CWNA Guide to Wireless LANs, Third Edition

Chapter 2: Wireless Local Area Networks

Objectives

- Explain the need for and sources of wireless networking standards
- Describe the features of the IEEE 802.11a/b/g/n WLANs
- List the different types of client hardware and software
- Describe the different functions of infrastructure devices

Understanding Standards

- Standards make it easier to purchase and use a wide variety of products

- Wireless technology based on standards
  - Standards help ensure different products from different vendors function in same capacity

The Need for Standards

- Standards for telecommunications have been essential since very beginning
  - Without standards telecommunications would essentially be impossible
- Advantages of standards:
  - Interoperability: ensures devices from one vendor will function with those from other vendors
  - Competition: any vendor can create a device based on a recognized standard and will add additional features to their products to make them more competitive (increases value for users)

The Need for Standards

- Advantages (continued):
  - Lower costs: competition results in lower costs for both users and manufacturers
  - Protection: help create a migration path for equipment upgrades
    - Newer standards are generally backward compatible

Sources of Standards

- *De facto standards (in practice)*: Common practices that the industry follows for various reasons
  - Ranging from ease of use to tradition to what majority of users do
  - Usually established by success in marketplace
- *De jure standards (in law)*: Official standards
  - Controlled by organization or body that has been entrusted with that task
  - Process for creating these standards can be very involved

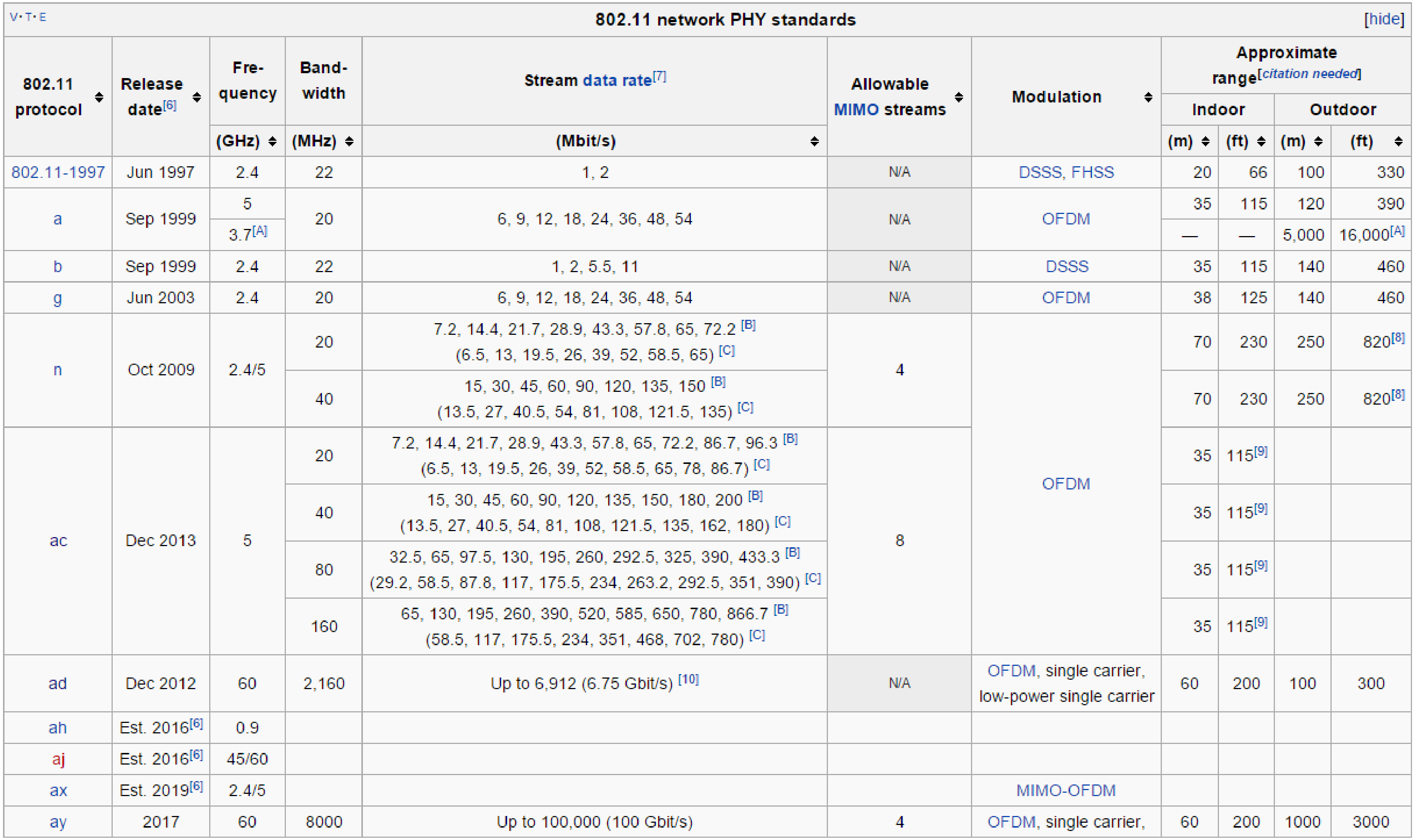
Sources of Standards

- *Consortia-created standards*: Usually industry-sponsored organizations that want to promote a specific technology
  - Goal is to develop a standard that promotes organization’s specific technology in little time

Types of Wireless LANs

- Since late 1990s, IEEE has approved four standards for wireless LANs:
  - IEEE 802.11
  - IEEE 802.11b
  - IEEE 802.11a
  - IEEE 802.11g
- In addition there have been several amendments
  - IEEE 802.11d, IEEE 802.11h, and others
- Currently one LAN standard, IEEE 802.11-2007 and one amendment, IEEE 802.11n-2009

IEEE 802.11



V·T·E 802.11 network PHY standards [hide]

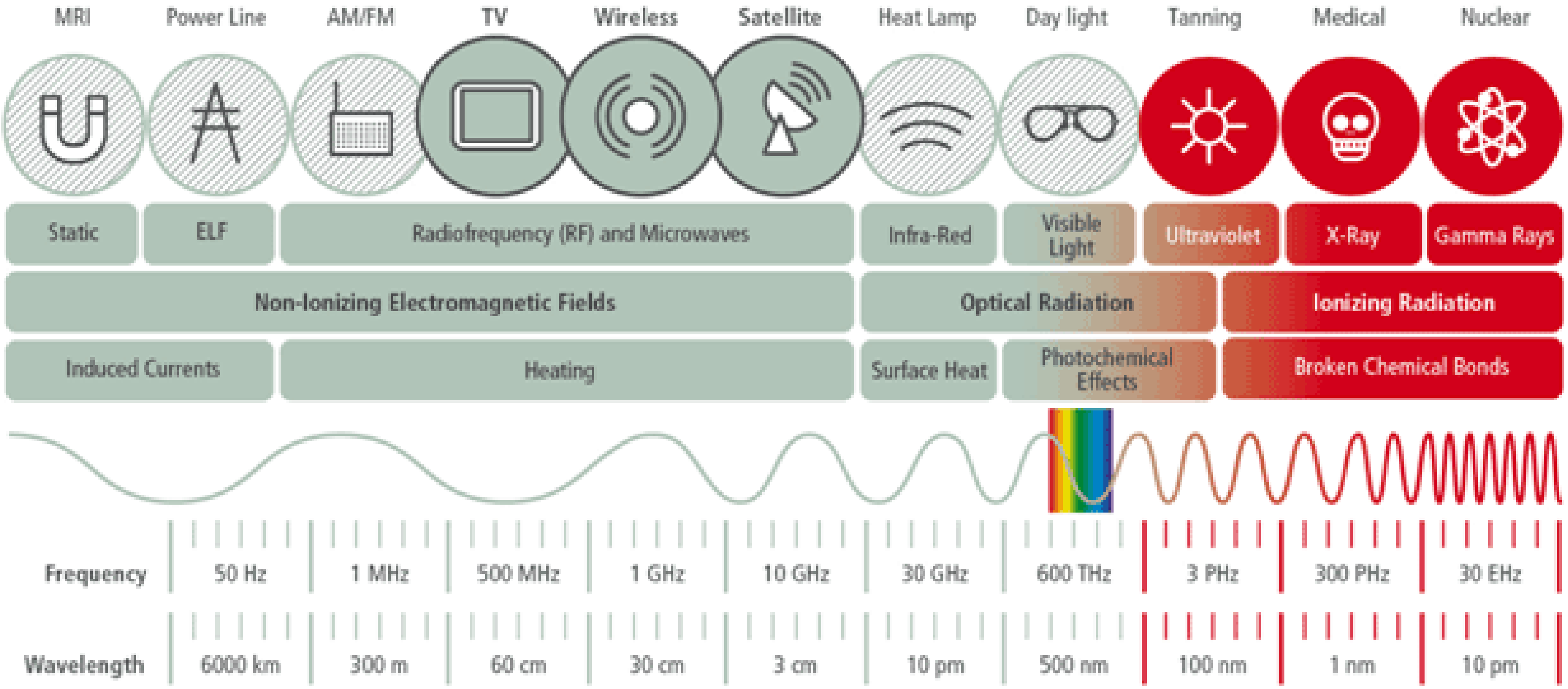
802.11 protocol	Release date[6]	Fre-quency	Band-width	Stream data rate[7]	Allowable MIMO streams	Modulation	Approximate range[citation needed]			
							Indoor		Outdoor	
		(GHz)	(MHz)	(Mbit/s)			(m)	(ft)	(m)	(ft)
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20	66	100	330
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35	115	120	390
		3.7[A]					—	—	5,000	16,000[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35	115	140	460
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38	125	140	460
n	Oct 2009	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2 [B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65) [C]	4	OFDM	70	230	250	820[8]
			40	15, 30, 45, 60, 90, 120, 135, 150 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135) [C]			70	230	250	820[8]
ac	Dec 2013	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3 [B] (6.5, 13, 19.5, 26, 39, 52, 58.5, 65, 78, 86.7) [C]	8		35	115[9]		
			40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200 [B] (13.5, 27, 40.5, 54, 81, 108, 121.5, 135, 162, 180) [C]			35	115[9]		
			80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3 [B] (29.2, 58.5, 87.8, 117, 175.5, 234, 263.2, 292.5, 351, 390) [C]			35	115[9]		
			160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7 [B] (58.5, 117, 175.5, 234, 351, 468, 702, 780) [C]			35	115[9]		
ad	Dec 2012	60	2,160	Up to 6,912 (6.75 Gbit/s) [10]	N/A	OFDM, single carrier, low-power single carrier	60	200	100	300
ah	Est. 2016[6]	0.9								
aj	Est. 2016[6]	45/60								
ax	Est. 2019[6]	2.4/5				MIMO-OFDM				
ay	2017	60	8000	Up to 100,000 (100 Gbit/s)	4	OFDM, single carrier,	60	200	1000	3000

IEEE 802.11-2007

- To reduce confusion, in 2007 IEEE combined the standards and amendments into a single standard – **IEEE 802.11-2007**
  - Officially retires all previous standards
  - It is still common to refer to them individually

- The new, single standard specifies technical corrections and clarifications to the original
  - Also includes enhancements for improved security, vendor-specific extensions and interpretations

Electromagnetic Spectrum

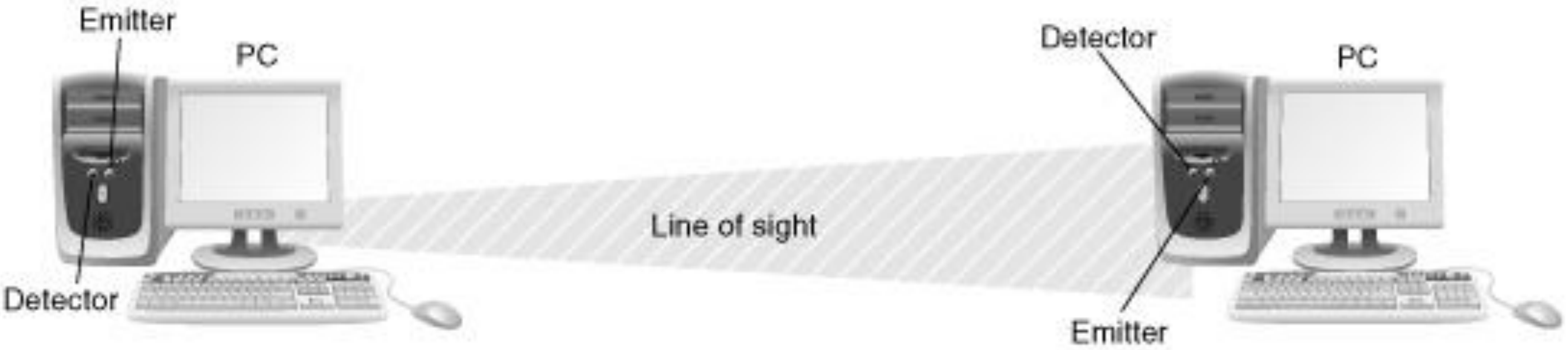


IEEE 802.11

- Specified that wireless transmission could take place via infrared (IR) or radio signals
- Infrared Transmissions:
  - Can send data by the intensity of the infrared light wave
  - **Light spectrum:** All types of light
  - **Infrared light**: Can be used for wireless transmissions
    - Invisible
  - **Emitter:** Device that transmits a signal
  - **Detector:** Device that receives a signal

