Wireless Security Handbook

Aaron E. Earle

© 2006 by Taylor & Francis Group, LLC
Chapter 10

Wireless Access Points

This chapter provides an overview of the many different types of wireless equipment. It predominantly focuses on local area wireless equipment: wireless devices, who makes them, what technologies they support, and in what scenarios they should be used. There are many wireless manufacturers out there, so many that an entire book could be put together to look at each of them in detail. This chapter attempts to address as many as possible, going in-depth only on the most commonly manufactured types.

The single most important piece of equipment in a wireless network is the access point. The access point is the piece of equipment that propagates the wireless signal into the air. There are many types of access points from many different vendors. Some of them are made for small office/home office (SOHO) and some are made for large enterprise deployments. Cisco is one of the biggest players in the access point market; others include Proxim, Aruba, Symbol, and SonicWall. As discussed previously, there is an overwhelming number of manufacturers trying to sell access points. Therefore, the focus stays with some of the most used products in the industry.

10.1 Linksys Access Points

Linksys was acquired by Cisco in 2004. Thus far, Cisco has decided to keep Linksys separate as a SOHO-only product line. This means that the equipment that Linksys has is primarily targeted at SOHO environments.
One interesting thing that Linksys has done is move most of its wireless products to an open source Linux kernel. A full list of all the Linksys access points with open source firmware is located below. This has allowed Linksys to utilize some already-existing open source code to achieve lower development costs.

Using an open source code has sparked many groups who have hacked into Linksys access points and made some interesting features available within their own firmware code releases. Some of the most common hacked firmware types are Wifibox, Batbox, and Alchemy. These firmware versions are rather easy to install and can quickly improve many of the features of a Linksys access point. Some of them have added functionality that was not present in the Linksys firmware releases.

Access points with open source firmware include:

- WRT54G
- WRE54G
- WPG54G
- WET54G
- WAP55AG
- WAP54G

Linksys currently has more than 12 access point models. Most of the access points look like the one shown in Figure 10.1. Some newer models have started to take on a more compact design like the one shown in Figure 10.2. This section looks at each of the two styles and sees how they function.

Looking at Figure 10.2, one can see the older body style. Linksys has ten access point models that follow this body style. Although this is the older body style, it is more likely that one will run into this access point style before the newer style is out in large numbers. The older Linksys access point has a number of indication lights. Each of these lights allow for an easy glance at what is working and what is not. Figure 10.3 provides an up-close look at these lights.

Lights appearing from left to right in Figure 10.3 include:

- **Power light.** This light indicator informs the user that power is being received at the access point. This light also signifies that the device is able to start the boot-up process. It will stay on the entire time the unit is powered up to indicate operation. When the unit is undergoing its self-diagnosis testing during boot-up, this light will flash.
- **Wireless light.** This light indicates that there is a wireless connection. It will blink if wireless traffic is passing through the access point.
Figure 10.1 Older-style Linksys access point.

Figure 10.2 Newer-style Linksys access point.
Port 1–4 light. This light indicates that there is a layer two connection to a wired device on one of the four wired ports of the device. When one of the connected devices starts to communicate, the light will blink.

Internet light. This light indicates that an Internet connection is made to the WAN port of the access point.

The older-style Linksys access points have many buttons, ports, and connections. Going from left to right in Figure 10.4, one can see all of the items detailing each one. First, on the far left, there is a reset button used to restore the configuration of a device to the factory defaults. Next, there is an Internet port used to attach an Ethernet cable to a high-speed Internet connection such as DSL or cable Internet. This port will allow
the use of any Ethernet-capable, high-speed access device. The next items are the four wired ports. This group of 10/100 wired ports allow small offices to connect up to four wired devices to the access point. The final item is the power connector.

Now on to the newer-style Linksys model. The front panel has some of the same lights shown in Figure 10.3, although some other lights have been added to help improve troubleshooting the device. Figure 10.5 shows the lights on the front of the access point.

