CWSP Guide to Wireless Security

Wireless LAN Vulnerabilities

Objectives

- Explain the main IEEE 802.11 security protections
- Describe the vulnerabilities of IEEE 802.11 authentication
- Tell how address filtering is limited
- List the vulnerabilities of WEP

Basic IEEE 802.11 Security Protections

- Protections can be divided into three categories
  - Access control
  - Wired equivalent privacy (WEP)
  - Authentication

Access Control

- Access control
  - Method of restricting access to resources
  - Intended to guard the *availability* of information
    - By making it accessible only to authorized users
  - Accomplished by limiting a device's access to the access point (AP)
- Access point (AP)
  - Contains an antenna and a radio transmitter/receiver
    - And an RJ-45 port (or similar): A registered jack connector and wiring pattern used for connection of a high-speed modem to a telephone network
  - Acts as central base station for the wireless network

Access Control (continued)

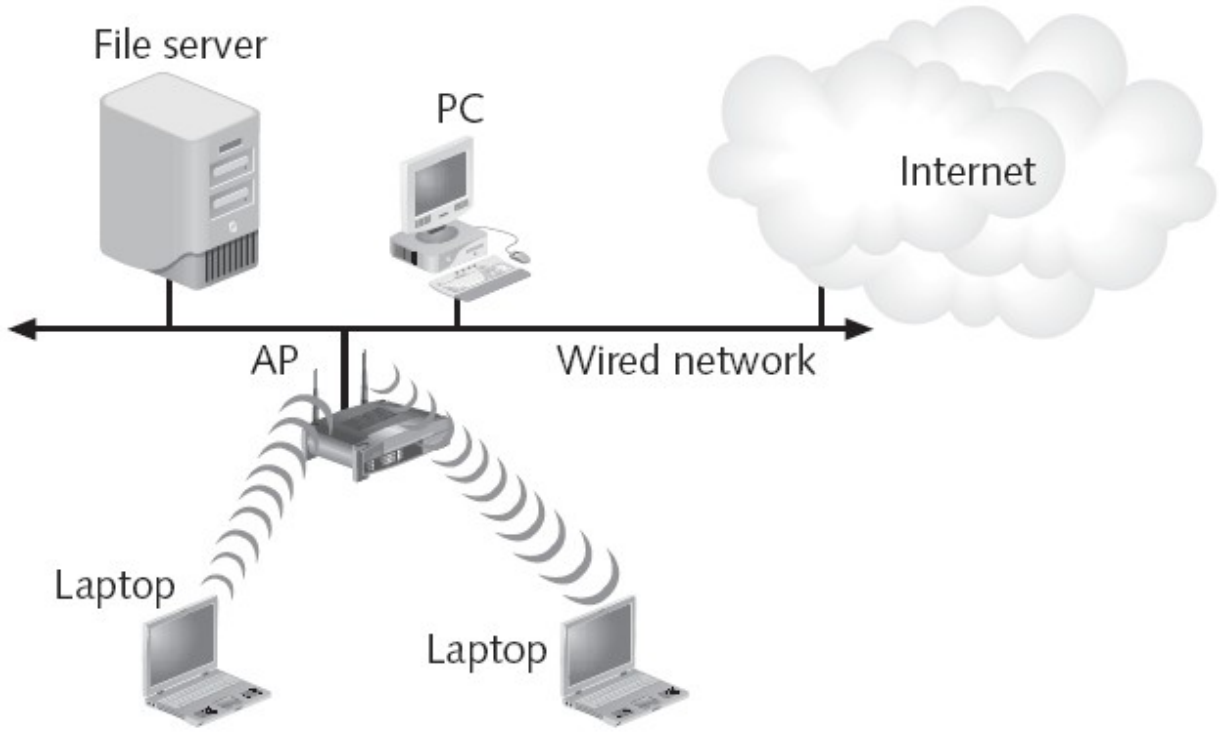


Figure 2-1 Access point as central base station

Access Control (continued)

- Almost all wireless APs implement access control
  - Through Media Access Control (MAC) address filtering
- Implementing restrictions
  - A device can be *permitted* into the network
  - A device can be *prevented* from the network
- MAC address filtering should not be confused with access restrictions
  - Access restrictions can limit user access to Internet

Access Control (continued)

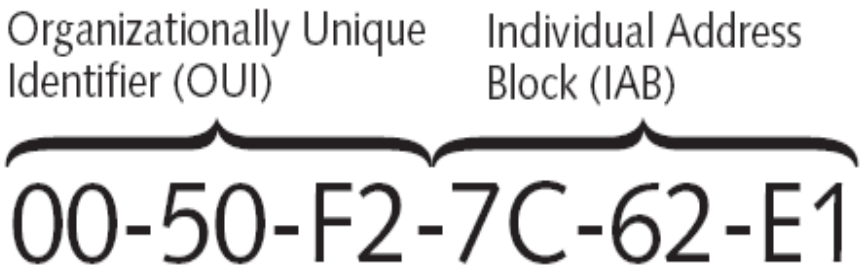


Figure 2-2 MAC address

OUI: a 24-bit number that is purchased from IEEE Registration Authority. This identifier uniquely identifies a vendor, manufacturer, or other organization (referred to by the IEEE as the **"assignee"**) globally.

IAB: is a block of identifiers that is formed by concatenating a 24-bit OUI. with an additional 12-bit extension identifier that is **assigned** *by the IEEE Registration Authority*, and then reserving an additional 12 bits for use by the assignee. The resulting 48-bit identifier uniquely identifies the assignee of the IAB and provides 4096 unique EUI-48 numbers for use by the organization that purchased the IAB

Access Control (continued)

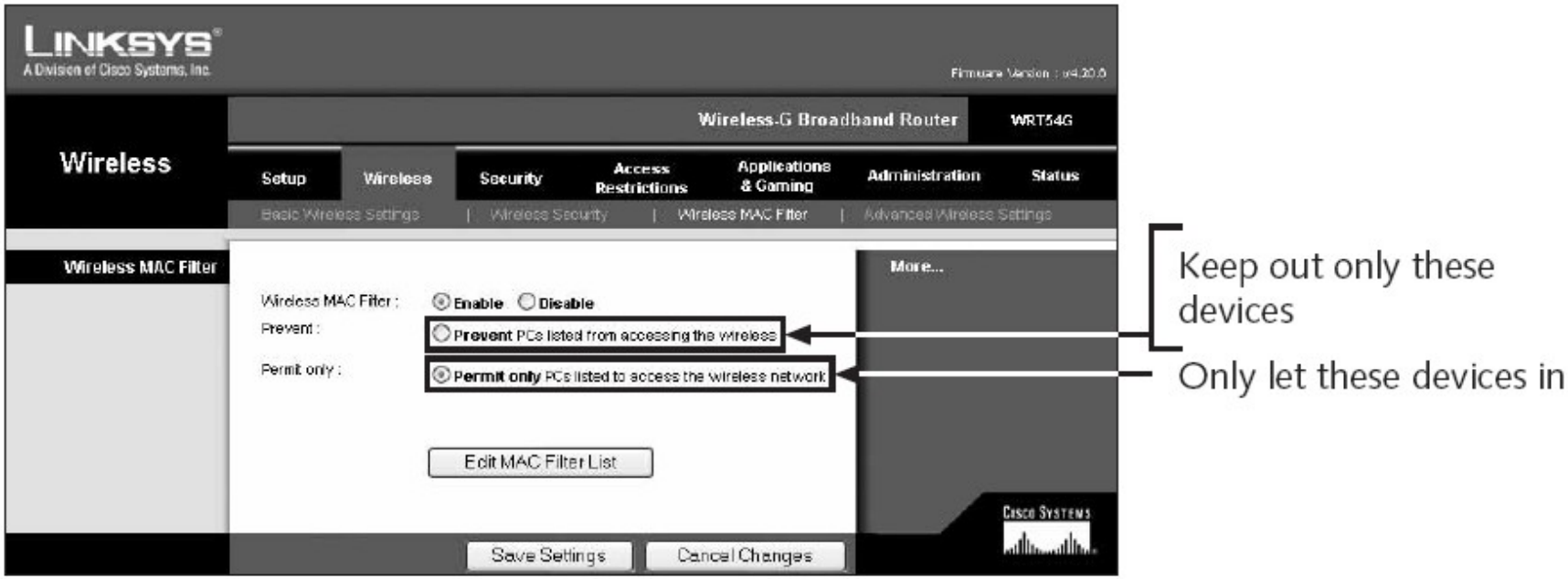


Figure 2-3 MAC address filter

Access Control (continued)

