP is used by Cisco to locate other Cisco devices. Unless you are using a network management system that takes advantage of CDP, you should disable it. If you do require CDP, you should consider whether you need the CDP broadcasts to be sent over the WLAN. If you do not, you should disable CDP on the Radio0-802.11B radio, as shown next. Click Apply when you are finished.

<table>
<thead>
<tr>
<th>Services: CDP Cisco Discovery Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDP Properties</td>
</tr>
<tr>
<td>Cisco Discovery Protocol (CDP): Enabled/Disabled</td>
</tr>
<tr>
<td>Packet Hold Time (optional): 180 (10-255 sec)</td>
</tr>
<tr>
<td>Packets Sent Every (optional): 60 (5-254 sec)</td>
</tr>
</tbody>
</table>

| Individual Port Enable: |
| Ethernet |
| Radio0-802.11B |

<table>
<thead>
<tr>
<th>CDP Neighbor Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>switch02-wcconsulting.com</td>
</tr>
<tr>
<td>local-hn</td>
</tr>
</tbody>
</table>
**Domain Name Service**  
DNS is used to allow the WAP to resolve names to IP addresses. It does not allow the WAP to operate as a DNS server. DNS is largely a service of convenience, allowing you to enter device names at various fields so that the WAP can automatically resolve and convert those names to IP addresses. Like all services, however, if you do not require this functionality, you should disable it. Remember, any running service is potentially vulnerable to current exploits as well as unknown future exploits.

**Restricting Wireless Mode**

Many WAPs support operating in 802.11a, 802.11b, 802.11g, or any combination thereof. If you do not need to support multiple wireless access modes, you should disable any unnecessary ones. For example, if you only need to support 802.11b in your environment, you should disable 802.11a and 802.11g. This will ensure that only individuals using the wireless mode you have defined have any chance of connecting to your environment.

The Cisco Aironet 1200 supports using multiple wireless modes through the implementation of multiple physical radio modules.

You can configure the wireless mode on the Linksys WAP54G at the Setup | Basic Setup screen, shown next. Simply select the access mode you want to use, or select Mixed to support both. Click Save Settings when you are finished.

```
<table>
<thead>
<tr>
<th>Setup</th>
<th>Status</th>
<th>Advanced</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Setup</td>
<td>Password</td>
<td>AP Mode</td>
<td></td>
</tr>
</tbody>
</table>

**Firmware Version**

v2.06, Dec 16, 2003

**AP Name**

nod01

**LAN Configuration Type**

Automatic Configuration - DHCP

**Wireless MAC Address**

00:94:28:4C:66:26

**Mode**

Mixed

**SSID**

G-Only

**SSID Broadcast**

Disable

**Channel**

Regulatory Domain: USA

**Wireless Security**

Enable / Disable

Edit Security Settings
```
You can configure the wireless mode on the Dell TrueMobile 2300 at the Advanced Settings | Advanced Wireless screen, shown next. Simply select the wireless mode from the drop-down selection and click Submit.

### Using MAC Address Filtering

One of the most valuable hardening steps you can undertake with your WAP is to implement MAC address filtering. MAC address filtering enables you to specify the MAC addresses that will be allowed to connect to the WAP. At that point, even if someone manages to obtain all the information necessary to connect to the WAP, if their MAC address is not permitted, they still cannot connect. The drawback to this method, however, is that it may require significant overhead for managing all the MAC addresses that may need to be permitted. In addition, MAC addresses can be spoofed, so it is not a panacea but rather another component of the hardening process.

The Cisco Aironet 1200 uses the well-documented Cisco access-list function to restrict/permit clients from establishing an association with the WAP. The first step is to build the access list. You can do this at the Services | Filters screen by selecting the MAC Address Filters tab, shown next.
Enter the appropriate filter index (ACL number) for the MAC address filter. Next, enter the MAC address you want to specify and a wildcard mask. Keep in mind that for Cisco, a value of “0” in the mask means that the corresponding bit in the MAC address must precisely match the filter entry. A value of “H” in the mask means that the corresponding bit in the MAC address is ignored for the purposes of filtering. This can be used, for example, to grant all of a certain vendor’s MAC addresses. Once you have entered this information, the next step is to decide whether the MAC address will be forwarded or blocked. My recommendation is to make the default action Block All and then configure a Forward action for the MAC addresses you explicitly want to forward. When you are finished, click Apply.