Lights appearing from left to right in Figure 10.5 include:

- **Power light.** This light indicator informs the user that the access point is receiving power. This light also signifies that the device is able to start the boot-up process. It will stay on the entire time the unit is powered up to indicate operation. When the unit is undergoing its self-diagnosis testing during boot-up, this light will flash.
DMZ light. This light indicates the use of a DMZ device. If no device is using the DMZ capability, it will blink during its self-diagnosis testing, as the unit boots up; once completely up, the unit will stop lighting the DMZ light, unless a device is set up to use the DMZ.

Internet light. This light indicates that an Internet connection is made to the WAN port of the access point.

Wireless G light. This light indicates that there is a wireless connection. It will blink if wireless traffic is passing through the access point.

Port 1–4 lights. This light indicates that there is a layer two connection to a wired device on one of the four wired ports of the device. When one of the connected devices starts to communicate, the light will blink.

The back of the newer-style Linksys access point is shown in Figure 10.6. Going from left to right one can see that there is an Internet connection used to access other networks. Next is the four-wired network ports used to connect other wired devices to the network. The first button on the back is the reset button, which is used to reset the configuration to the factory default. The final item is the power connector.

Linksys access points use a Web interface to configure them. To access it, a user must type the IP address of the access point into an Internet browser such as Internet Explorer. When the user does this, he is prompted to enter a username and password. On Linksys access points, the default username is admin and the password is admin. Once the user has logged in to the device, a set-up screen appears like the one in Figure 10.7. This will allow the user to set up the access point. This screen allows a user to set up the WAN connection identifying the network information needed to access other networks. It will also allow a user to set up the LAN network information. This device can be a DHCP server, allowing dynamic network configuration information to be pushed out to connecting devices. This screen also allows for a number of advanced features, such as port forwarding, firewall filtering, and MAC-based security.
Cisco has had a stronghold on the enterprise wireless market since its acquisition of Aironet in 1999. Cisco has created multiple product offerings that fit a large array of needs. Once Aironet and Cisco became the same company, their product line began to move toward Cisco’s own code.

**Figure 10.7** Linksys management screen.

### 10.2 Cisco Access Points

Cisco has had a stronghold on the enterprise wireless market since its acquisition of Aironet in 1999. Cisco has created multiple product offerings that fit a large array of needs. Once Aironet and Cisco became the same company, their product line began to move toward Cisco’s own code.
Once this happened, the market began to see the major benefit that Cisco’s wireless access points bring to the table. They allow anyone familiar with Cisco router and switch configurations to understand access point configuration with ease. This was due to the fact that Cisco had integrated its IOS code with the Aironet access point, creating an access point that looked, felt, and operated like any other Cisco router or switch.

Cisco has three main models of access points: 350, 1200, and 1100 series. Each comes in a wide array of types that use different technologies. For example, the 1200 can use 802.11b, 802.11g, and 802.11a. This section looks at all three types of access points and details what connections they have, what protocols and standards they support, and how they operate.

### 10.2.1 Cisco Aironet 350 Series

The first access point is the older Cisco 350 series lineup. These devices are no longer available through Cisco Systems, although they are still very prevalent across many companies. Currently, the Cisco 350 devices are end of sale. However, they are still not end of life, which means that Cisco will support them. When these devices were sold, they came in a hardened model with a metal casing and in a plastic model that had the antennas affixed to the access point. Both 350 models only work with the 802.11b technology, and that technology only. Figure 10.8 shows the 350 series access point.

![Cisco 350 model](image)
Both of the 350 series access points have the same light and connector layout. The only difference between them is the hardened shell and the ability to affix external antennas to the hardened model. To note is that the plastic 350 series access points were available with the option of affixing external antennas, although this was quickly replaced by the hardened cases. Looking at the front of the 350 series access point, one can see in Figure 10.9 that there are three lights. Each of the functions of the lights is detailed below.