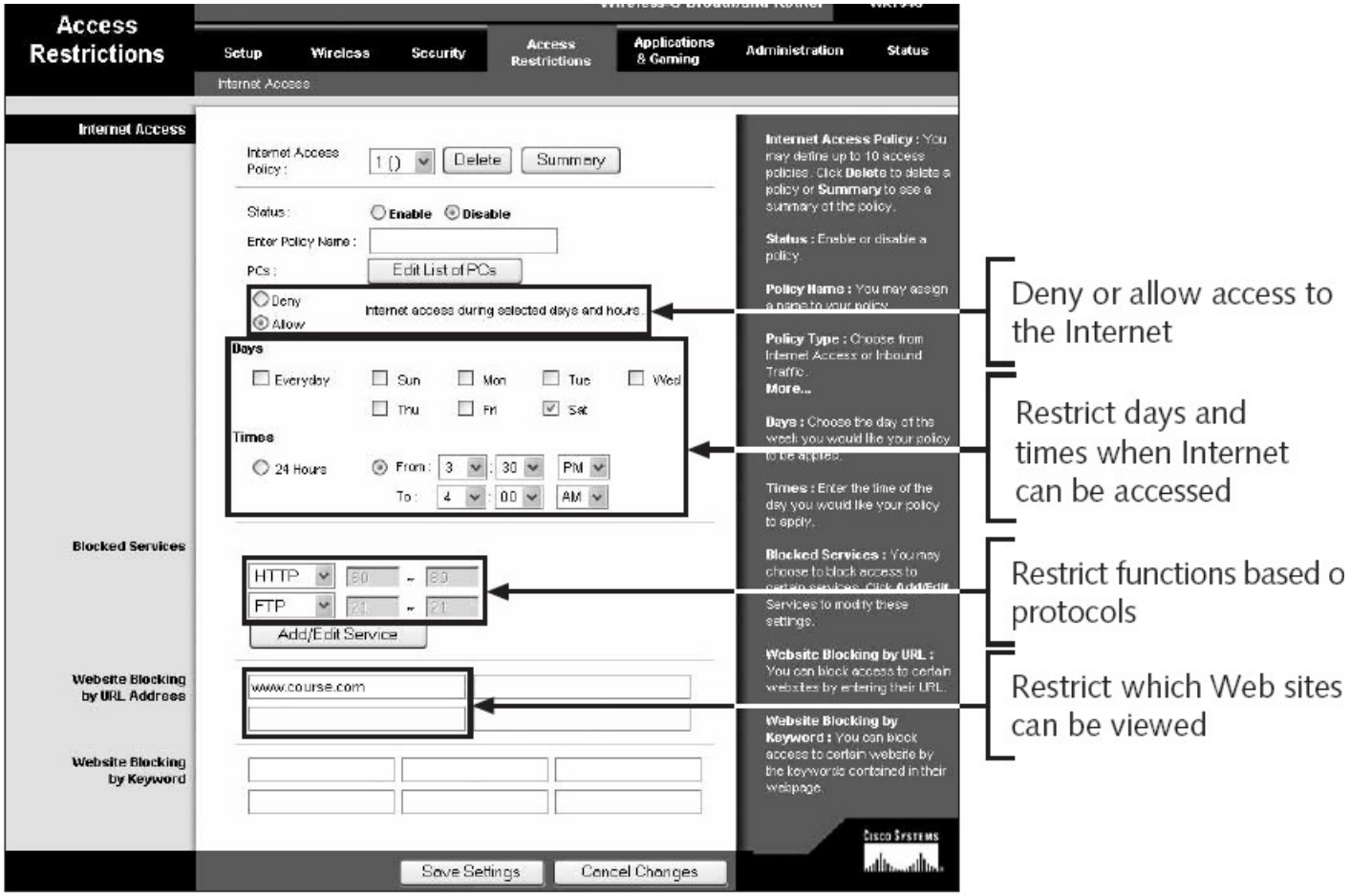


Figure 2-4 Access restrictions

Access Control (continued)

- MAC address filtering
  - Considered a basic means of controlling access
  - Requires pre-approved authentication
  - Makes it difficult to provide temporary access for “guest” devices

Wired Equivalent Privacy (WEP)

used for Encryption

- Intended to guard confidentiality
  - Ensures that only authorized parties can view the information
- WEP accomplishes confidentiality by “scrambling” the wireless data as it is transmitted
  - Used in IEEE 802.11 to encrypt wireless transmissions
- Cryptography
  - Science of transforming information so that it is secure while it is being transmitted or stored
  - WEP is a form of Cryptography

Wired Equivalent Privacy (WEP) (continued)

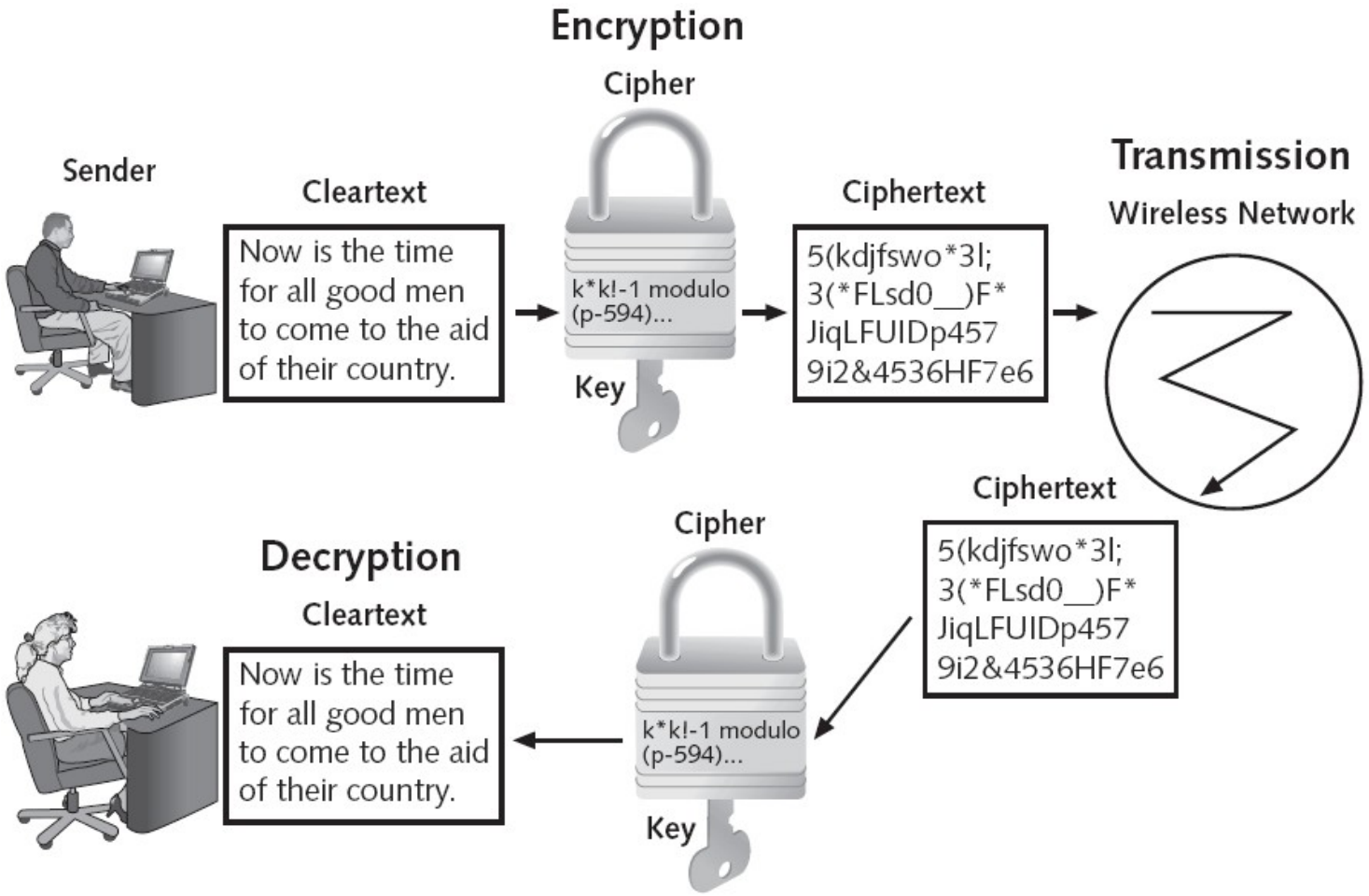


Figure 2-5 Cryptography

Wired Equivalent Privacy (WEP) (continued)

- WEP implementation
  - WEP was designed to meet the following criteria:
    - Efficient
    - Exportable
    - Optional
    - Reasonably strong
    - Self-synchronizing
  - WEP relies on a secret key shared between a wireless client device and the access point
    - Private key cryptography or symmetric encryption

Wired Equivalent Privacy (WEP) (continued)