The next step is to apply that ACL to the WAP. You can do this at the Security Advanced Security screen by clicking the Association Access List tab, shown next. Select the filter from the drop-down list and then click Apply.
You can enable MAC address filtering on the Linksys WAP54G at the Advanced Filters screen, shown next. Simply select Enable from the drop-down box and specify how you want to perform the filtering. You can either filter to prevent the listed MAC addresses from being able to connect or to permit the listed MAC addresses to be able to connect. I recommend the latter in most circumstances, because it is generally easier to figure out who you want to allow to connect, as opposed to figuring out who you want to prevent. You can filter up to 40 MAC addresses by using the drop-down box to select MAC 21-40. When you have finished entering the MAC addresses to filter, click Save Settings.

The Dell TrueMobile 2300 uses a simplified MAC filtering process. You simply enter the MAC addresses you want to permit to connect. This is done at the Advanced Settings | Access Control Settings screen, shown next. Check the box Enable MAC.
Access Control and then add the MAC addresses you want to permit. When you are finished, click Submit.

Hardening Wireless LAN Connections

All the hardening steps you have undertaken to secure your WAP and define who can connect to it are pointless exercises if you do not also harden the wireless connections themselves. The four main wireless connection methods you need to be aware of and know how to configure are as follows:

- Wired Equivalent Privacy (WEP)
- WiFi Protected Access (WPA) using pre-shared keys
- WPA using RADIUS
- Virtual private networks

A fifth type of wireless connection is the wide-open connection. This connection uses no form of authentication or encryption. Anyone with a wireless card can connect to the WAP and get access to the network. This type of connection is typically used for providing WiFi hotspots. By default, most WAPs ship configured in this manner. The recommendations that follow detail the methods you can use to harden the default configuration.
Hardening Wired Equivalent Privacy (WEP)

As the name implies, WEP was designed to provide privacy to wireless connections on par with a wired connection. WEP was part of the original 802.11 standard and is used by all three wireless standards. WEP was designed to prevent eavesdropping and data tampering and to prevent unauthorized access to the wireless network. WEP functions by utilizing the RC4 cipher stream and combining a 40-bit or a 104-bit WEP key with a 24-bit random number known as the initialization vector (IV). This results in either a 64-bit or 128-bit encryption key. Because the IV changes with every message, a new encryption key is generated for each message. WEP functions by combining the encrypted data packet (known as the ciphertext) with the clear-text IV before transmitting. The IV is sent in clear text due to the destination needing to know the IV used to generate the encryption key. The receiver then uses the WEP key and attached IV to decrypt the packet.

Unfortunately, for all this effort, WEP has some significant security flaws that make it a very ineffective protocol. Although WEP is better than nothing, a hacker can crack WEP in 15 minutes or less, depending on the amount of traffic they can sniff. This is attributed to the following flaws:

- **WEP key recovery**  
  WEP uses the same WEP key and a different IV to encrypt data. The IV has a limited range of values (from 0 to 16777215) to choose from and eventually it uses the same IV over and over. By sniffing the wireless network and picking the same IVs out of the datastream, a hacker can gain enough information to figure out what the WEP key is.

- **Unauthorized data decryption**  
  Once the WEP key is known, a hacker can transform the ciphertext into its original form and gain access to the original unencrypted data.

- **Violation of data integrity**  
  Once the original data has been decrypted, a hacker could potentially use the hacked WEP key to change the ciphertext and forward the changed message to the destination.

- **Poor key management**  
  WEP keys are typically static keys that, once configured on a device, remain the same from that point forward. The problem is exacerbated when an employee leaves the company because the WEP key really needs to be changed to ensure security. Unfortunately, this is not a

RSA Security has developed a solution that addresses the weak WEP key methods. It is called the Fast Packet Keying Solution and utilizes a hashing mechanism to dynamically generate unique WEP keys for each packet, thus preventing a hacker from being able to determine the WEP key. You can find more information about this at http://www.rsasecurity.com/newsletter/wireless/2002_winter/feature.html and http://www.rsasecurity.com/rsalabs/technotes/wep-fix.html.

- **Unauthorized data decryption**  
  Once the WEP key is known, a hacker can transform the ciphertext into its original form and gain access to the original unencrypted data.

