CWNA Guide to Wireless LANs, Third Edition

Chapter 11: Managing a Wireless LAN

Objectives

- Describe security defenses for WLANs
- List the tools used for monitoring a wireless network
- Explain how to maintain a WLAN

Procedural Security Defenses

- Security defenses go beyond technical solutions
- Involve implementing correct security procedures
- Procedural security defenses:
  - Managing risk
  - Creating defenses against attacks

Managing Risk

- Determine nature of risks to organization's assets
  - First step in creating security policy
- **Asset**: Any item that has value
  - Cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources
  - Can form part of the organization's corporate identity
- **Threat**: type of action that has the potential to cause harm

Managing Risk

- **Threat agent**: person or element that has the power to carry out a threat
  - In information security, could be a person attempting to break into a secure network
- **Vulnerability**: flaw or weakness that allows a threat agent to bypass security
- **Exploiting**: taking advantage of a vulnerability
- **Risk**: the likelihood that a threat agent will exploit a vulnerability
  - Most risks should be diminished if possible

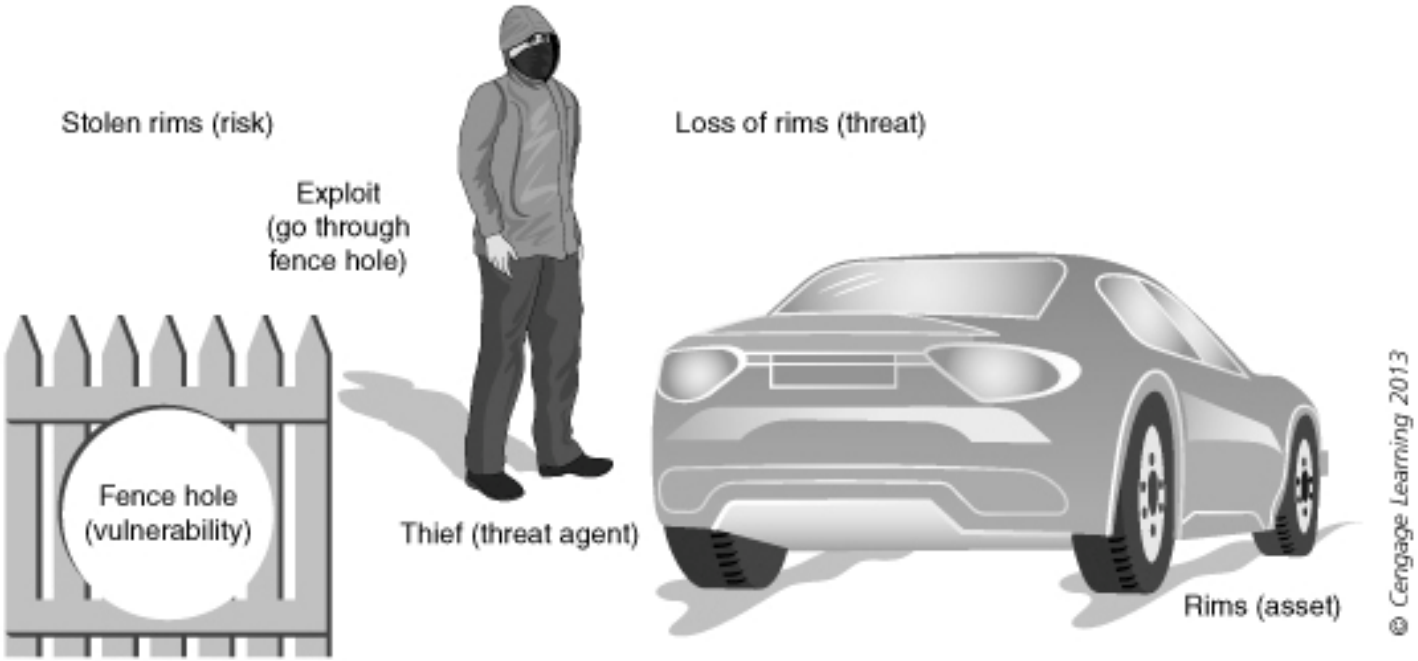

Figure 11-1 Information security components analogy

Managing Risk

- **Social engineering attacks:** Relies on tricking or deceiving someone to access a system
  - Impersonation: create a fictitious character and then play out the role of that person on a victim
  - Phishing: sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate sender in order to trick the user into surrendering private information

Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system o help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify
http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow
Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Helpful links
Search eBay - Find other items of interest
My eBay - Track your buying and selling activity
Discussion boards - Get help from other eBay members
eBay Help - Find answers to your questions

Learn More: Get notifications right on your desktop before an auction ends with the eBay Toolbar !

TaylorMade
IKEA BMW Nike
John Deere

Find it on ebay

Buy in Bulk and Save More!