- WEP implementation (continued)
  - Options for creating keys
    - 64-bit key
    - 128-bit key
    - Passphrase
  - APs and devices can hold up to four shared secret keys
    - One of which must be designated as the default key

Wired Equivalent Privacy (WEP) (continued)

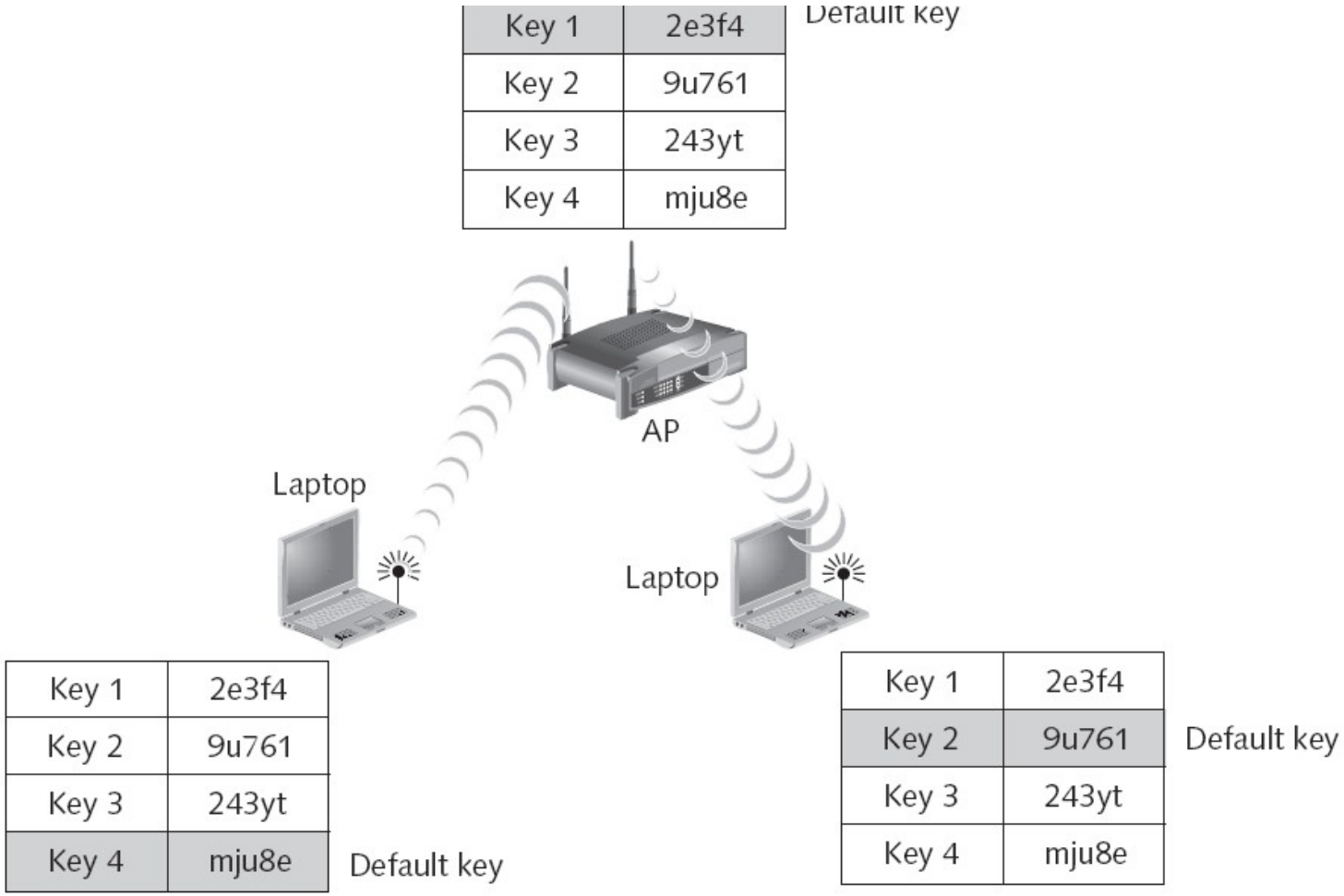


Figure 2-6 Default WEP key

Wired Equivalent Privacy (WEP) (continued)

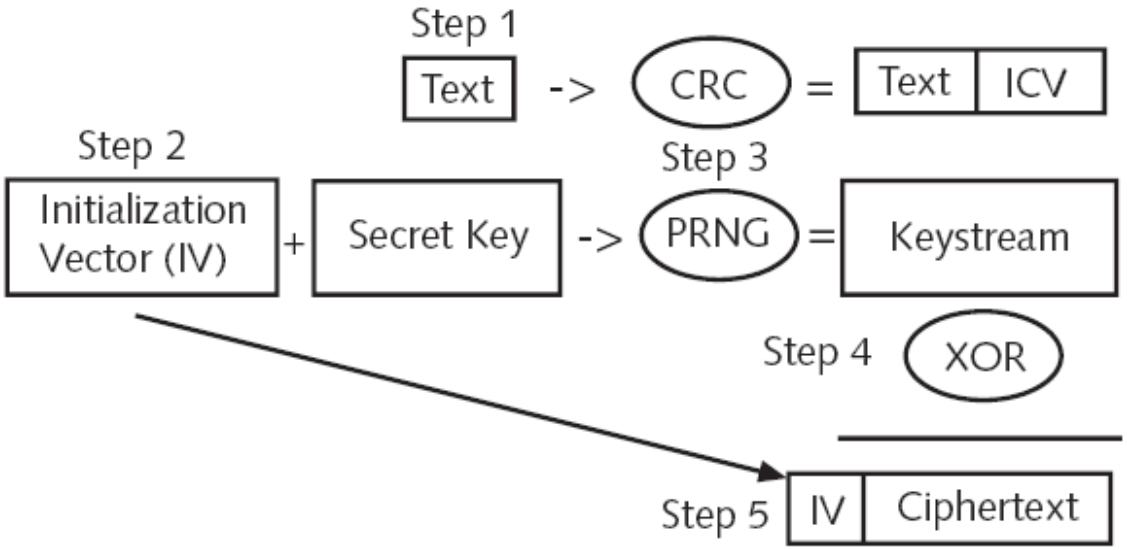


Figure 2-7 WEP encryption process

Wired Equivalent Privacy (WEP) (continued)