The lights going from top to bottom in Figure 10.9 are:

- **Ethernet activity light.** This light indicates the status of the Ethernet network connection. The indicator will blink green when a packet is received or transmitted over the Ethernet infrastructure. It will blink red when there is no connection to the Ethernet network.

- **Association status light.** The association status indicator light signals the operational status of the device. When the light is blinking green, it indicates that the access point is operating normally, although it is not connected to any wireless clients. When the light is steady green, it indicates that the access point is associated with at least one wireless client.

- **Radio activity light.** The radio indicator blinks green to indicate the presence of radio traffic activity. It is usually off unless there is traffic on the wireless, at which point it will blink green.

On the back of the 350 series access point is an RS-232 connection for terminal emulation and a single Ethernet port. On the hardened access point, there are two RP-TNC connectors that attach to external antennas. Figure 10.10 details the connections located on the back of the Cisco 350 series wireless access points.
The 350 series access point has no power plug for the unit. This is because the unit works off Power over Ethernet (POE). POE is a method by which power can travel down a network cable. This power is used to power a small device such as an access point or VoIP phone. To use the POE, one must have a switch that can provide POE. If no such switch is available that can support POE, one can use the small power converter that ships with the access point. This small power cord takes a Category 5 connection from the network and another Category 5 connection from the access point and provides power down the cable. One note about using power injectors is physical real estate. In larger companies, physical rack space is at a premium. Using a power injector means that a physical device like the one in Figure 10.11 needs to exist between the telecommunication closet and the access point. The most logical place to put this device would be inside this closet on a shelf. The physical real estate needed for this shelf and power injector is one of the most commonly missed items when planning for a Cisco wireless network.

Looking at Figure 10.11, one can see the power injector that comes with the Cisco 350 access point and one that comes with the 1200 series access point. They have a power connector that is used to connect external power to the injector and two Ethernet connectors (one for a connection...
to the network, which is not powered, and one connection to the access point, which is powered). The DC voltage used to power the access point is $-48$ VDC. There is a newly adopted POE standard called 802.3af. Some of the older access points are not considered 802.3af compliant. Cisco states that these devices will work correctly on its POE solutions, although to use another vendor’s 802.3af-compliant switch the access points must be 802.3af compliant. Today, all the access points shipping from Cisco are 802.3af compliant.

The operating systems on these units are unlike the familiar IOS that Cisco bases most of its products on. This was due to the acquisition of Aironet; along with acquiring the company, Cisco also acquired the access point code. This meant that the setup and management of the access point is different from most other Cisco devices. To fix that, Cisco needed to change the code into IOS. In late 2003, Cisco created a software code release that converted the old VxWorks operating system into IOS. Thus, in this subsection, the focus is on VxWorks for the 350 series only. This is because when we talk about the 1200 and 1100 series, it is obvious that they only use IOS (IOS is discussed later).

Connecting to the access point can be accomplished in a number of ways. First, to access it without any knowledge of its setup, one needs to access it though the console. This is the RS-232 connection on the back of the device shown in Figure 10.10. A serial DB-9 cable comes with the access point. It is blue and should have two ends that look alike. To note is that most Cisco equipment comes with what is called a rollover cable. This cable is used to access the equipment through the console port. The 350 series access points are one of the few Cisco devices that have a different cable for console management than the normal Cisco console cable. Once this cable is connected to both the access point and an open Com port on a workstation, a terminal emulator program must be open. One emulator that is part of Microsoft Windows is called hyper terminal. Other emulators can be downloaded from the internet or purchased. Make sure the terminal emulator program is correctly configured following the details below.

To connect a workstation correctly to an access point, the setup on a terminal emulator program needs to have the following settings:

- **Com Port**: set this to 1 or the com port to which the cable is connected
- **Bits per second (baud rate)**: 9600
- **Data bits**: 8 bits
- **Parity**: no parity
- **Stop bits**: 1 bit
- **Flow control**: Xon/Xoff
Once the cable is connected and the terminal emulator program is set up correctly, try to launch the session and connect the access point. At this point, one should see a cryptic-looking menu system similar to that in Figure 10.12. This is the VxWorks operating system. One can navigate by typing the first characters of a command into the window. The commands have brackets around them; some of them have different navigation keys than their names imply. Look out for what is typed in the brackets on the screen to make sure that the correct information is entered.

