GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

“Securing the Cisco Aironet 1200 Access Point”

Written By
Jeffrey Turner
October 8th, 2004

© SANS Institute 2004, Author retains full rights.

GSEC Practical Assignment v. 1.4c

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of contents

Abstract 4
Access Point Overview 4
1.0 Network Setup 4
1.1 Address Assignment 4
1.2 Access Point Placement 5
1.3 Web Interface 6
2.0 Home Page 6
3.0 Express Setup 7
- 3.1 Access Point Name 7
- 3.2 Configuration Sever Protocol 7
- 3.3 SNMP Community 7
- 3.4 SSID 8
- 3.5 Role in Radio Network 9
- 3.6 Optimize Radio Network 9
- 3.7 Aironet Extensions 9

4.0 Network Map 9
5.0 Association 9
6.0 Network interfaces 10
- 6.1 IP Address 10
- 6.2 FastEthernet 10
- 6.3 Radio-802.11G 10
  - 6.3.1 Detailed Status 10
  - 6.3.2 Settings 10

7.0 Security 15
- 7.1 Admin Access 15
- 7.2 SSID Manager 16
  - 7.2.1 Authentication Settings 17
  - 7.2.2 Authenticated Key Management 20
  - 7.2.3 Accounting Settings 20
  - 7.2.4 General Settings 21
  - 7.2.5 SSID Properties 21
- 7.3 Encryption Manager 21
  - 7.3.1 Encryption Mode 21
  - 7.3.2 Encryption Keys 21
  - 7.3.3 Global Properties 22
- 7.4 Server Manager 22
- 7.5 Local RADIUS Server 23
- 7.6 Advanced Security 23

8.0 Services 23
- 8.1 Telnet/SSH 23
- 8.2 Hot Standby 24
- 8.3 CDP 24
- 8.4 DNS 24

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8.5 Filters 24
8.6 HTTP 24
8.7 Proxy Mobile IP 24
8.8 QoS 24
8.9 SNMP 25
8.10 NTP 25
8.11 VLAN 25
8.12 ARP Caching 25
9.0 Wireless Services 25
10.0 System Software 26
10.1 Software Upgrade 26
10.2 System Configuration 26
11.0 Event Log 26
Conclusion 27
References 27

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

Wireless is becoming a very important part of the corporate structure. Wireless technology has improved dramatically and only promises to get better. The increase in productivity and social acceptance of wireless are two reasons why corporate environments are embracing wireless technology. In a study released by Cisco, "the study queried end-users and IT network administrators from more than 400 medium and large organizations in the United States using wireless LANs. Most notably, end-users in the study reported that using WLANs increased their productivity by as much as 27 percent, largely because they have the ability to stay connected to the network on average 3.75 hours more hours per day."[1]

One of Cisco's wireless products currently being in corporate environments is the Cisco Aironet 1200 Access Point. The purpose of this paper is to explain how to implement a Cisco Aironet 1200 Access Point within an organization. The focus of this paper outlines the various configuration options of the access point (AP) and wireless security best practices to achieve a defense-in-depth solution.

Access Point Overview

The Cisco Aironet 1200 access point supports the IEEE 802.11b, 802.11a and 802.11g specifications. The 802.11b/g model does not include antennas and must be purchased separately. The Cisco 1200 access point contains many security features and can be configured by using a web browser, Telnet, Secure Shell (SSH) or Simple Network Management Protocol (SNMP). This paper will detail configuring the AP using the web interface option.

1.0 Network Setup

1.1 IP Address Assignment

Configuring the AP using a web browser requires the device to have an IP address. The IP address can be assigned manually or via Dynamic Host Configuration Protocol (DHCP). Configuring the AP with a static IP address will prevent having to determine the IP address every time a change is needed or auditing performed.

[1] Moskowitz, Robert. WLAN Testing Reports "Debunking the Myth of SSID Hiding." URL: http://www.icsalabs.com/html/communities/WLAN/wp_ssid_hiding.pdf (12 Aug 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.2 Access Point Placement

Often, access points are added to the wired network using the default settings. Information sent across the wireless connection is usually not deemed important or sensitive. However, security should be the principal part of any wireless installation. The location of the access point should not put the wired network at risk. For added security, place the access point in a Demilitarized Zone (DMZ) used specifically for wireless devices and setup appropriate filters so all connections pass through the firewall.

Users requiring access to resources on the wired network should use a virtual private network (VPN) using (Internet Protocol Security) IPsec. The VPN gives users a secure encrypted session to the wired network. When utilizing a VPN, make sure that all traffic goes through the encrypted VPN connection. Do not allow split tunneling with VPN clients. Split tunneling allows access to both the local network and internet access. If an attacker were to compromise the wireless client, the entire network could be in jeopardy. Disabling split tunneling will help protect the wired network in case the access point or wireless client gets compromised. **Figure 1** is an example of the AP placement.

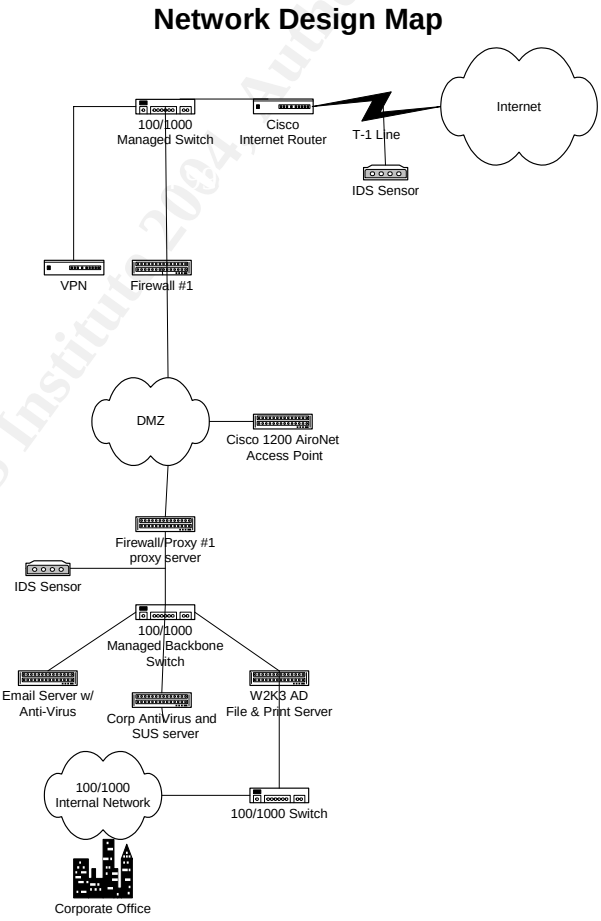


Figure 1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.3 Web Interface

Once the access point has an IP address, open a web browser and type the IP address. A pop-up box will appear asking for a user name and password. The default username and password is **Cisco** and the password is case-sensitive. The access point summary status page should appear. **Figure2** shows an example of the summary page is shown.