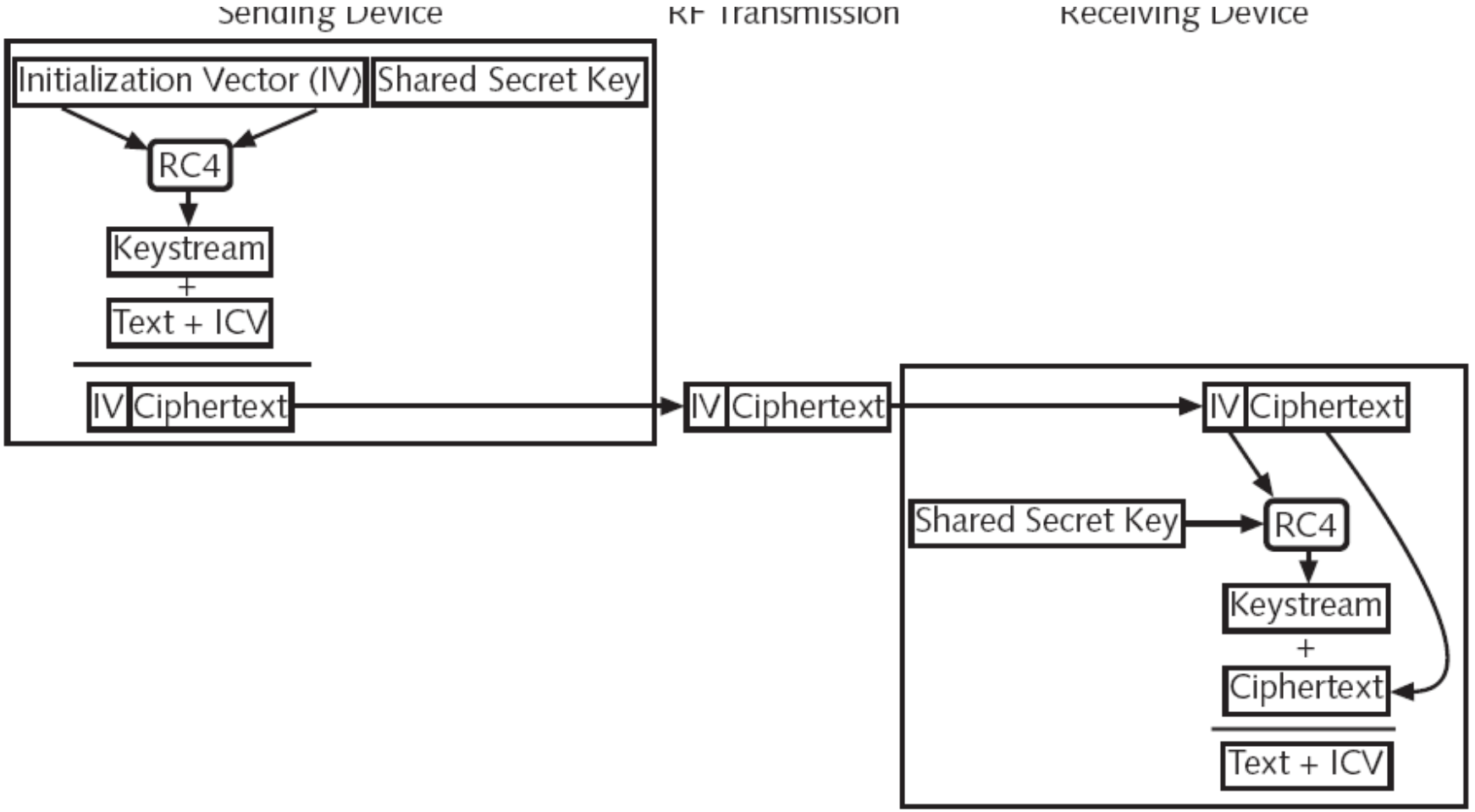


Figure 2-8 Transmitting with WEP

Quick Quiz 1

1. _____ is defined as a method of restricting access to resources.

2. _____ is the science of transforming information so that it is secure while it is being transmitted or stored.

3. An encryption algorithm is known as a(n) _____.

4. The IEEE standard also specifies that the access points and devices can hold up to four shared secret keys, one of which must be designated as the _____.

Authentication

- Devices connected to a wired network are assumed to be authentic
- Wireless authentication requires the wireless device to be authenticated
  - Prior to being connected to the network
- Types of authentication supported by 802.11
  - Open system authentication
  - Shared key authentication

Authentication (continued)

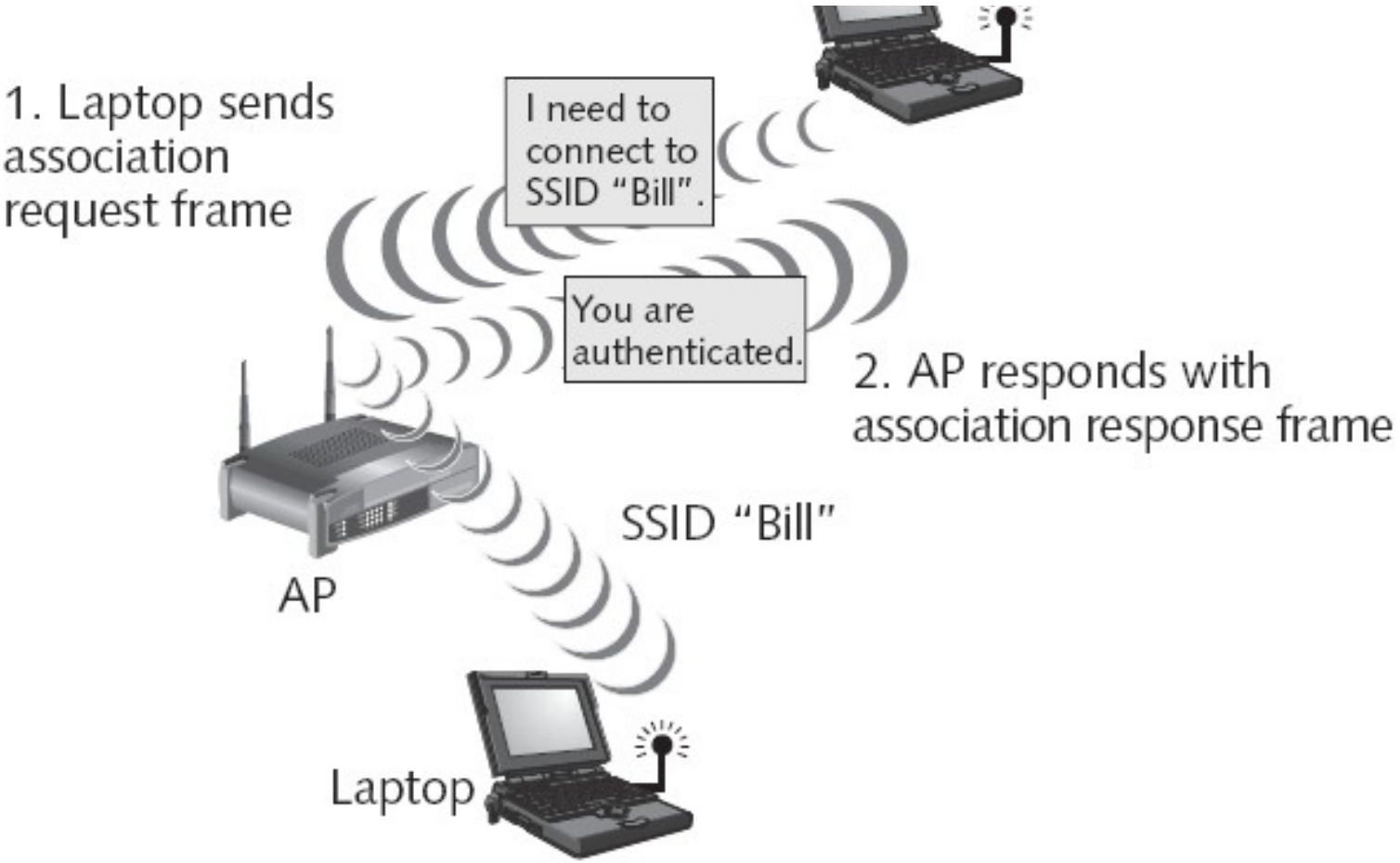


Figure 2-9 Open system authentication

Authentication (continued)

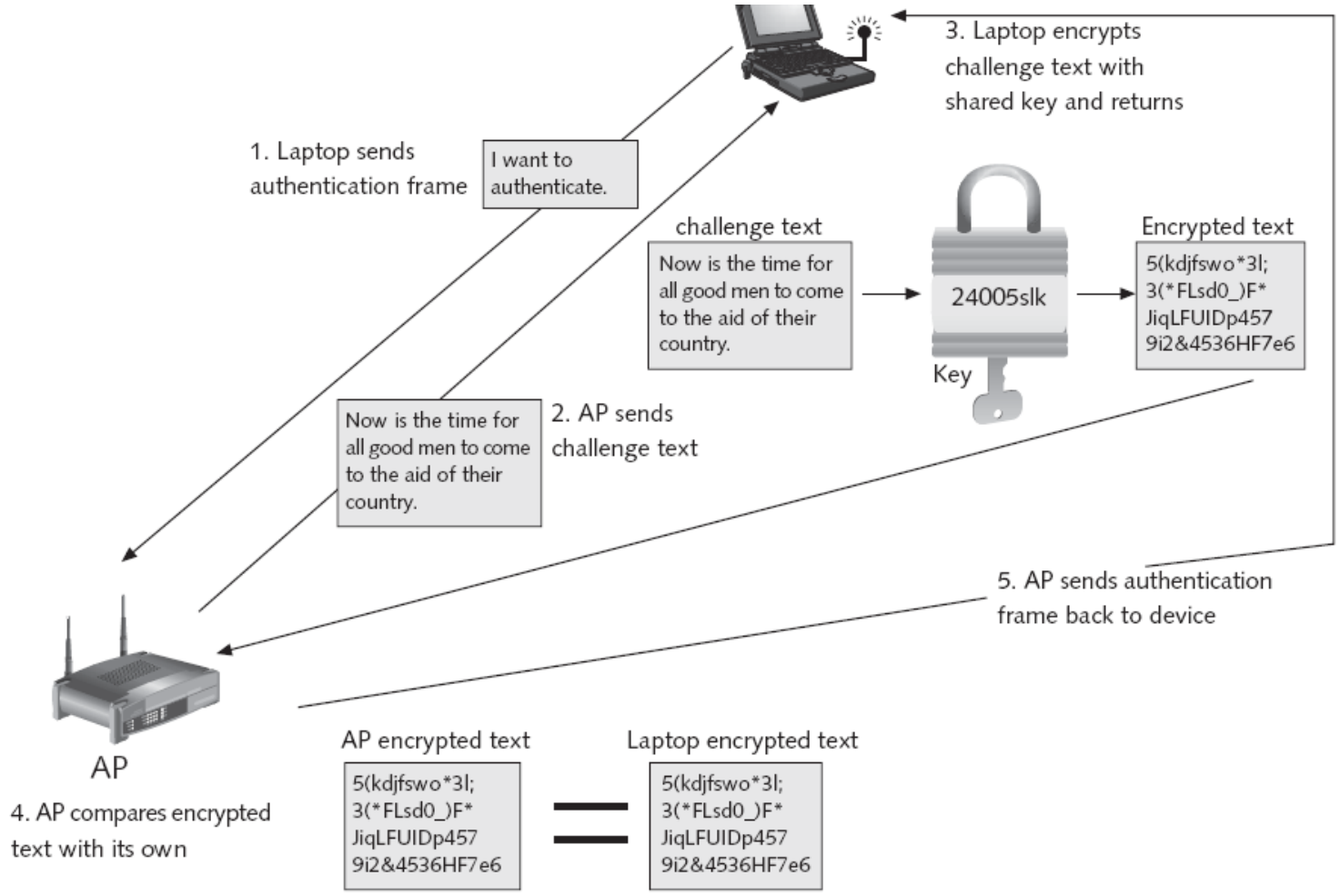


Figure 2-10 Shared key authentication

Vulnerabilities of IEEE 802.11 Security

- 802.11 security mechanisms for wireless networks
  - Proved to provide a very weak level of security