IEEE 802.11

- Infrared transmissions (continued):
  - Transmissions can be either directed or diffused
  - **Directed transmission**: requires that the emitter and detector be directly aimed at one another in a line of sight (LoS) path
  - **Diffused transmission**: relies on reflected light
    - Emitters have a wide-focused beam instead of narrow and are pointed at a ceiling (reflection point)
  - Disadvantages include lack of mobility, limited range, confined to indoor use, slow transmission speed



© Cengage Learning 2013

Figure 2-1 Directed infrared transmission

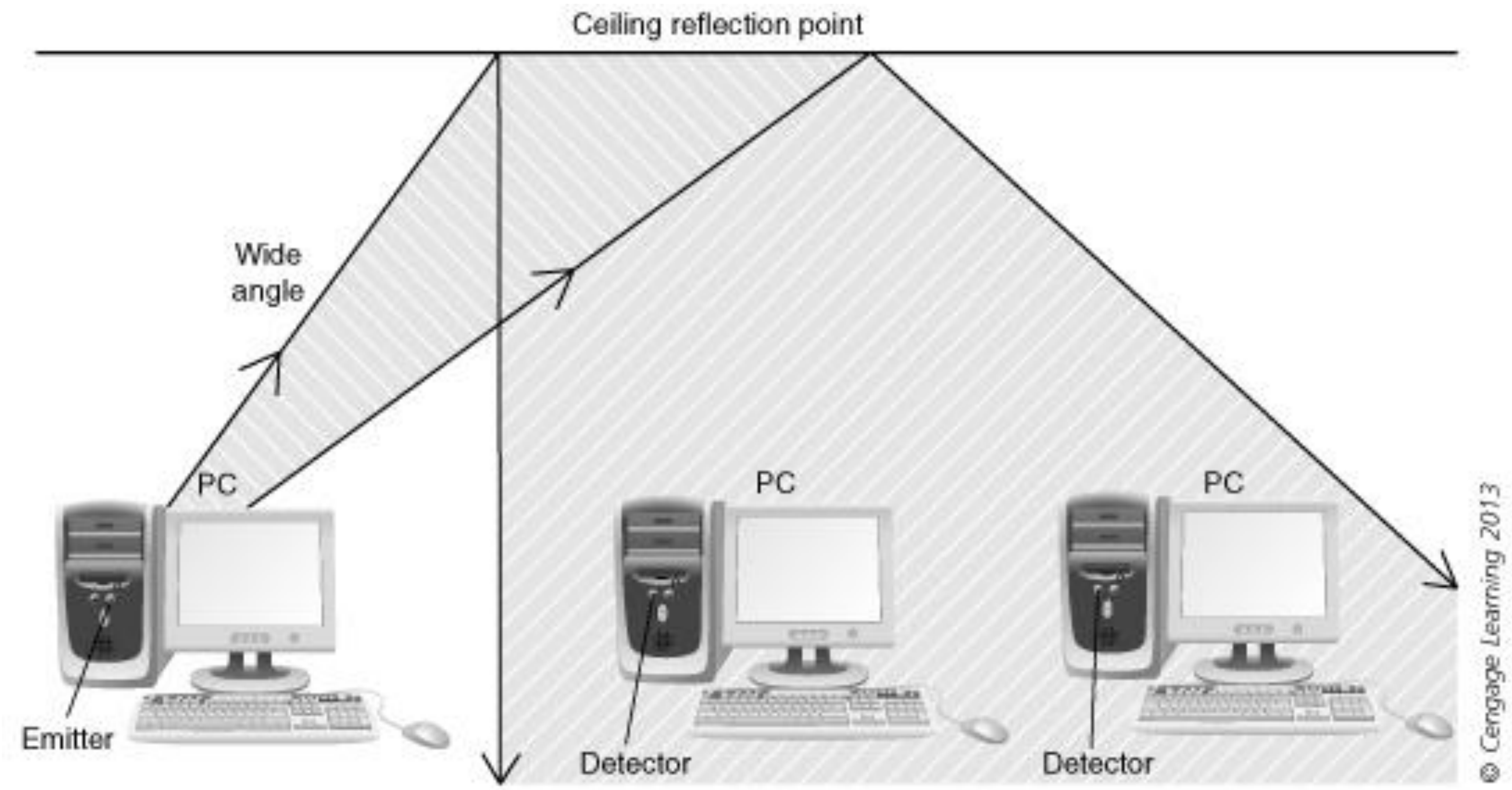
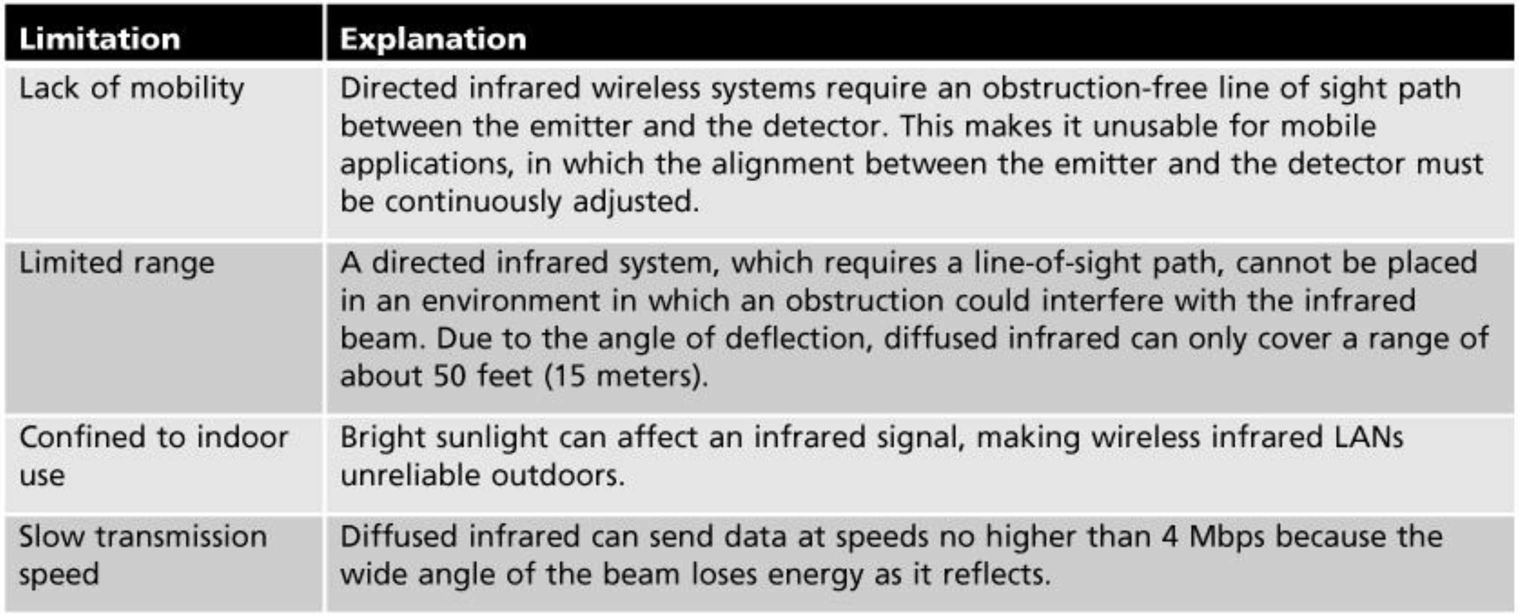


Figure 2-2 Diffused infrared transmission

Table 2-1 Limitations of infrared wireless systems



Limitation	Explanation
Lack of mobility	Directed infrared wireless systems require an obstruction-free line of sight path between the emitter and the detector. This makes it unusable for mobile applications, in which the alignment between the emitter and the detector must be continuously adjusted.
Limited range	A directed infrared system, which requires a line-of-sight path, cannot be placed in an environment in which an obstruction could interfere with the infrared beam. Due to the angle of deflection, diffused infrared can only cover a range of about 50 feet (15 meters).
Confined to indoor use	Bright sunlight can affect an infrared signal, making wireless infrared LANs unreliable outdoors.
Slow transmission speed	Diffused infrared can send data at speeds no higher than 4 Mbps because the wide angle of the beam loses energy as it reflects.

© Cengage Learning 2013

IEEE 802.11

- **Radio Wave (RF)Transmissions:**
  - Radio waves can penetrate through objects
    - Provides mobility
  - Radio waves travel longer distances
  - Can be used indoors and outdoors
  - Radio waves can travel at much higher speeds than infrared transmissions
  - IEEE 802.11 standard outlining radio wave transmissions has become preferred method for wireless LANs

IEEE 802.11b

- 802.11 standard's 2 Mbps bandwidth not sufficient for most network applications
- **802.11b** amendment added two higher speeds (5.5 Mbps and 11 Mbps) to original 802.11 standard
  - Uses ISM band
- Supports wireless devices up to 107 meters (350 feet) apart
  - Radio waves decrease in power over distance
  - 802.11b standard specifies that, when devices move out of range to transmit at 11 Mbps, devices drop transmission speed to 5.5 Mbps

IEEE 802.11b

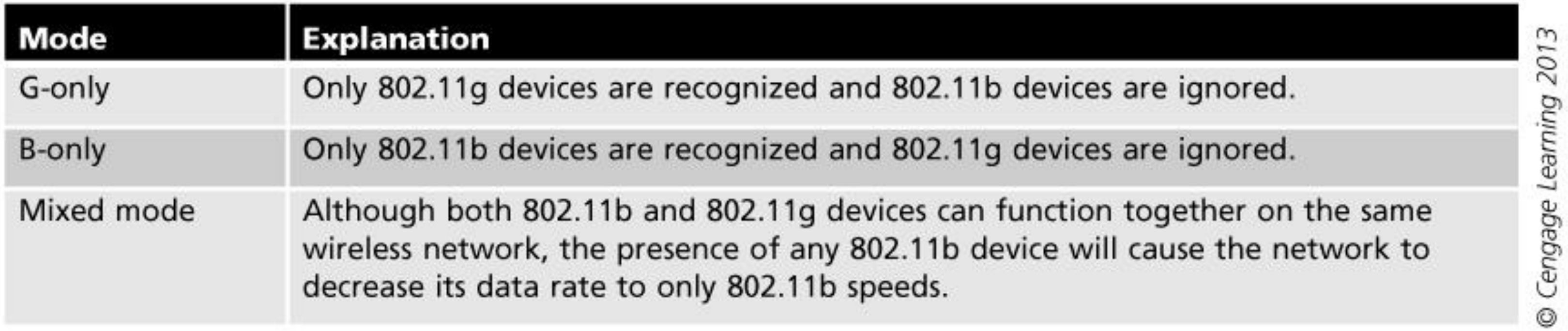
- **Station (STA):** officially term given to a wireless device
- Other factors that determine speed of transmission include number of wireless devices in the network and the type of obstructions between devices
- Two terms for measuring wireless network speeds:
  - **Data rate**: theoretical maximum rated speed of a network
  - **Throughput**: measure of how much actual data can be sent per unit of time across a network

IEEE 802.11a

- **IEEE 802.11a** standard specifies maximum rated speed of 54 Mbps
  - Also supports 48, 36, 24, 18, 12, 9,and 6 Mbps transmissions
- 802.11a and 802.11b published at same time
  - 802.11a came to market later due to technical issues and high production cost
- Range of 802.11a is less than that of 802.11b
  - Devices can typically be no more than 100 feet apart

IEEE 802.11g

- Effort to combine best features of 802.11a and 802.11b
  - Data transfer rates to 54 Mbps
  - Support devices up to 115 meters apart
- 802.11g standard specifies that devices operate in the same radio frequency as IEEE 802.11b
  - Supports devices that are farther apart with higher speeds (up to 350 feet or 107 meters)
- Most WLAN equipment allows both 802.11 g and 802.11b wireless devices to function together



Mode	Explanation
G-only	Only 802.11g devices are recognized and 802.11b devices are ignored.
B-only	Only 802.11b devices are recognized and 802.11g devices are ignored.
Mixed mode	Although both 802.11b and 802.11g devices can function together on the same wireless network, the presence of any 802.11b device will cause the network to decrease its data rate to only 802.11b speeds.

