CWSP Guide to Wireless Security

Enterprise Wireless Hardware Security

Objectives

- List and describe the functions of the different types of wireless LAN hardware used in an enterprise
- Tell how access control and protocol filtering can protect a WLAN
- Describe the functions of Quality of Service, handoffs, and power features of wireless networking hardware

Enterprise WLAN Hardware

- Wireless hardware
  - Access points
  - Remote wireless bridges
  - Wireless routers
  - Wireless gateways
  - Wireless switches
  - Wireless mesh routers

Access Point

- AP parts
  - An antenna and a radio transmitter/receiver to send and receive signals
  - An RJ-45 wired network interface that allows it to connect by cable to a standard wired network
  - Special bridging software to interface wireless devices to other devices
- Basic functions
  - Acts as the base station for the wireless network
  - Acts as a bridge between wireless and wired network

Access Point (continued)

- Range of an access point depends on:
  - Type of wireless network that is supported
  - Walls, doors, and other solid objects can reduce the distance the signal may travel
- Number of wireless clients supported varies
  - Theoretical: 100 clients
  - For light traffic: 50 clients
  - For heavy traffic: 20 clients

Remote Wireless Bridge

- Bridge
  - Connects two network segments together
  - Segments can use different types of physical media
  - Software for transmitting and receiving signals
- Remote wireless bridge
  - Wireless device designed to connect two or more wired or wireless networks
  - Transmits at higher power than APs
  - Uses a highly directional or semi-directional antenna

Remote Wireless Bridge (continued)

- Highly directional antennas
  - Usually concave, dish-shaped devices used for long distance, point-to-point wireless links
- Semi-directional antenna
  - Focuses the energy in one direction
  - Does not have the high power level of a highly directional antenna
  - Primarily used for short- and medium-range remote wireless bridge networks

Remote Wireless Bridge (continued)

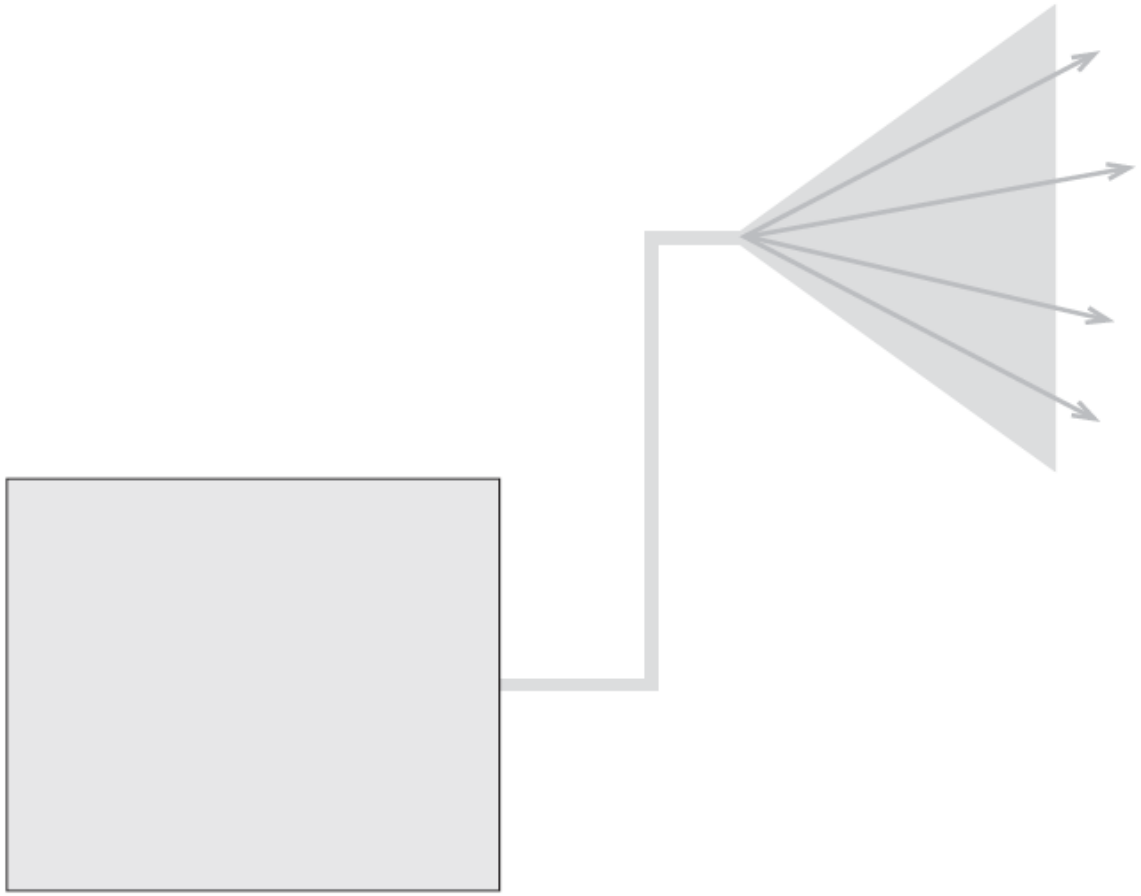

Figure 6-1 Semi-directional antenna pattern

Remote Wireless Bridge (continued)

- Delay spread
  - Minimizes the spread of the signal so that it can reach farther distances
- Remote wireless bridges support two types of connections
  - Point-to-point connections
  - Point-to-multipoint connections

Remote Wireless Bridge (continued)