Authentication

- Open system authentication vulnerabilities
  - Authentication is based on a match of SSIDs
  - Several ways that SSIDs can be discovered
  - Beaconing
    - At regular intervals the AP sends a beacon frame
  - Scanning
    - Wireless device is set to look for those beacon frames
  - Beacon frames contain the SSID of the WLAN
  - Wireless security sources encourage users to disable SSID broadcast

Authentication (continued)

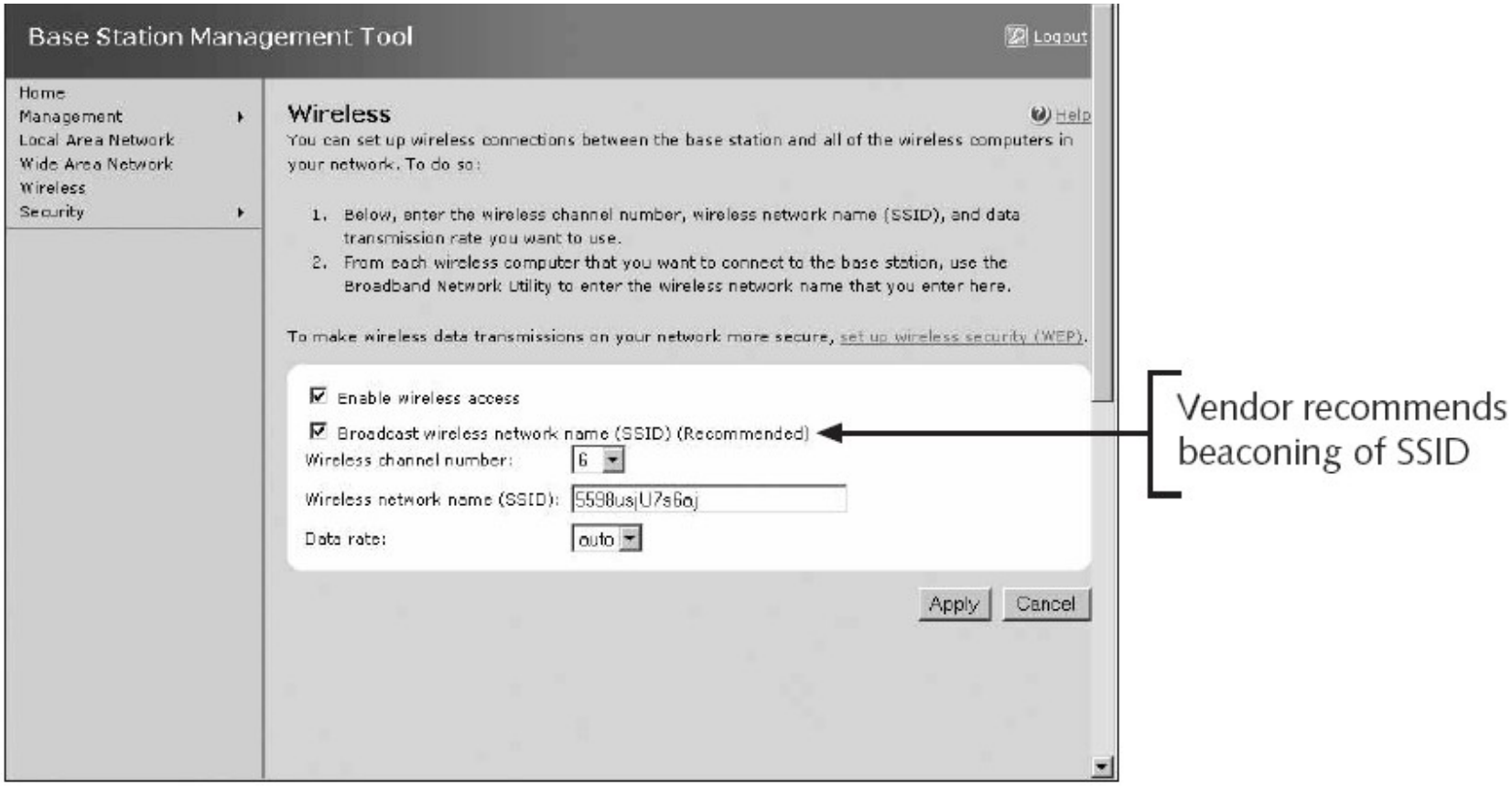


Figure 2-11 Turning off SSID beaconing discouraged

Authentication (continued)

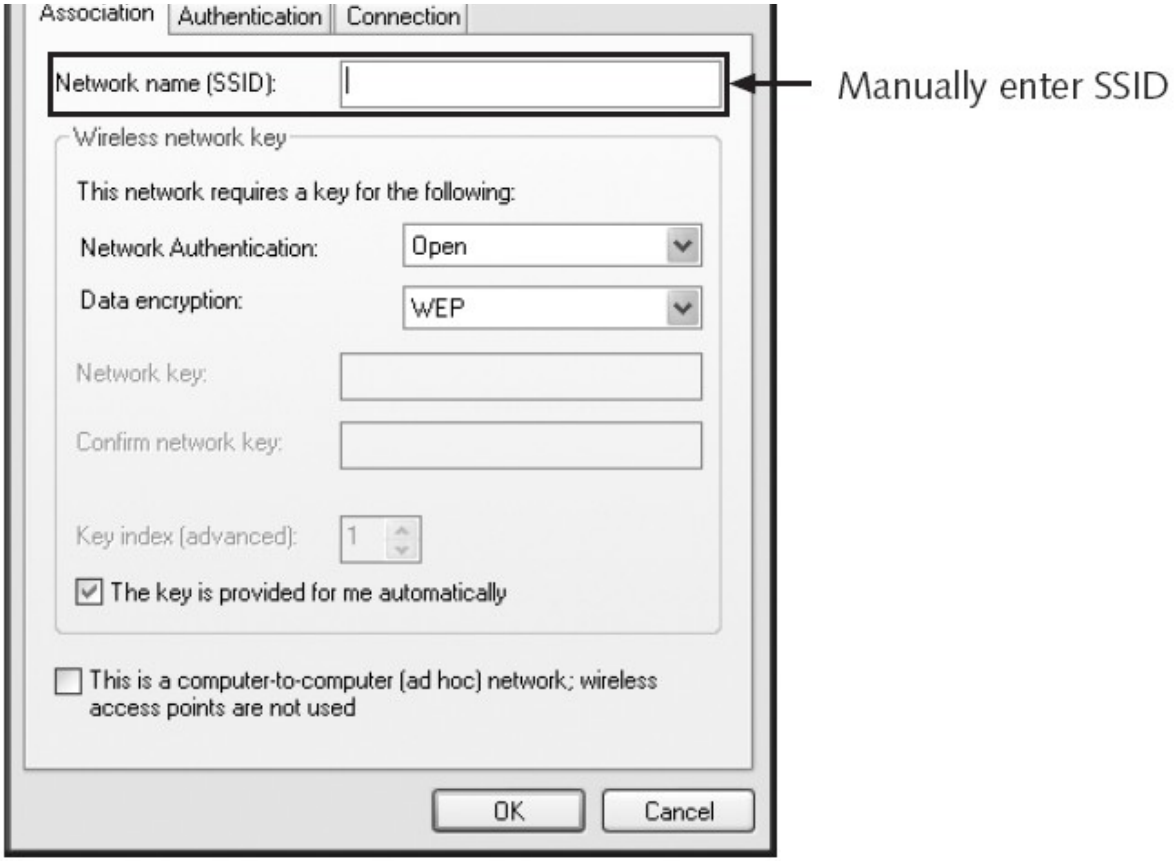


Figure 2-12 Enter SSID

Authentication (continued)