© Cengage Learning 2013

Table 2-2 IEEE 802.11g configuration options

IEEE 802.11n-2009

- Ratified on September 11, 2009
- Four significant improvements over previous standards:
  - *Speed:* up to 600 Mbps
  - *Coverage area:* Double the indoor range and triple the outdoor range
  - *Interference:* uses different frequencies to reduce interference
  - *Security:* requires the strongest level of wireless security

WLAN Client Hardware and Software

- Wireless hardware and software can be divided into:
  - Wireless client network interface cards (hardware)
  - Wireless client utility software to support the hardware

Wireless Client
Network Interface Card (NIC)

- **Network interface card (NIC):** Connects computer to network so that it can send and receive data
- Today's computers typically have NIC components built directly into the motherboard
- NICs for wired networks have an RJ-45 connection used to connect the device to the network via a cable
- Wireless NICs perform same function, but without wires
  - Categorized into wireless NIC devices for desktop computer and for portable devices

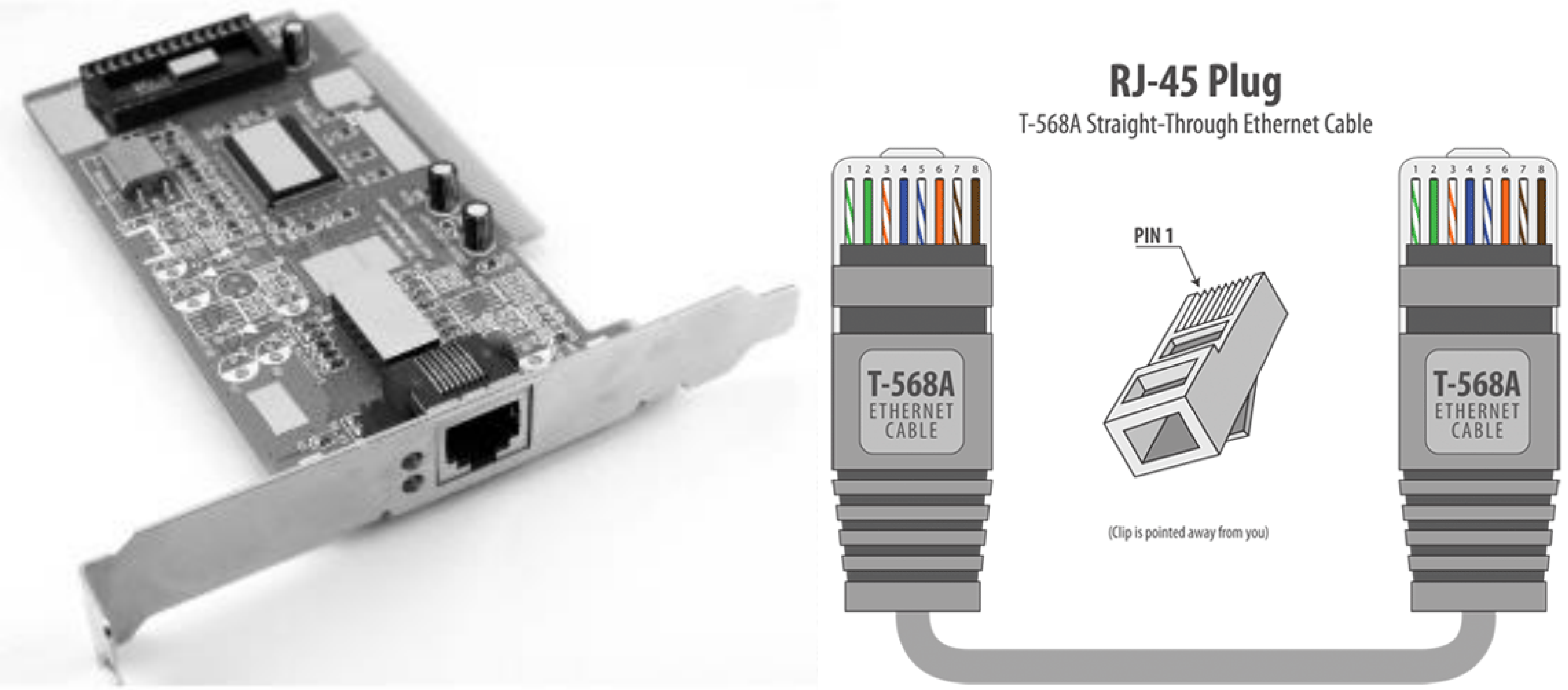
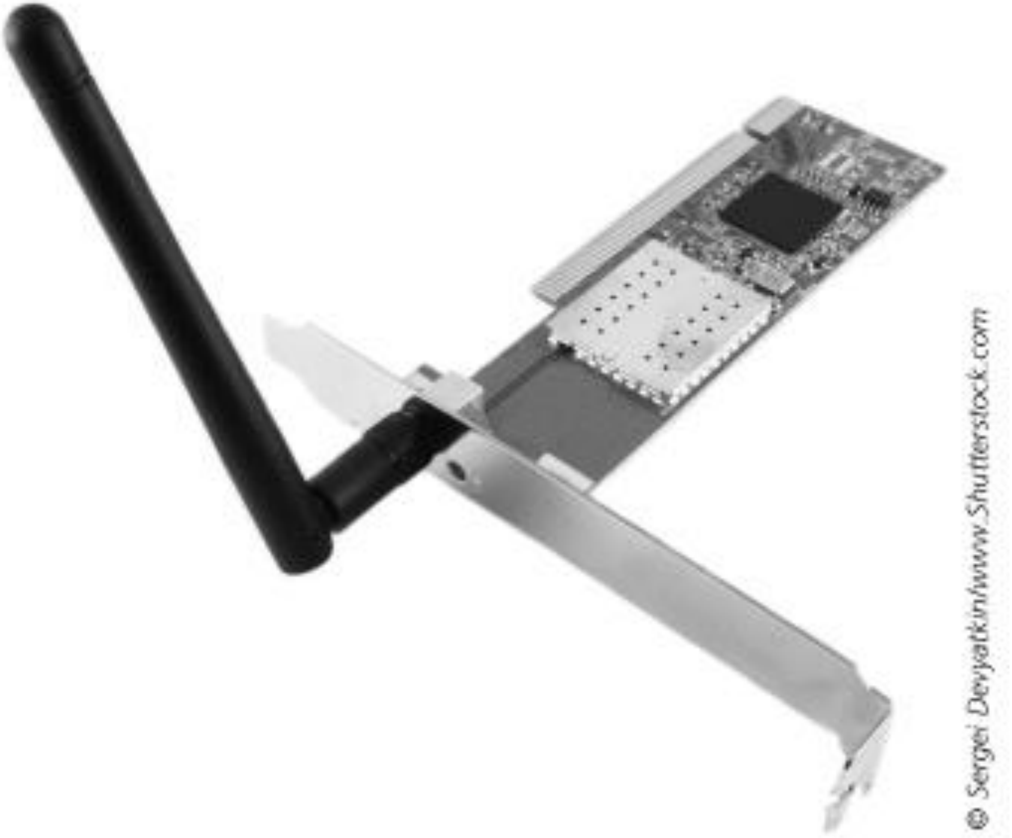


Figure 2-3 Network interface card (NIC) for a wired network

Cards for Desktops

- Internal wireless NICs have largely been replaced by external wireless NICs that plug into the Universal Serial Bus (USB) port

- Desktop computers are now shipping with wireless NICs as standard equipment (along with a wired NIC)



© Sergei Devyatkin/www.Shutterstock.com

Figure 2-4 Internal wireless NIC

Cards for Portable Devices

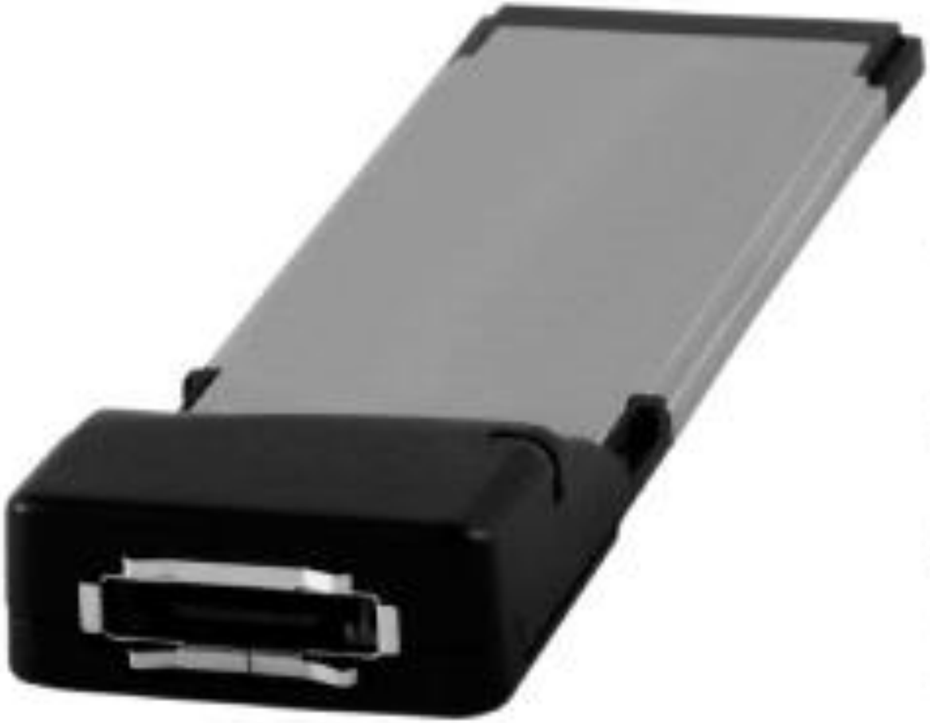
- Portable laptop computers often support wireless NICs in different form factors (sizes and shapes)
- **Large form factor cards**: credit card-size and slides into a slot on a laptop
  - Originally known as **PCMCIA (Personal Computer Memory Card International Association) cards**
  - Now known as **PC Card**
  - **CardBus**: enhanced type of PC Card that includes a bus mastering feature (allows a controller on the bus to talk to other devices or memory bypassing the CPU)

Cards for Portable Devices

- PC Card and CardBus devices are being replaced by ExpressCard technology
  - Designed to deliver high-performance modular expansion in a smaller size

- **Small form factor cards**:
  - CompactFlash (CF): wireless CF NICs were primarily designed for use in personal digital assistant (PDA)

  - Secure Digital (SD): started as a portable device for digital cameras and PDAs
  - Secure Digital Input Output (SDIO): combination of an SD card and an I/O device (wireless NIC)



