

Computer Networking

Lecture 7

Hassan Alamri

Computer Networking: A Top-Down
Approach", James Kurose and Keith Ross ,
5th edition

Agenda

- Wireless Technology overview
- The IEEE 802.11 WLAN Standards
- Secure Wireless LANs
- CDMA Overview

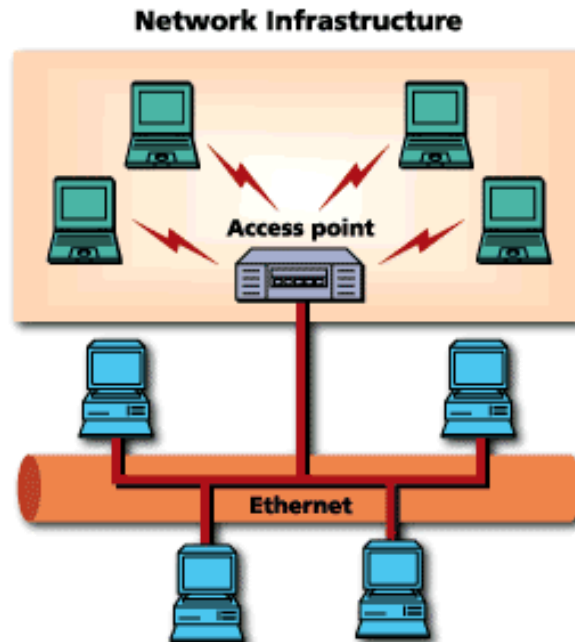
Wireless?

- A wireless LAN or WLAN is a wireless local area network that uses radio waves as its carrier.
- The last link with the users is wireless, to give a network connection to all users in a building or campus.
- The backbone network usually uses cables

Common Topologies

The wireless LAN connects to a wired LAN

- There is a need of an access point that bridges wireless LAN traffic into the wired LAN.
- The access point (AP) can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



Common Topologies

Complete Wireless Networks

- The physical size of the network is determined by the maximum reliable propagation range of the radio signals.
- Referred to as **ad hoc** networks
- Are self-organizing networks without any centralized control
- Suited for temporary situations such as meetings and conferences.



How do wireless LANs work?

Wireless LANs operate in almost the same way as wired LANs, using the same networking protocols and supporting the most of the same applications.

How are WLANs Different?

- They use specialized **physical and data link** protocols
- They integrate into existing networks through **access points** which provide a bridging function
- They let you stay connected as you **roam** from one coverage area to another
- They have unique **security** considerations
- They have specific **interoperability** requirements
- They require **different hardware**
- They offer **performance** that differs from wired LANs.

Physical and Data Link Layers

Physical Layer:

- The wireless **NIC** takes **frames** of data from the link layer, scrambles the data in a predetermined way, then uses the modified data stream to modulate a **radio carrier signal**.

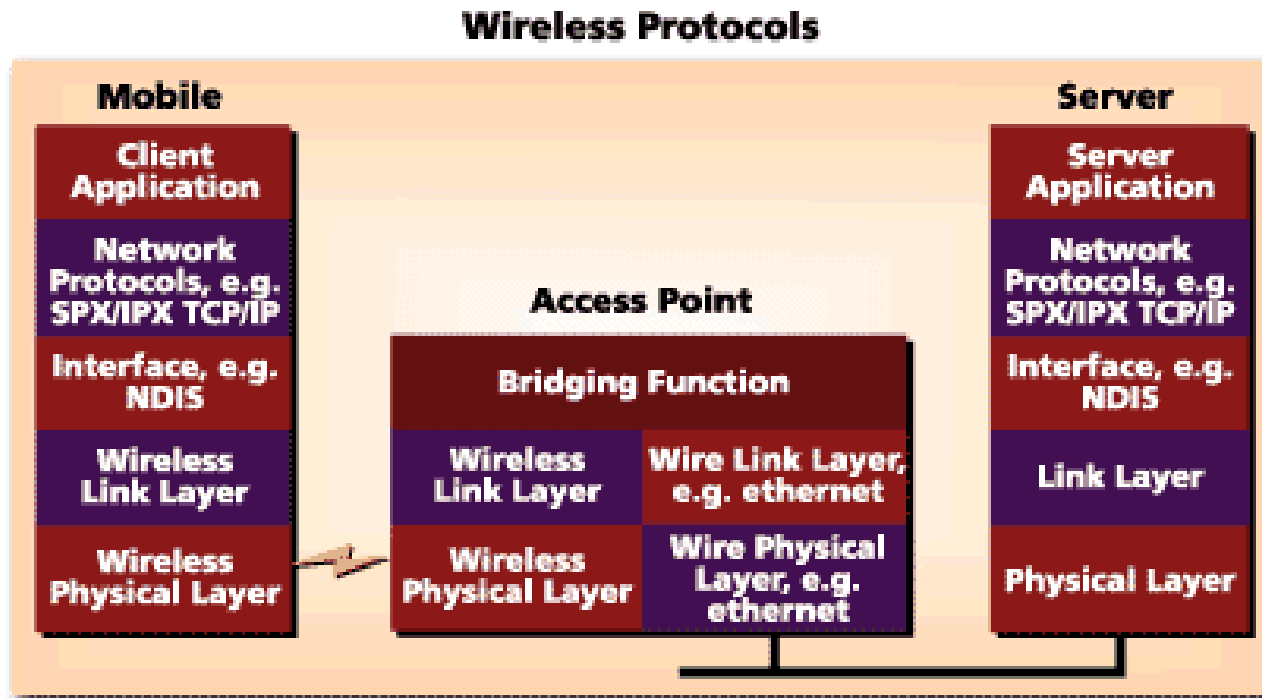
Data Link Layer:

- Uses **Carriers-Sense-Multiple-Access with Collision Avoidance (CSMA/CA)**.

Integration With Existing Networks

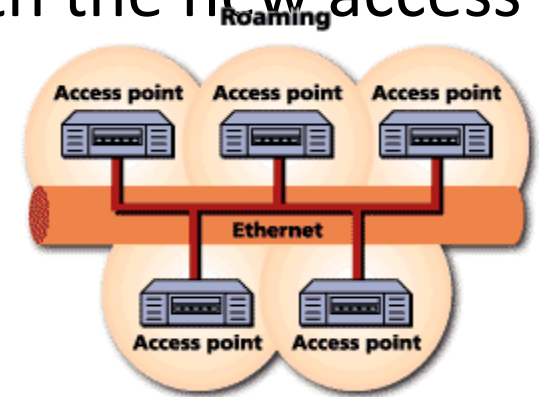
- Wireless Access Points (APs) - a small device that bridges wireless traffic to your network.
- Most access points bridge wireless LANs into Ethernet networks, but Token-Ring options are available as well.

Integration With Existing Networks



Roaming

- Users maintain a continuous connection as they roam from one physical area to another
- Mobile nodes automatically register with the new access point.
- Methods: DHCP, Mobile IP
- IEEE 802.11 standard does not address roaming, you may need to purchase equipment from one vendor if your users need to roam from one access point to another.



Security

- In theory, spread spectrum radio signals are inherently difficult to decipher without knowing the exact hopping sequences or direct sequence codes used
- The IEEE 802.11 standard specifies optional security called "**Wired Equivalent Privacy**" whose goal is that a wireless LAN offer privacy equivalent to that offered by a wired LAN. The standard also specifies optional authentication measures.

Hardware

- PC Card, either with integral antenna or with external antenna/RF module.
- ISA Card with external antenna connected by cable.
- Handheld terminals
- Access points