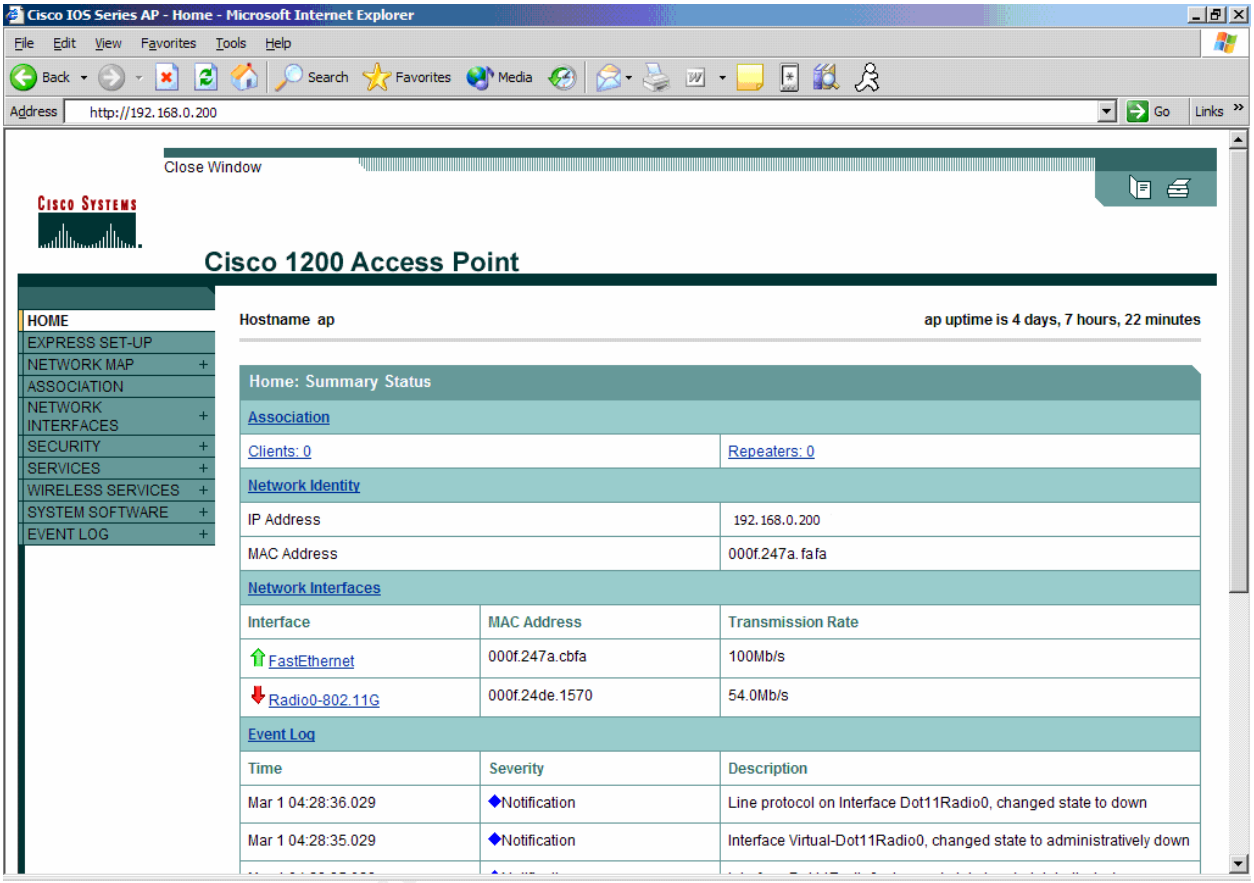


Figure 2

2.0 Home Page

The summary page provides status information of the access point. Information such as device uptime, number of clients currently connected and whether the Ethernet and wireless interfaces are active is displayed. One of the most important parts of the summary page is the event log. The event log details various events taking place on the AP and should be viewed by the network or system administrator as part of their auditing routine. The left side of the summary page contains links to additional configuration settings.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Other items on the summary page are hyperlinks to other information and configuration options. After the AP is configured; the hyperlinks are very useful for viewing statistics or modifying IP address information. The hyperlinks provided on the summary page are:

- Association
- Clients
- Repeaters
- Network Interfaces
- Event Log

3.0 Express Setup

The express setup page contains basic configuration settings for the AP. On this page, the AP name, Service Set Identifier (SSID), IP Address settings, and Simple Network Management Protocol (SNMP) settings can be configured.

3.1 Access Point Name

The default name of the access point is **AP** but the name is usually changed to describe the physical location of the access point.

3.2 Configuration Server Protocol

As stated earlier, you can configure the AP with either a static IP address or have one assigned by a DHCP server. If the AP will be assigned static IP address, the subnet mask and default gateway need to be filled in as well. If the IP address is assigned by a DHCP server, the IP address of the AP can be determined by using the Cisco IP Setup utility or by looking in the database of leased IP addresses on the DHCP server.

3.3 SNMP Community

SNMP allows the AP to be remotely configured and managed using various SNMP management software products. The SNMP community name is essentially a password needed to view or configure the AP from a remote location. The default community name of the AP is **defaultCommunity** with read only access. AP settings can be modified via SNMP by simply changing the SNMP setting to read-write and using a SNMP management software program. The SNMP name should be changed from the default setting. When changing the SNMP name, do not rename it to public, admin, private or leave it blank.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

SNMP can be a useful tool for remote management. However, SNMP has some serious flaws that can put a network at risk of being compromised. The CERT Coordination Center has an advisory explaining the flaws in greater detail, refer to the following web site,

http://www.cert.org/advisories/CA-2002-03.html#vendors

3.4 SSID

All wireless clients are required to know the SSID when connecting to the AP. The default SSID for the Cisco AP is **tsunami;** however, this should be changed from the default setting. The SSID field allows up to 32 alphanumeric characters and is case sensitive. Utilizing capital letters and symbols will make guessing the SSID is more difficult but tools such as NetStumbler and Windows XP will detect any SSID broadcasts. In addition, the SSID should not form a word that can be found in the dictionary. An example of a suitable SSID name is *TAPwco83!04*. The SSID example is actually short for the phrase "This AP was configured on 83104." The only invalid characters when creating the SSID are *?*, ", $, [, \,], and +. In addition,!, #, and ; cannot be the first character of the SSID. The SSID should be changed periodically to help prevent a potential compromise of the wireless network.

SSID broadcasting is disabled by default. Broadcasting the SSID makes it easier to associate with an AP but also makes it easier for unauthorized connections to be established. Disabling the SSID broadcast will make it more difficult for anyone to associate with the AP. However, there are also tools that will detect hidden wireless networks as well. One program, Kismet, detects hidden wireless networks by simply collecting wireless traffic.

