CprE 530

Lecture 7

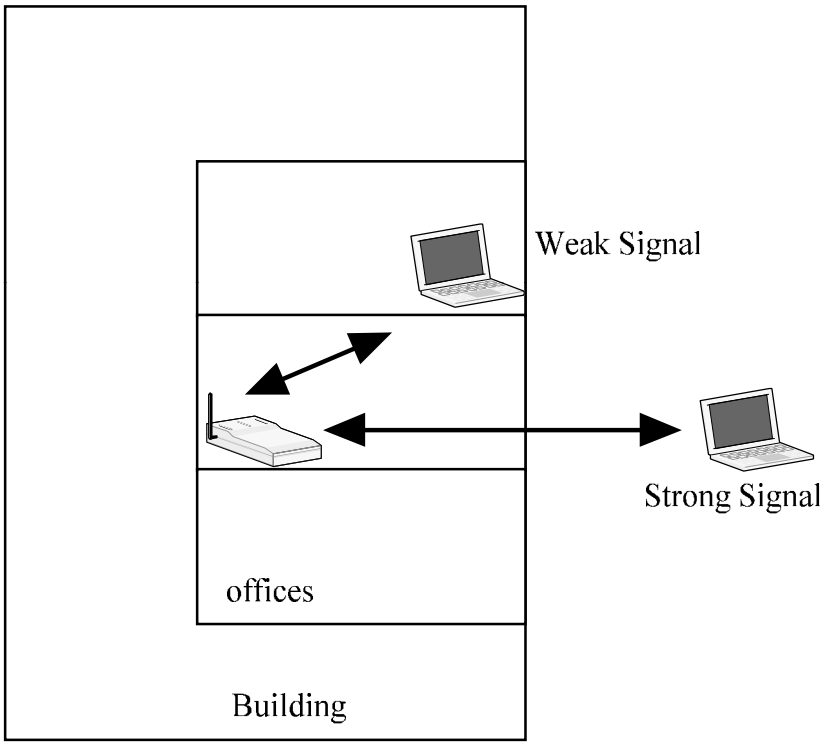
Topics

- Wireless Security
  - Standard
  - Devices
  - Protocol
  - Packet Format
  - Vulnerabilities
  - Mitigation

Wireless Standards

Name	Frequency	Data Rate	Max Distance
802.11a	5 GHz	54Mbps	30 meters
802.11b	2.4 GHz	11Mbps	30 meters
802.11g	2.4 GHz	11-54 Mbps	30 meters
802.11n	2.4 GHz	200-500 Mbps	50 meters