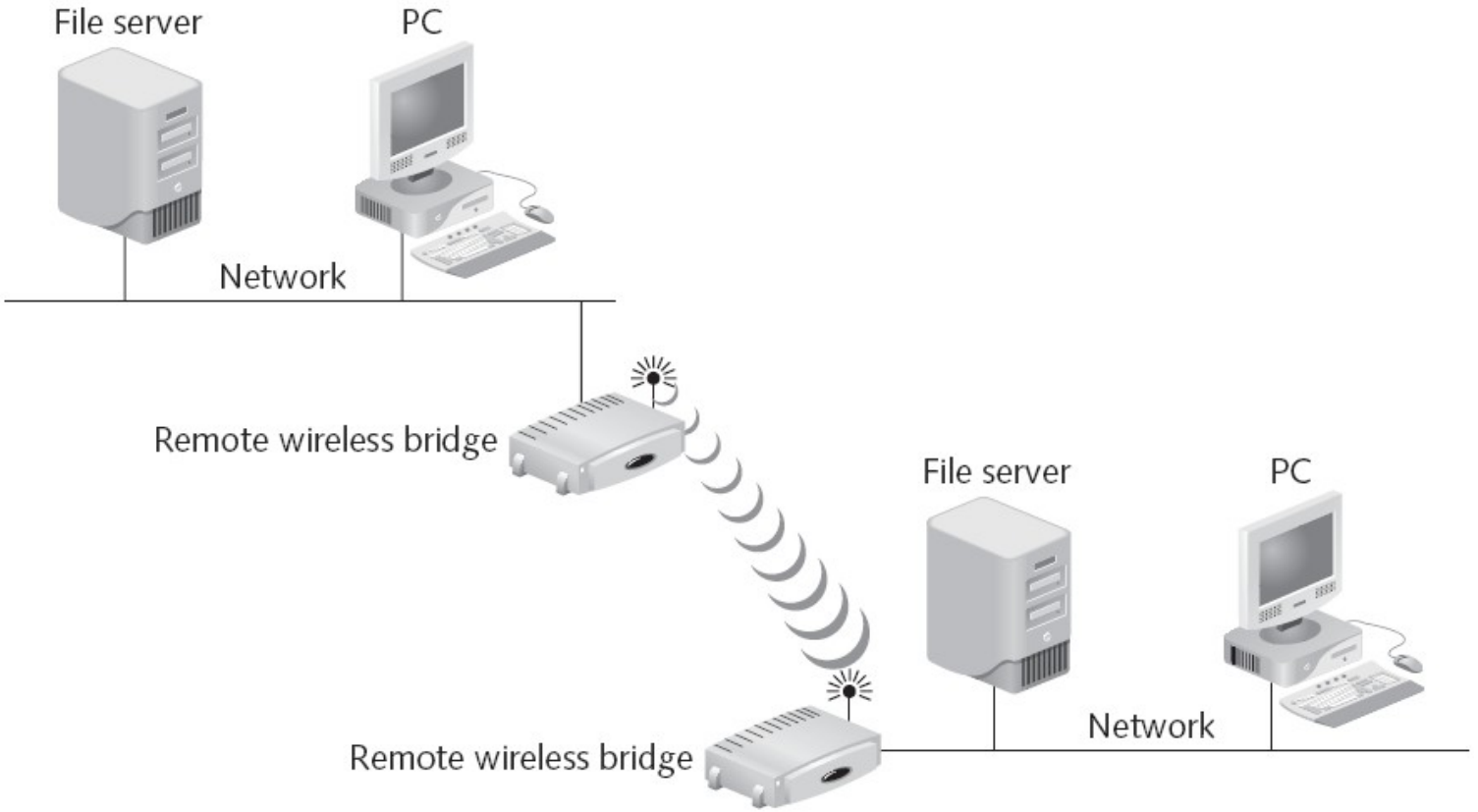

Figure 6-2 Point-to-point remote wireless bridge

Remote Wireless Bridge (continued)

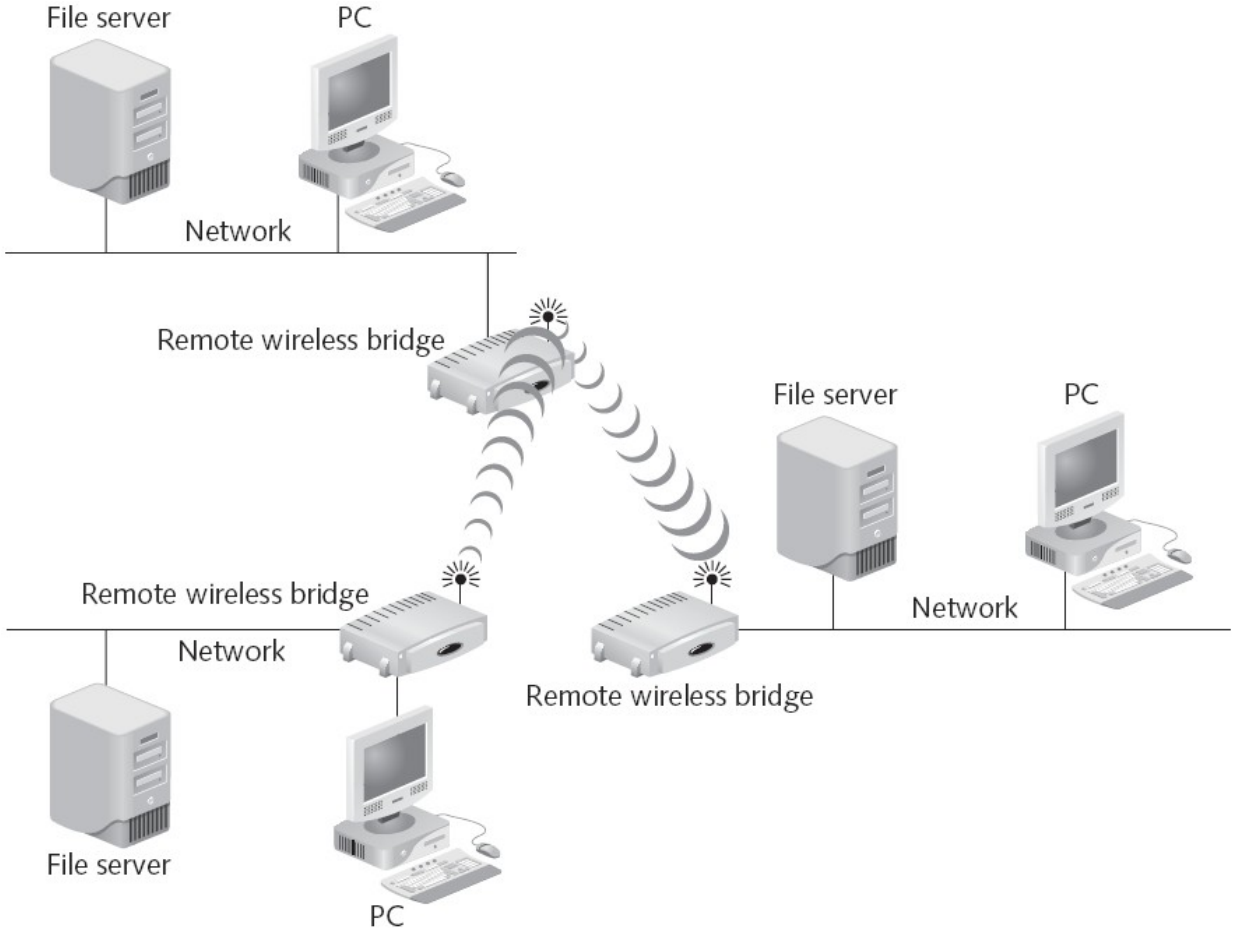

Figure 6-3 Point-to-multipoint remote wireless bridge

Remote Wireless Bridge (continued)