Trading guidelines
eBay will not request personal data (password, credit card/bank numbers, and so on) in an email. Learn how to protect your account

Figure 11-2 Phishing Message

Defenses Against Attacks

- Defenses against attacks include:
  - Using security policies
  - Conducting effective security training for users
  - Implementing physical security procedures

Security Policy

- **Security policy:** Document that states how an organization plans to protect the company's information technology assets
- Can serve several functions:
  - Describe an overall intention and direction
  - Details specific risks and explains how to address them
  - Help to install security awareness in the organization's culture
  - Help ensure that employee behavior is directed and monitored to ensure compliance with security requirements

Security Policy

- Security policy cycle:
  - First phase involves a vulnerability assessment (an evaluation of exposure of assets to attackers, forces of nature, or any other harmful entity)
  - Five key elements:
    - Asset identification
    - Threat evaluation
    - Vulnerability appraisal
    - Risk assessment
    - Risk mitigation

Security Policy

- Security policy cycle (continued):
  - Second phase: use the information from the vulnerability assessment study to create the policy
  - Final Phase: review the policy for compliance
    - When new assets that need protection are identified or new risks need to be addressed, the cycle begins over again

Security Policies

- Types of security policies:
  - **Acceptable use policy (AUP)**: defines the actions users may perform while accessing systems and networking equipment
  - **Password policy**: addresses how passwords are created and managed
  - **Wireless policy**: specifies the conditions that wireless devices must satisfy in order to connect to the organization's network