Even with the SSID disabled, the SSID is transmitted with every packet across the wireless network in clear text. If an attacker wanted to determine the SSID, wireless sniffers such as AirSnort or AiroPeek could be used to sniff wireless network traffic and determine the SSID. According to Cisco's documentation "The SSID is not designed, nor intended for use, as a security mechanism. In addition, disabling SSID broadcasts might have adverse effects on Wi-Fi interoperability for mixed-client deployments. Therefore, Cisco does not recommend using the SSID as a mode of security."[2]

[2] "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite." URL: http://cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml (12 Aug 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.5 Role in Radio Network

The Cisco AP can be configured as an AP or a repeater. Configuring the device as a repeater essentially extends an existing wireless signal a longer distance. An alternate method to achieving a longer or stronger wireless signal may be to utilize the various directional antennas available.

3.6 Optimize Radio Network

The wireless signal can be adjusted for either throughput or distance. The wireless signal can also be adjusted so it is only available within a certain radius, such as, a department, conference room or individual office. From a security standpoint, restricting the wireless signal within a certain radius helps control who connects to it.

3.7 Aironet Extensions

If all of the AP's and clients on the wireless network are Cisco products, you can enable this feature and take advantage of roaming from one AP to another without having to manually re-associate to an AP. The power level settings of clients connecting to the AP can also be controlled.

4.0 Network Map

Using the network map feature, information about what devices are connected to the wireless network can be seen. This feature is disabled by default but can be very useful if a good snapshot of devices on the wireless network is needed. One drawback to enabling this feature is the additional load on the AP during the network discovery process.

There is also an option to find out where adjacent AP's are on the wireless network. This is useful when multiple AP's are spread across the WLAN and information about them is needed. Information displayed about adjacent AP's are the SSID, channel, MAC address, whether the AP is using 802.11b, 802.11a or 802.11g. This tool is also useful for finding rogue access points existing on the network.

5.0 Association

The association page provides information of all wireless clients currently associated with the AP. Any AP's configured as repeaters will be shown here as well. To manage the wireless network properly, this page should be reviewed on a regular basis as part of the normal auditing routine.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.0 Network Interfaces

The network interface summary page displays status and other information pertaining to the Ethernet and wireless interfaces of the access point. The summary page also has hyperlinks displaying additional statistics for both interfaces.

6.1 IP Address

This is where the AP is configured to use a static IP address or DHCP. If using DHCP and the server doesn't use a client identifier, select the *"Disable DHCP Address Binding"* option. The client identifier is used by the DHCP server to issue consistent IP Addresses. [3]

6.2 FastEthernet

This screen displays various statistics on the Ethernet interface. The health of the Ethernet interface and possible issues occurring on the interface can be seen here. The settings tab allows the Ethernet interface to be disabled and duplex mode options set.

6.3 Radio-802.11G

The network interface summary for the wireless interface displays basic statistics and information. Additional information and configuration details specific to the wireless interface can be seen by selecting the additional tabs – *Detailed Status, Settings and Carrier Busy Test*.

6.3.1 Detailed Status

To gather specific information related to the wireless interface, select the "*Detailed Status"* tab. The firmware version and serial number of the wireless interface are also displayed on this page. When implementing a WLAN or adding additional AP's, viewing the information in this area will help determine if the wireless network is operating at peak efficiency.

6.3.2 Settings

The wireless interface can be configured in a multitude of ways. Everything from disabling the radio to configuring the AP to only use specific channels can be done on this tab. Options available within this tab are:

---

[3] "Online Help for Cisco IOS Release 12.2(15)JA." URL: http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/122-15.JA/1400br/h_ap_network-if_ipaddress.htm (13 Sept 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Enable Radio
Turning the wireless radio signal on or off is as simple as enabling or disabling this option. Using this option, instead of unplugging the access point at night, use this setting to disable the wireless signal. It is easier to turn on and the access point settings will not be lost. The default setting is enabled.

Current Status
The software and hardware status for the wireless interface is shown by either two green arrows pointing up or two red arrows pointing down. Disabling the radio signal causes the status to display two red arrows point down.

Role in Radio Network
If the Ethernet connection is ever lost, the AP can continue operating as a normal access point, a repeater or shut down the wireless signal. The default setting is to continue acting as a normal access point.

Data Rates
The AP can be configured to maximize the range or throughput of the wireless signal. The configuration also allows a custom setup between throughput and range. The AP data rates can also be set back their default settings by selecting the *Set to Default* button.

CCK Transmitter Power
The complementary code keying (CCK) modulation is used to reach the lower data rates between 5.5Mbps and 11Mbps. If clients are having problems while connected between these rates, there may be wireless interference taking place. Lowering the power can reduce or eliminate the interference. The default setting is maximum power.

OFDM Transmitter Power
The orthogonal frequency division multiplexing (OFDM) modulation is used to reach the higher data rates up to 54Mbps. If clients are having problems while connected at these rates, there may be interference taking place. Lowering the power can reduce or eliminate the interference. The default setting is maximum power.

Limit Client Power
The AP can control the power level wireless clients can use. If you are using special antennas with the Cisco AP, you may need to adjust these settings. If the access point is using special antennas to extend the signal range, these settings may need to be adjusted if they are out of the allowed FCC range. The default setting is maximum power.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Default Radio Channel
Some wireless channels are used more than others so the AP can be configured to a specific channel. The default setting is Least Congested Frequency so the access point will automatically determine which channel is best.

Least Congested Channel Search
The Default Radio Channel uses the channels highlighted on the list when searching for the best channel. If there is a channel that should not be used, the channel(s) should be omitted from the search. The default setting has all eleven channels selected.

World Mode Multi-Domain Operation
This option allows power level and frequency configuration settings to be broadcast on the wireless network. This setting should remain disabled to prevent this configuration information from being broadcast to potential attackers.

Radio Preamble
Under most circumstances there is no need to change this setting from short to long. A short radio preamble will increase the performance of all wireless devices that support it. Any devices using a long preamble should be replaced or performance will suffer.

Transmit and Receive Antenna
Most AP's will have two antennas – one responsible for transmitting the wireless signal and another for receiving the wireless signal. The Cisco AP can also be configured so that the antennas are configured as diversity antennas. Diversity antennas enable wireless clients to use the antenna with the best signal, depending on the physical location of the client. According to the International Engineering Consortium, "diversity antennas improve the overall reception." [4] The default setting is diversity. The AP can also use a directional antenna to allow more control over the wireless signal direction.