- **Violation of data integrity**  
  Once the original data has been decrypted, a hacker could potentially use the hacked WEP key to change the ciphertext and forward the changed message to the destination.

- **Poor key management**  
  WEP keys are typically static keys that, once configured on a device, remain the same from that point forward. The problem is exacerbated when an employee leaves the company because the WEP key really needs to be changed to ensure security. Unfortunately, this is not a
practical solution if your company has hundreds or thousands of wireless devices because they will all need to be configured with the new WEP key.

### ONE STEP FURTHER

Some vendors address the key-management issue through the use of proprietary “dynamic WEP” mechanisms. This causes the systems to dynamically generate WEP keys that devices will use in conjunction with 802.1x authentication. Essentially, a new secret key is generated for each client that is authenticated. Although this can increase the security of WEP, because these are proprietary implementations, they are only practical if you use wireless devices that support the mechanism.

- **No access point authentication**  
  WEP functions by allowing the wireless clients to authenticate the WAP; however, the WAP has no means of authenticating the client. Consequently, a hacker can reroute the data to access points through an alternate and unauthorized path.

Although these flaws may seem to imply that one should not use WEP, this is not correct. If you have the ability to use a better protection mechanism, such as WPA or 802.11i, do so. If you can’t, though, WEP is still better than nothing—even with the flaws.

For your Cisco Aironet 1200, you can configure WEP at the Security | Encryption Manager screen, shown next. Select WEP Encryption and choose Mandatory from the drop-down list. Enter the four 128-bit encryption keys and click Apply when you’re finished.

![Security: Encryption Manager](https://example.com/security-encryption-manager.png)

For your Linksys WAP54G, the first step of configuring WEP is to enable wireless security at the Setup | Basic Setup screen. Next, you should click Edit Security Settings. This will present you with the Security Settings screen, shown next. Select WEP for the
security mode. Select “128 bits 26 hex digits” for the WEP Encryption. Enter a passphrase that meets the requirements of your password security policy and click Generate. This will generate the WEP keys you will need to enter on your wireless clients. When you have finished, click Save Settings to close the Security Settings screen.

You can enable WEP on your Dell TrueMobile 2300 at the Basic Settings | Wireless Security screen. Once you check Enable Wireless Security and select WEP from the Network Authentication drop-down list, you will be presented with the WEP Settings section, shown next. Select “104 bits (13 characters)” for Key Length and enter a 13-character key value for all four keys that conforms to your password security policy. When you have finished, click Save & Apply. When prompted, click Save & Restart.
Hardening WiFi Protected Access (WPA)

WPA is a subset of the 802.11i standard and was created to address the vulnerabilities of WEP.

802.11i

802.11i is an emerging technology that is designed to address all the security flaws related to WEP and is the direction that wireless security is heading. 802.11i incorporates all the aspects of WPA, including 802.1x authentication, Temporal Key Integrity Protocol (TKIP), and Michael Message Integrity Check (MMIC). In addition, 802.11i addresses a number of issues that WPA does not. 802.11i uses stronger encryption than WPA through the implementation of Advanced Encryption Standard (AES). This presents one of the biggest hindrances to 802.11i, however, because the processing overhead of AES is significant enough to require hardware upgrades to support it in many cases. 802.11i will also support roaming, which allows users to move between WAPs without losing their connection when they switch from the old WAP to the new WAP.

If you do not need wireless now, I recommend that you wait for 802.11i to be finalized and for 802.11i products to come out.

In fact, the hardening procedure for WEP is simply to use WPA instead. WPA is actually a combination of a few different techniques that mitigate the problems that WEP exposes. The first is the use of 802.1x authentication to address authentication issues. The second is the use of Temporal Key Integrity Protocol (TKIP) to address encryption issues. The final is a Michael Message Integrity Check (MMIC) to address message integrity. WPA is forward compatible with 802.11i.

802.1x Authentication

The 802.1x specification was originally defined for wired networks and provides a mechanism for allowing a client (known as a supplicant) to be authenticated by a network device such as a WAP (known as an authenticator) through the use of a RADIUS server (known as an authentication server). It is important to understand that the WAP does not perform the authentication; rather, it acts as a middleman by passing the client’s credentials to the RADIUS server and letting it handle the actual authentication of the client.