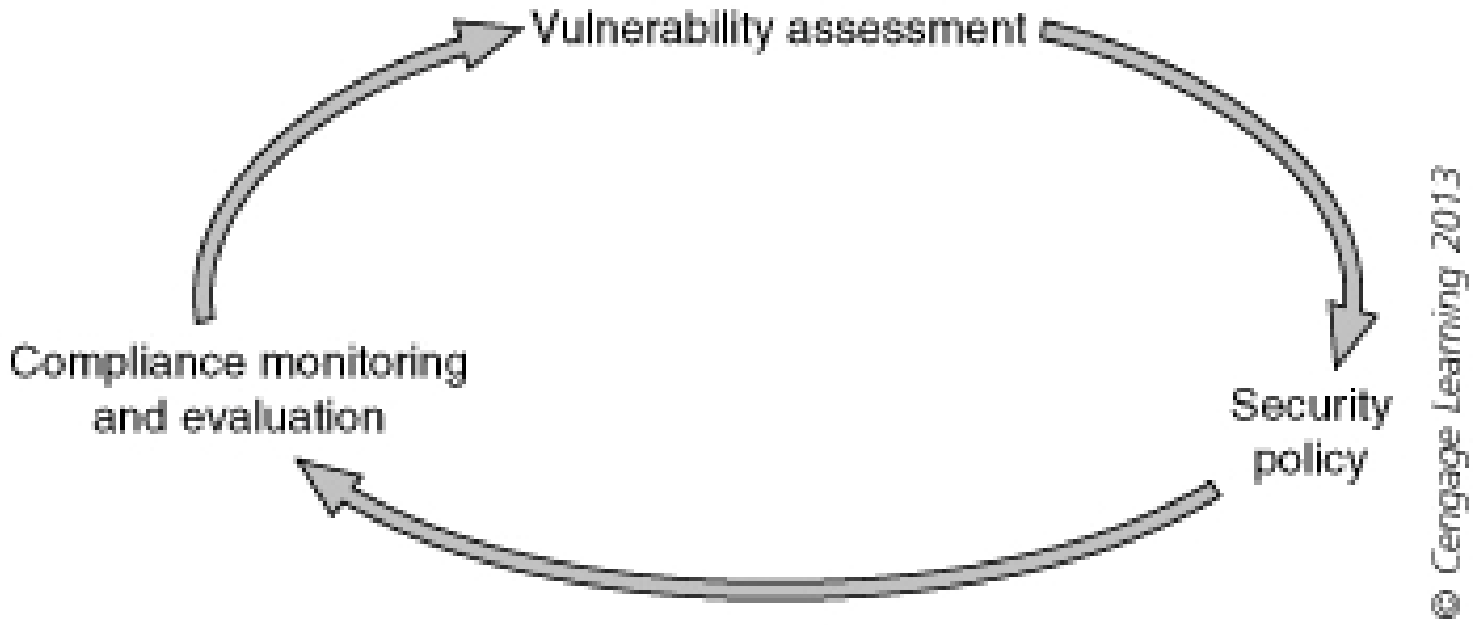

Figure 11-3 Security policy cycle

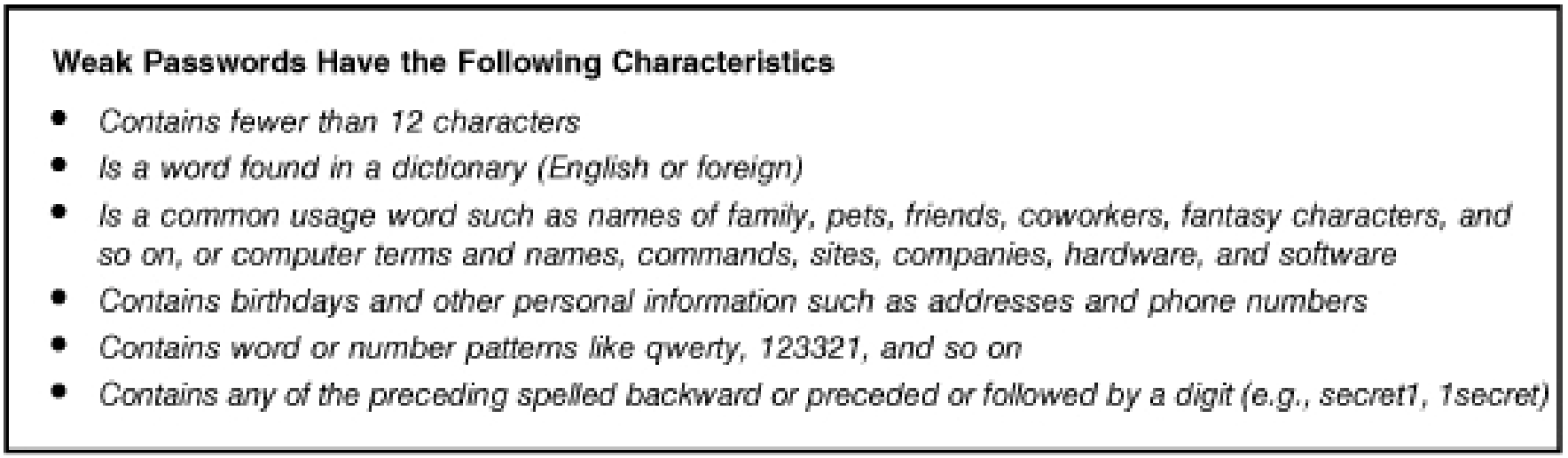

Figure 11-4 Weak password information

Strong Passwords Have the Following Characteristics

- *Contain both uppercase and lowercase characters (a-z, A-Z)*
- *Have digits and punctuation characters as well as letters (0-9, !@#$%^& *()_+=[]{})*
- *Are at least 12 characters long*
- *Are not words in any language, slang, dialect, or jargon*
- *Are not based on personal information*

Figure 11-5 Strong password information

Security Policies

- Effective security policy must balance trust and control
- Too much trust may lead to security problems
- Too little trust may make it difficult to find and keep good employees
- Control must also be balanced
  - If policies are too restrictive or too hard to comply with, employees will either ignore them or find ways to circumvent the controls

Awareness and Training

- Opportunities for security education and training:
  - When a new employee is hired
  - After a computer attack has occurred
  - When an employee is promoted or given new responsibilities
  - During an annual departmental retreat
  - When new user software is installed
  - When user hardware is upgraded

Physical Security

- **Door locks**: consider using a deadbolt lock for rooms that require enhanced security
- **Video surveillance**: closed circuit television (CCTV) is frequently used for surveillance in areas that require security monitoring
- **Fencing**: securing an area by erecting a barrier
- **Cable locks**: inserted into the security slot of a portable device and the cable connected to the lock that is secured to a desk or chair

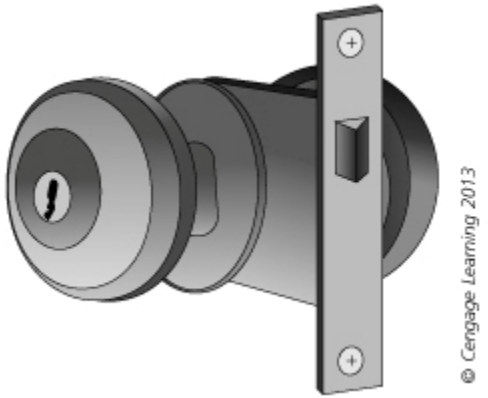

Figure 11-6 Residential keyed entry lock

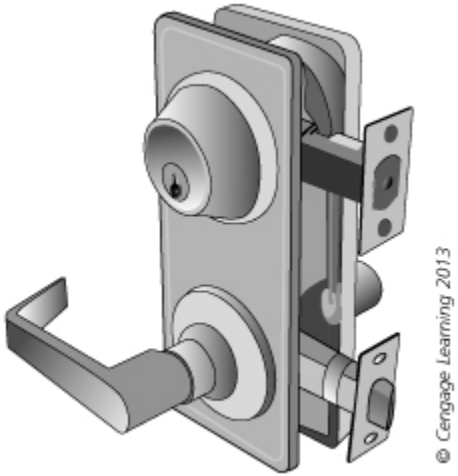

Figure 11-7 Deadbolt lock

Figure 11-8 Cable lock

Monitoring the Wireless Network

- Network monitoring provides valuable data regarding current state of a network
  - Generate network baseline
  - Detect emerging problems
- Monitoring a wireless network can be performed with two sets of tools:
  - Utilities designed specifically for WLANs
  - Standard networking monitoring tools

WLAN Monitoring Tools

- Two classifications of tools:
  - Operate on wireless device itself
  - Function on AP

- **Mobile Device Utilities:**
  - Most OSs provide basic utilities for monitoring the WLAN
  - Some vendors provide more detailed utilities