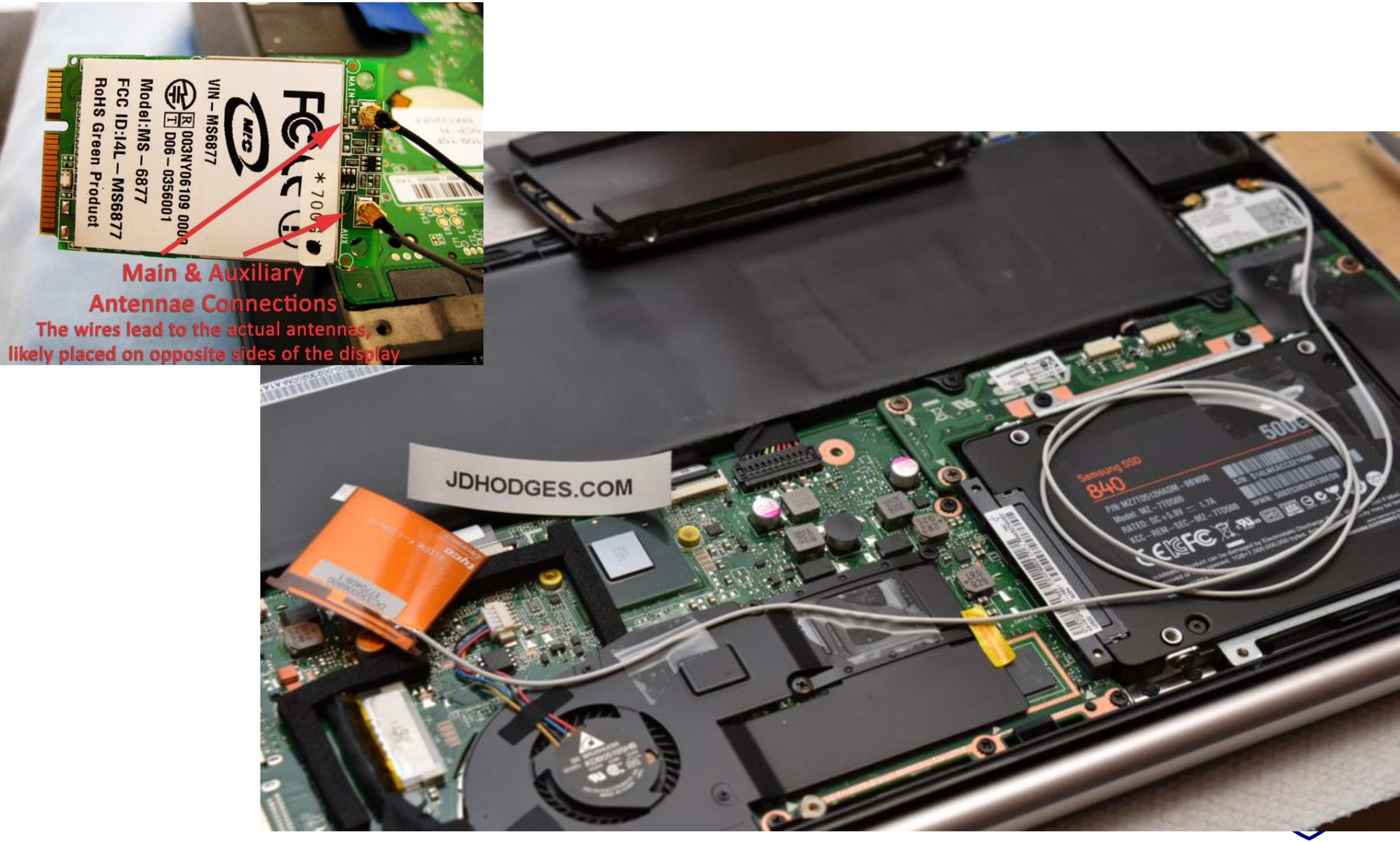
© gigello/www.Shutterstock.com

Figure 2-7 ExpressCard wireless NIC

Cards for Portable Devices

- **Internal cards**: Peripheral Component Interconnect (PCI) expansion slots are being replaced with PCI Express (PCI-e)
  - Laptop computers have Mini-PCI or Mini-PCI-e slots
  - Most laptops come with a wireless Mini-PCI or Mini-PCI-e NIC installed
  - Vendors embed an antenna to improve the reception of the wireless signal

Cards for Portable Devices



Main & Auxiliary Antennae Connections

The wires lead to the actual antennas, likely placed on opposite sides of the display

Client Utility Software

- Software interfaces between the wireless NIC and computer
  - Can be part of the operating system or a separate third-party utility program

- **Wireless Zero Configuration (WZC)** service:
  - Wireless connection management utility (introduced in Windows XP) that operates as a Windows service
  - Automatically determines which wireless network to connect to based on default settings and preference set by user
- **WLAN AutoConfig**: replace WZC in Windows 7

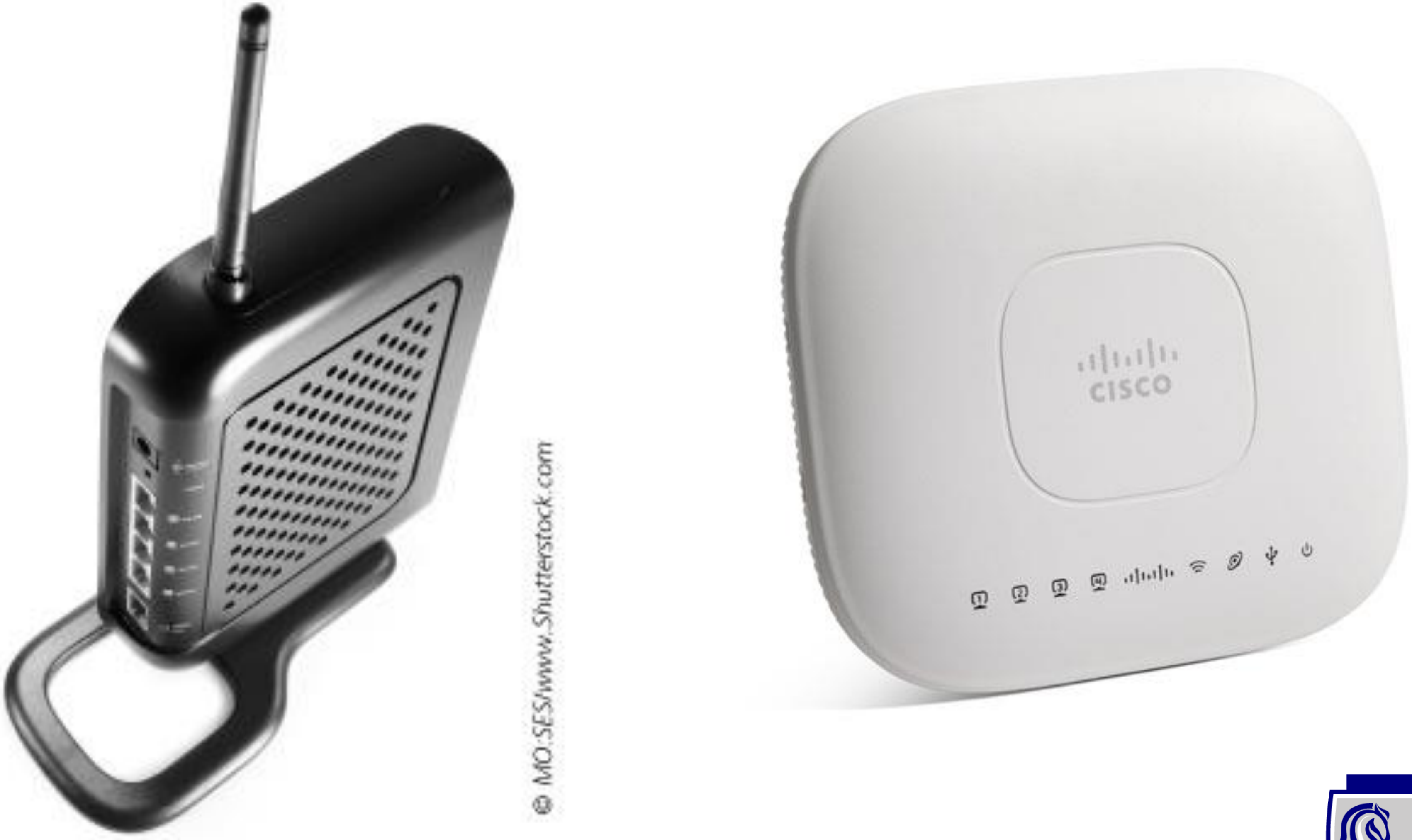
WLAN Infrastructure Devices

- Wireless hardware devices used to create a wireless network infrastructure:
  - Access points
  - WLAN bridges
  - Gateways
  - Power over Ethernet devices

Access Points (APs)

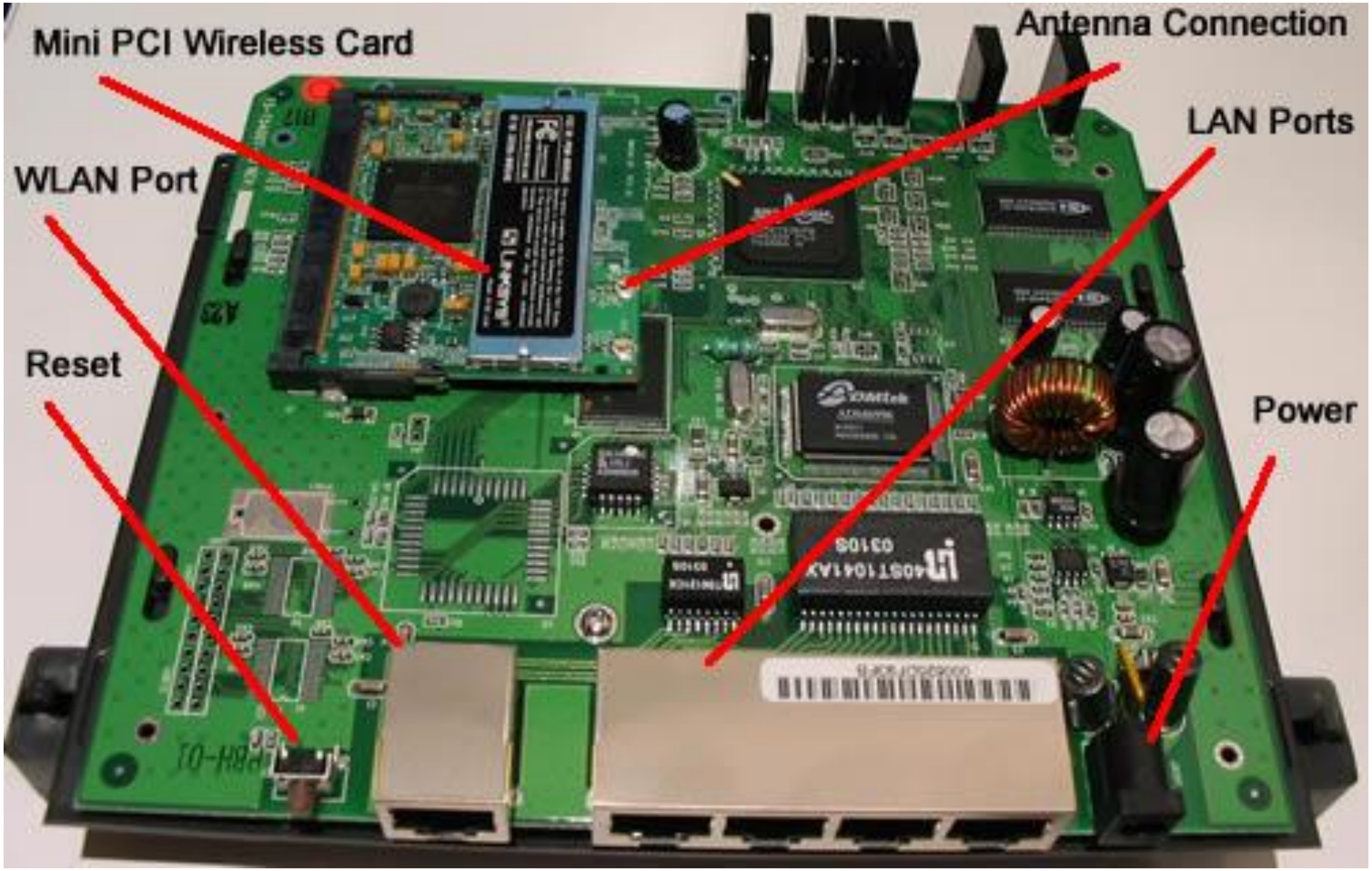
- Three major parts:
  - Antenna and radio transmitter/receiver
    - To send and receive signals
  - Special bridging software
    - To interface wireless devices to other devices
  - RJ-45 wired network interface
    - Allows it to connect to a wired network

- Two basic function:
  - Base station for wireless network
  - Bridge between wireless and wired networks