802.1x uses a combination of the Extensible Authentication Protocol (EAP) and RADIUS for authenticating clients and distributing keys. RADIUS is used primarily for carrying the authentication and configuration information between the authenticator and the RADIUS server. RADIUS does not have a mechanism for using anything other than password-based authentication. To address this, EAP is used to provide the means to support authentication, such as public key-based authentication (that is, shared secret). Essentially, the WAP uses EAP to communicate with the client and RADIUS to communicate with the RADIUS server, encapsulating the data as required. EAP utilizes three common authentication means: EAP-MD5, EAP-TLS, and EAP-TTLS. In addition, Cisco has a proprietary implementation known as Lightweight EAP (LEAP). However,
LEAP uses a weaker authentication algorithm. This, combined with its proprietary nature, makes LEAP not a recommended solution. Finally, Microsoft has implemented Protected EAP (PEAP), which was designed to overcome some of the limitations and vulnerabilities of the other EAP methods. PEAP can use MS-CHAP-v2 authentication within the EAP-TTLS tunnel to actually authenticate the user based on Active Directory. Many vendors support PEAP, so much so that it is currently undergoing evaluation to become a standard.

**Temporal Key Integrity Protocol**
Although 802.1x addresses authentication problems with WEP, it does not address the security problems related to the weak encryption keys used by WEP and the ability for a hacker to determine what the WEP key is. TKIP fixes this. TKIP uses 256-bit long encryption keys that are generated through a more sophisticated procedure to provide a much stronger encryption key. TKIP functions by adding the client MAC address and a 48-bit IV to a 128-bit temporal key (which is shared among clients) to guarantee that the encryption key is unique. The temporal key is changed every 10,000 packets to further ensure that hackers cannot begin decoding all packets if they are able to ascertain the encryption key, thus strengthening the security of the network.

**Message Integrity Check**
WPA also uses a MIC that is known as Michael to verify message integrity. A 64-bit message is calculated using the Michael algorithm, which can be used to detect potential tampering of the message or data.

**Hardening WPA Using Pre-shared Keys**
WPA using pre-shared keys (WPA-PSK) is a very common method of configuring wireless connections. This is due to the fact that using pre-shared keys does not require an investment in any AAA mechanisms such as RADIUS. The drawback is the same as any other use of pre-shared keys—it does not scale as well in large environments as RADIUS does. Also, because the keys are human generated, they are more susceptible to cracking.

Configuring the Cisco Aironet 1200 for WPA-PSK is a multistep process. The first step is to configure TKIP as the cipher and to clear all encryption keys at the Security | Encryption Manager screen, as shown next. When you are finished, click Apply.
The next step is to configure the WPA-PSK settings for the SSID at the Security SSID Manager screen. First, select the SSID you want to configure. Next, scroll down to the Authenticated Key Management section (shown next), select Mandatory, and check WPA for Key Management. Enter the WPA Pre-shared Key value. When you are finished, click Apply.

For the Linksys WAP54G, you configure the WPA settings at the Security Settings screen (shown next), just like the WEP configuration. Simply select WPA Pre-shared Key from the Security Mode drop-down box. For the WPA Algorithm setting, select TKIP or AES. AES is more secure, but it can have a negative impact on performance and is not supported by all wireless NICs. Next, enter the WPA shared key that should be used. The shared key should conform to your password security policy. Finally, enter the group key renewal time (default 300 seconds) and click Save Settings when you are finished.
You can configure WPA using pre-shared keys on the Dell TrueMobile 2300 at the Basic Settings | Wireless Security screen, shown next. Simply check to enable wireless security and select WPA for the network authentication method. Enter the appropriate WPA pre-shared key and select the proper key format and WPA group rekey interval (default 300). Finally, specify whether to use TKIP or AES (Dell has the same limitations as Linksys). When you are finished, click Save & Apply and then click Save & Restart when prompted.
Configuring WPA Using RADIUS/802.1x

NOTE The Dell TrueMobile 2300 wireless access router does not support WPA and RADIUS/802.1x.

Using WPA with RADIUS/802.1x allows you to take full advantage of the benefits of the increased security that WPA provides while gaining the scalability that WPA with pre-shared keys does not provide. Before you can configure the WAP to use RADIUS, you need to make sure you have configured your RADIUS server to accept client connections from the WAP and have configured a shared secret. We will look at how to add and configure RADIUS clients in more detail in Chapter 9.