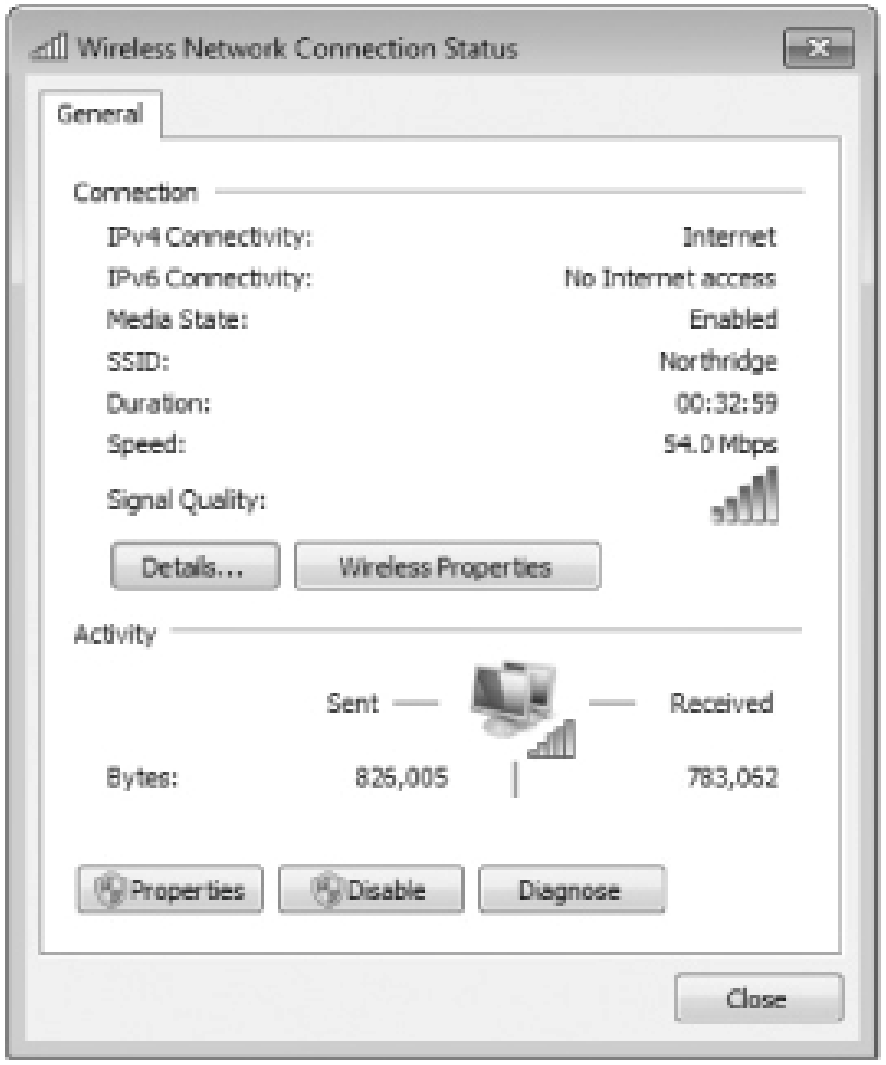

Figure 11-9 Windows 7 Wireless Network Connection Status

WLAN Monitoring Tools

- **Access Point Utilities**
  - All APs have WLAN reporting utilities
  - Many enterprise-level APs provide utilities that offer three types of information:
    - Event logs
    - Statistics on wireless transmissions
    - Information regarding connection to wired network