Ethernet Encapsulation Transform
The two options available under this section is RFC1042 or 802.1H. According to the RFC1042 specification, "IP datagrams and ARP requests and replies are transmitted in standard 802.2 LLC Type 1 Unnumbered Information format." [5] As a result, RFC1042 is used by most major wireless vendors to encapsulate IP data. 802.1H can be used only if Cisco devices

[4]. "Smart Antenna Systems." International Engineering Consortium URL: http://www.iec.org/online/tutorials/smart_ant/topic02.html (13 Sept 2004)
[5] "A Standard for the Transmission of IP Datagrams over IEEE 802 Networks." Network Working Group Request for Comments: 1042. February 1988. URL: http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc1042.html (13 Sept 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

are being used. The default setting of RFC1042 should be sufficient for most implementations.

Reliable Multicast to WGB
If the WLAN contains Cisco wireless bridges (perhaps connecting two buildings), enabling this option will ensure that any multicast packets are sent to the bridges. Enabling this option will adversely affect the number of clients that connect to the AP.

Public Secure Packet Forwarding
Keeping this setting disabled prevents wireless clients from communicating to each other. Having this option enabled allows anyone using the wireless connection to setup FTP servers or peer-to-peer networks. These connections would drastically reduce the wireless bandwidth or cause the AP to crash.

Short Slot-Time
This setting is supposed to increase 802.11g the throughput from 24 megabits per second (Mbps) to 54Mbps. However, all the devices associated to the AP have to support the short slot time setting or the maximum throughput will only be 24Mbps not 54Mbps." Disabling short slot time causes all the devices to have a maximum throughput of only 24Mbps.

Beacon Period
The beacon period is the pulse of the AP. The default setting is 100 which means every 100 Kilomicroseconds (Kusec), the AP sends out a pulse (packet) to the other wireless clients.

Data Beacon Rate (DTIM)
DTIM is short for Delivery Traffic Indication Message. This message is the "pulse" sent by the AP at set intervals to clients associated to the AP. The default setting is 2 Kusec. If the Beacon Period and DTIM are left at their default settings, a pulse is sent to wireless clients associated to the AP every 200 Kusecs informing them that a packet is coming.

Max. Data Retries
The AP uses this to determine how many times it should try delivering data packets to a wireless client. The default setting is 64 times. Some other AP's may set this at 32 to reduce traffic. Too many data retries on the WLAN may indicate a performance issue.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

RTS Max Retries
"As an optional feature, the 802.11 standard includes the RTS/CTS (Request to Send/Clear to Send) function to control station access to the medium." [6] Utilizing this feature, the AP and client check with each other to see if it is OK to send the packet. This results in fewer collisions.

This setting specifies the maximum attempts the AP will try to send a request to send (RTS) packet to a client. If the RTS threshold is set to 2347, the setting will not be used. The default is to retry the RTS packet 64 times.

Fragmentation Threshold
The fragmentation threshold works in conjunction with the RTS settings. Usually, this setting is only lowered if there are a high number of retransmissions taking place and adjusting the RTS settings doesn't help.

RTS Threshold
To optimize the performance of the WLAN, this setting can be used to minimize collisions from occurring between the wireless client and AP. The default threshold setting is 2312. To disable the RTS threshold, change the setting to 2347. If the AP is experiencing a high number of retransmissions (as indicated under the Detailed Status tab), adjusting this value will help lower the retransmissions occurring between the wireless clients and AP. Just make sure the network throughput does not suffer. If the performance drops after adjusting this setting, disable the RTS threshold (change the number to 2347) and try using a different channel on the access point.

Repeater Parent AP Timeout
This is used only if an AP is configured as a repeater. The default setting is 0 (disabled). If the AP is a repeater, this setting will have the repeater attempt to locate the associated AP until that time expires.

Repeater Parent AP MAC
If the wireless network has AP's configured as repeaters, this option allows the MAC addresses of up to four repeaters to be assigned to the AP. If any of the four repeaters loses communication with the AP, the repeater(s) will attempt to locate the AP for a specified number of seconds. The number of seconds is determined by the *Repeater Parent AP Timeout* option.

[6] Geier, Jim. "Improving WLAN Performance with RTS/CTS." Wi-Fi Planet. 13 August 2002. URL: http://www.wi-fiplanet.com/tutorials/article.php/1445641 (16 Sept 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.0 Security

This section is the heart of how secure (or insecure) the AP is configured. The security summary page displays what security features are enabled on the AP. The page displays the AP administrators, their rights, the SSID, Encryption settings, and if any authentication servers are used by the AP. Similar to other summary pages, each of these features include hyperlinks so an administrator can view and modify the security settings. An example of the summary page is shown in **Figure 3**.