- Open system authentication vulnerabilities (continued)
  - Not always possible or convenient to turn off beaconing the SSID
    - Prevents wireless devices from freely roaming (if turned off)
    - When using Microsoft Windows XP
      - Device will always connect to the AP broadcasting its SSID
    - SSID can be easily discovered even when it is not contained in beacon frames
      - It is transmitted in other management frames sent by the AP

Authentication (continued)

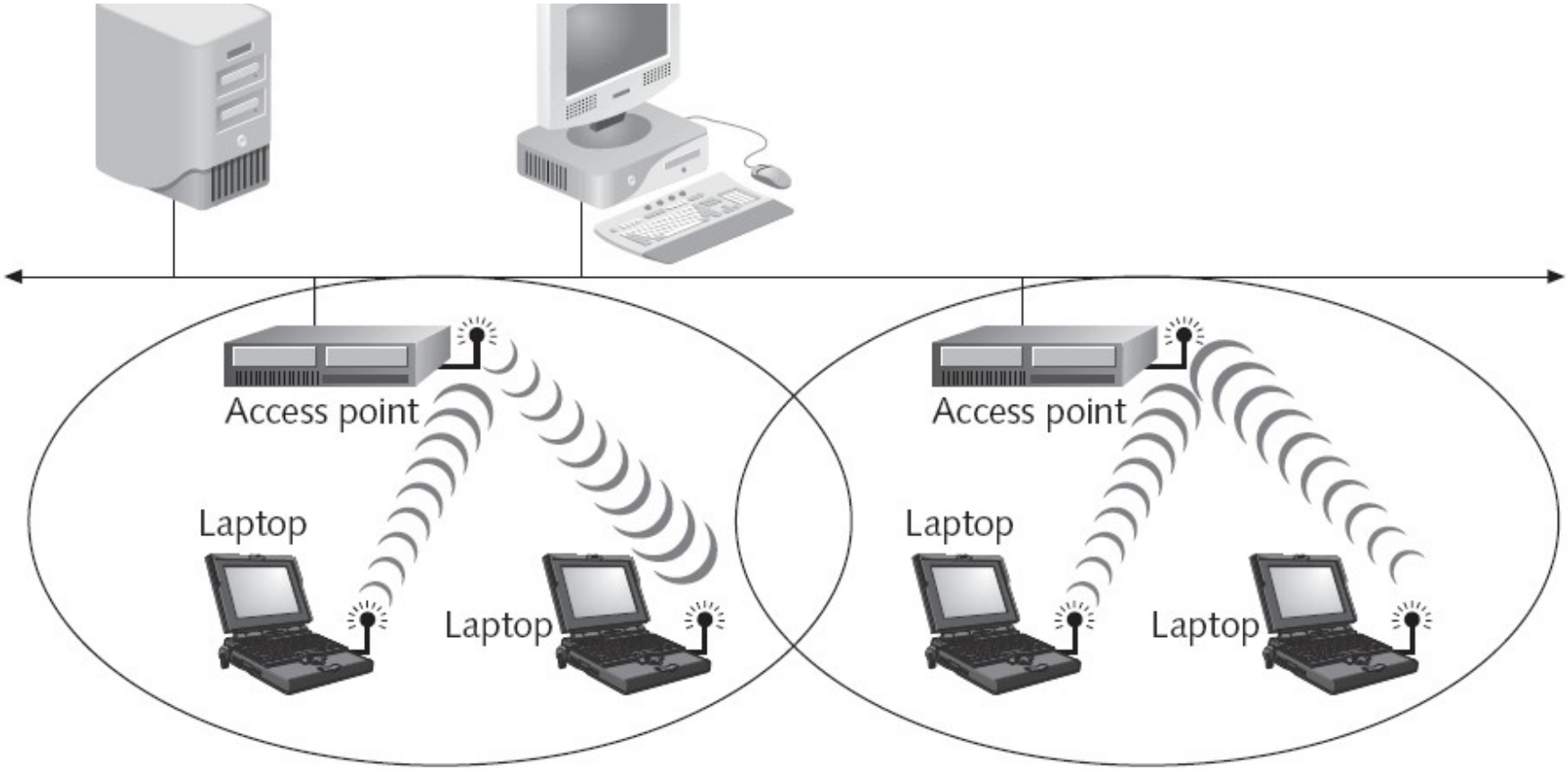


Figure 2-13 Multiple access points in WLAN

Authentication (continued)

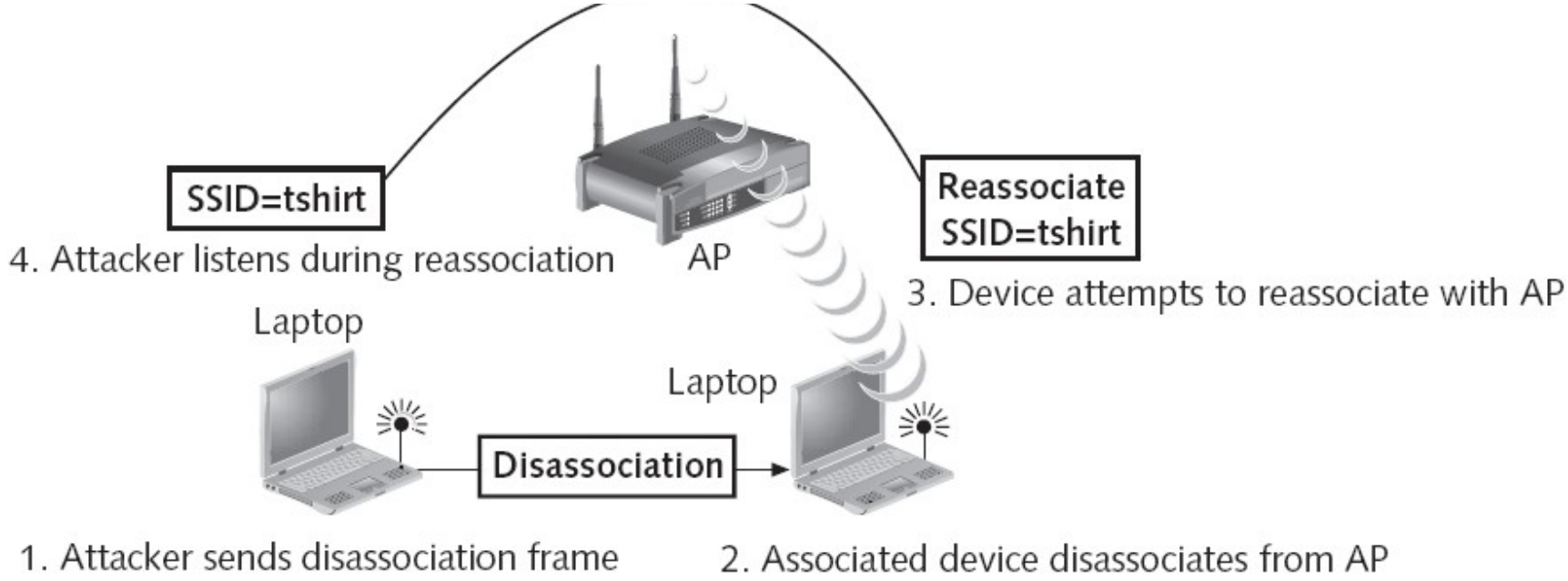


Figure 2-14 Forcing renegotiation

Authentication (continued)

- Shared key authentication vulnerabilities
  - Key management can be very difficult when it must support a large number of wireless devices
    - Attacker can “shoulder surf” the key from an approved device
  - Types of attacks
    - Brute force attack
    - Dictionary attack
  - Attacker can capture the challenge text along with the device’s response (encrypted text and IV)
    - Can then mathematically derive the keystream

Authentication (continued)

Authentication Type	Attack Technique	Description
Open system authentication	View SSID	Look at SSID on authenticated device
Open system authentication	Accept SSID	Receive SSID from passive scanning
Open system authentication	Steal SSID	View plaintext SSID during negotiation phase with AP or force renegotiation
Shared key authentication	View SSID	Steal a device or shoulder surf
Shared key authentication	Brute force attack	Break default key by attempting combinations
Shared key authentication	Dictionary attack	Break default key by using dictionary words
Shared key authentication	Steal challenge text and encrypted text	Use challenge text and encrypted text to mathematically derive keystream

Address Filtering

- Managing a larger number of MAC addresses can pose significant challenges
  - Does not provide a means to temporarily allow a guest user to access the network
  - MAC addresses are initially exchanged in plaintext
    - Attacker can easily see the MAC address of an approved device and use it
  - MAC address can be “spoofed” or substituted

Address Filtering (continued)