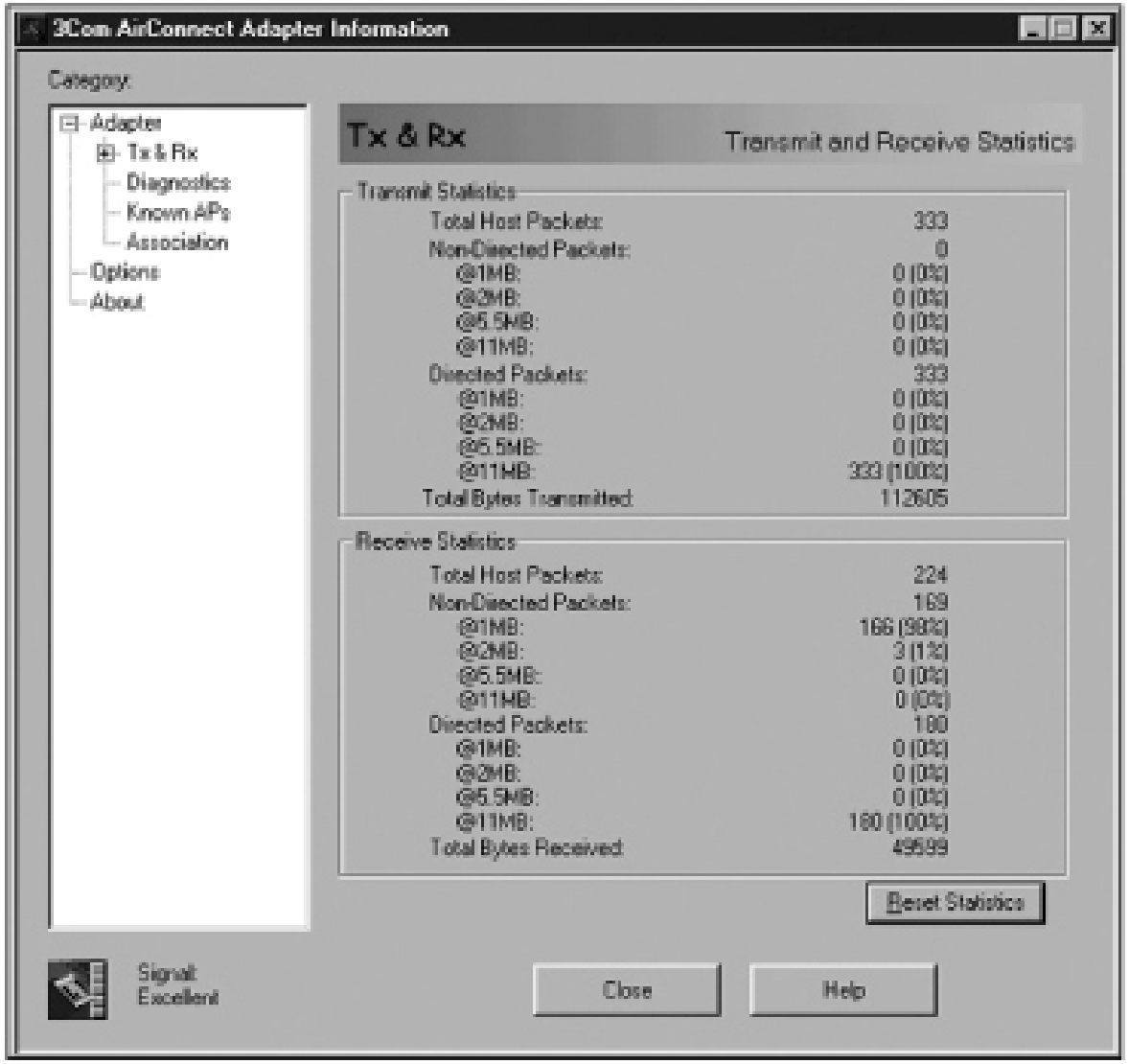

Figure 11-10 Transmit and receive statistics displayed in AirConnect

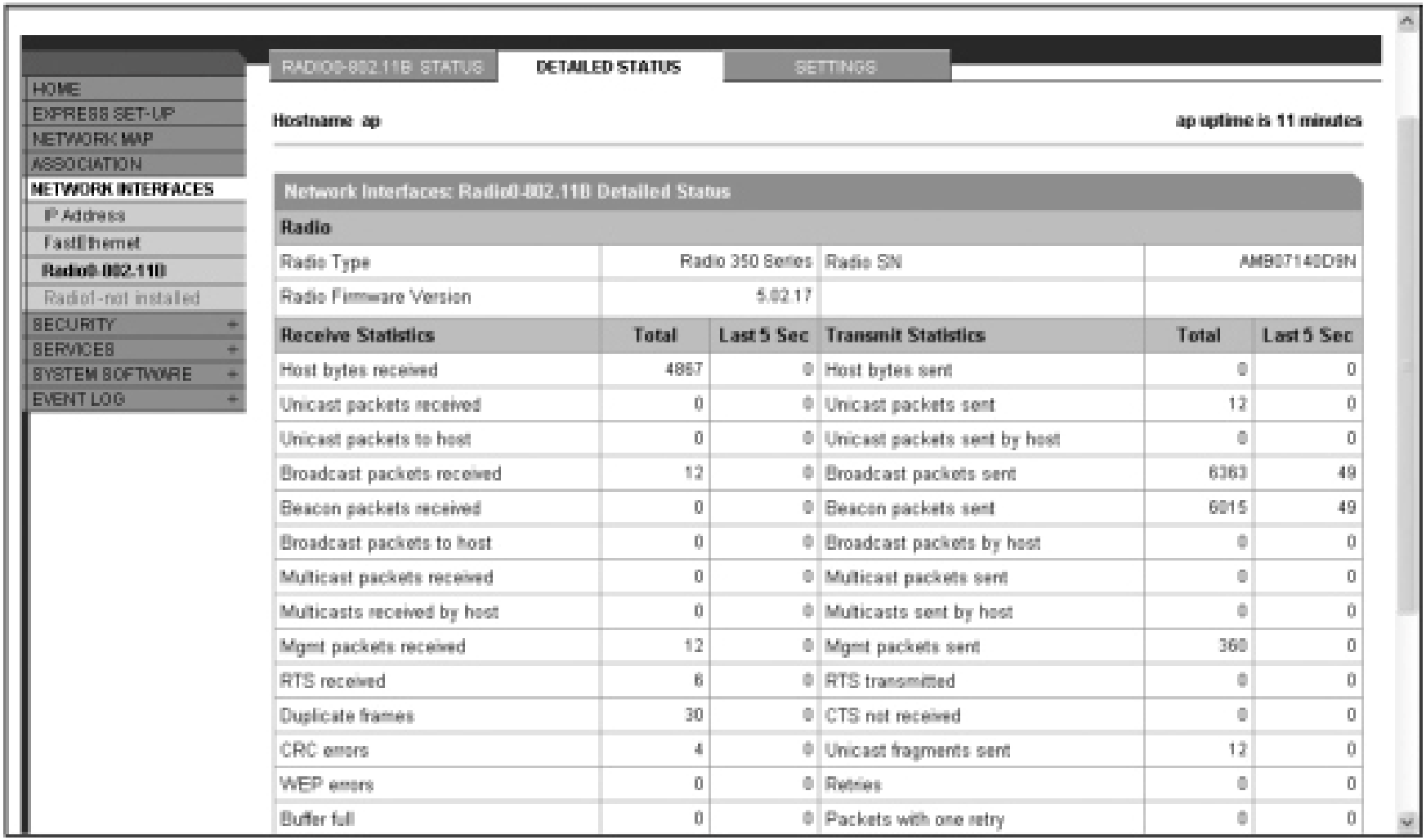

Figure 11-11 AP wireless statistics on Cisco AP

Standard Network Monitoring Tools

- Drawbacks to relying solely on info from AP and wireless devices:
  - Data collection can be labor- and time-intensive
  - Timeliness : data sometimes can only be used after a problem occurs
  - Retention of data can be difficult