- Remote wireless bridge modes
  - Access point mode
    - Standard AP
  - Root mode
    - Acts as a root bridge and can communicate only with other non-root bridges
  - Non-root mode
    - Can transmit only to a root bridge
  - Repeater mode
    - Extends the distance between LAN segments

Remote Wireless Bridge (continued)

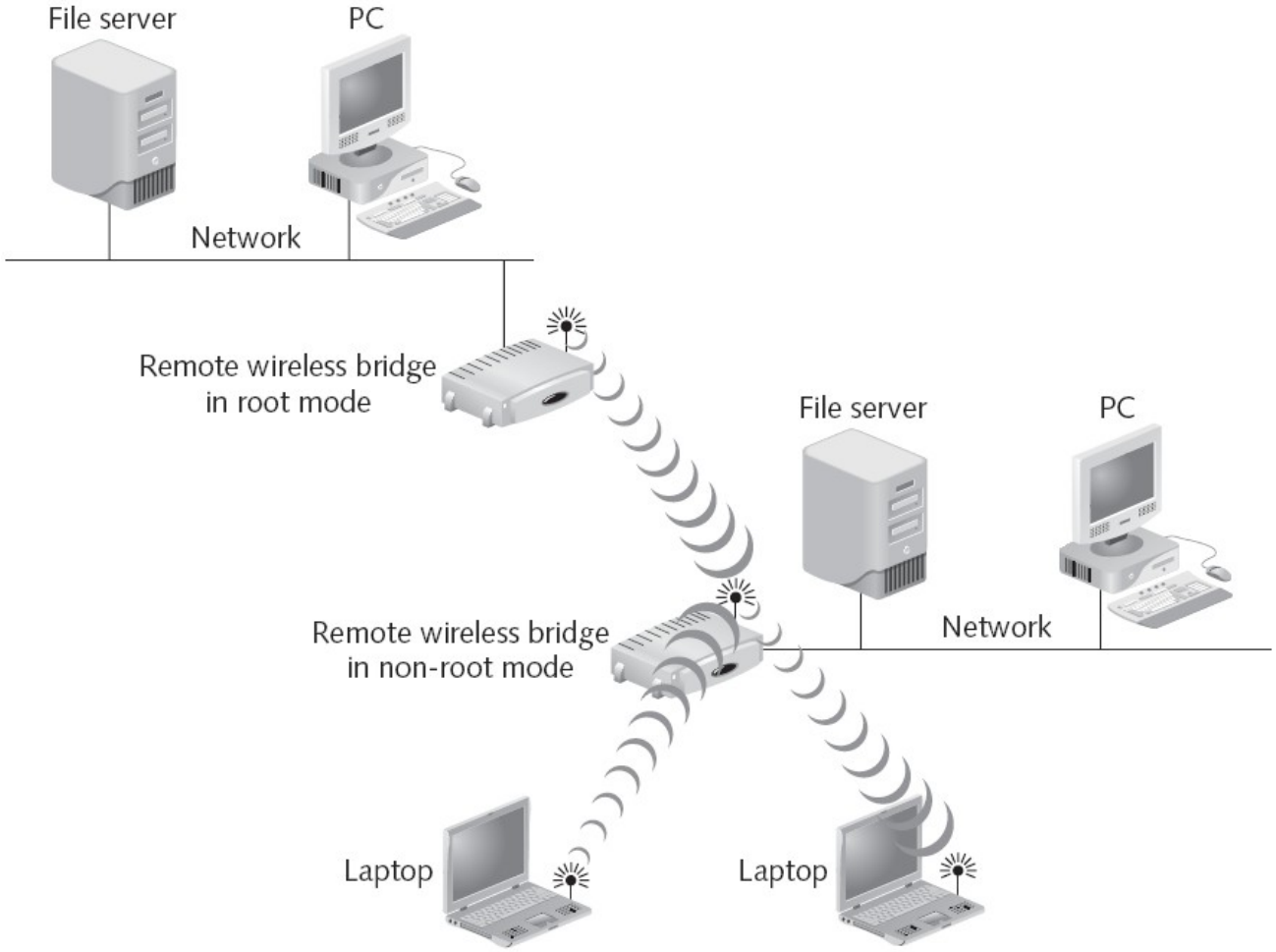

Figure 6-4 Root mode and non-root modes

Remote Wireless Bridge (continued)