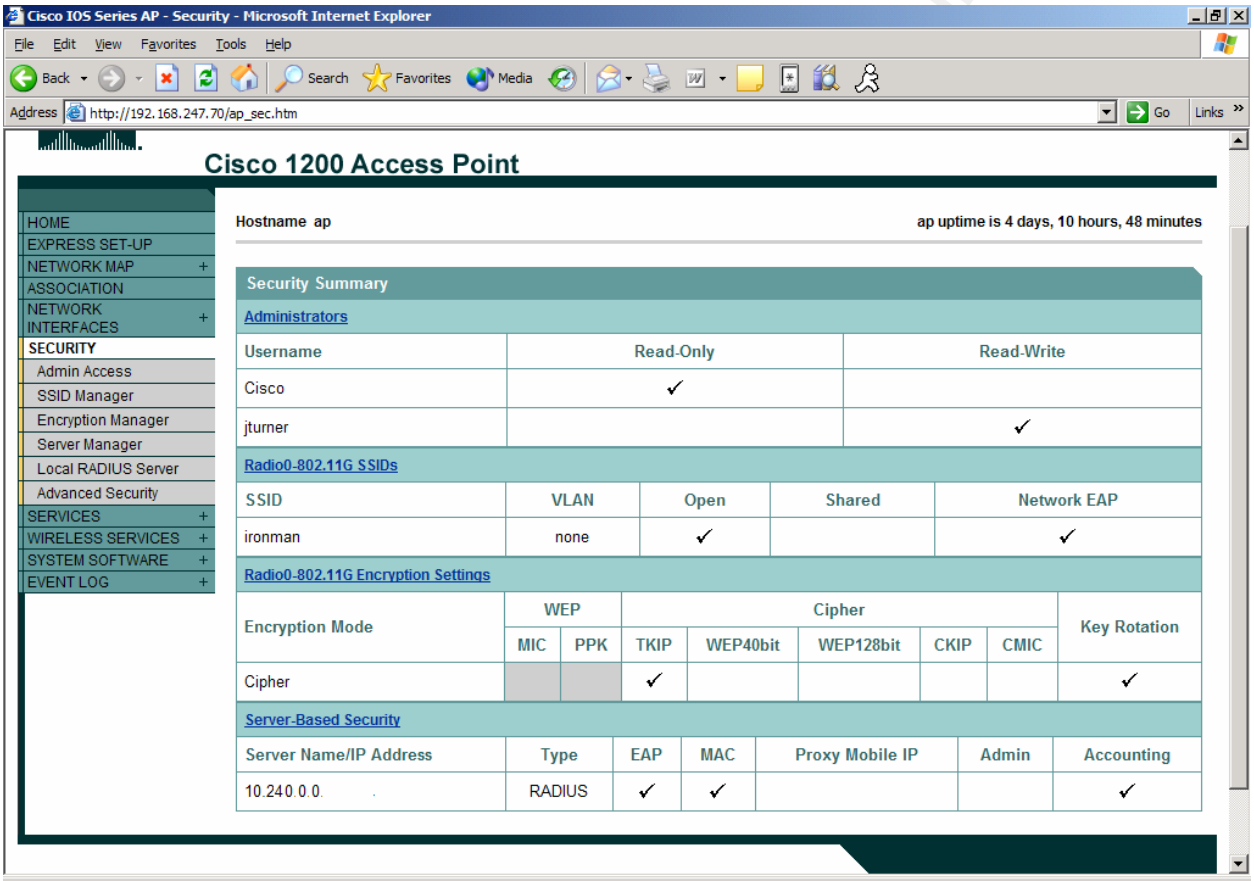


Figure 3

7.1 Admin Access

The AP offers four ways to authenticate an administrator. All four options can be configured but only one method is used. The four options are:

Default Authentication – an authentication password is set and only the password will be used for authentication. Think of this as a secret code word. It doesn't matter what username you enter when asked for the logon credentials, the AP only verifies the password is correct.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Local Users List – The AP stores a list of usernames and passwords local on the AP. The list can contain users with read-only or read-write access.

Authentication Server Only – Users attempting to administer the AP need to be authenticated by some type of authentication server before access is allowed. During authentication, the access point passes the credentials over to the authentication server to verify access. An example of an authentication server is a Remote Authentication Dial-In User Service (RADIUS) server.

Authentication Server if not found in Local List – This option uses an authentication server as the primary method of verification. If the authentication server is not accessible, the local user list is used to verify administrator access to the AP.

The most secure method is Authentication Server Only. If the authentication method is not Authentication Server Only, make sure to create strong passwords and change them often. A good password should be at least 12 characters in length, contain special characters, numbers, upper and lower case letters. The password should not form a word that can be found in the dictionary. Attackers often use words found in the dictionary to guess passwords. When forming a password, consider using a phrase that can be remembered and use the letters contained in the phrase to create the password. Refer to the "SSID" section listed earlier in the document for an example.

7.2 SSID Manager

The access point allows a default and a guest SSID. Both the default and guest SSID for the AP is ***tsunami.*** The SSID should be something other than the default setting. Attackers often obtain access to the WLAN because the access point is left with the default settings. If the AP was configured using Express Setup, the SSID will be listed on this page.

As mentioned earlier, the SSID field allows up to 32 alphanumeric characters and is case sensitive. It is important to create a SSID that is not easily guessed. Utilizing capital letters and symbols will make guessing the SSID more difficult. For more information on how to name the SSID, refer to the SSID section under **Express Setup**, listed earlier in this paper.

The SSID Manager page also contains authentication settings that can be configured to secure both the AP and WLAN. If the wired network has a switch that supports a Virtual Local Area Network (VLAN), a VLAN can be setup to create a VLAN segment for the wireless network. Utilizing these settings, adds

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

multiple layers of security helping to provide a defense-in-depth solution for the AP and any wireless clients associating to it.

7.2.1 Authentication Settings

Three methods of authorization allow a wireless client to associate with the AP. The AP can be configured to use Open Authentication, Shared Authentication or Network EAP. If none of these authentication settings are selected, any wireless client having the correct SSID can connect to the AP and access the wireless network. It is highly recommended that at least one of the authentication settings is enabled.

Open Authentication

Using open authentication, any wireless client can associate with the AP. Before wireless clients can send data on the wireless network, they have to know the Wired Equivalent Privacy (WEP) key so data can be encrypted and sent over the wireless network. WEP uses both a shared secret and the RC4 algorithm to encrypt the data. Each wireless client connecting to the AP has to know the shared secret or access will not be allowed to the WLAN. The shared secret is manually configured on each wireless client.

WEP uses the physical and data link layers of the OSI model to secure wireless transmissions. WEP has been proven to be an insecure encryption protocol. Software tools such as WEPWedgie and WEPAttack crack the 802.11 WEP encryption keys by exploiting a weakness in the RC4 key. By simply collecting and analyzing packets of encrypted traffic, the secret key can be obtained. If using the right tools, cracking the WEP key only takes a couple of hours. Changing the WEP keys regularly can add an additional layer of security to the WLAN.

The AP can also be configured to use open authentication with MAC authentication, Extensible Authentication Protocol (EAP) or both. MAC authentication (MAC filtering) only allows the node addresses contained on an approved list to access the wireless network. So if a wireless client knows the shared secret and the wireless client's node address is in the approved list of MAC addresses, the wireless client can send and receive encrypted data across the WLAN. Unfortunately, the MAC address is sent in clear text. This means that a potential attacker could use a packet analyzer such as Ethereal or WLANDump to find a MAC address and use tools like SirMACsAlot, SMAC, NetStumbler and even Windows XP to spoof (imitate) a MAC address. Using the spoofed MAC address, the attacker has access to the wireless network.

EAP authentication requires an authentication server such as RADIUS or Cisco's TACACS+ server. EAP authentication is the most secure type of authentication and multiple types of EAP are available. The current EAP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

authentication types are EAP-MD5, EAP-TLS, EAP-SIM, EAP-LEAP, EAP-PEAP, EAP-FAST and EAP-TTLS. The most secure of the EAP types are EAP-PEAP and EAP-TTLS. Both provide the strongest security because they rely on mutual authentication between the AP and the wireless client. PEAP is the easiest of the two to implement because it comes standard with Windows 2000 and Windows XP. EAP-TTLS requires a 3rd party client to be installed on each wireless client.

When using open authentication, use it in conjunction with MAC and EAP authentication. This option is currently the most secure solution. If there is a choice to configure the AP with no authentication or open authentication, go with open authentication. Using encryption that is insecure is better than no encryption at all.

Shared Authentication

Shared authentication also uses WEP to encrypt data across the wireless network. However with shared authentication, the wireless client asks to be associated to the AP instead of being associated with the AP and having to supply the correct key. Once the client asks for permission, the AP responds by sending a random challenge message back to the client. The challenge is for the client to prove it has the correct key. The wireless client sends a response back to the AP in encrypted form using the shared key. The AP verifies the response and if the key was not correct, the client is not associated to the access point. The problem with the entire verification process is the challenge message is sent in clear text. If an attacker wanted to access the wireless network, the dialog between the wireless client and the AP could be monitored. Once the attacker sees the challenge message in clear-text and what the message looks like in encrypted form, two of the three pieces of the RC4 algorithm are known. Using the right software, the attacker figures out the WEP key.