Table 2-2 MAC address attacks

Attack Technique	Description
Key management	Take advantage of difficulty in managing large number of MAC addresses
Steal MAC address	Access MAC address as exchanged in plaintext
Spoof MAC address	Substitute approved MAC address on wireless device

WEP

- Vulnerabilities are based on how WEP and the RC4 cipher are implemented
- WEP can use a 64-bit or 128-bit encryption key
  - 24-bit initialization vector (IV) and a 40-bit or 104-bit default key
  - Relatively short length of the default key limits its strength
- Implementation of WEP creates a detectable pattern for attackers
  - IVs are 24-bit numbers
  - IVs would start repeating in fewer than seven hours

WEP (continued)

- Implementation of WEP creates a detectable pattern for attackers (continued)
  - Some wireless systems always start with the same IV
- Collision
  - Two packets encrypted using the same IV
- Keystream attack
  - Determines the keystream by analyzing two colliding packets

WEP (continued)

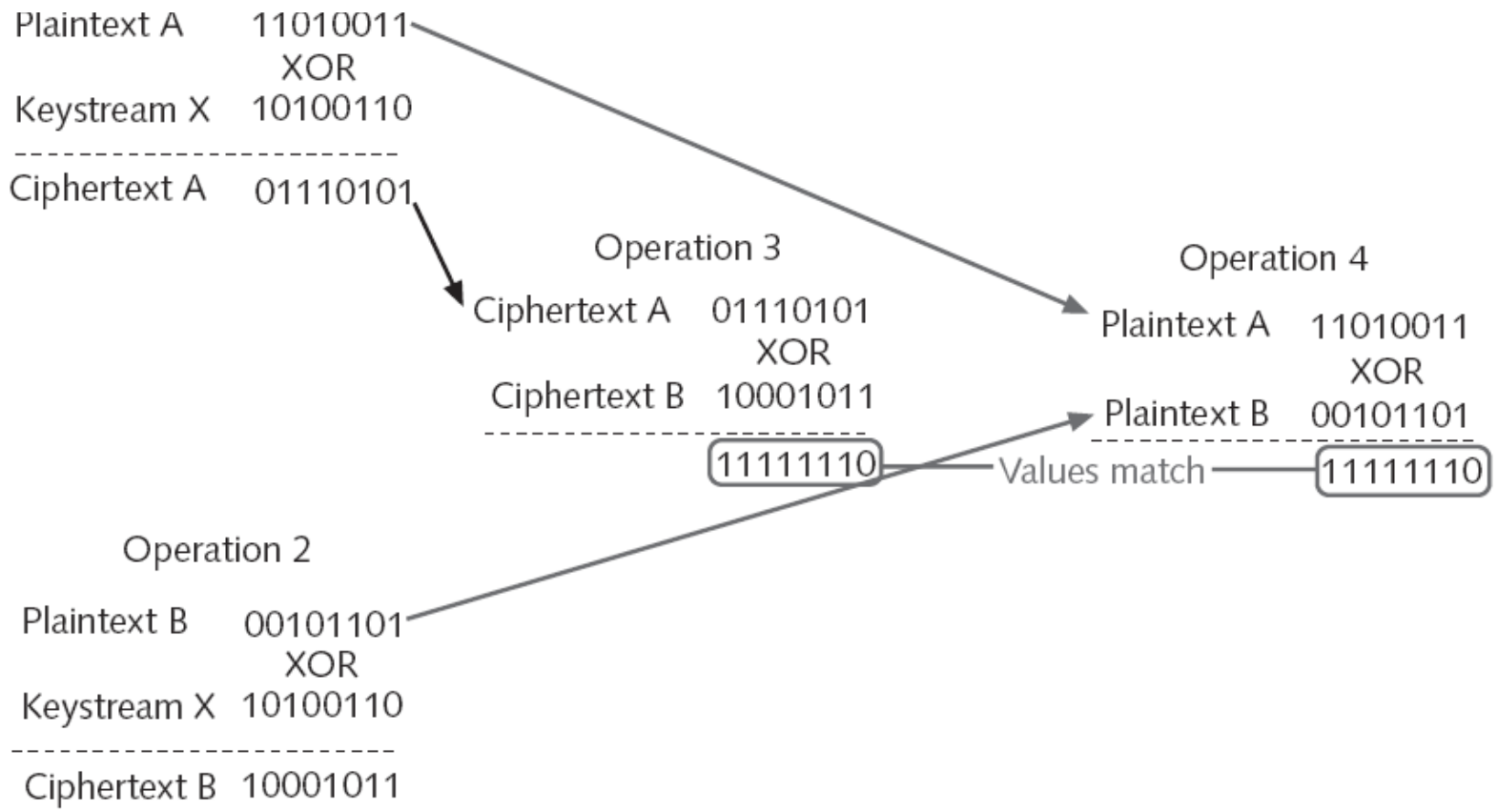


Figure 2-15 XOR operations

WEP (continued)

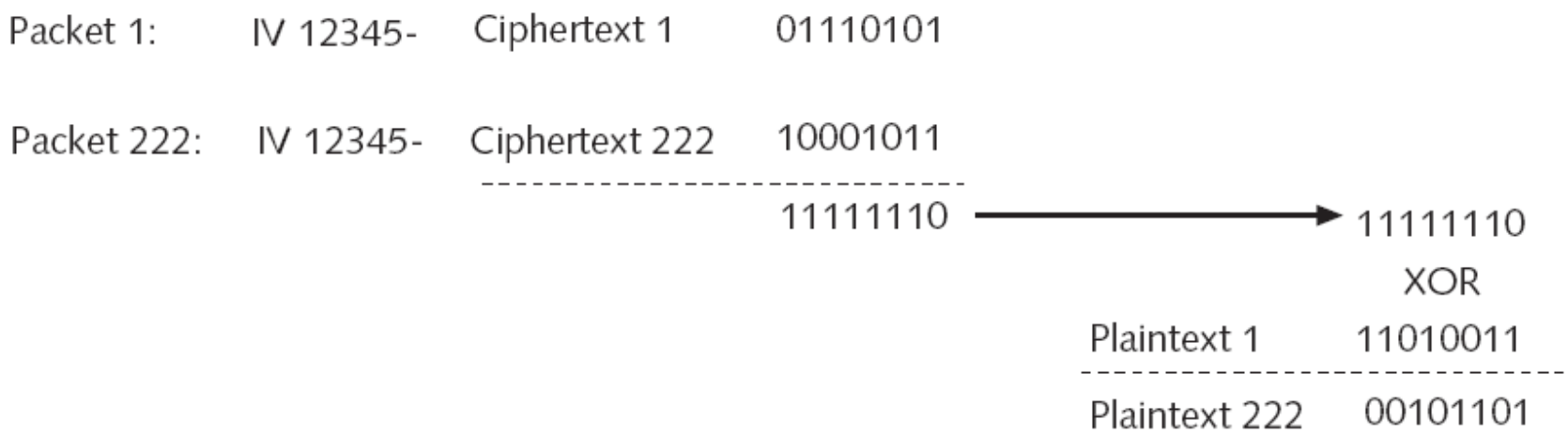


Figure 2-16 Capturing packets

WEP (continued)

- RC4 issues
  - RC4 uses a pseudo random number generator (PRNG) to create the keystream
    - PRNG does not create a true random number
  - First 256 bytes of the RC4 cipher can be determined
    - By bytes in the key itself
  - RC4 source code (or a derivation) has been revealed
    - Attackers can see how the keystream itself is generated
- RC4 discussed in next slide

The key-scheduling algorithm (KSA)

```
i := 0
 j := 0
 '"while"' GeneratingOutput:
     i := (i + 1) mod 256
     j := (j + S[i]) mod 256
     swap values of S[i] and S[j]
     K := S[(S[i] + S[j]) mod 256]
     output K
 '"endwhile"'
```

The pseudo-random generation algorithm (PRGA)

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap values of S[i] and S[j]
    K := S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

WEP (continued)

- WEP attack tools
  - AirSnort, Aircrack, ChopChop WEP Cracker, and WEP Crack

WEP (continued)

Table 2-3 WEP attacks

Attack Technique	Description
Weak key	WEP default keys are shortened to 40 or 104 bits and make it easier for attackers to break
Keystream	View collisions to derive plaintext values
RC4 pseudo random number	RC4 generates weak keys