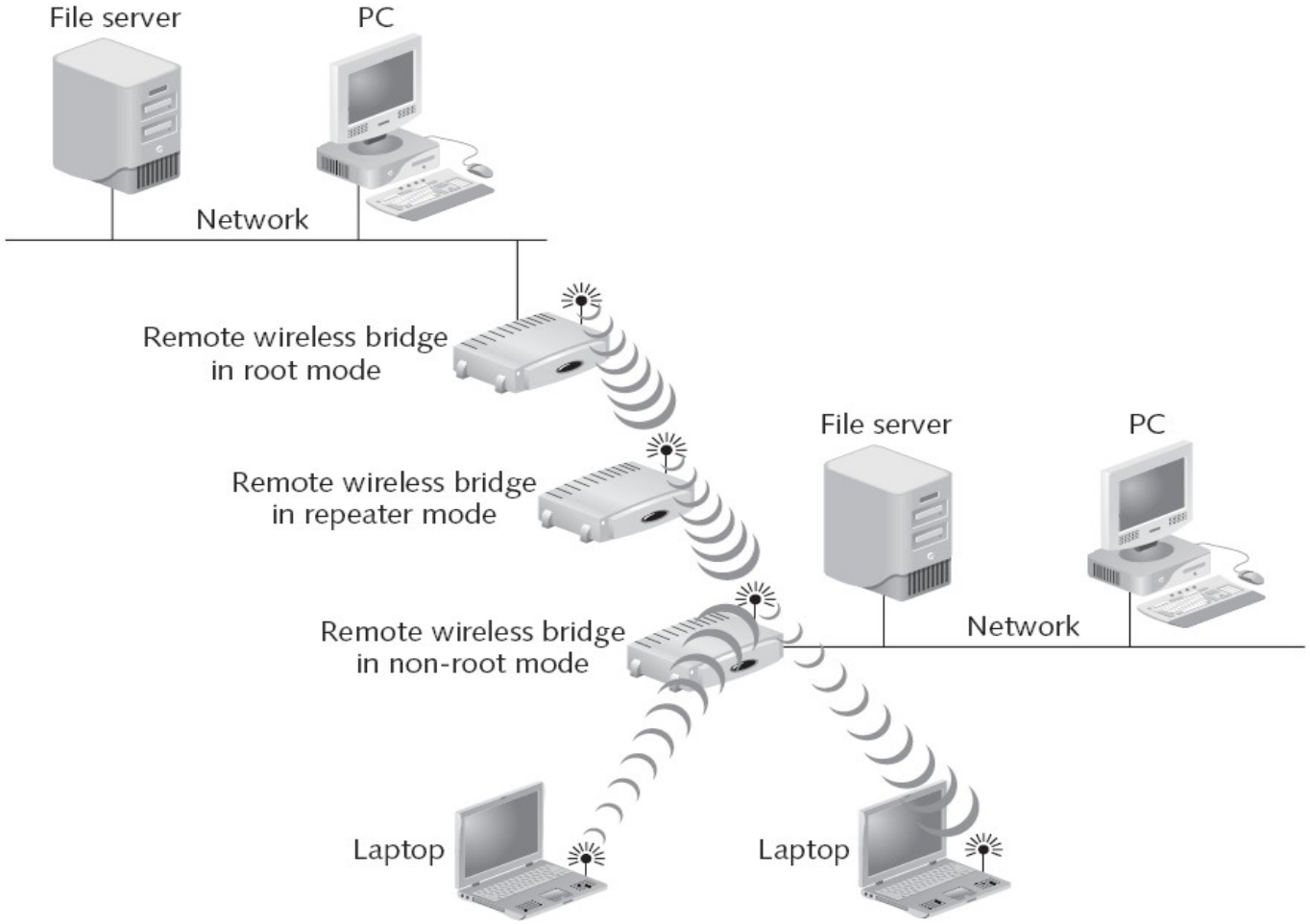

Figure 6-5 Repeater mode

Remote Wireless Bridge (continued)

- Remote wireless bridges
  - Cost-effective alternative to expensive leased wired options for connecting remote buildings
  - Distance can be up to 29 kilometers (18 miles) transmitting at 11 Mbps
    - Or up to 40 kilometers (25 miles) transmitting at 2 Mbps

Wireless Router

- Router
  - Transfers packets between networks
  - Selects the best link (route) to send packets
- Wireless router
  - Combines an access point with a router
  - Typically with multiple ports
- Advantages
  - Connects multiple networks
  - Improves network performance
  - Shares single IP address

Wireless Router (continued)

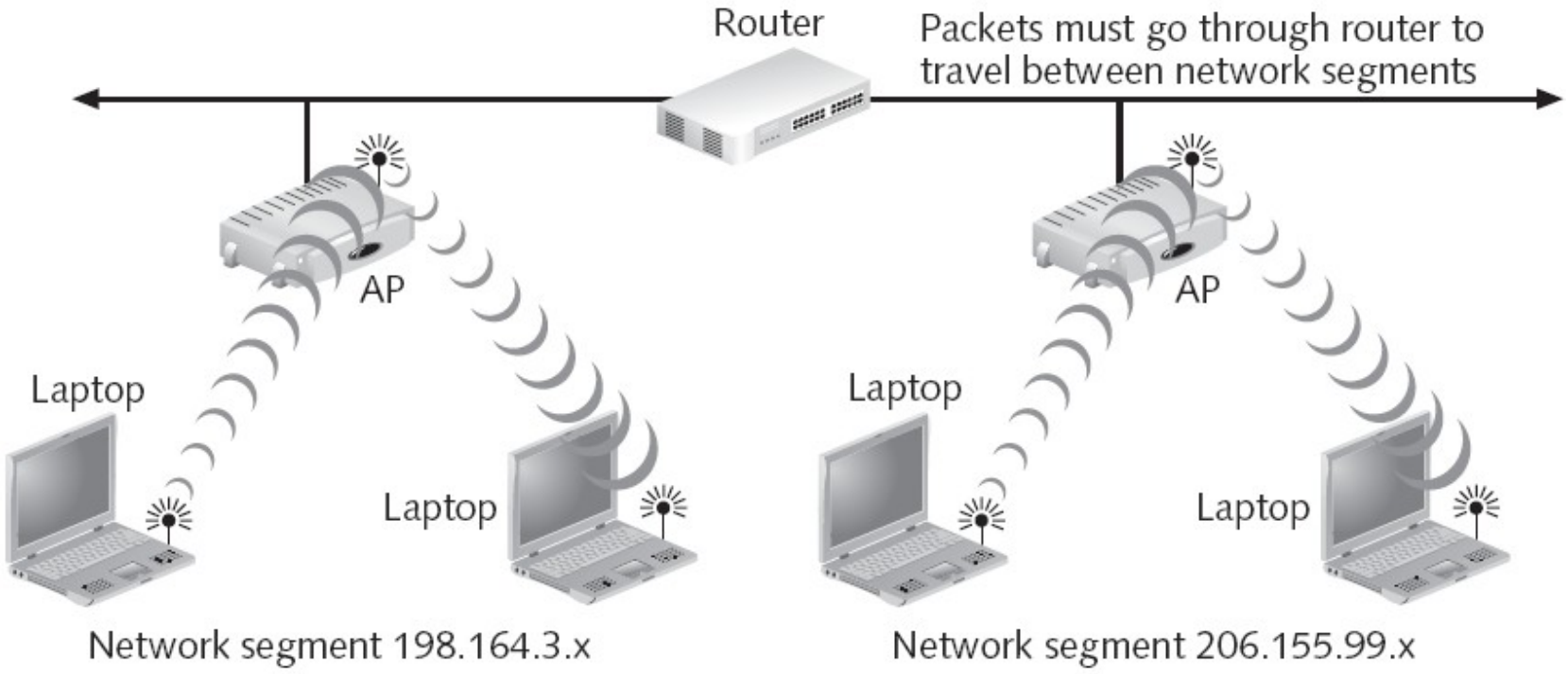

Figure 6-6 Passing packets through a router

Wireless Router (continued)