The AP can also be configured to use shared authentication and MAC authentication, shared authentication and Extensible Authentication Protocol (EAP) or both. Shared authentication is not as secure as open authentication. It is recommended that open authentication with EAP and MAC authentication be used instead of shared authentication, because shared authentication is easier to crack.

Network EAP

Network EAP uses Cisco's Lightweight Extensible Authentication Protocol (LEAP) and requires a RADIUS server that supports the LEAP authentication protocol. Using LEAP is more secure than using open and shared authentication. However, LEAP has a flaw that allows an attacker to launch a dictionary attack to guess passwords. Tools such as Asleap, exploit the weakness of the LEAP protocol. In August 2004, Cisco released EAP-FAST to use as another option instead of LEAP.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The AP can also be configured to use network-EAP and MAC authentication. Using network-EAP is more secure than open or shared authentication. However, there are other EAP types like PEAP and TTLS that are more secure. Below is a table provided by Cisco (**Figure 4**) showing the common EAP types. [7]

	EAP-FAST	**Cisco LEAP**	**PEAP with Generic Token Card (GTC)**	**PEAP with Microsoft Challenge Authentication Protocol (MS-CHAP) v.2**	**EAP-TLS**
User authentication database and server	NT domains, Active Directory, LDAP (limited)	NT domains, Active Directory	OTP, LDAP, Network domain server (NDS), NT domains, Active Directory	NT domains, Active Directory	OTP, LDAP, NDS, NT domains, Active Directory
Operating system support	Driver: • Windows XP • Windows 2000 • Windows CE With third-party utility: • Other OS[1]	Driver: • Windows 98 • Windows 2000 • Windows NT • Windows Me • Windows XP • Mac OS • Linux • Windows CE • DOS	Driver: • Windows XP • Windows 2000 • Windows CE With third-party utility: • Other OS	Driver: • Windows XP • Windows 2000 • Windows CE With third-party utility: • Other OS	Driver: • Windows XP • Windows 2000 • Windows CE With third-party utility: • Other OS
Credentials used	Windows password, LDAP user ID/password (manual provisioning required for PAC provisioning)	Windows password[2]	Client: • Windows • NDS • LDAP password; OTP or token Server: • Digital certificate	Windows password	Digital certificate
Single sign on using Windows log-in	Yes	Yes	No	Yes	No

[7] "EAP-FAST" URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml (23 Sept 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Password expiration and change	Yes	No	No	Yes	-
Works with fast secure roaming	Yes	Yes	No	No	No
Works with WPA	Yes	Yes	Yes	Yes	Yes

[1] OS = Operating system

[2] Requires strong passwords. Read more at: Cisco Response to Dictionary Attacks on Cisco LEAP

Figure 4

7.2.2 Authenticated Key Management

The AP can be configured to use Cisco Centralized Key management (CCKM) or Wi-Fi Protected Access (WPA) to manage keys. The configuration allows both methods to be used or just one. Key management is not mandatory.

CCKM is a proprietary key management solution that only works with Cisco devices. Using CCKM, a wireless client can roam from one AP to another and automatically associate with other AP's. CCKM uses network-EAP, which is also vulnerable to dictionary attacks.

WPA is a new interim security method that uses 802.1X specification for authentication and Temporary Key Integrity Protocol (TKIP) for encryption. 802.1X uses one of the EAP types and a form of network authentication such as a RADIUS server or pre-shared key.

TKIP is the replacement for WEP and is more secure because it uses rotating keys when encrypting data on the WLAN. Currently, there are no tools available to expose any TKIP weaknesses. WPA can also use Advanced Encryption Standard (AES) and is included with the new 802.11i standard. AES allows a key size of up to 256-bit and will replace TKIP as the encryption method used for encrypting data-
WPA can also use an ASCII or Hexadecimal pre-shared key to authenticate wireless clients. If using a pre-shared, either CCKP, WPA or both have to be enabled. As with WEP, the pre-shared key should be changed periodically.

7.2.3 Accounting Settings

Accounting allows the authentication server to log information regarding any client attempting to associate to the AP. The log is stored on the authentication server and should be viewed periodically to address any issues.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

7.2.4 General Settings

The EAP client option is used by AP's configured as repeaters and is used to associate with an AP using network EAP. If the wireless network doesn't contain any AP's configured as repeaters, this setting should not be used.

7.2.5 SSID Properties

The SSID properties allows a default SSID to be set for regular wireless clients accessing network resources and a guest mode SSID for visitors who need to connect to the WLAN. The default setting does not have a guest SSID selected. If a guest SSID is created, it should follow the same guidelines mentioned in the ***Express Setup*** section of this paper. The option to force infrastructure clients should also be checked. This prevents wireless clients who are supposed to be using the default SSID from using the guest mode SSID.

7.3 Encryption Manager

The encryption manager page allows the AP to be configured for various encryption modes and keys.

7.3.1 Encryption Modes

The three encryption modes supported by the AP are no encryption, WEP encryption and cipher. Cipher mode can use WEP 128-bit, WEP 40-bit, TKIP, CKIP, CMIC, CKIP+CMIC, TKIP+WEP 128-bit, or TKIP+WEP 40-bit. In addition, the AP can be configured so that it is mandatory for all wireless clients to connect using WEP. If enabling WEP encryption, using Message Integrity Checking (MIC) and Per Packet Keying to increase security. Enabling MIC prevents the packets from being altered. Per Packet Keying rotates keys at an interval determined by the Broadcast Key Rotation Interval option. TKIP encryption is much more secure than WEP encryption. When configuring the AP, using TKIP will make it the most secure.

7.3.2 Encryption Keys

This option has four encryption keys that can be created to use with WEP encryption. The encryption keys have to be typed in hexadecimal form and can have a key size of either 40-bit or 128-bit. Using a 128-bit WEP key is more secure than a 40-bit WEP key. As mentioned earlier, WEP is insecure and shouldn't be used if TKIP can be used instead. The only reason WEP should be configured on an AP is to support older wireless

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

clients who are not capable of utilizing TKIP. If at all possible, have all wireless clients use TKIP.

7.3.3 Global Properties

Under the global properties option, the AP can be configured to set a Broadcast Key Rotation Interval and WPA Group Key Update. The default setting for the Broadcast Key Rotation Interval is every 900 seconds (every 15 minutes). This setting should be sufficient in most cases.

The default settings on the WPA Group Key Update option enables group key on membership termination and on member's capability change. This means that WPA clients receive a new key every time a WPA wireless client or WEP client disconnects from the AP. Using WPA group key update will add adds another security layer to the access point.

7.4 Server Manager

The server manager page allows the AP to be configured with a RADIUS or TACACS+ authentication server.