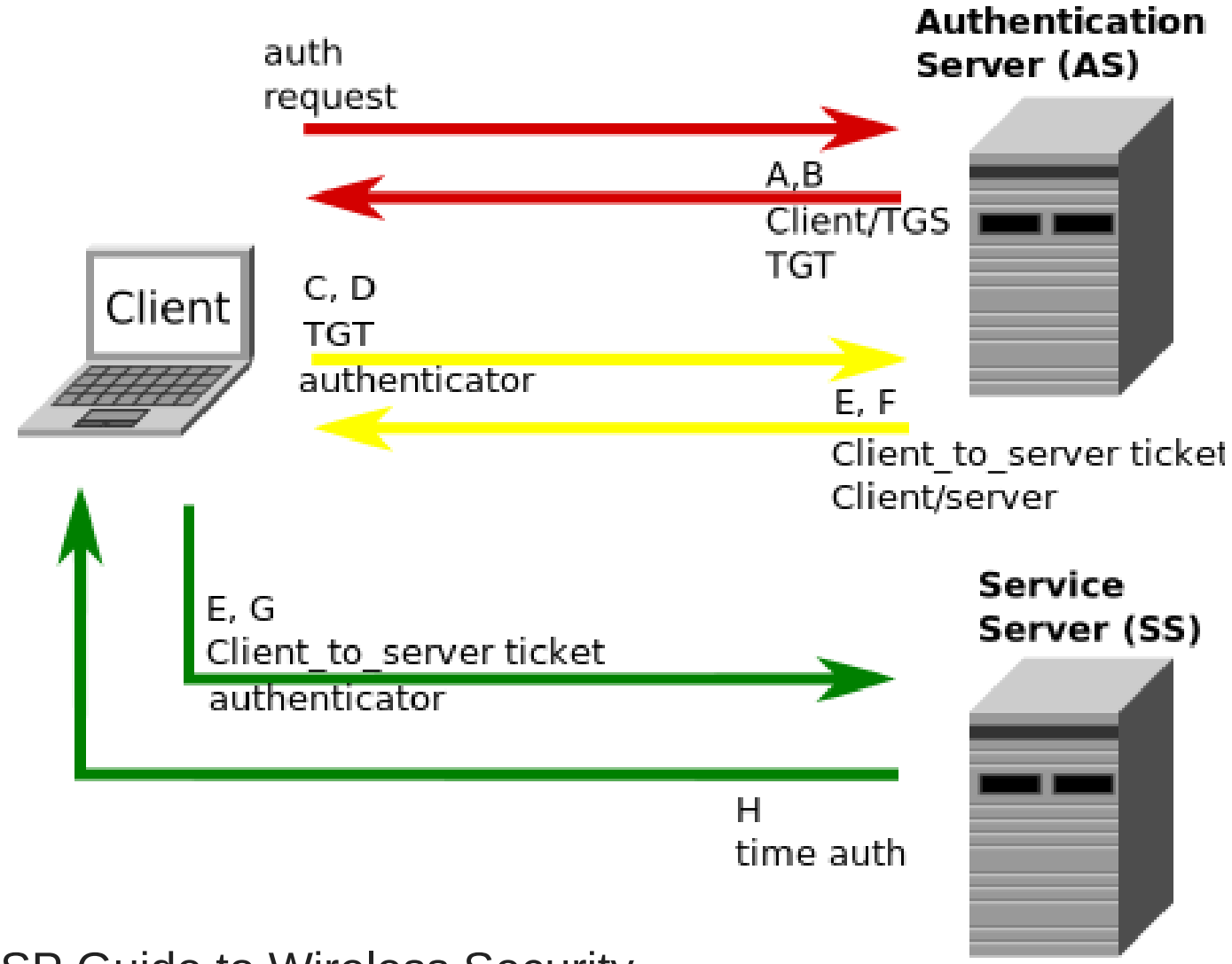
WEP2

- Attempted to overcome the limitations of WEP by adding two new security enhancements
  - Shared secret key was increased to 128 bits
    - To address the weakness of encryption
  - Kerberos authentication system was used
- Kerberos
  - Developed by Massachusetts Institute of Technology
  - Used to verify the identity of network users
  - Based on tickets
- WEP2 was no more secure than WEP itself

Dynamic WEP

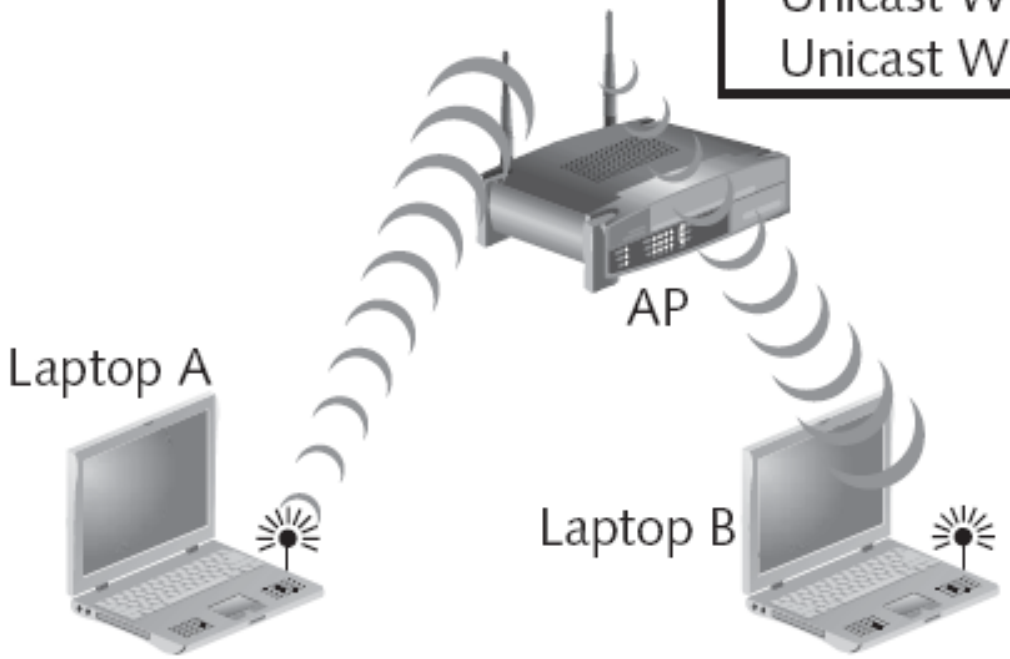
- Solves the weak initialization vector (IV) problem
  - By rotating the keys frequently
- Uses different keys for unicast traffic and broadcast traffic
- Advantage
  - Can be implemented without upgrading device drivers or AP firmware
  - Deploying dynamic WEP is a no-cost solution with minimal effort
- Dynamic WEP is still only a partial solution

Kerberos


Authentication Server (AS)
auth request
A,B
Client/TGS TGT
Client
C, D
TGT
authenticator
E, F
Client_to_server ticket
Client/server
E, G
Client_to_server ticket
authenticator
Service Server (SS)
H
time auth

Dynamic WEP (continued)

Laptop A	
Unicast WEP Key 98siKjfud&	3:30–4:00
Unicast WEP Key 234TgdbYuw	4:00–4:30
Laptop B	
Unicast WEP Key 8uji98s7af	3:30–4:00
Unicast WEP Key nb&67jsMni	4:00–4:30



Key 1wa3sedazs	
y 98siKjfud&	3:30–4:00

Broadcast WEP Key 1wa3sedazs	
Unicast WEP Key 8uji98s7af	3:30–4:00

Quick Quiz 2

1. At regular intervals (normally every 100 ms) the AP sends a(n) _____ frame to announce its presence and to provide the necessary information for other devices that want to join the network.

2. A(n) _____ is a method of determining the keystream by analyzing two packets that were created from the same IV.

3. _____ was developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of network users.

4. _____ traffic is traffic destined for only one address.

Summary

- It was important that basic wireless security protections be built into WLANs
- Protection categories: access control, WEP, and authentication
- Wireless access control is accomplished by limiting a device's access to the AP
- WEP is intended to ensure that only authorized parties can view the information
- Wireless authentication requires the wireless device to be authenticated prior to connection to the network

Summary (continued)

- Security vulnerabilities exposed wireless networking to a variety of attacks
- WEP implementation violates the cardinal rule of cryptography
  - Avoid anything that creates a detectable pattern
- WEP2 and dynamic WEP were both designed to overcome the weaknesses of WEP
  - Each proved to have its own limitations
  - They were never widely implemented

Quiz

1. _____ is defined as a method of restricting access to resources.

2. _____ is the science of transforming information so that it is secure while it is being transmitted or stored.

3. An encryption algorithm is known as a(n) _____.

4. The IEEE standard also specifies that the access points and devices can hold up to four shared secret keys, one of which must be designated as the _____.

Quiz

5. At regular intervals (normally every 100 ms) the AP sends a(n) _____ frame to announce its presence and to provide the necessary information for other devices that want to join the network.

6. A(n) _____ is a method of determining the keystream by analyzing two packets that were created from the same IV.

Quiz

7. _____ was developed by the Massachusetts Institute of Technology (MIT) and used to verify the identity of network users.

8. _____ traffic is traffic destined for only one address.