Figure 10.12  Cisco 350 VxWorks console screen.
Having learned how to connect to the Cisco 350 access point via the console, there are some other ways of setting up and managing this device. This device has a built-in Web interface like the one on the Linksys access points. To access it, one must know the IP address of the unit so one can enter that into a Web browser. By default, all Cisco access points get their address via DHCP. This makes finding the access point's IP address difficult the first time. Cisco stepped in and created a tool called IP setup utility (IPSU) that can find the access point's IP address from its MAC address. For this tool to work, it must be installed on a workstation that is on the same network segment as the access point. Once this software is installed, one can launch the application, type in the MAC address of the access point, and it will show the IP address. The MAC address of any Cisco access point is written on the back of the unit.

Now that the IP address is known, connecting to the access point is possible through the Web. To do so, just type in the http:// and the IP address of the access point. This will bring up the Web interface. For VxWorks, this method is the preferred method of configuration. One key advantage that Cisco has made for itself in the large enterprise space is the ability to create configuration scripts for almost all of its products. With VxWorks, still being an Aironet/Cisco code, this was not achieved. This meant that the ability to easily script the configuration in VxWorks was rather difficult. Looking at Figure 10.13, one can see what the Web interface looks like for the VxWorks operating system.

The final method of accessing the access point's management functions is through telnet. This has a very similar look and feel to the console although it can be done remotely from any connection with IP connectivity. In some newer versions of code, Secure Shell (SSH) can also be used. Telnet is prone to eavesdropping because its authentication takes place in cleartext. To telnet into an access point, all one needs is a telnet program. UNIX and Windows both have telnet ability right from a command line or shell. Most Cisco equipment can perform a telnet action from one device to another.

10.2.2 Cisco 1200 Series Access Point

Now to the Cisco 1200 series access points. These all come in a plenum-rated metal case; the case is shown in Figure 10.14. These access points have the latest and greatest features available from Cisco. They are capable of supporting 802.11b, 802.11g, and 802.11a simultaneously. To support 802.11a, a paddle card must be installed into the access point. This card is shown in Figure 10.15.

Delving deeper into the access point itself, one can see from Figure 10.14 that the access point has the same LED layout as the 350. Each
Ethernet activity, association status, and radioactivity light performs the same function as detailed above for the 350 series. Looking at the connections on the device in Figure 10.16, one can see that the 1200 access point has two antenna leads, a power connection, an RJ-45 console port, and an RJ-45 Ethernet access port. One big difference between the 350 and 1200 series is the more common use of the correct Cisco-style console cable. The 1200 access point has the same Cisco console cable that almost all other Cisco equipment has. Another big difference is the directly connected power port. This is now included in this model, unlike the 350, which required POE from a switch or injector. The 1200 series access point is capable of POE and can be plugged in with direct power from a power cord. This allows for maximum flexibility with regard to powering the device. Also, all currently shipping 1200 units from Cisco are 802.3af compliant.

The 1200 series access point was made with the capability to upgrade to new technologies. This was often a requirement of customers. They wanted the capability to support technologies that were close to being released, although not available at the current time. To make sure that
they did not have to replace all their wireless networks, most customers required that the access point have easy upgradeability, to include support for other, newer technology. In the case of the Cisco 1200 series access point, this change was as easy as swapping out one card for another. This allowed the device to go from 802.11b to 802.11g rather easily. When the 1200 first came out, 802.11g was still being standardized. This meant that Cisco had to release the 1200 with 802.11b technology. To upgrade to 802.11g, a new radio must be installed. Cisco wanted to make the transition from 802.11b to 802.11g an easy one and did so by making it easy to change out the radio cards. Looking at Figure 10.17, one can see how the radio comes out.