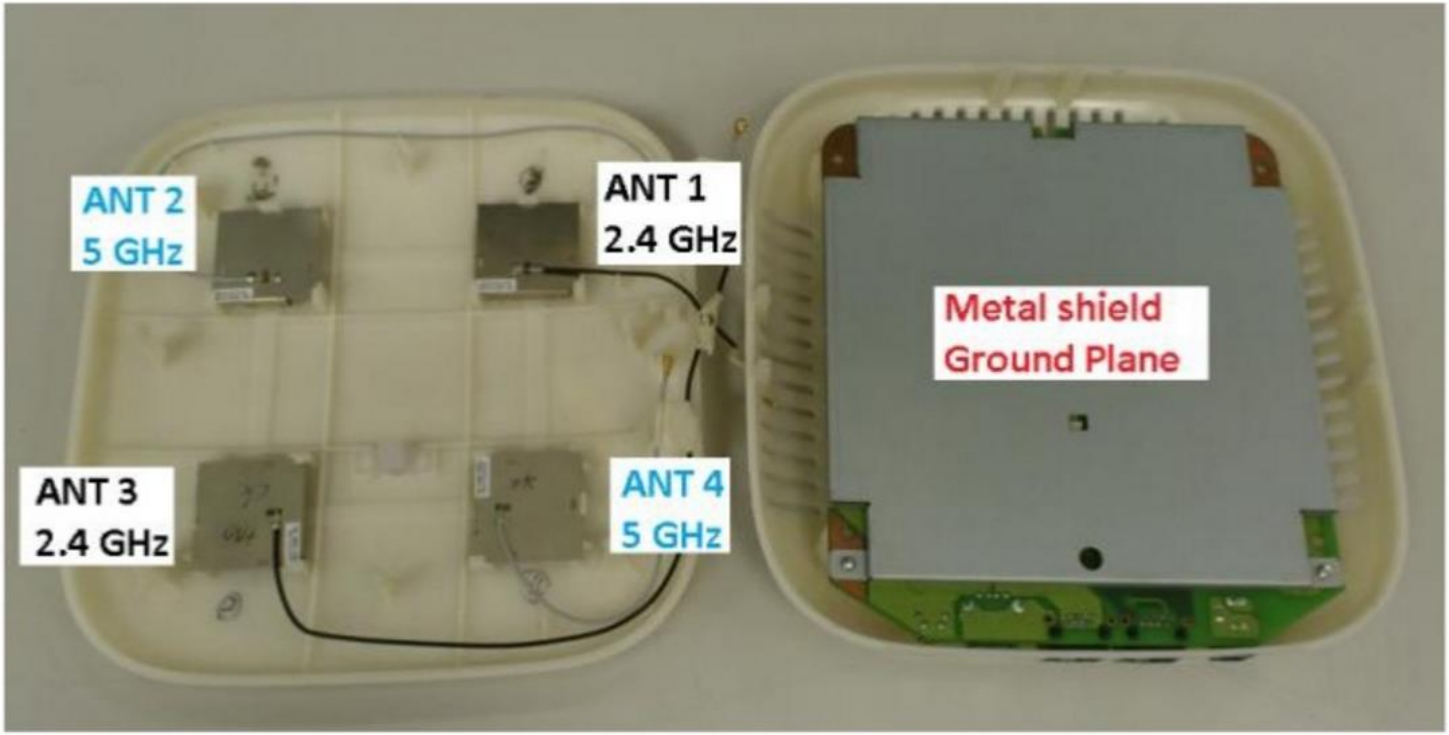


© MO:SES/www.Shutterstock.com

Figure 2-9 Access point



Inside Access point



(2) Discrete single band 2.4 GHz single radiating element antennas

(2) Discrete single band 5.0GHz single radiating element antennas

Inside Access point Cisco 700i

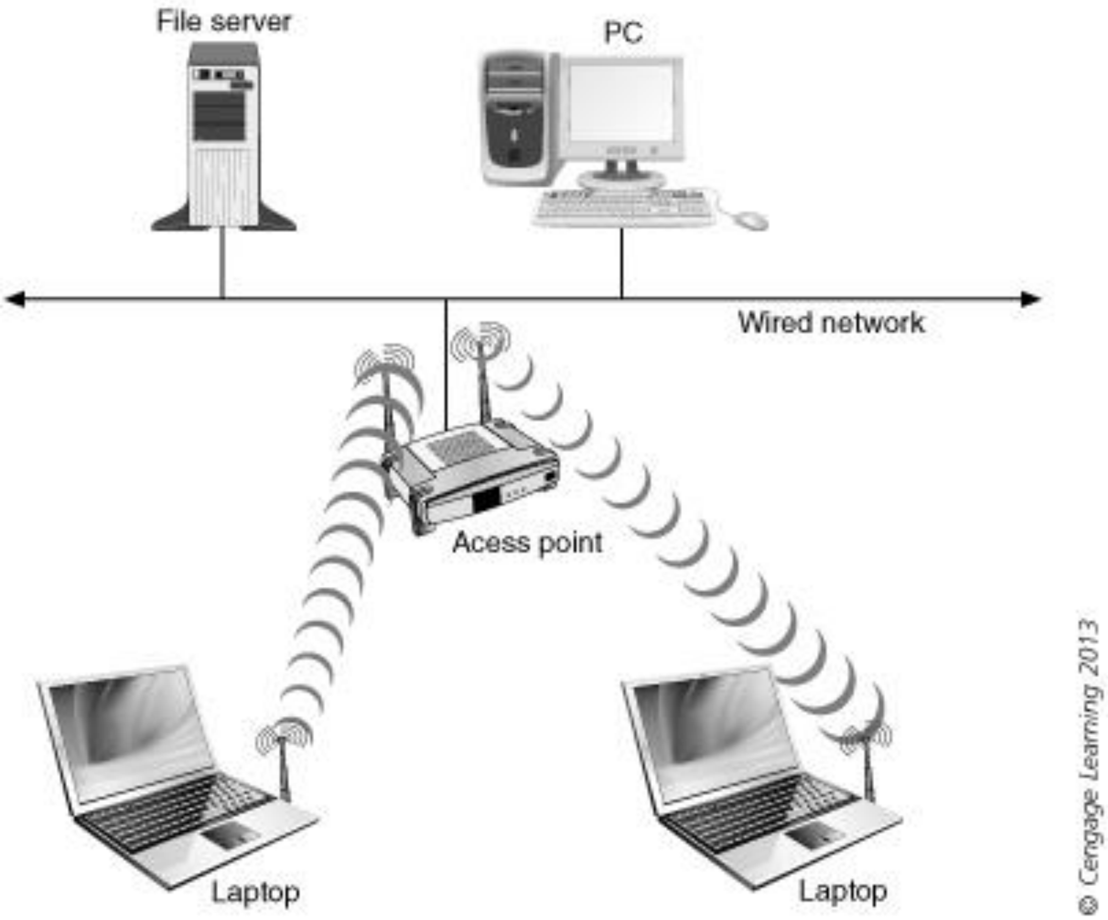


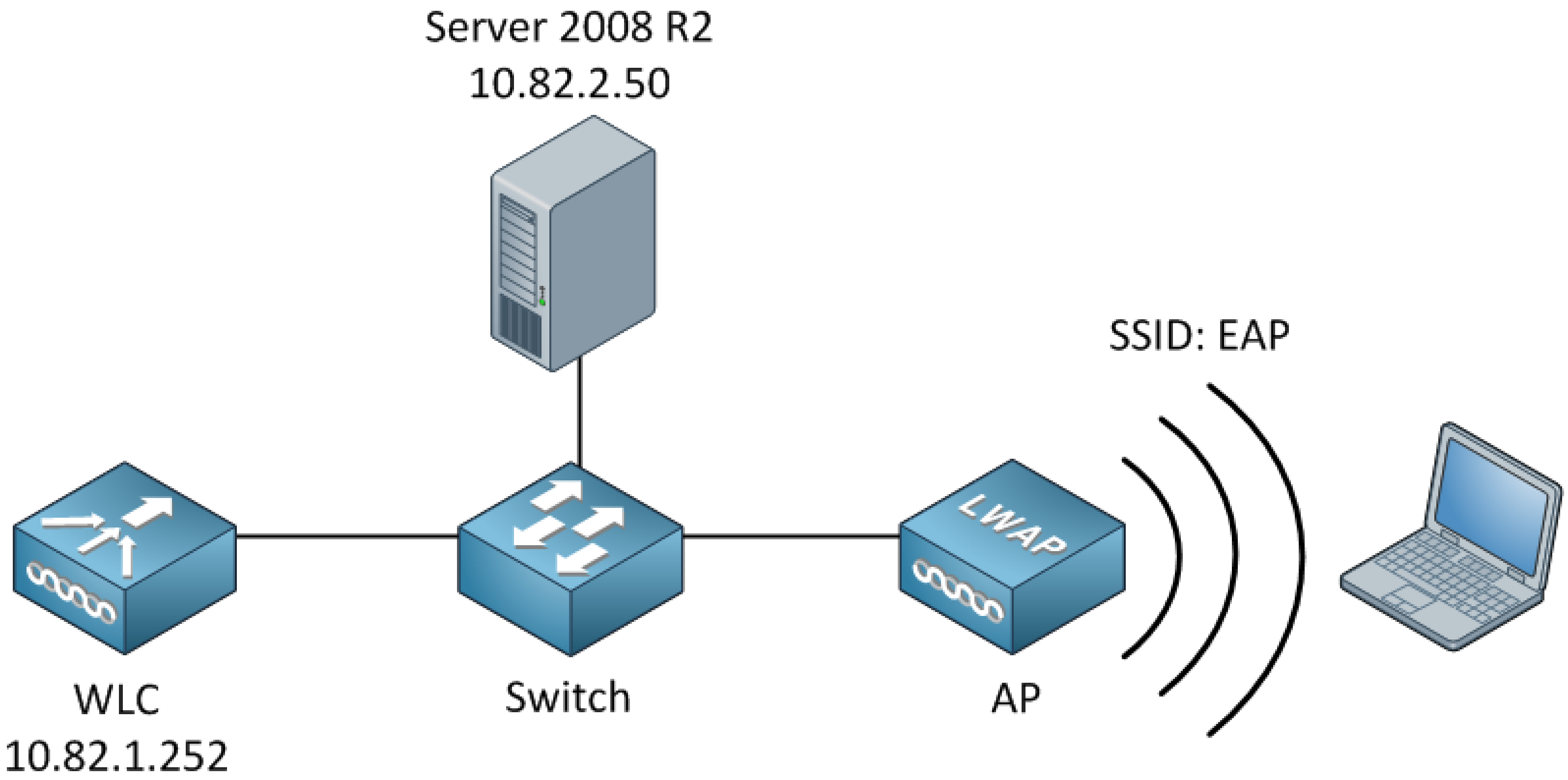
Figure 2-10 AP connected to wireless network

Access Point (APs)

- **Autonomous Access Points:** standard APs
  - Considered independent because they are separate from other network devices
  - Have intelligence to manage authentication, encryption, and other functions for wireless clients
  - Also called **fat access points**

- **Lightweight Access Points**: also called **thin access points**
  - Does not contain management and configuration functions
  - Those features are contained in a central device called wireless LAN controller (WLC) or wireless switch

Wireless LAN controller (WLC)



Access Point (APs)

- WLC: distributes configuration information automatically to all lightweight access points
- **Remote office WLAN controller**: used to manage multiple WLCs at remote sites from a central location
- Disadvantages of lightweight access points:
  - Do not provide integration of wired and wireless networks
  - Devices are proprietary – all lightweight APs and WLCs must be from the same vendor