- "Standard" network monitoring tools:
  - **Simple Network Management Protocol (SNMP)**
  - **Remote Monitoring (RMON)**

Simple Network Management Protocol (SNMP)

- Protocol allowing computers and network equipment to gather data about network performance
  - Part of TCP/IP protocol suite

- **Software agent** loaded onto each network device that will be managed using SNMP
  - Monitors network traffic and stores info in **management information base (MIB)**
  - **SNMP management station:** Computer with the SNMP management software

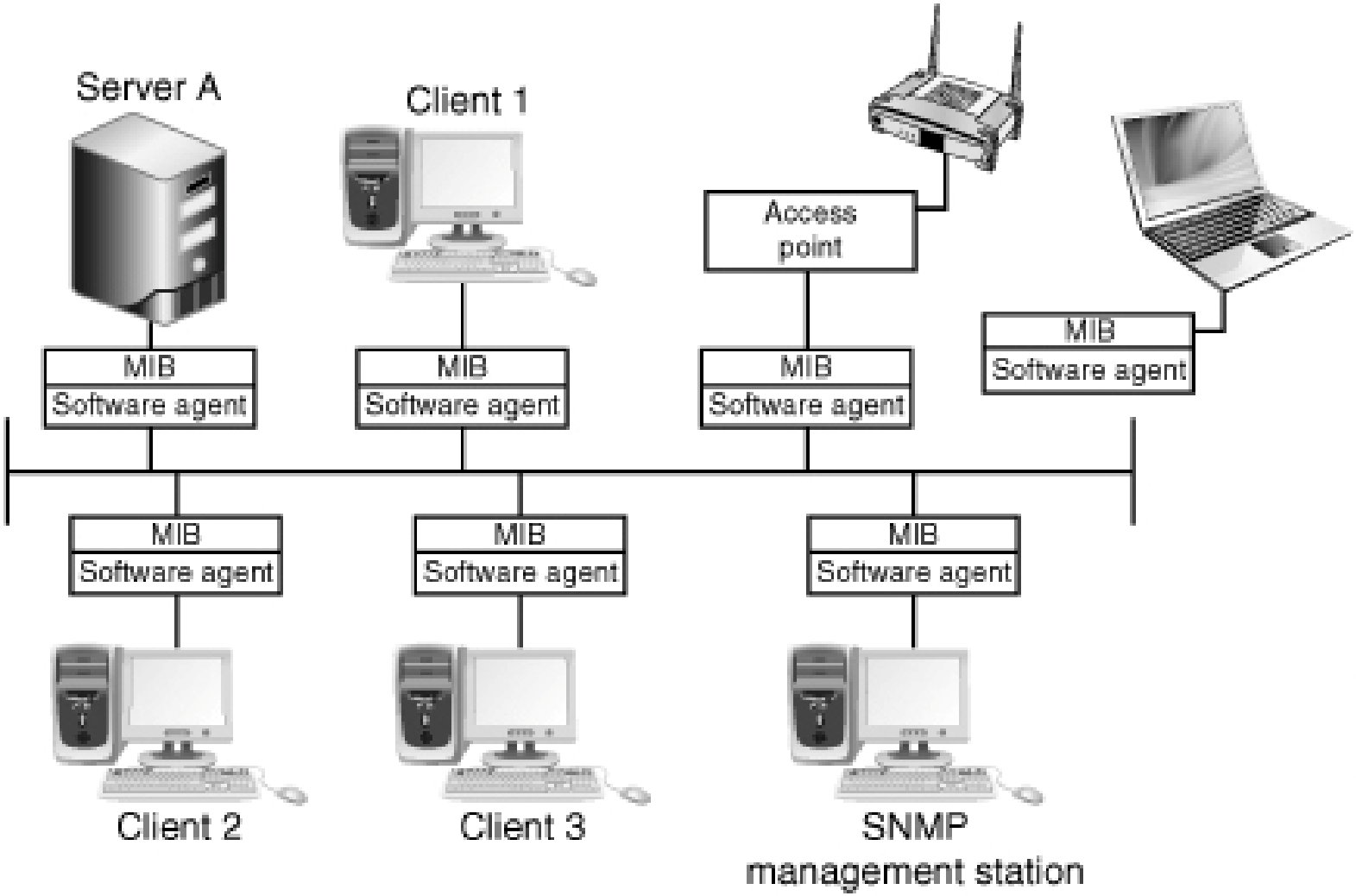

Figure 11-13 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol

- SNMP management station communicates with software agents on network devices
  - Collects data stored in MIBs
  - Combines and produces statistics about network

- Whenever network exceeds predefined limit, triggers an **SNMP trap**
  - Sent to management station