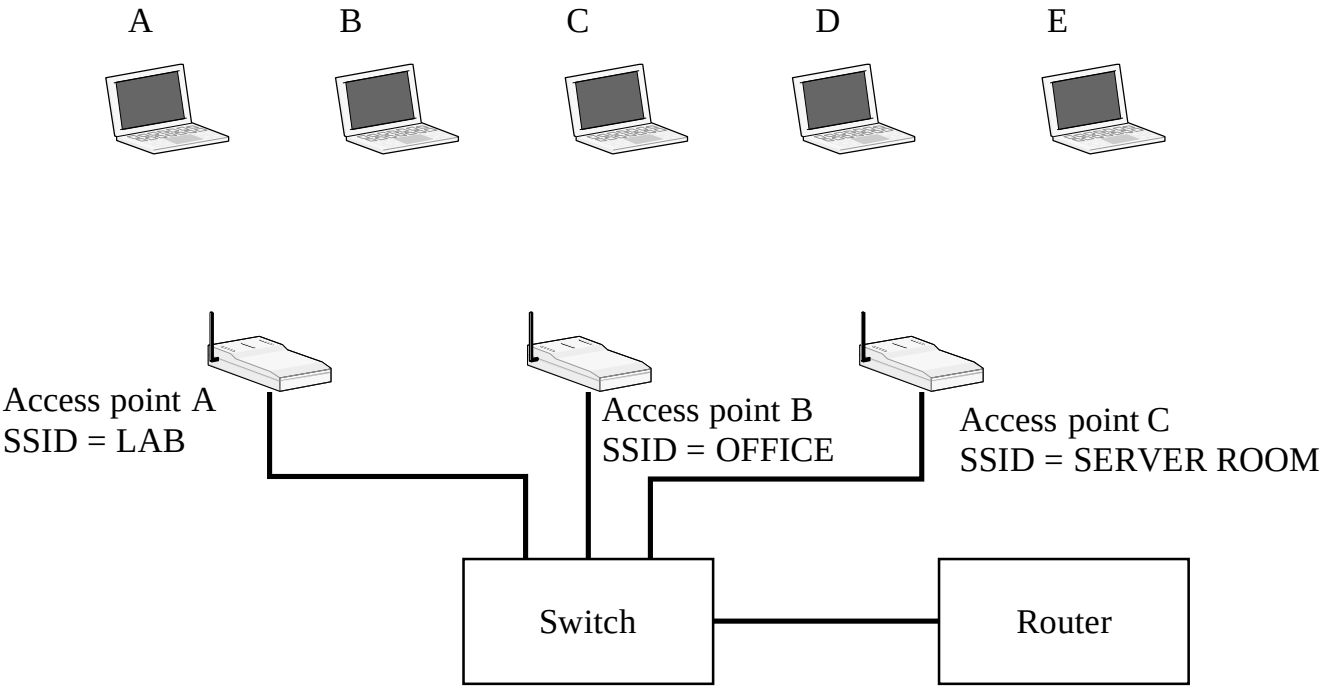
Signal Reflection



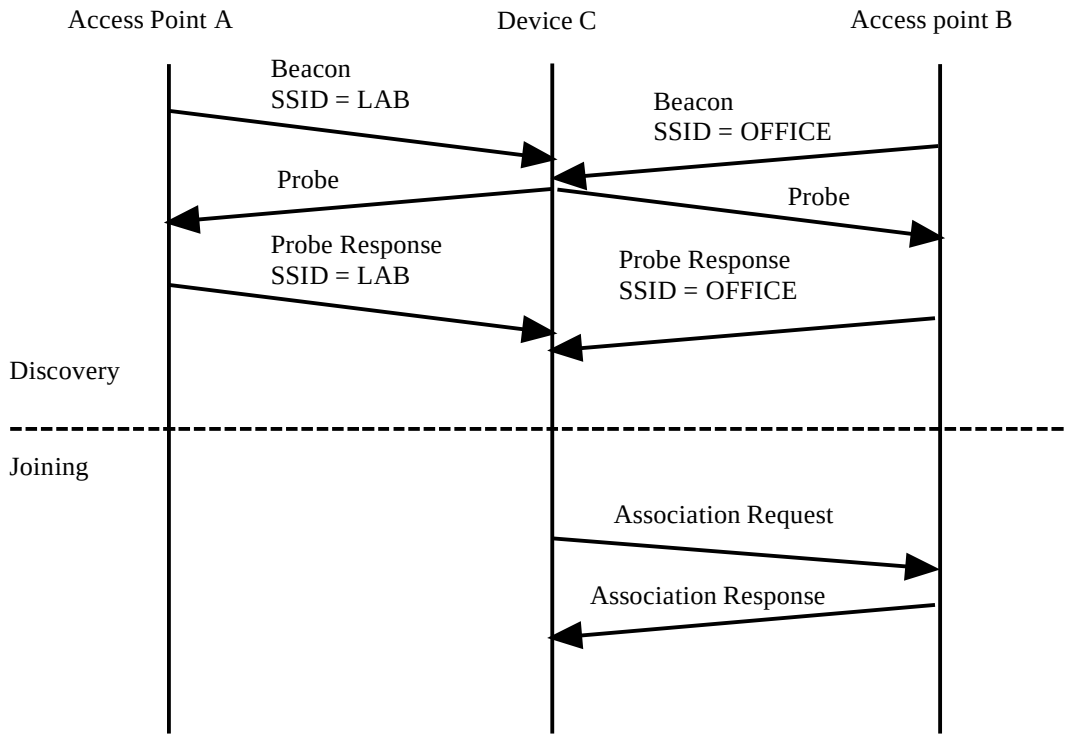
Wireless Ethernet 802.11

- Two topologies
  - IBSS Independent Basic Service Set
    - Ad-hoc, all stations are peers
  - ESS Extended Service Set
    - AP – Access points connected to a network
    - Station plus the AP form a BSS