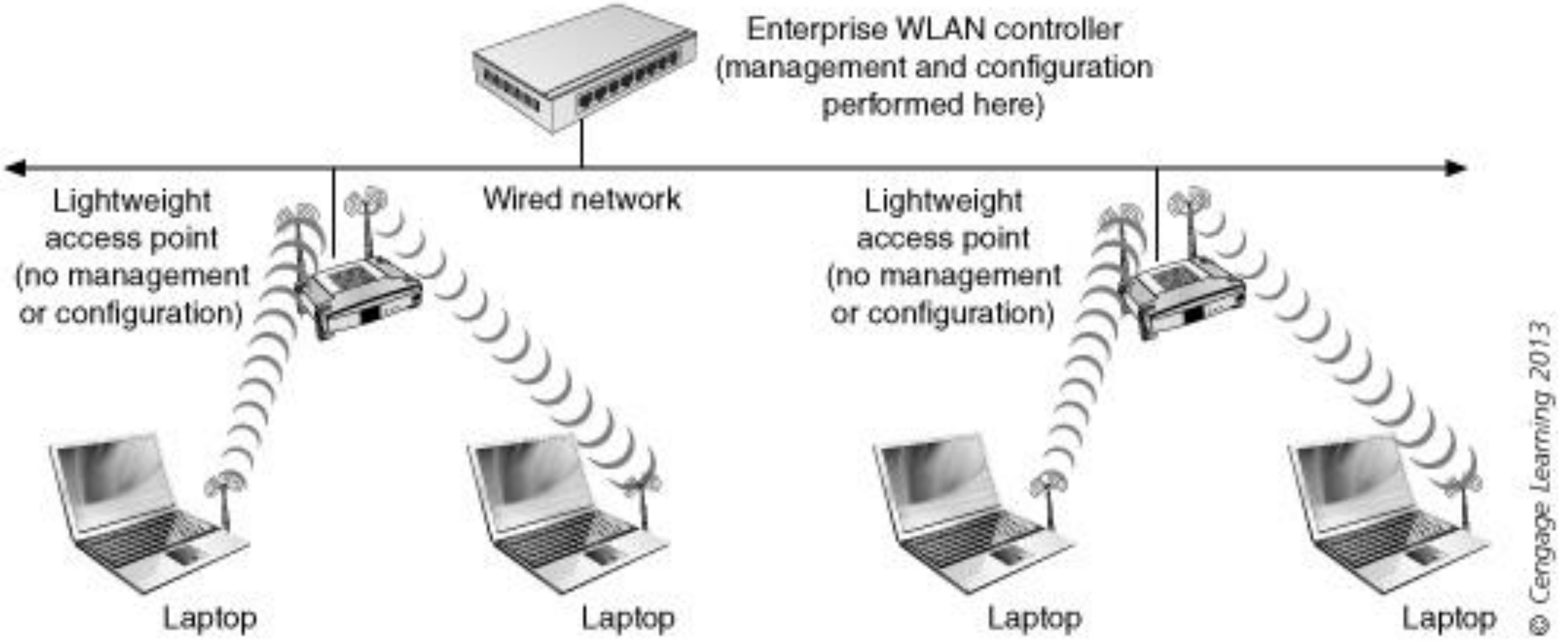
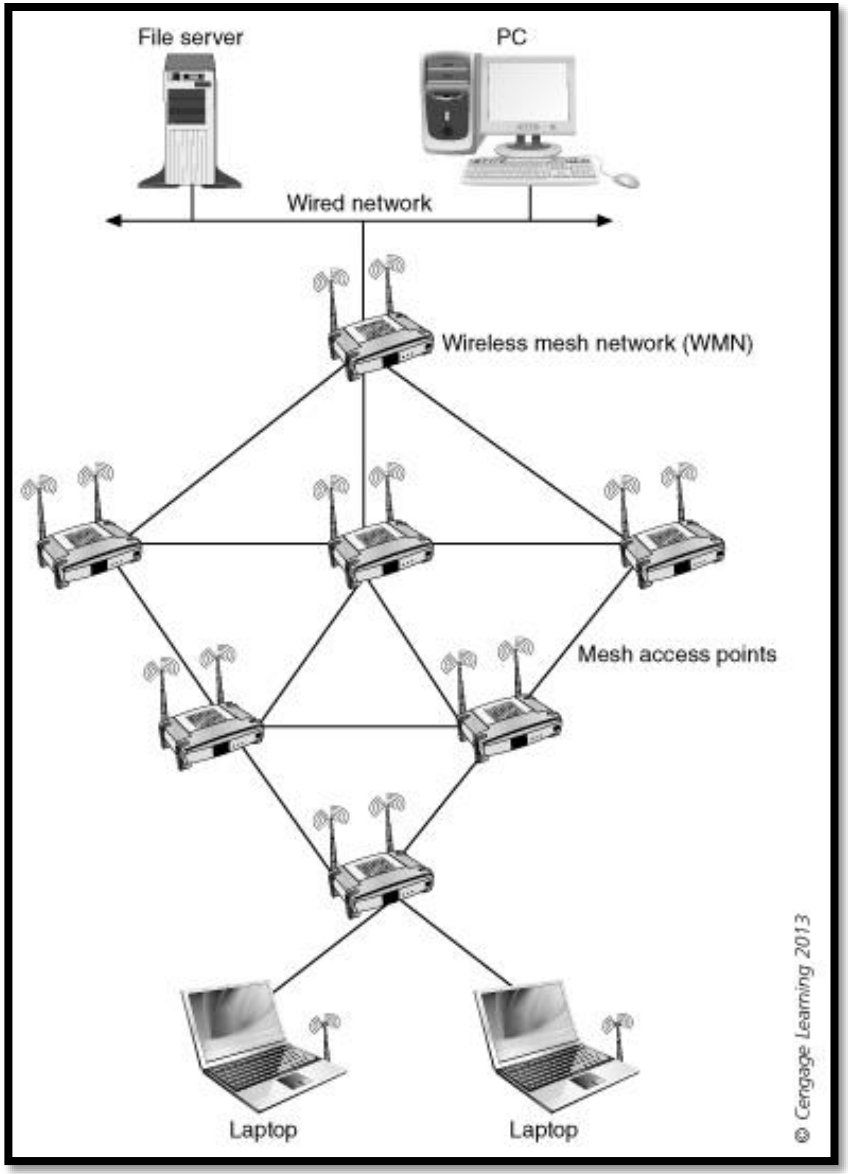

Enterprise WLAN controller (management and configuration performed here)
Wired network
Lightweight access point (no management or configuration)
Lightweight access point (no management or configuration)
Laptop
Laptop
Laptop
Laptop
© Cengage Learning 2013

Figure 2-11 Lightweight access point with enterprise WLAN controller

Access Point (APs)

- **Mesh Access Points**: communicates with the next closest mesh access point
- **Wireless mesh network (WMN):** created by dozens or even hundreds of mesh access points
  - Also known as wireless mesh routers (function in a similar manner to routers)
  - Only one mesh AP must be physically connected to the wired network
- **Backhaul wireless mesh network**: connects mesh access points to an Internet connection



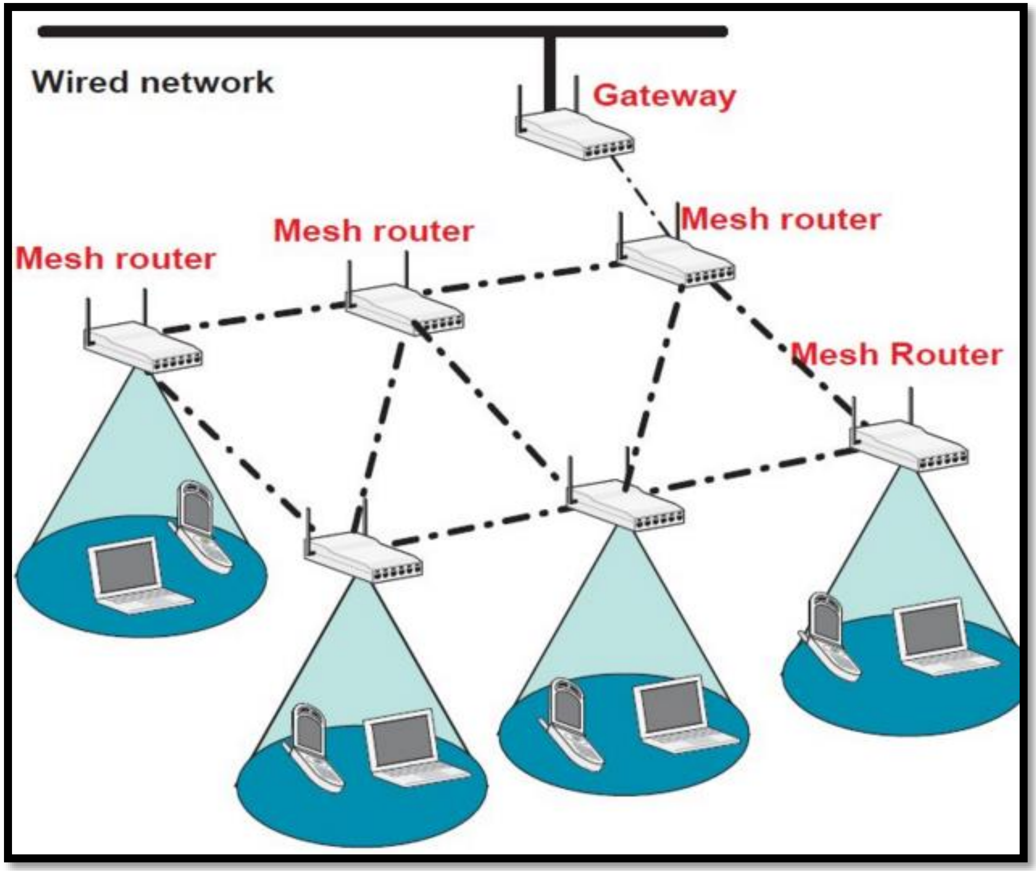


Figure 2-12 Wireless mesh network

Access Point (APs)

- Advantages of mesh access points
  - Low-cost installation
  - Large coverage area
  - Easy-to-change coverage area
  - Can be installed in areas without wired infrastructure
  - Self-configuring WMN
  - Self-healing WMN
  - Fast installation

WLAN Bridges

- **Bridge:** Connects two network segments together
  - Even if they use different types of physical media
- **Wireless workgroup bridge**: used to connect a wired network segment to a wireless network segment
  - Does not function as a an access point
  - Only supports wired devices, not any other wireless devices

WLAN Bridges

- **Remote wireless bridge:** Connects two or more wired or wireless networks together that are separated by a longer distance
  - Transmit at higher power than WLAN APs
  - Use directional antennas to focus transmission in single direction
  - Have software enabling selection of clearest transmission channel and avoidance of noise and interference
  - Supports two types of connections
    - Point-to-point (PtP): two buildings are connected
    - Point-to-multipoint (PtMP): multiple buildings are connected