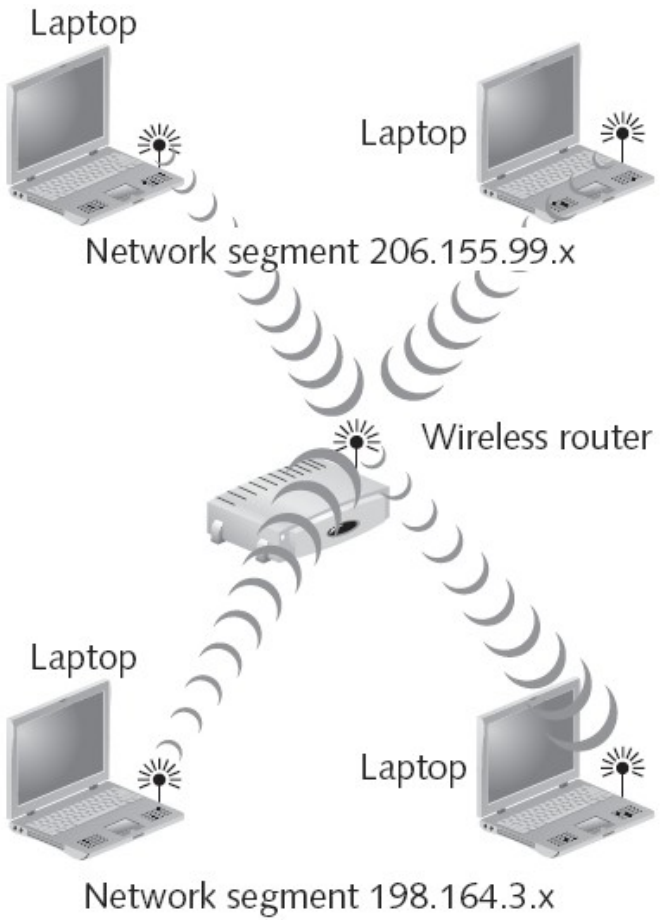

Figure 6-7 Multiple segments connected to a wireless router

Wireless Gateway

- Gateway
  - Acts as an entrance to another network
- Wireless gateway
  - Combines an access point, router, network address translation, and other networking features
- Enterprise wireless gateway functions
  - Authentication
  - Encryption
  - Intrusion detection and malicious program protection
  - Bandwidth management
  - Centralized network management

Wireless Switch

- Switch
  - Joins multiple computers within one LAN
  - Contains more “intelligence” than a hub

- One of the challenges of a wireless LAN in an enterprise setting
  - Integrates management of wired and wireless networks

Wireless Switch (continued)

- Wireless switch
  - Often a rack-mounted unit
  - Performs user authentication and encryption

- Thin access point (used when authentication is done by switch, instead of regular AP)
  - Simplified radios with a media converter for the wired network

Wireless Switch (continued)

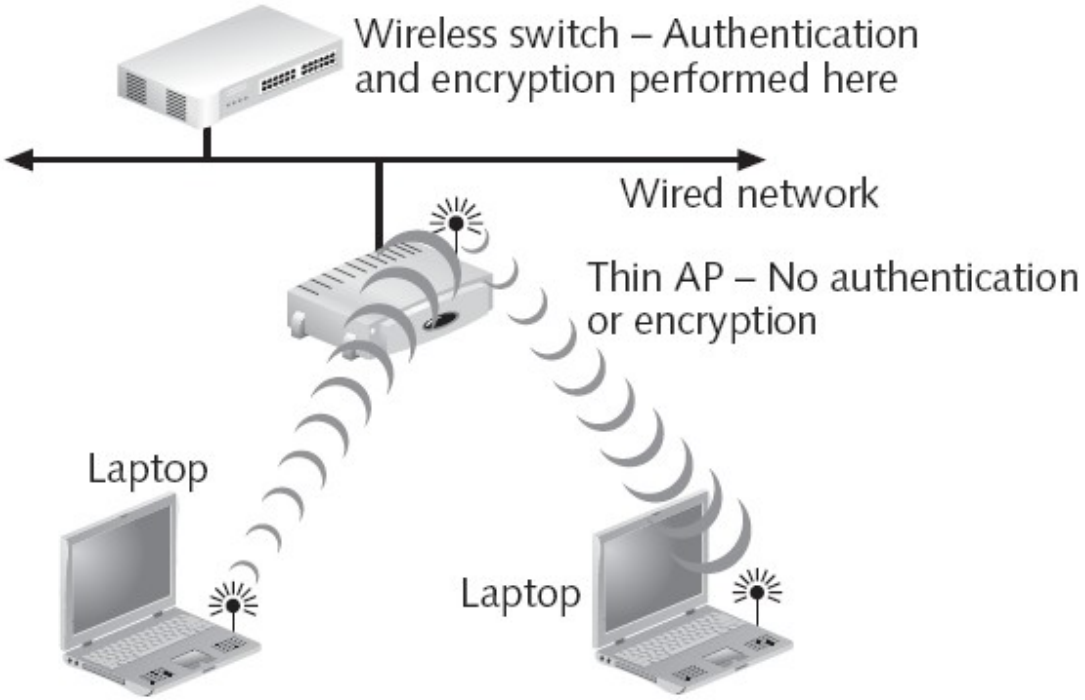

Figure 6-8 Wireless switch and thin access point

Wireless Switch (continued)

- Advantages
  - Simplified wireless network management
  - Eliminates handoff procedures
- Disadvantages
  - All thin APs and wireless switches are proprietary
  - Thin APs do not provide true convergence of the wired and wireless networks

Wireless Switch (continued)

- IEEE 802.1v protocol
  - Assists the management of WLAN devices via protocol features:
  - Load balancing
  - Automatic configuration
  - Preserves battery life

Wireless Mesh Routers

- Limitations of connecting APs to a router via the wired network
  - Placement of APs is limited
  - APs have a limited range
- Mesh networks
  - Solve these limitations
  - Provide multiple paths through which data can travel
  - Best example: the Internet
- Wireless mesh network
  - Allows for multiple paths for wireless transmissions

Wireless Mesh Routers (continued)