Wireless Network Environment



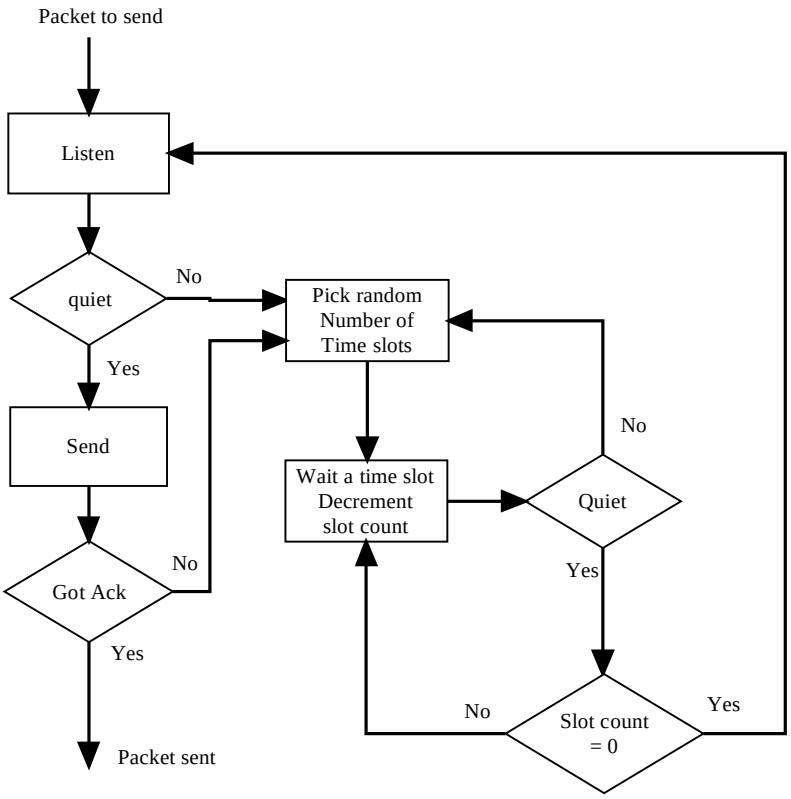
Discovery and joining



IEEE 802.11

- CSMA/CA
  - Wait till medium is free
  - Backoff after defer random amount
  - Exponential backoff for retransmission
  - Backoff timer resets if idle
  - Get an ACK if frame was received correctly