Figure 11-14 SNMP trap on Cisco AP

Remote Monitoring (RMON)

- SNMP-based tool used to monitor networks using dedicated hardware devices
- Allows remote network node to gather network data at almost any point on a LAN or WAN
  - Uses SNMP and incorporates special database for remote monitoring
- WLAN AP can be monitored using RMON
  - Gathers data regarding wireless and wired interfaces

Maintaining the Wireless Network

- Wireless networks are not static
  - Must continually be modified, adjusted, and tweaked
- Modifications often made in response to data gathered during network monitoring
- Two of most common functions are to:
  - Upgrade AP firmware
  - Perform RF site tuning

Upgrade Firmware

- **Firmware**: Software embedded into hardware to control the device
  - Electronic "heart" of a hardware device
  - Resides on **EEPROM**
    - Nonvolatile storage chip

- Most APs use a browser-based management system

- Keep APs current with latest changes by downloading the changes to the APs

Upgrade Firmware

- General steps to update AP firmware:
  - Download firmware from vendor's Web site
  - Select "Upgrade Firmware" or similar option from AP
  - Launching the update

- Enterprise-level APs often have enhanced firmware update capabilities
  - e.g., may be able to update System firmware, Web Page firmware, and radio firmware separately

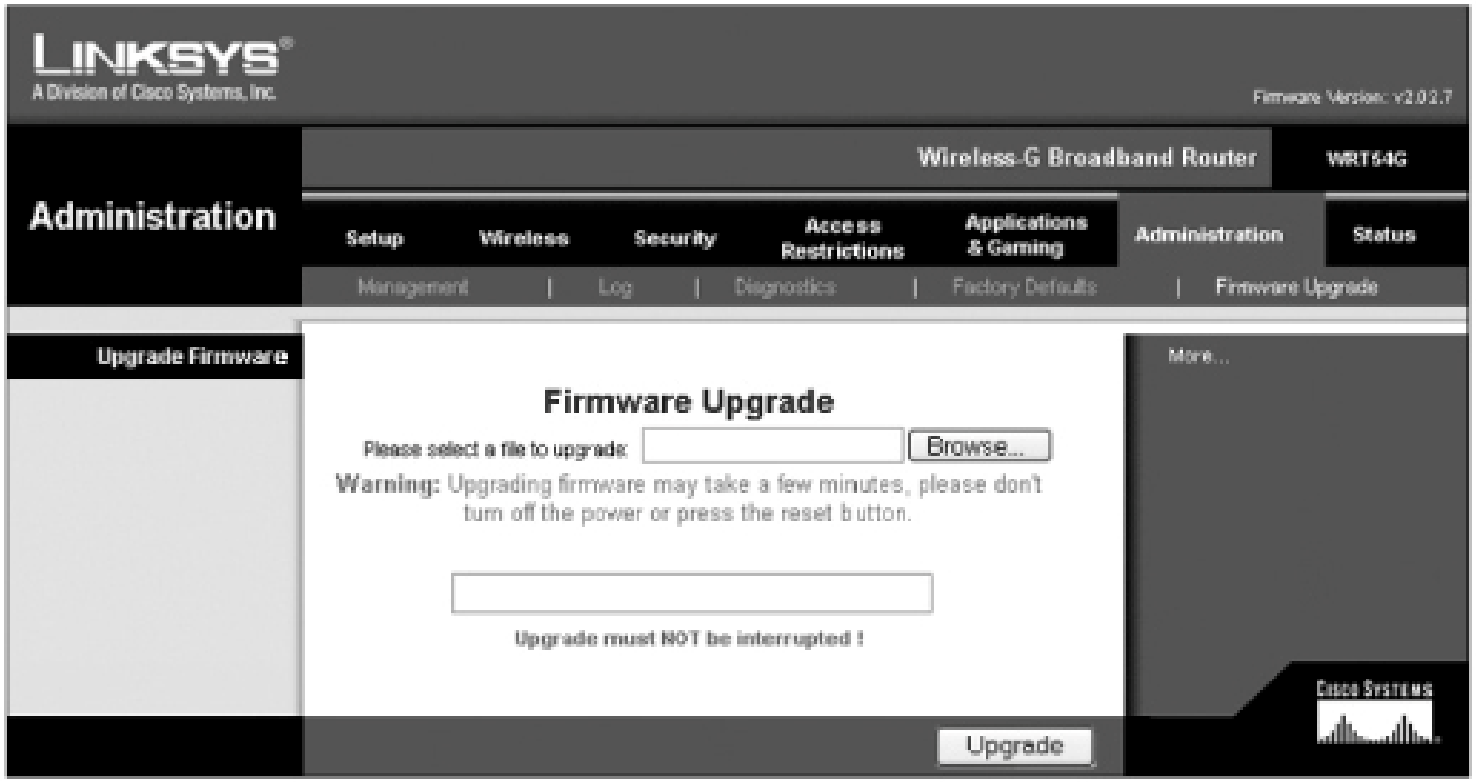

Figure 11-15 Firmware upgrade with separate file download

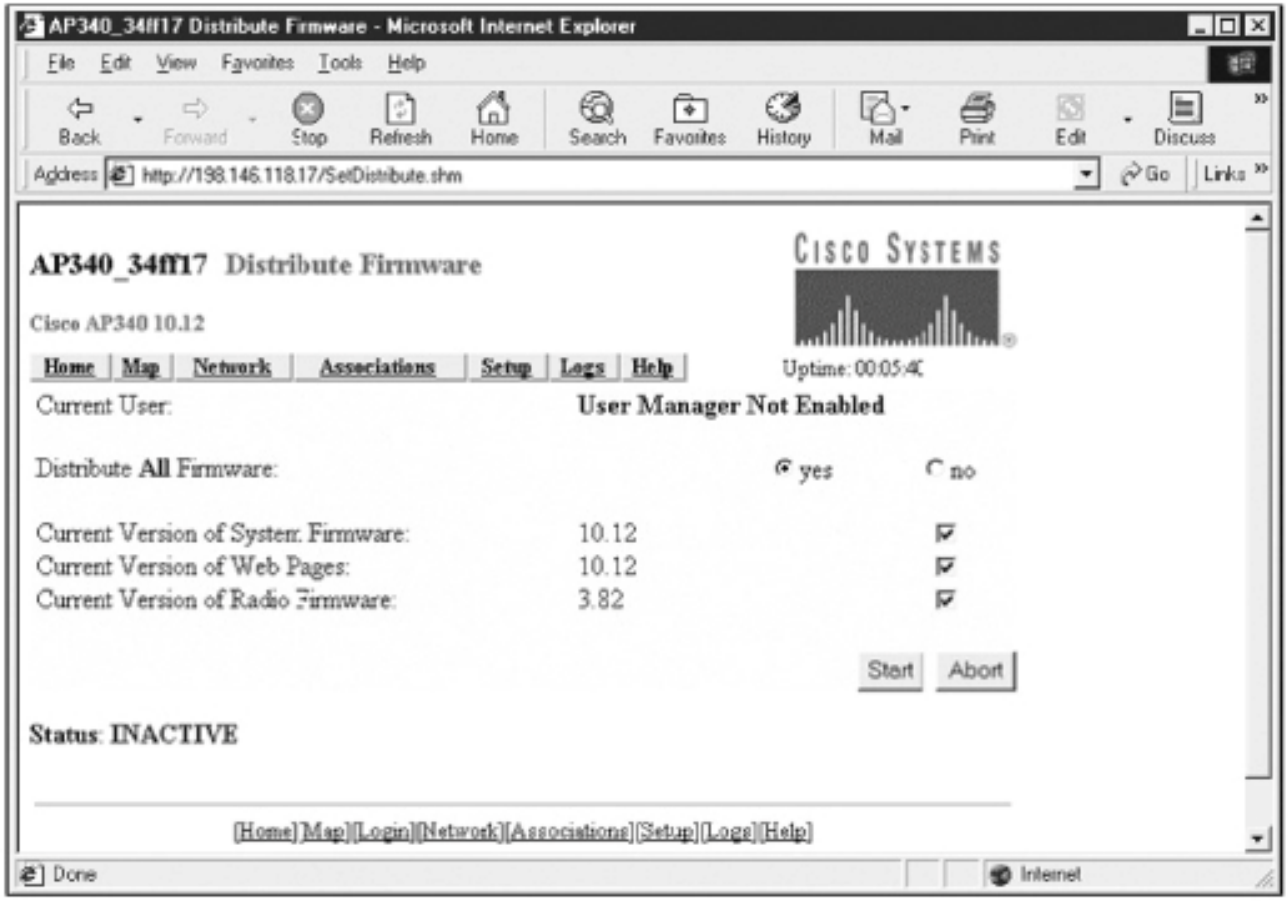

Figure 11-16 Separate firmware upgrades

Upgrade Firmware

- With many enterprise-level APs, once a single AP has been upgraded to the latest firmware, can distribute to all other APs on the WLAN
  - Receiving AP must be able to hear IP multicast issued by Distribution AP
  - Receiving AP must be set to allow access through a Web browser