NOTE The Cisco Aironet 1200 WAP does not support WPA and RADIUS/802.1x without the use of a third-party supplicant such as the Funk Odyssey Client (http://www.funk.com) or the Meetinghouse Data Communications AEGIS client (http://www.meetinghousedata.com/). Refer to these vendors for the client-side configuration to support WPA and RADIUS/802.1x.

Configuring the Cisco Aironet 1200 to support WPA and RADIUS/802.1x is a multistep process. First, you need to make sure you have installed and configured Cisco Secure ACS on your network. We will cover installing and configuring the Cisco Secure ACS in detail in Chapter 9. Second, you will need to install a third-party supplicant on the wireless client. This is extremely important because Cisco devotes only one sentence to this—and it’s buried deep in a technical note. If you don’t do this, you will likely find yourself spending a couple hours thinking, “I’ve done everything that should make it work.”

The actual WAP configuration is relatively straightforward. You need to configure the encryption cipher just like you did for the WPA-PSK configuration. The difference is at the Security | SSID Manager screen. Select the SSID you want to configure and scroll down to the Authentication Settings section. Select the Open Authentication check box and choose “With EAP” from the drop-down list. Next, select the Network EAP check box with <No Addition> in the drop-down list, as shown here. When you are finished, click Apply.
To configure WPA with RADIUS on the Linksys WAP54G, you will need to return to the Security Settings screen, shown here. Select WPA RADIUS for the security mode and specify the WPA algorithm. Enter the IP address and port number for the RADIUS server. Enter the shared key that is required to allow the WAP to authenticate with the RADIUS server and then specify the key renewal timeout. When you have finished, click Save Settings.

**Hardening WLANS with Virtual Private Networks**

Virtual private networks (VPNs) are not strictly wireless security protocols; however, they offer an excellent security mechanism for wireless networks right now. Because VPNs were designed to secure data in an inherently insecure environment (the Internet) and because WLANs are inherently insecure, VPNs make an excellent workaround to address WLAN security issues. Essentially, implementing a VPN over your wireless network requires your wireless clients to be running the appropriate VPN client software and the implementation of a VPN concentrator (for example, a Nortel Contivity Extranet Switch) that the WLAN connects to. The resources that the wireless clients need access to would reside on the other side of the VPN concentrator. Once the wireless client has connected to the WLAN, it simply uses the VPN client to connect to the VPN concentrator, and all the subsequent data is sent through the VPN tunnel. Implementing a VPN for all your wireless connections is as close to a bulletproof solution as you can implement. We will cover how to design a VPN for your WLANs in Chapters 11 and 12.

**Hardening Windows XP Wireless Clients**

Configuring your wireless connections on the WAP is only half the battle. You also need to properly configure the wireless NIC to allow the client to connect to the WAP. As with your WAP, you have three connection methods to configure:

- WEP
- WPA using pre-shared keys
- WPA using RADIUS/802.1x
Hardening with WEP

To configure WEP on a wireless NIC, open your network connections, right-click the wireless NIC, and select Properties. Then click the Wireless Networks tab, shown here:

Notice that an available network is already listed. This is a WAP that belongs to one of my neighbors and is broadcasting its SSID. It’s really just that easy to locate an open WAP. To illustrate how easy it is to connect to an open WAP, I have personally pulled over on the side of the road near a residential area to access the Internet and send an instant message to a buddy of mine when my cell phone battery died. You absolutely have to harden your wireless network if you are going to use wireless in your environment.

At the Wireless Networks tab, click Add to add a new wireless network. At the Wireless Network Properties dialog box, enter the SSID of the WAP to which you want to connect. These values must be the same on both the wireless client and the WAP. Select Shared for the Network Authentication field and WEP for the Data Encryption field. Uncheck the box The key Is Provided for Me Automatically and enter the appropriate WEP key, as shown next. When you’re finished, click OK to close the Wireless Network Properties dialog box. Then click OK again to close the Wireless Network Connection Properties dialog box. In a few moments, the wireless NIC will authenticate with and connect to the WAP.
Hardening with WPA
Using Pre-shared Keys
To configure WPA with pre-shared keys, you need to return to the Wireless Network Properties dialog box, as previously detailed. From the Network Authentication drop-down list, select WPA-PSK. From the Data Encryption drop-down list, select TKIP or AES, as required by your WAP configuration. Enter the pre-shared key, as shown here, and click OK to close the Wireless Network Properties dialog box. Then click OK to close the Wireless Network Connection Properties dialog box. In a few moments, the wireless NIC will authenticate with and connect to the WAP.