Backup RADIUS server

The AP can also be configured with a backup RADIUS server by putting in the name or IP address of the backup RADIUS server and the shared secret. The shared secret is needed by the AP so the RADIUS server knows the AP is appoved to access the RADIUS server for user authentication. If the shared secret on the RADIUS server is different than the shared secret on the AP, no association can be made to the AP by the wireless client.

Corporate Servers

The AP is configured with the name or IP address of either RADIUS or TACACS+ servers used for authentication. Only one type of authentication server can be selected. If the RADIUS or TACACS+ server listens on a different port other than the default, enter the authentication and accounting port the server is listening on. Many RADIUS servers use UDP port 1645 or 1812 for authentication and UDP port 1646 or 1813 for accounting. The default ports for a TACACS+ server is TCP port 49. Depending on the type of RADIUS server you have, these ports may be different. If the AP is in a DMZ, a filter exception is needed on the firewall so the AP to contact the authentication server using the necessary port.

Default Server Priorities

For extra protection, up to three server names or IP addresses can be assigned to each of the following:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- EAP Authentication Server
- MAC Authentication Server
- Accounting Server
- Admin Authentication (RADIUS)
- Admin Authentication (TACACS+)
- Proxy Mobile Authentication

Global Properties
Server Manager has another page that is used for specifying various values for authentication servers. This page is optional but does contain some settings that could possibly be used depending on the authentication server, but in most cases will not be used.

7.5 Local RADIUS Server
If no authentication servers exist, the AP can be configured as its own RADIUS server. This is not the best choice since RADIUS authentication information is stored on the access point. However, configuring the AP as a RADIUS server provides better security than WEP. The only stipulation is that the user passwords should use NT hash not text.

7.6 Advanced Security
This page is to determine how MAC address and EAP authentication are handled. MAC address authentication can be handled by a list stored on the AP, authentication server or combination of both options. Using MAC address authentication adds another layer in achieving the defense-in-depth security model for the AP. The EAP authentication tab provides configuration options on EAP client timeouts and EAP re-authentication intervals. The default setting is sufficient in most cases.

8.0 Services

The services page displays a status summary of various services. The services that can be used by the access point are Telnet/SSH, Hot Standby, CDP, DNS, Filters, HTTP, Proxy Mobile IP, QoS, SNMP, NTP, VLAN and ARP Caching.

8.1 Telnet/SSH
To increase security of the AP, SSH should be used instead of telnet. Telnet sends passwords in clear-text while Secure Shell (SSH) sends passwords in encrypted form. SSH also verifies users are legitimate and compresses and encrypts data. If the AP is to be managed remotely, disable telnet.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8.2 Hot Standby

A spare AP can be configured as backup to the primary AP. Even with a backup AP, if the primary AP goes down for any reason, wireless clients will be disconnected and have to reassociate to the backup access point. Implementing this feature is a good idea and can be used as part of a disaster recovery plan.

8.3 CDP

The AP can be configured to use the Cisco Discovery Protocol (CDP). This option is for Cisco devices such as routers and switches and is used by a network, system or security administrator using CDP to manage all Cisco devices.

8.4 DNS

The AP can be configured to use up to three DNS servers. If the wireless clients are using the WLAN for internet access, at least one DNS server will need to be configured. DNS will also need to be enabled if the wireless clients are running Active Directory and use the WLAN to connect to network resources.

8.5 FILTERS

The AP can allow or block certain IP protocols. For example, if the AP is to only be used for internet access, the access point can be configured so only port 80 (HTTP) and 53 (DNS) are allowed. Using filters is another way the AP can be configured for increased security.

8.6 HTTP

This option allows the AP to be managed using a web browser. The default uses port 80; however, changing the port to something above 1024 will make it harder for someone to “accidentally” find the web configuration page. Another reason to change the port is so it is harder for programs like APTools to discover AP’s managed by a web interface.

8.7 Proxy Mobile IP

This option is used in conjunction with clients that may associate with a different AP depending on where the wireless device is at the time. Wireless clients can use this feature to automatically associate to other AP’s while keeping the same IP address and wireless connection. Depending on the layout of the WLAN, it may be less expensive to use a directional antenna instead of having multiple AP’s. The proxy mobile IP is disabled by default.

8.8 QoS

If a specific type of traffic (i.e. video or voice) is being used, the Quality of Service (QoS) feature can be used to give certain types of traffic favor over other types being sent. If no audio or video is being transmitted on the WLAN, this setting can remain disabled.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8.9 SNMP

SNMP allows the AP to be remotely configured and managed by various SNMP management software products. The SNMP community name is essentially a password needed to view or configure the AP from a remote location. The default community name of the AP is **defaultCommunity** with read only access. AP settings can be modified via SNMP by simply changing the SNMP setting to read-write and using a SNMP management software program. SNMP is disabled by default and should be left at the default setting. If SNMP is used, make sure to follow the guidelines discussed in the **Express Setup** section of this paper.

8.10 NTP

The AP can synchronize itself with a network time source (NTP) to maintain a consistent time. If this is enabled, a filter exception is usually needed at the firewall to allow NTP to be used. Having the correct date and time on log files is crucial. Using NTP helps by keeping an accurate time on the log files.

8.11 VLAN

If the AP is currently in a DMZ, isolated from the wired network with no other wired devices, enabling the VLAN option on the AP isn't necessary. However, if the AP is on the same network switch as other wired clients, configuring the AP to use a VLAN will add an extra layer of security. The VLAN can be setup so no communication occurs with the wired network. In the event the wireless network is compromised, the wired clients will be unaffected. If implementing a VLAN, there can only be one SSID associated with each VLAN. Most layer 3 switches allow for the creation of at least one VLAN; however, consult with network switch vendor for verification.

8.12 ARP Caching

Depending on the number of clients associating to the AP, enabling Address Resolution Protocol (ARP) caching can reduce the number of ARP broadcasts occurring on the wireless network. The less ARP broadcasts taking place, the less traffic on the wireless network.

If ARP caching is used, one possible attack that can take place is ARP cache poisoning. ARP cache poisoning is a type of man-in-the-middle attack. The only way to prevent a man-in-the-middle attack is by using mutual device authentication method such as LEAP or PEAP. By using LEAP or PEAP, an ARP cache poisoning attack will be prevented.

9. 0 Wireless Services

The wireless services page displays a summary of AP information and Wireless Domain Service (WDS) information. The AP information page contains the option to enable or disable WDS for the access point.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

WDS allows wireless clients to securely roam to different AP's across the wireless network without losing the wireless connection. When using WDS, instead of the RADIUS server performing the authentication, the process is handled entirely by the AP. Since WDS uses LEAP and Cisco Centralized Key management (CCKM), roaming to different AP's on the WLAN is considered to be secure. The main drawback of WDS is that all wireless clients have to use Cisco wireless cards.

10.0 System Software

The system software page summary displays the product number, serial number, firmware version, firmware filename, boot loader version and access point uptime. When software enhancements and fixes become available, this page displays all the information needed to install the correct software.