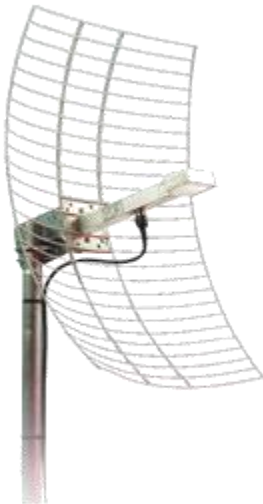
Hardware



CISCO Aironet 350 series



Wireless Handheld Terminal



Semi Parabolic Antenna

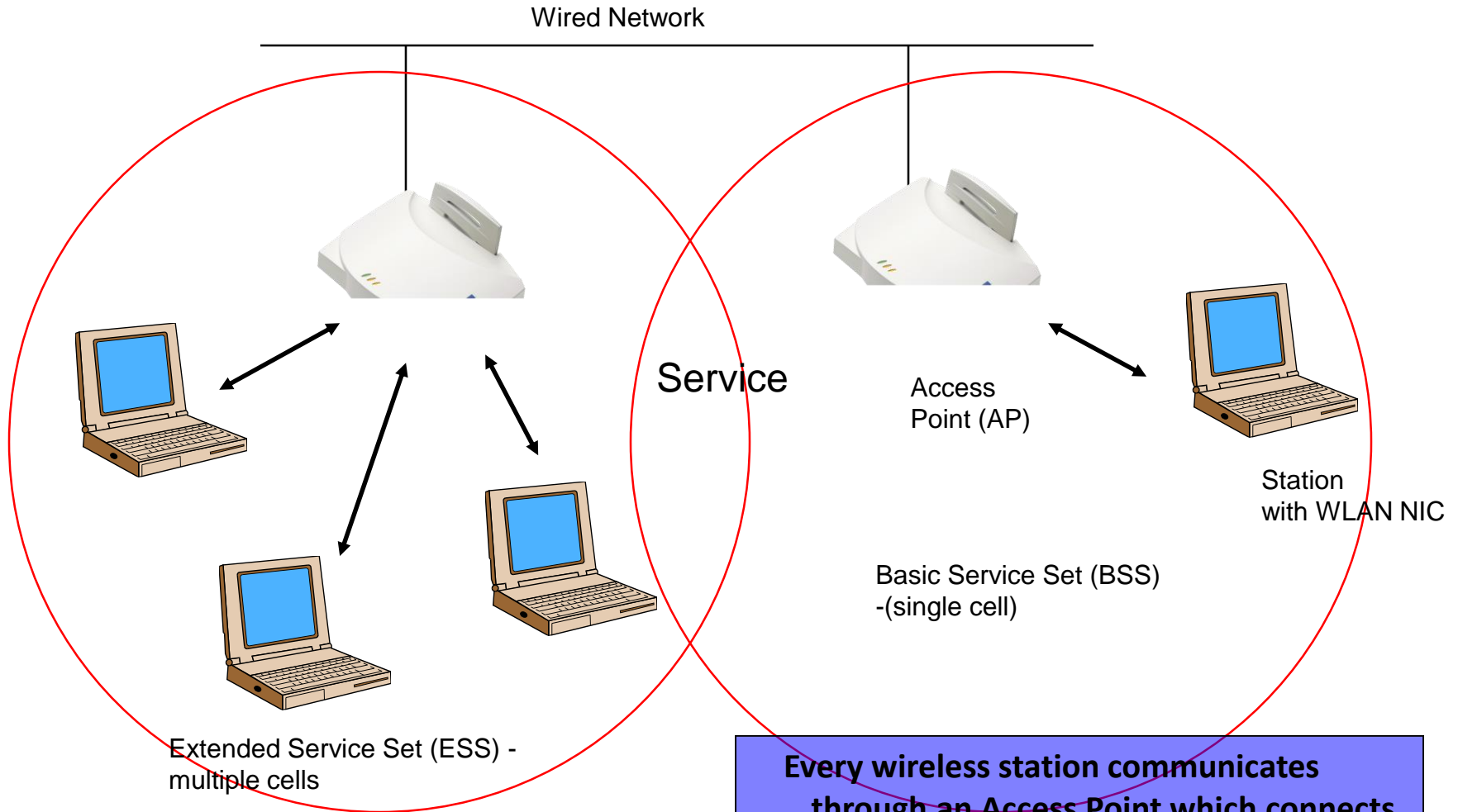


BreezeCOM AP

Performance

- **802.11a** offers speeds with a theoretically maximum rate of 54Mbps in the 5 GHz band
- **802.11b** offers speeds with a theoretically maximum rate of 11Mbps at in the 2.4 GHz spectrum band
- **802.11g** is a new standard for data rates of up to a theoretical maximum of 54 Mbps at 2.4 GHz.

INFRASTRUCTURE MODE



Every wireless station communicates through an Access Point which connects the station to the wired network

What is 802.11?

- A family of wireless LAN (WLAN) specifications developed by a working group at the Institute of Electrical and Electronic Engineers (IEEE)
- Defines standard for WLANs using the following four technologies
 - Frequency Hopping Spread Spectrum (FHSS)
 - Direct Sequence Spread Spectrum (DSSS)
 - Infrared (IR)
 - Orthogonal Frequency Division Multiplexing (OFDM)
- Versions: 802.11a, 802.11b, 802.11g, 802.11e, 802.11f, 802.11i

802.11a Vs. 802.11b

802.11a vs. 802.11b	802.11a	802.11b
Raw data rates	Up to 54 Mbps (54, 48, 36, 24, 18, 12 and 6 Mbps)	Up to 11 Mbps (11, 5.5, 2, and 1 Mbps)
Range	50 Meters	100 Meters
Bandwidth	UNII and ISM (5 GHz range)	ISM (2.4000— 2.4835 GHz range)
Modulation	OFDM technology	DSSS technology

Security Problems

- Security features in Wireless products are frequently not enabled.
- Use of static WEP keys (keys are in use for a very long time). WEP does not provide key management.
- Cryptographic keys are short.
- No user authentication occurs – only devices are authenticated. A stolen device can access the network.
- Identity based systems are vulnerable.
- Packet integrity is poor.

CDMA

- CDMA – Code Division Multiple Access
 - Fully digital wireless data transmission system
 - Not designed for voice at all
 - Uses special random numbers to encode bits of information.
 - Allows multiple access by assigning different users different random numbers on the same channel.
 - Users have control of a very wide channel bandwidth 1.5 to 5 MHz
 - The only limit to the system is the computing prowess of the base station and it's ability to separate noise from actual data.
 - Shannon's Theorem / SQR

Reference

- Computer Networking: A Top-Down Approach", James Kurose and Keith Ross , 5th edition