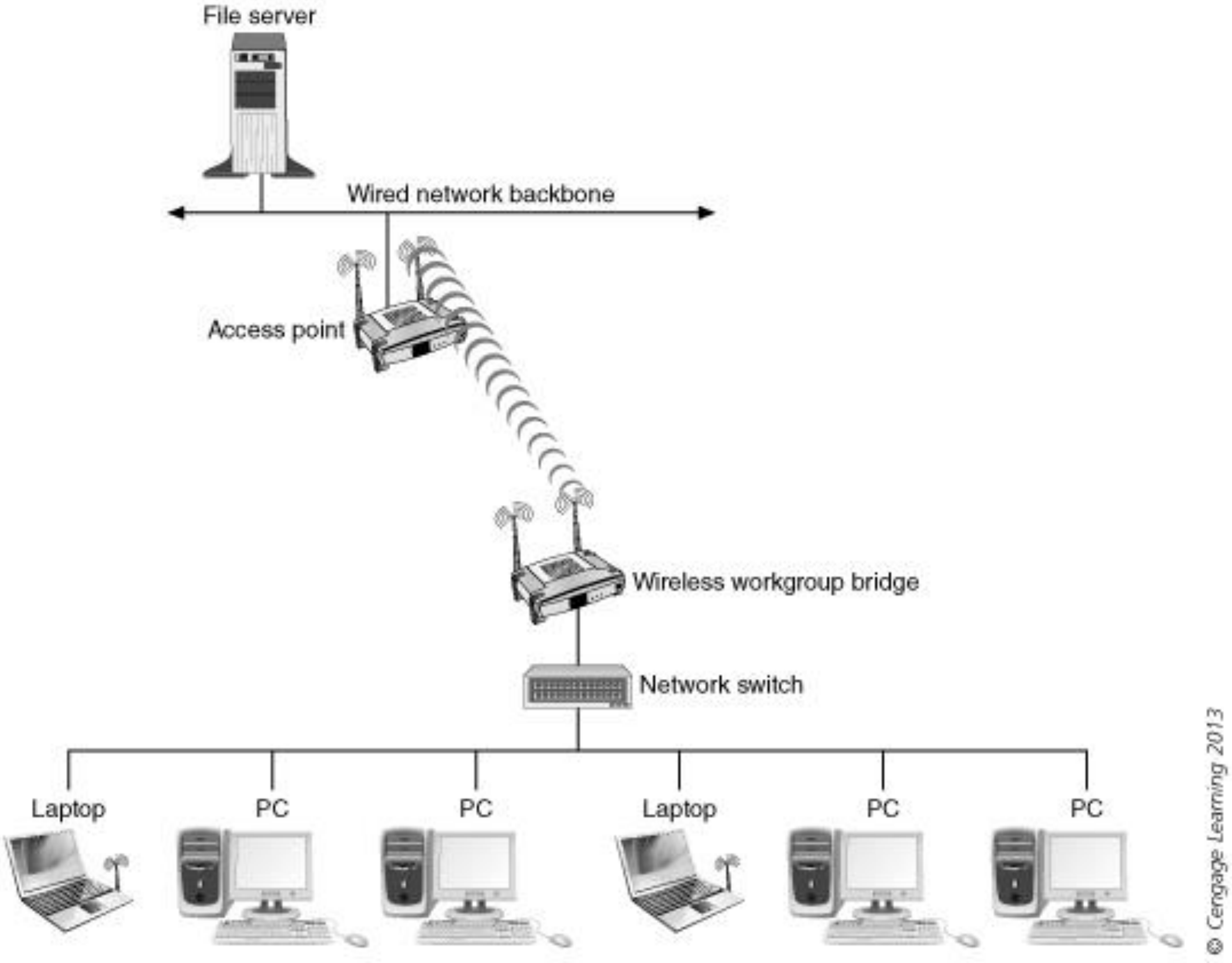
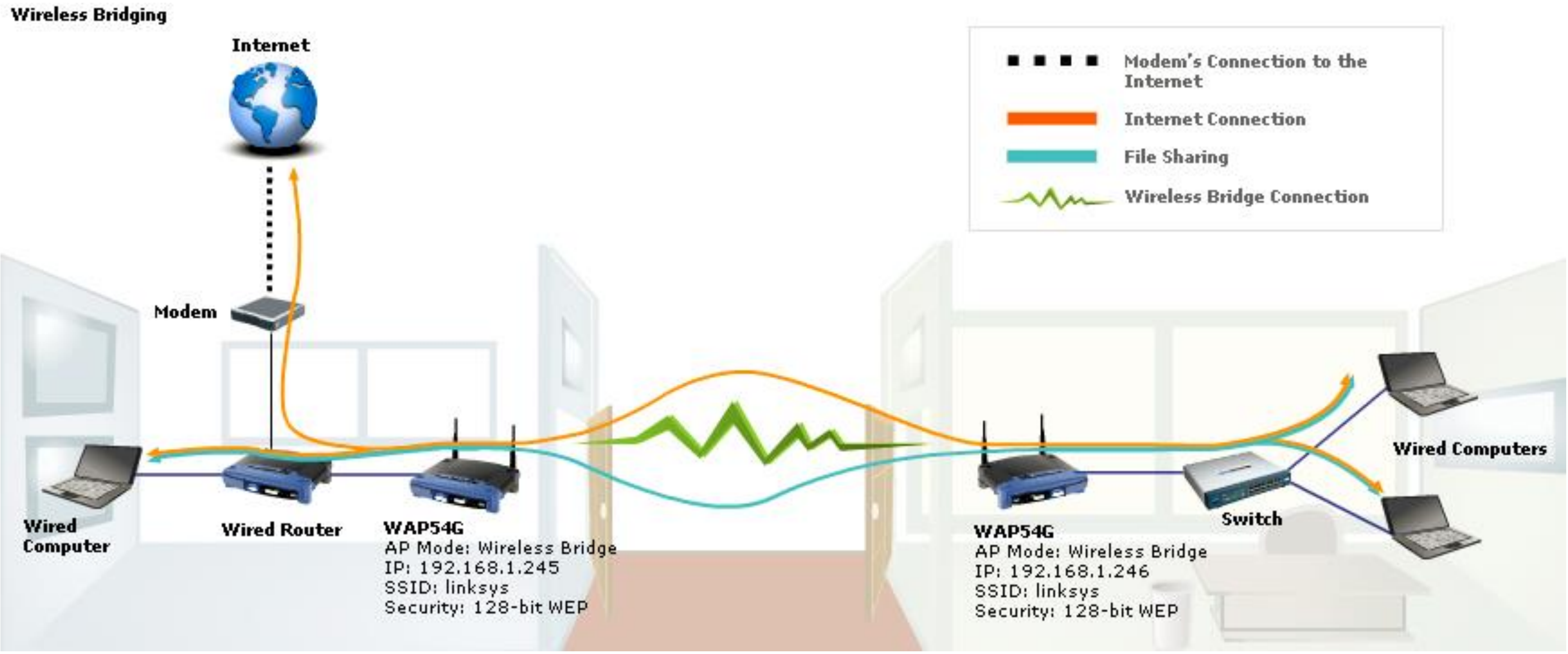
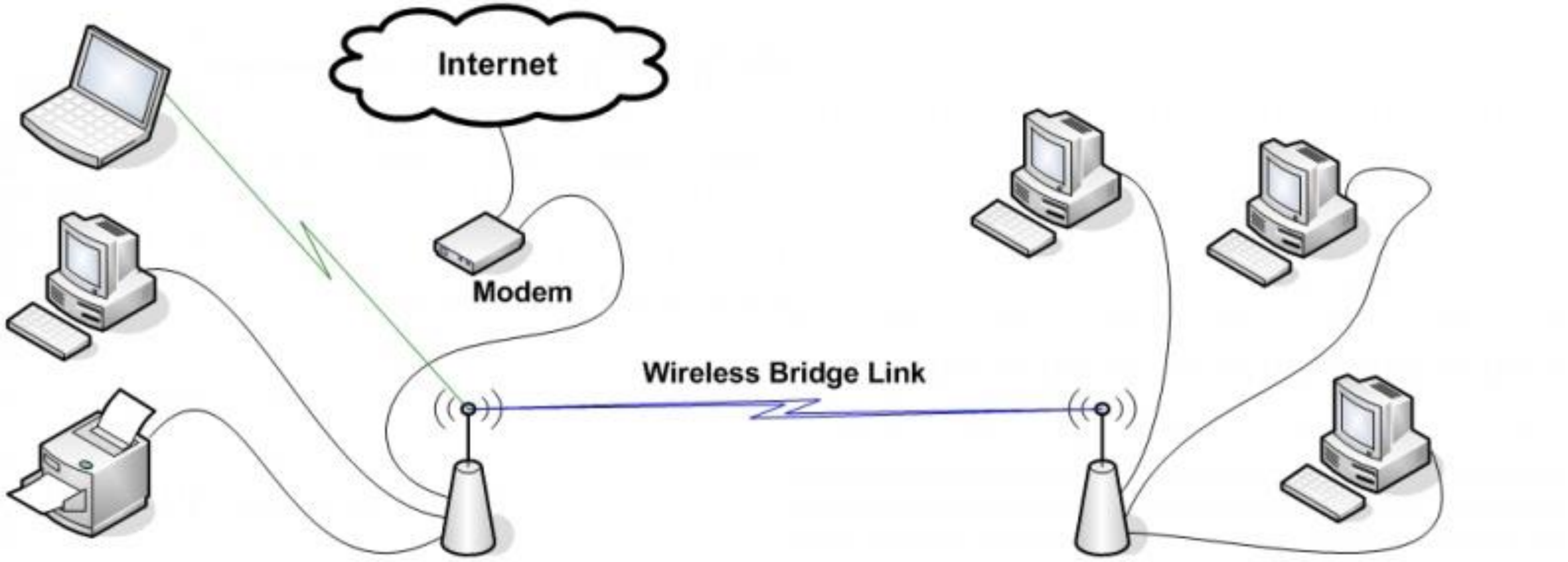


Figure 2-13 Wireless workgroup bridge



Wireless bridge



Wireless bridge

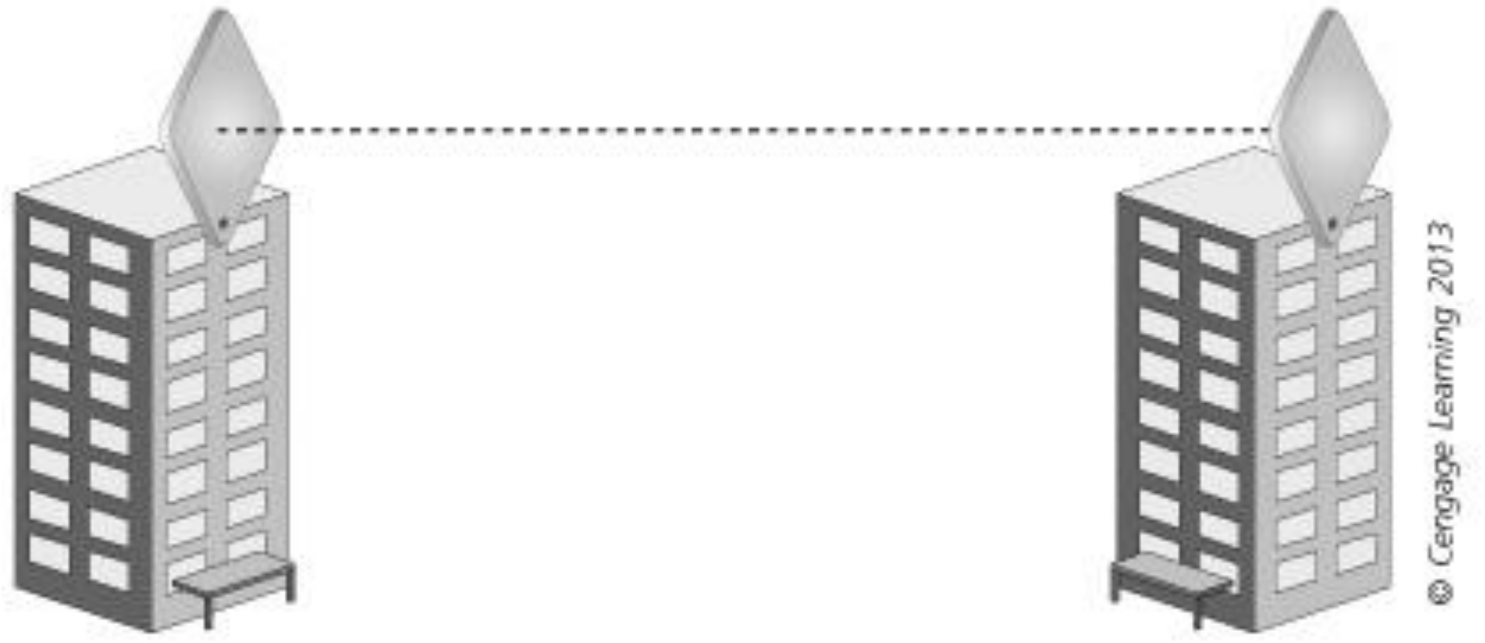


Figure 2-14 Point-to-point remote wireless bridge

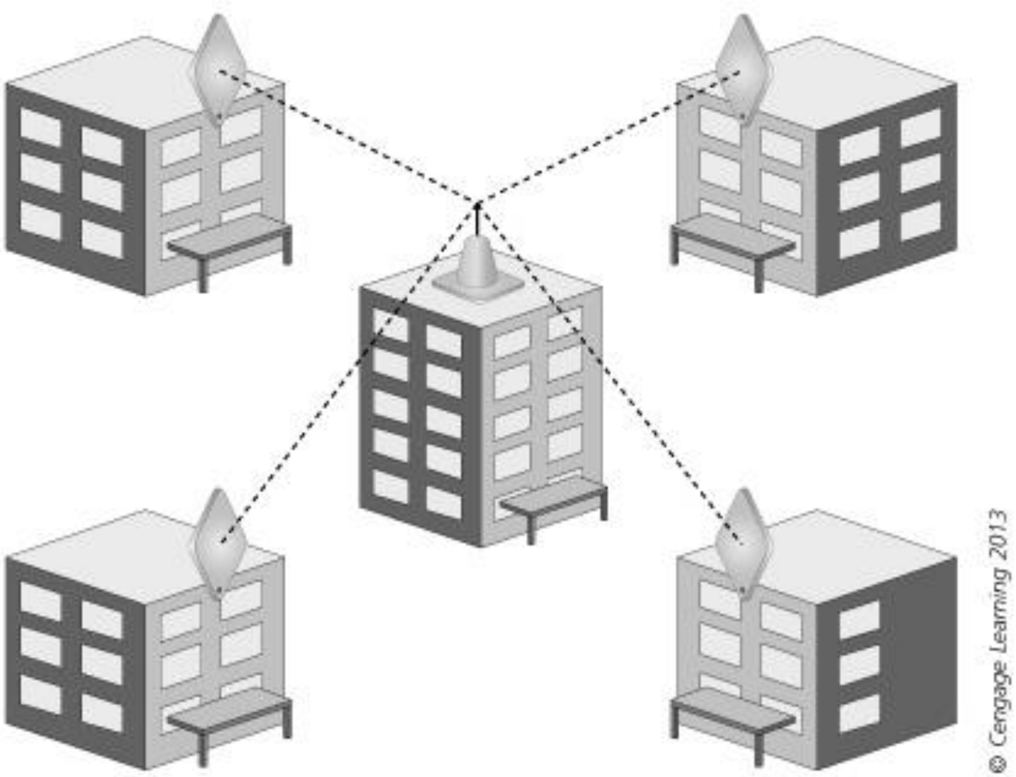


Figure 2-15 Point-to-multipoint remote wireless bridge

WLAN Bridges

- Four modes:
  - **Root mode: Root bridge** can only communicate with other bridges not in root mode
  - **Non-root mode**: Can only transmit to another bridge in root mode
  - **Repeater mode:** Extend distance between LAN segments
    - Placed between two other bridges
  - **Access point mode:** Functions as standard AP
- Offer a cost-effective alternative to leased wired options for connecting remote buildings