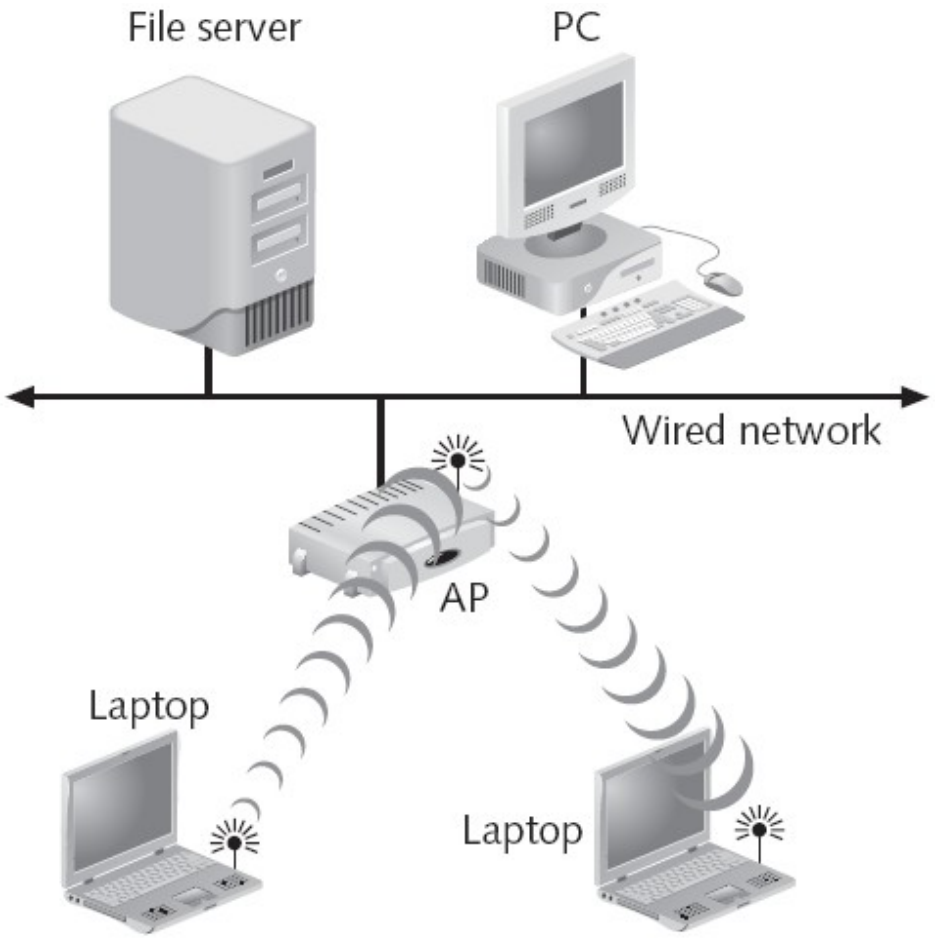

Figure 6-9 Single path for data between devices

Wireless Mesh Routers (continued)

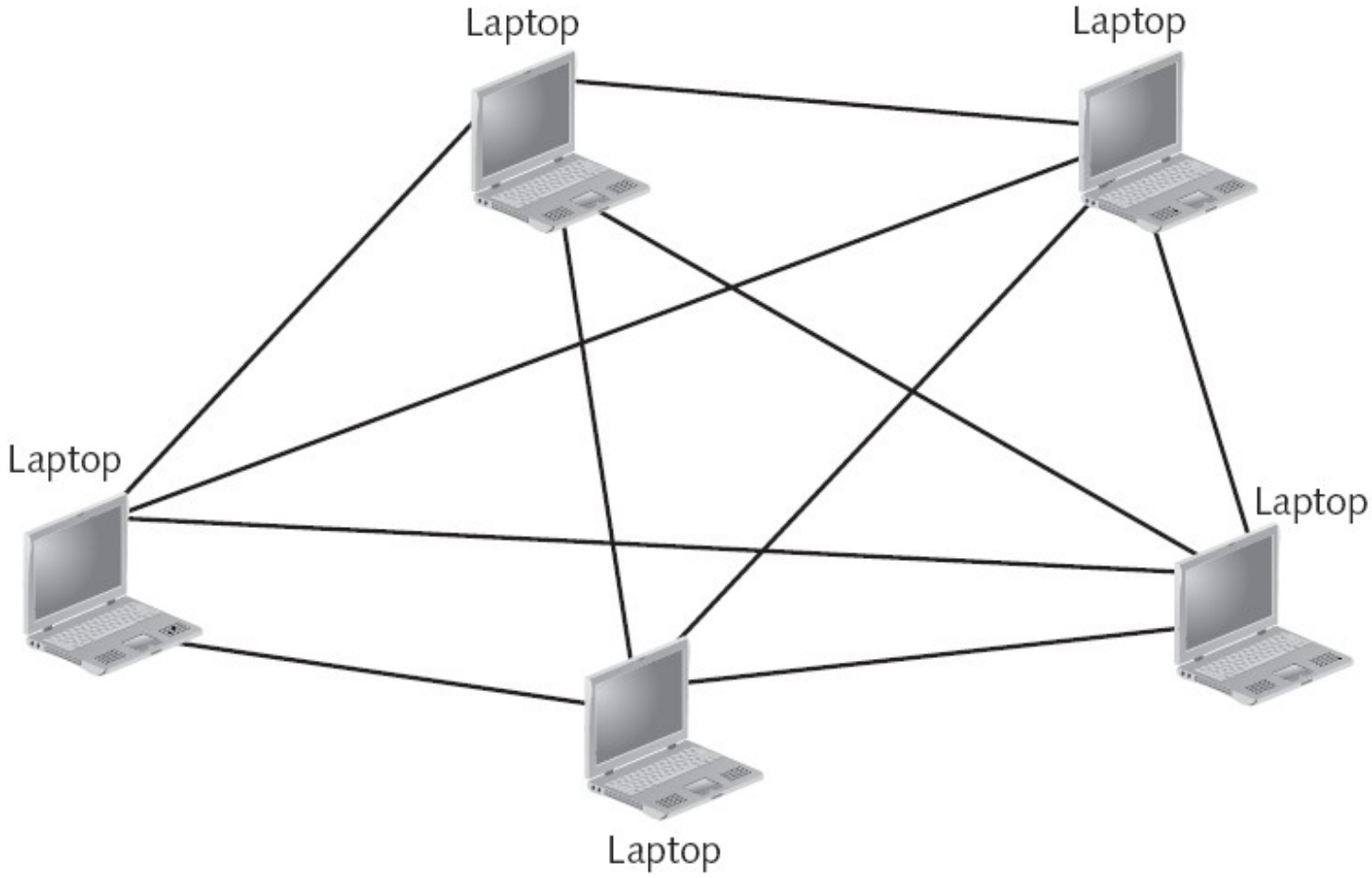

Figure 6-10 Multiple data paths

Wireless Mesh Routers (continued)

- Wireless mesh network types
  - Ad hoc wireless mesh network
    - Allows greater distances away from the access point
    - Each client device can act as a relay station for signals
    - Advantages
      - Decentralized network
      - Can decrease costs
      - Can also be reliable

Wireless Mesh Routers (continued)