You need to obtain the WPA Wireless Security Update for Windows XP (Microsoft Knowledge Base Article 815485) at http://support.microsoft.com/?kbid=815485.
Hardening with WPA Using RADIUS/802.1x

To configure WPA using Radius/802.1x, you need to return to the Wireless Network Properties dialog box, as previously detailed. From the Network Authentication drop-down list, select WPA. From the Data Encryption drop-down list, select TKIP, as shown at right.

Next, click the Authentication tab to specify the EAP method, as shown at left. For the EAP type, select Protected EAP (PEAP). This will cause the wireless client to use WPA and PEAP as the 802.1x authentication method to connect to the WAP. The WAP then encapsulates the user authentication passed using MS-CHAP-v2 into a RADIUS datagram and sends the authentication request to the RADIUS server. The RADIUS server responds with the authentication response, and the WAP either permits the connection, if the user was authenticated, or denies the connection, if the user was not authenticated.

Using the Funk Odyssey Client Version 2.28.0.798 to Support WPA and RADIUS/802.1x

Once you have installed the Odyssey client, select the Odyssey Client Manager from the Start menu. This will cause the Odyssey Client Manager to open, as shown here.
In the column on the left, select Networks and then click Add. Enter the appropriate SSID and select WPA for the association mode and TKIP for the encryption method, as shown at left. In the Authentication section, select the profile to use. When you are finished, click OK.

The next step is to configure the profile you specified in the network’s configuration. Select Profiles and click Properties to edit the initial profile. Select the Authentication tab and click Add to add EAP/PEAP, as shown at right. When you are finished, click OK.

The last step is to click Connection and select the network you configured from the drop-down list, as shown at left. As soon as you do this, the client will begin authenticating.
When the authentication has successfully completed, your screen should look something like this:

![Odyssey Client Manager](image)

**Summary**

The term “wireless network” is perhaps the ultimate oxymoron when discussing network security. You want your network to be as secure as possible, but by its very nature the wireless data is transmitted over radio waves that can be captured by anyone within range. On the surface one would think that trying to secure your network and provide wireless access would be mutually exclusive. At the same time, though, the ease of connectivity and the flexibility of accessing the network over a wireless connection are causing more and more networks to include wireless connectivity. It is the classic challenge of functionality versus security. Our responsibility, then, is to take the necessary precautions to ensure that our wireless connections are as secure as they can be.

Because WEP is effectively a broken protocol, you should only use it as a last resort. If your devices support WPA, use WPA. Furthermore, you should use WPA with RADIUS/802.1x authentication so that you do not have to rely on shared keys for authentication. If you have to use WEP, you should seriously consider requiring all WEP-based wireless connections to use a VPN to gain access to the production/wired network resources. We will look at how you can design this VPN network architecture in Chapter 12.

Once you have decided on the wireless protocol, you need to harden the WAP. By default, most vendors ship their WAPs allowing all connections as well as using many default settings that you’ll need to change. The first step is to harden your remote administration capabilities by changing any default usernames and implementing passwords that conform to your password security policy. Next, you should disable
SSID broadcasts to keep the WAP from advertising itself to unknown users. If someone is going to connect to the WAP, they should know the SSID already. You also need to implement whatever logging facilities are supported so that you can better monitor the connections being made and, more important, the connections being denied. You also need to disable or harden all services that the WAP is running, paying special attention to ensuring that you do not leave the default SNMP community strings in place. Next, you should explicitly define the wireless mode that the WAP should operate in. If you know that all your users will connect using 802.11g, you should configure the WAP to only allow 802.11g connections. Although this does not necessarily prevent someone from connecting, it at least ensures that they have to have a NIC that supports the wireless mode you have specified. The last step is to implement MAC address filtering to explicitly permit only those MAC addresses you want to be able to connect to your network and denying everything else.

If you follow these hardening steps for your WLAN, you will greatly mitigate the risk related to offering wireless network access to your users.