Gateways

- **Gateway**: network device that acts as an entrance to another network
- Two types of wireless gateways: **Enterprise Encryption Gateways (EEG)** and **residential WLAN gateways**
- EEG: provides encryption and authentication services for a wireless network
  - Typically serves as the entry point to the wired network
  - Relieves an AP from burden of encryption and authentication

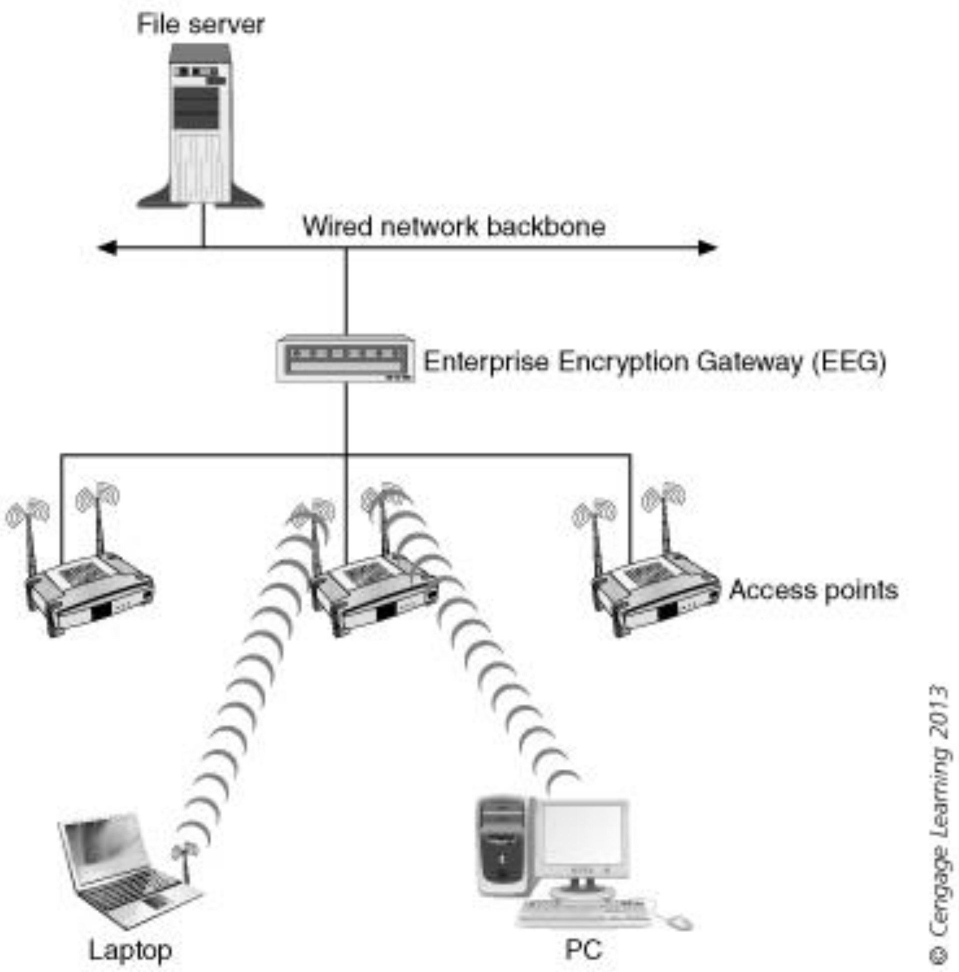


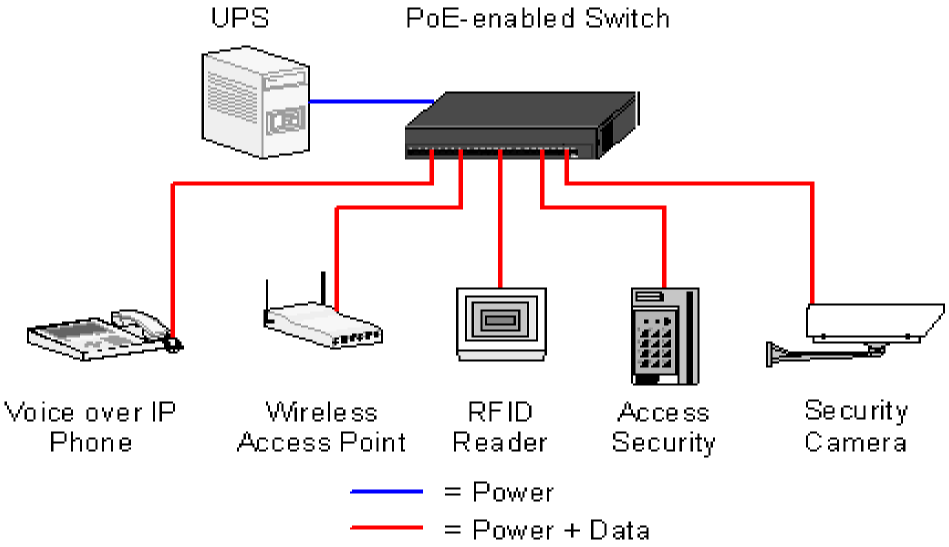
Figure 2-16 Enterprise Encryption Gateway (EEG)

Gateways

- **Residential WLAN Gateway**: Combines features of an AP, firewall, router, DHCP server into a single hardware device
  - Also known as wireless broadband routers
- Windows 7 added two significant wireless functions to complement WLAN gateways
  - **Windows Connect Now (WCN):** computer can scan for a newly installed WCN capable device
  - Wireless Hosted Network: allows for **Virtual WiFi** and offers a software-based wireless access point **(SoftAP)** that uses a designated virtual wireless NIC

Power over Ethernet (PoE) Devices

- Devices that obtain power through the unused wires in a standard UTP Ethernet cable
  - Eliminates the need to install electrical wiring where devices might need to be located
- *PoE-enabled Ethernet switch*: power sourcing equipment (PSE) that provides both electrical power and data
- *PoE injectors*: can inject power into an Ethernet cable
  - A standard Ethernet switch can supply data while the PoE injector provides the power



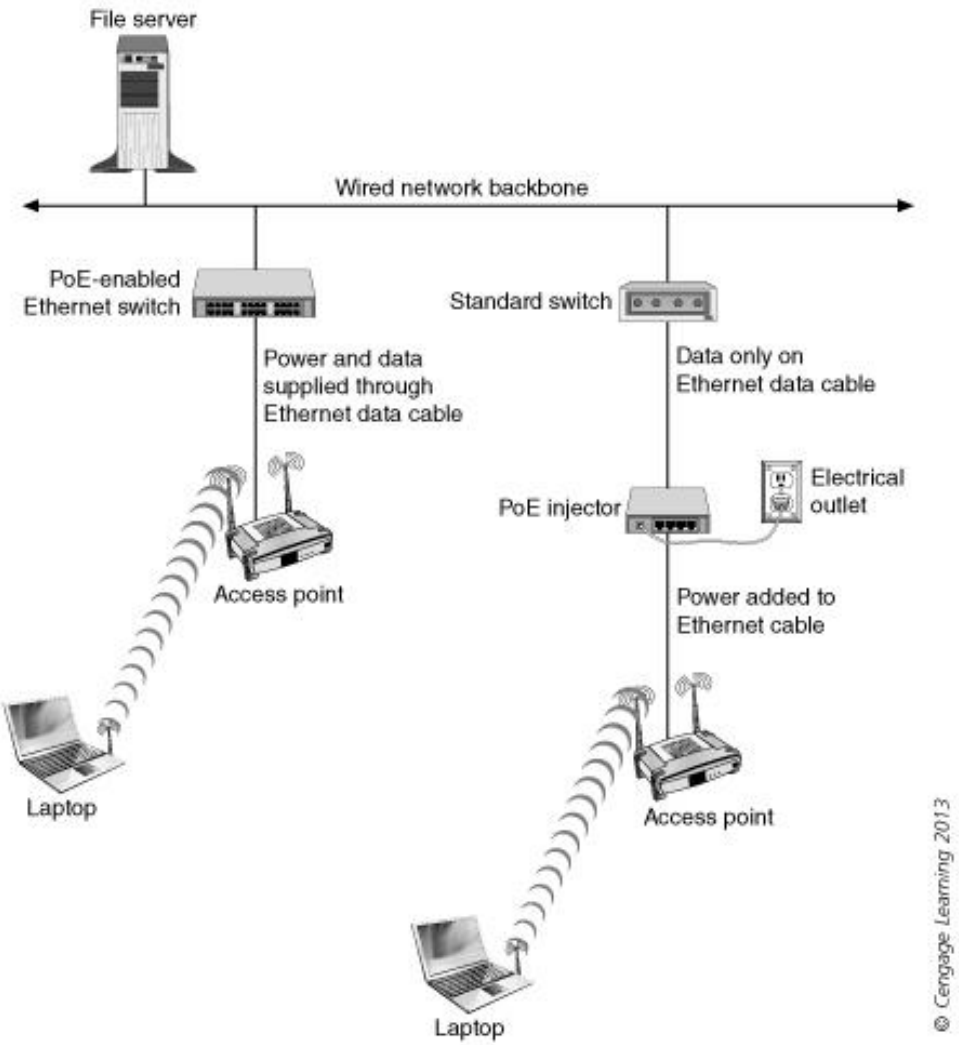

File server
Wired network backbone
PoE-enabled Ethernet switch
Power and data supplied through Ethernet data cable
Access point
Laptop
Standard switch
Data only on Ethernet data cable
PoE injector
Electrical outlet
Power added to Ethernet cable
Access point
Laptop
© Cengage Learning 2013

Figure 2-18 Power over Ethernet

Summary

- Standards ensure that devices from one vendor will interoperate with those from other vendors, and create competition between vendors
- There currently are three standards or types of wireless LANs: IEEE 802.11b, IEEE 802.11a, and IEEE 802.11g
- Wireless LAN devices are in many respects similar to those found in a wired network; the main difference is that wireless devices use an antenna or other means to send and receive signals instead of a wired connection

Summary

- An access point (AP) is both the base station for the wireless network and a bridge to connect the wireless network with the wired network
- A mesh access point does not have to be individually connected by a cable to the existing wired network
- A wireless workgroup bridge is a wireless device designed to connect a wired segment and a wireless segment (that are relatively close) together

Summary

- A remote wireless bridge connects two or more networks that are separated by a longer distance
- A gateway acts as an entrance to another network
- There are two types of gateways in wireless networks: Enterprise Encryption Gateway and a residential WLAN gateway
- Power over Ethernet technology allows an AP to be in almost any location because power is supplied through the Ethernet cable