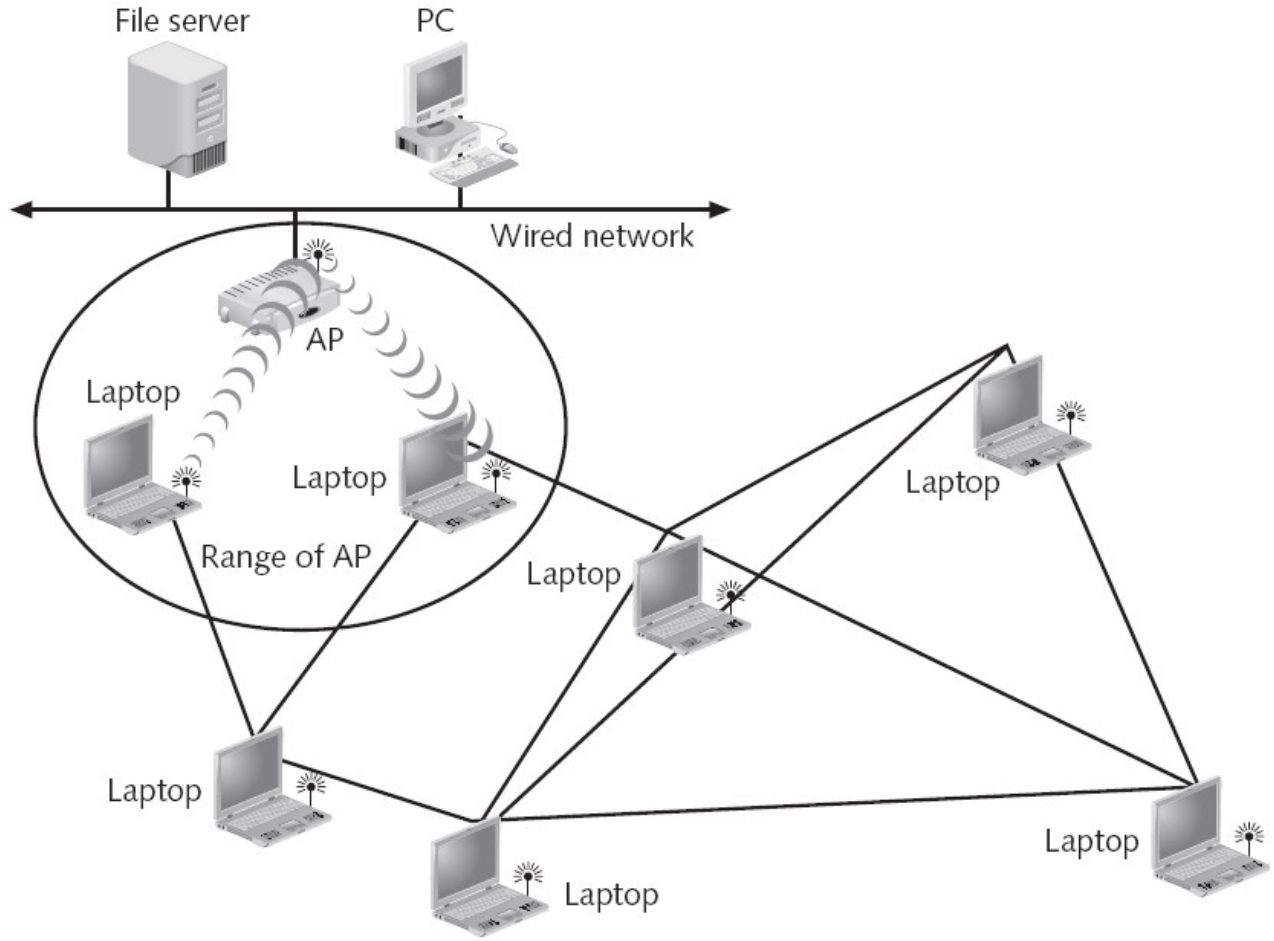

Figure 6-11 Ad hoc wireless mesh network

Wireless Mesh Routers (continued)

- Wireless mesh network types (continued)
  - Backhaul wireless mesh network
    - Connects special access points, known as wireless mesh routers
      - In a mesh configuration
    - Provides alternative data paths for the “backside” connection to the Internet
    - Backhaul
      - Connection from the routers to the Internet
    - Used extensively in outdoor municipal WLANs
    - Can be quickly deployed in an emergency

Wireless Mesh Routers (continued)