The 1200 series access point runs IOS. Most Cisco products run this operating system. It is laid out the same way as other Cisco devices. This means that anyone familiar with a Cisco router or IOS-based switch should be able to pick up the access point IOS without too many issues. This IOS still has the ability to allow connections from the console, telnet, Web browser, and SSH. One of the big differences in IOS versus VxWorks is the ability to script configurations. With IOS, text configurations are easily
put into and pull out of any 1200 IOS-based access point. This means that basic standards can be inserted into engineering templates and some assurance can be given that all access points will share these common settings.

Figure 10.18 reveals the IOS Web-based interface. It looks very different from the VxWorks. It has all the same functions of VxWorks, although it is
Figure 10.17  Cisco 1200 radio replacement.

Figure 10.18  Cisco 1200 IOS-based web access screen.
laid out a little neater. When using this configuration tool, one of the quickest ways to get the access point up and running is the express setup page.

When one consoles or telnets into an access point, one gets what is called a command line interface (CLI). This is very similar to a Cisco router. Once logged in, one is in user mode, which is a very restrictive mode and allows for only simple viewing commands. To get into the next privilege mode, called the EXEC mode, one must type “enable” into the command line. This should change the prompt from > to #. Now this mode can run all viewing commands. If one wants to make a change, one must enter another mode, called global configuration mode. This mode allows one to make changes. To get into global configuration mode, one types “configuration terminal” into the command prompt. One can make changes that apply to the entire device, including changing the device’s name, setting the clock, adding users, etc. The final menu type is called interface configuration mode. This menu allows one to perform actions on certain types of interfaces, such as the 802.11b radio, or a particular VLAN. To get to the interface configuration menu, one must already be in global configuration mode and then type “configure interface dot11radio0.” This gets you into the configuration menu for the 802.11b radio. Whatever designator is assigned to the interface one wants to configure is the one that must be referenced in the command. Figure 10.19 provides all the details and shows what the IOS command line looks like. Looking at this figure, one can see that one of Cisco’s features is support for the tab command. In most UNIX operating systems and Cisco IOS, the tab key can be used to complete a command. As one can see from Figure 10.19, to enter enable mode, all that is needed is “en.” This can also apply to other menu items such as global configuration mode; typing in “config t” can easily access this mode.

10.2.3 Cisco 1100 Series Access Point

The final wireless access point from Cisco discussed herein is the 1100 series. This access point was created for a low-cost, small office access point. It is only available in 802.11g or 802.11a. Unlike the 1200 series, it cannot run two radios at once. Older 1100 access points ran 802.11b standard. To upgrade from 802.11b to 802.11g, one only needs a small radio chip. This makes the 1100 a modular upgradeable radio. Both the 1200 and 1100 series access points only need a single screw to get to each of their radio cards. The 1100 series access points do not support external antennas, unlike the 1200 series, which does support external antennas. The 1100 has a 2.2-dBi omni antenna permanently affixed to the unit. This makes the unit difficult to use in places where external
antennas would be needed. If one needs an access point that requires external antennas, go with the 1200 series. If the solution is for a small office, then the 1100 series is a more cost-effective option. The 1100 series access point is capable of being powered by POE. Looking at Figure 10.20, one can see that the 1100 series access point looks similar to the 1200, although it is slightly smaller and has affixed antennas.

Other than the many physical differences between the 1100 and 1200 series access points, from software perspective the two are very similar. Both run IOS and operate under the general command structure. This makes an 1100 and a 1200 look almost the same from a remote console perspective. This also helps with large companies that manage both 1200 and 1100 series access points. They both look and feel the same from a software configuration standpoint.
10.3 Chapter 10 Review Questions

1. What is the correct DC voltage used to power a Cisco 1200 series access point when using POE?
   a. −23
   b. −34
   c. −99
   d. −48

2. The cable used to connect to a Cisco 1200 series access point is commonly referred to as a ____________.
   a. Patch cable
   b. Coaxial
   c. Roll down
   d. Roll over