10.1 Software Upgrade

When the time comes to update the firmware, this page provides the information to complete the update. Simply download the appropriate file from the Cisco web site to a computer and use this page to install the update using TFTP or a web interface.

In the past, TFTP has been susceptible to buffer overflows which may cause the device to crash or reboot. For those desiring to disable TFTP as an option for updates, TFTP can be disabled by using Internetwork Operating System (IOS) commands.

10.2 System Configuration

This page allows the access point configuration file to be backed up. The configuration file can also be replaced with another configuration file or a default configuration file. The access point can also be restarted from this page. Having a backup configuration file should be done whenever changes are made to the access point. In the event the file becomes corrupt, the backup file can be restored.

11.0 Event Log

The event log can be configured to show items ranging from simple debugging information to emergency items requiring immediate attention. The event log can also send messages to a syslog server. If a syslog server exists, sending event log information to the syslog server should be done. Having all the logs on a centralized server makes it easier for auditing. If any critical alerts are logged, the system, network or security administrator can be notified. For instructions on how to setup a syslog server, refer to the following web site,

http://www.sans.org/rr/papers/33/198.pdf.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Conclusion

Using the information contained in this paper, the Cisco Aironet 1200 Access Point will be ready for corporate use. Throughout the paper, various tools used by attackers were mentioned. The best thing an administrator can do is become familiar with the tools. Performing periodic security audits will hopefully keep the network secure and resolve any vulnerabilities before an attacker finds them. The attacker already knows how to use the tools. They are just hoping you do not know.

References

1. Paul, Lauren Gibbons. "Sidebar: Getting to 802.11i."Computerworld. 03 May 2004. URL: http://www.computerworld.com/mobiletopics/mobile/technology/story/0,10801,92768,00.html?from=story_picks (03 Sept 2004).

2. "Aironet 1200 Series Access Point Installation and Configuration Guide, 12.2(8)JA." URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_installation_and_configuration_guide_chapter09186a0080147d6f.html (12 Aug 2004)

3. Finlay, Ian A. "A Brief Tour of the Simple Network Management Protocol." CERT Coordination Center. 1 December 2003.
URL: http://www.cert.org/archive/pdf/snmp.pdf (12 Aug 2004)

4. Moskowitz, Robert. WLAN Testing Reports "Debunking the Myth of SSID Hiding." URL: http://www.icsalabs.com/html/communities/WLAN/wp_ssid_hiding.pdf (12 Aug 2004)

5. "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite." URL: http://cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml (12 Aug 2004)

6. "Cisco Fast Secure Roaming." URL: http://cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801c5223.html (13 Sept 2004)

7. "Online Help for Cisco IOS Release 12.2(15)JA." URL: http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/122-15.JA/1400br/h_ap_network-if_ipaddress.htm (13 Sept 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8. Case, David A. **"**Radio Testing: An Insider's Guide From an Outsider's View" Evaluation Engineering.
URL: http://evaluationengineering.com/archive/articles/1103emc.htm (13 Sept 2004)

9. "Appendix B - Channels, Power Levels, Antenna Gains"
URL:
http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_chapter09186a008007f7fe.html. (13 Sept 2004)

10. "Smart Antenna Systems." International Engineering Consortium
http://www.iec.org/online/tutorials/smart_ant/topic02.html (13 Sept 2004)

11. "A Standard for the Transmission of IP Datagrams over IEEE 802 Networks." Network Working Group Request for Comments: 1042. February 1988.
URL: http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc1042.html (13 Sept 2004)

12. "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band." IEEE Computer Society. 27 June 2003.
URL: http://systems.cs.colorado.edu/downloads/802-standards/802.11g.pdf (16 Sept 2004)

13. Geier, Jim. "Improving WLAN Performance with RTS/CTS." Wi-Fi Planet. 13 August 2002.
URL: http://www.wi-fiplanet.com/tutorials/article.php/1445641 (16 Sept 2004)

14. "5-Minute Security Advisor - Strengthening Wireless Authentication."
URL: http://www.microsoft.com/technet/community/columns/5min/5min-208.mspx (17 Sept 2004)

15. Weatherspoon, Sultan. "Overview of IEEE 802.11b Security."
URL: http://www.intel.com/technology/itj/q22000/articles/art_5.htm (17 Sept 2004)

16. Cam-Winget et al. "EAP Flexible Authentication via Secure Tunneling (EAP-FAST)." 9 February 2004.
URL: http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-00.txt (21 Sept 2004)

17. "System Configuration User Guide for Cisco Secure ACS for Windows Server 3.2."
URL:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_chapter09186a0080205a6b.html#wp436984 (11 Aug 2004)

18. Lowdermilk, Ryan. "Auditing the Cisco Aironet 1200 Wireless Access Point." 10 October 2003.
URL: http://www.giac.org/practical/GSNA/Ryan_Lowdermilk_GSNA.pdf (3 Oct 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

19. URL: www.sans.org/rr/papers/6/117.pdf

20. Mangla, Anoop. “VLAN for Secure WiFi.” PCQuest. 7 June 2004.
URL: http://www.pcquest.com/content/search/showarticle.asp?artid=58122 (17 Sept 2004)

21. Whalen, Sean. “An Introduction to Arp Spoofing.” PacketStormSecurity. April 2001.
URL: http://packetstormsecurity.com/papers/protocols/intro_to_arp_spoofing.pdf (18 Sept 2004)

22. Fleck, Bob, Dimov, Jordan. “Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network.”
URL: http://www.cigitallabs.com/resources/papers/download/arppoison.pdf (18 Sept 2004)

23. “Cisco Aironet 1300 Series Outdoor Access Point/ Bridge Software Configuration Guide, 12.2(15) JA”
URL:
http://www.cisco.com/en/US/products/ps5861/products_configuration_guide_chapter09186a008021e5e0.html (18 Sept 2004)

24. “National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information.” CNSS. June 2003
URL: http://www.nstissc.gov/Assets/pdf/fact%20sheet.pdf (18 Sept 2004)

25. “New Study Points to Substantial Financial Returns from Broad-Based Wireless LAN Deployments.”
URL: http://newsroom.cisco.com/dlls/hd_111203b.html (17 Aug 2004)

26. Murphy, Richard. “How to Integrate Centralized Logging with Centralized Monitoring.” 27 July 2001
URL: http://www.sans.org/rr/papers/33/198.pdf (3 Oct 2004)

27. **“**Internet Authentication Service for Windows 2000**.”**
URL:
http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/ias.mspx (17 Aug 2004)

28. IEEE. “802.11g IEE Standard for Technology Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band.” 27 June 2003
URL: http://standards.ieee.org/getieee802/download/802.11g-2003.pdf (17 Sept 2004)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

29. “EAP-FAST” URL:
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml (23 Sept 2004)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.