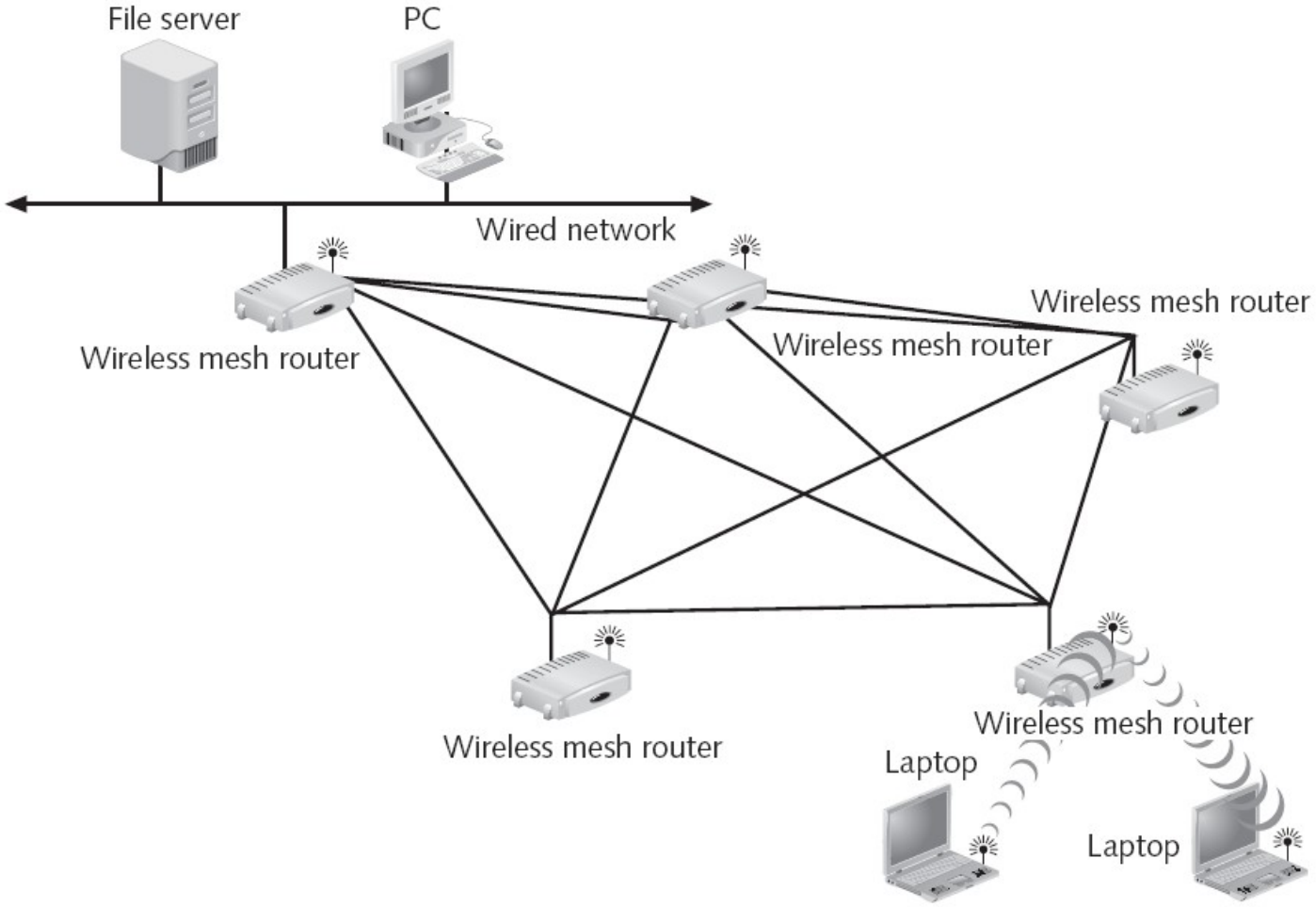

Figure 6-12 Backhaul wireless mesh network

Wireless Mesh Routers (continued)

IEEE 802.11s task group works on standards for mesh networks

- Over 70 different wireless mesh routing protocols
  - Differ in the following features:
    - Algorithm
    - Management data versus transmit data
    - Number of radios

Hardware Security Features

- Features include:
  - Controlling access to hardware
  - Protocol filtering

Controlling Access to Hardware

- Access control
  - Restricts the user to accessing only the resources essential for the user to do his or her job
  - Limits access to resources based on the users' identities and their membership in various groups
- Mandatory access control (MAC)
  - Most restrictive model
  - User is not allowed to give access to another user to use or access anything on the network
  - All controls are fixed in place
  - Typically used in military environments

Controlling Access to Hardware (continued)

- Role based access control (RBAC)
  - Administrator assigns permissions to a position (role)
    - Assign users and other objects to that role
- Discretionary access control (DAC)
  - Least restrictive model
  - User can adjust the permissions for other users over network devices
  - Poses risks in that incorrect permissions may be granted or given

Controlling Access to Hardware (continued)

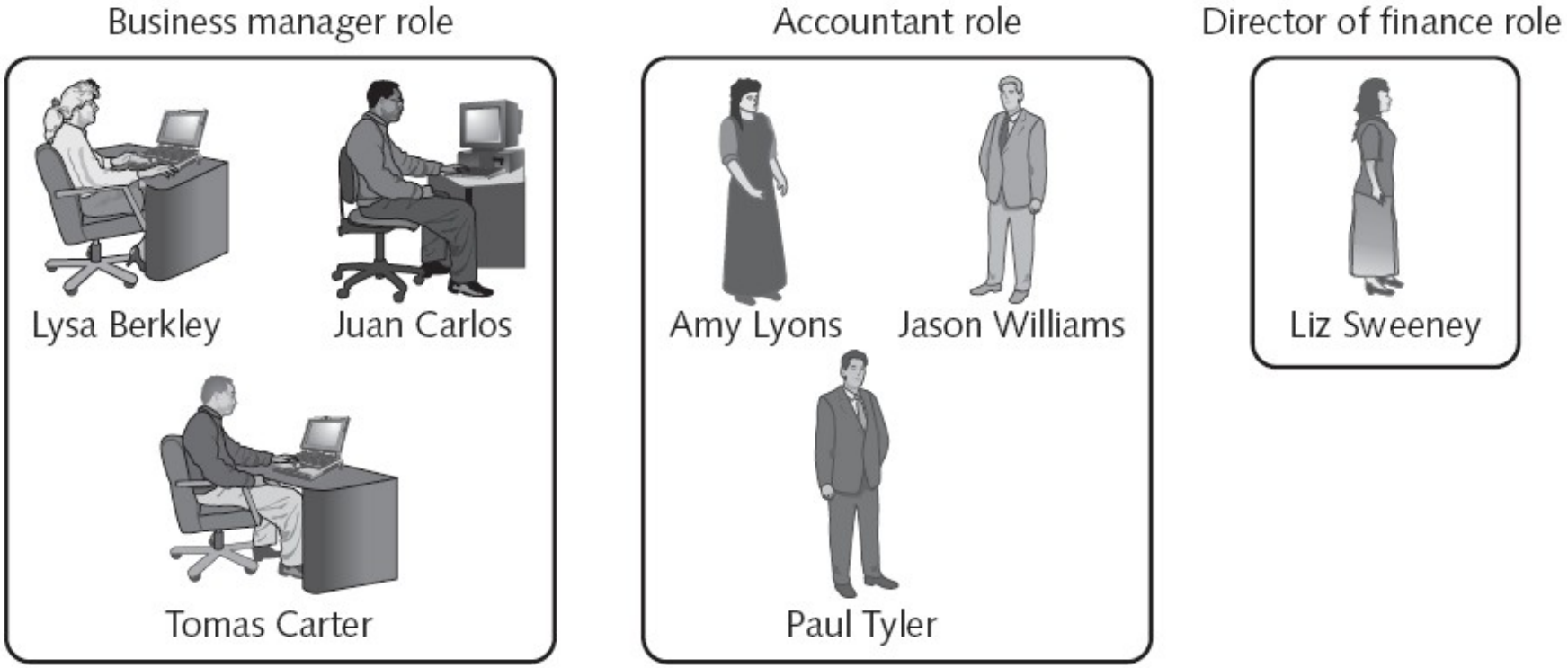

Figure 6-13 Role based access control (RBAC)

Protocol Filtering

- Filtering restricts the traffic on a network based on specific criteria
- Types of filtering
  - Address filtering
  - Data filtering
  - Protocol filtering
- Some access points can be configured to filter unwanted protocols
  - From either entering or leaving the wireless network

Protocol Filtering (continued)



Figure 6-14 Limited protocol filtering

Handoffs

- Inter-Access Point Protocol (IAPP) (IEEE 802.11F)
  - 802.11 standard did not specify how communications were to take place between access points
  - 802.11F specified information that access points need to exchange to support WLAN roaming
- Fast Handoff (IEEE 802.11r)
  - VoWLAN mobile phones need fast handoff
  - Allows a wireless client to determine the QoS (and security) being used at a different AP
    - Before making the transition

Summary

- Wireless hardware
  - Access points
  - Remote wireless bridges
  - Wireless routers
  - Wireless gateways
  - Wireless switches
  - Wireless mesh routers
- Access control limits access to resources
  - Based on the users' identities and membership

Summary (continued)

- Some access points can be configured to filter unwanted protocols