  - If Receiving AP has specific security capabilities enabled, must contain in its approved user lists a user with the same user name, password, and capabilities as user logged into Distribution AP

RF Site Tuning

- **RF site tuning:** Adjustments to a WLAN performed as part of routine maintenance
  - Adjust radio power levels on all access points
    - Firmware upgrades may increase RF coverage areas
  - Adjust channel settings
  - Validate coverage area
  - Modify integrity and throughput
  - Document changes

Summary

- One of the first steps in implementing procedural security defenses is to manage risk
- One of the greatest risk that organizations face today are social engineering which involve manipulating human nature in order to persuade the victim to provide information or take actions
- A security policy is a document that states how an organization plans to protect the company's information technology assets

Summary

- There are several types of security policies: an acceptable use policy, a password policy, and a wireless policy are all examples
- Another defense is to provide training that encourages users to be aware of security issues and procedures
- Securing the devices so that unauthorized users are prohibited from gaining physical access to the equipment is an important security procedure

Summary

- Monitoring a wireless network can be performed with two different tools:
  - Specific WLAN utilities for the access point or wireless device
  - Standard networking tools such as Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON)
- One function of maintaining a wireless LAN is to upgrade the firmware on the access point
- Once an AP's firmware has been upgraded several settings may need to be adjusted as part of routine maintenance (RF site tuning)