IEEE 802.11 Protocol

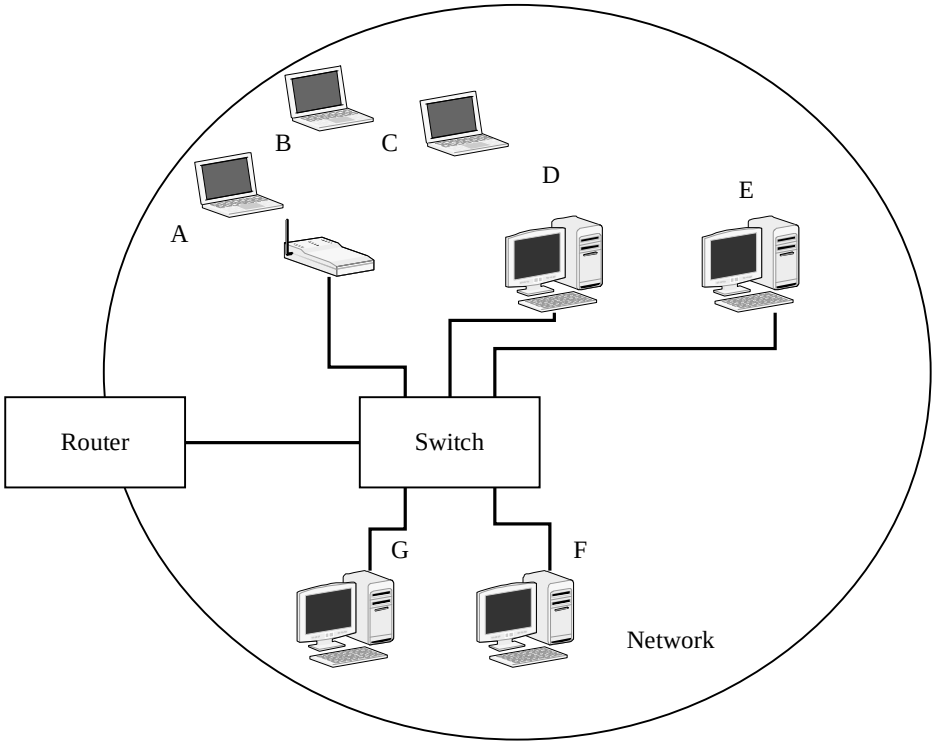


IEEE 802.11 Access Points

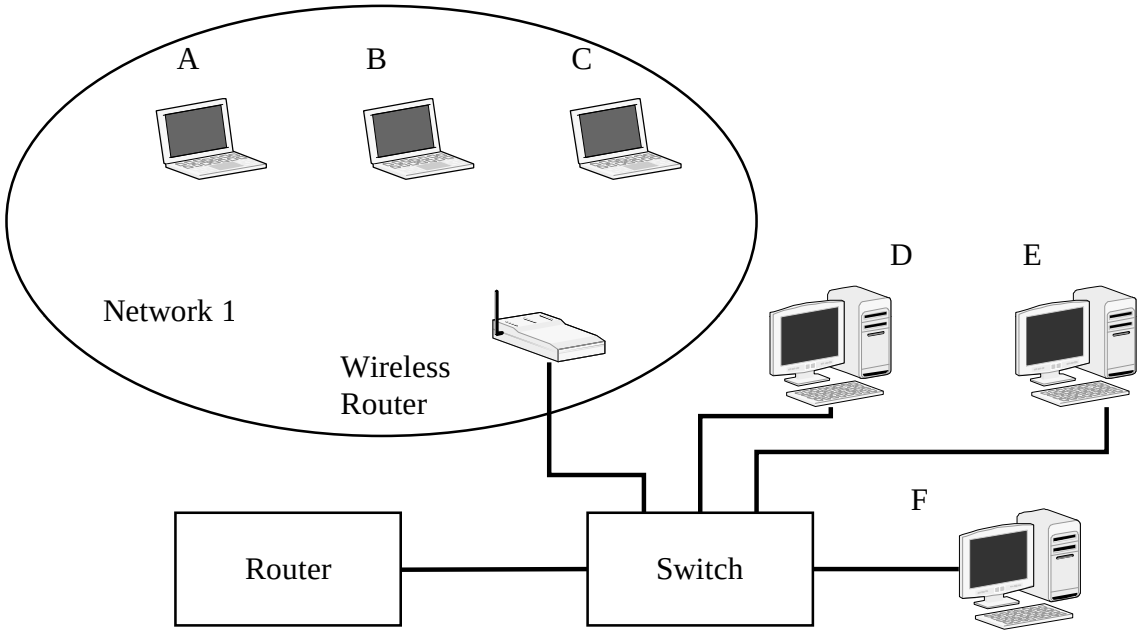
Two types

- Extended network
  - Access point makes the wireless devices look like they are on the same network as the wired devices
- Wireless router
  - Access point acts as a router

Extended Network

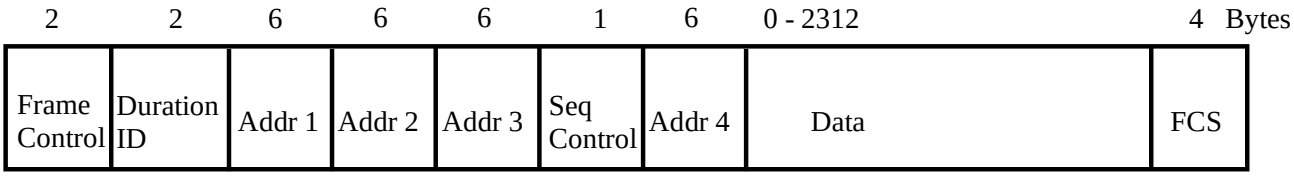


Wireless Router



Network 2

802.11 Frame Format



•**Frame Control:** Used to identify the frame type and other frame specific information.
•**Duration/ID:** Used to manage the access control protocol.
Address 1: Used to identify the destination of the transmitted packet. This is used by the hardware controller to determine if the frame should be read. If it does not match the address of the controller the remainder of the frame is ignored.

802.11 Frame Format

- **Address 2:** Address of the transmitting device.
- **Address 3:** Used when the access point is part of an extended network where the access point will relay the traffic.
- **Address 4:** Used when the access point is part of an extended network where the access point will relay the traffic

802.11 Frame Format

- **Sequence Control:** Used by the acknowledgement process.
- **Data:** The data field contains the data. The data field length is limited to 2312 bytes. Wireless Ethernet does not have a minimum data length.
- **Frame Check Sequence (FCS):** This field is used to help verify that the frame has not been corrupted during transmission.

Header Based

- Setting the destination address as a broadcast address can cause traffic problems
- Denial of Service
  - Invalid headers will cause loss of access or loss of association
- Not easy to fix

Protocol-Based

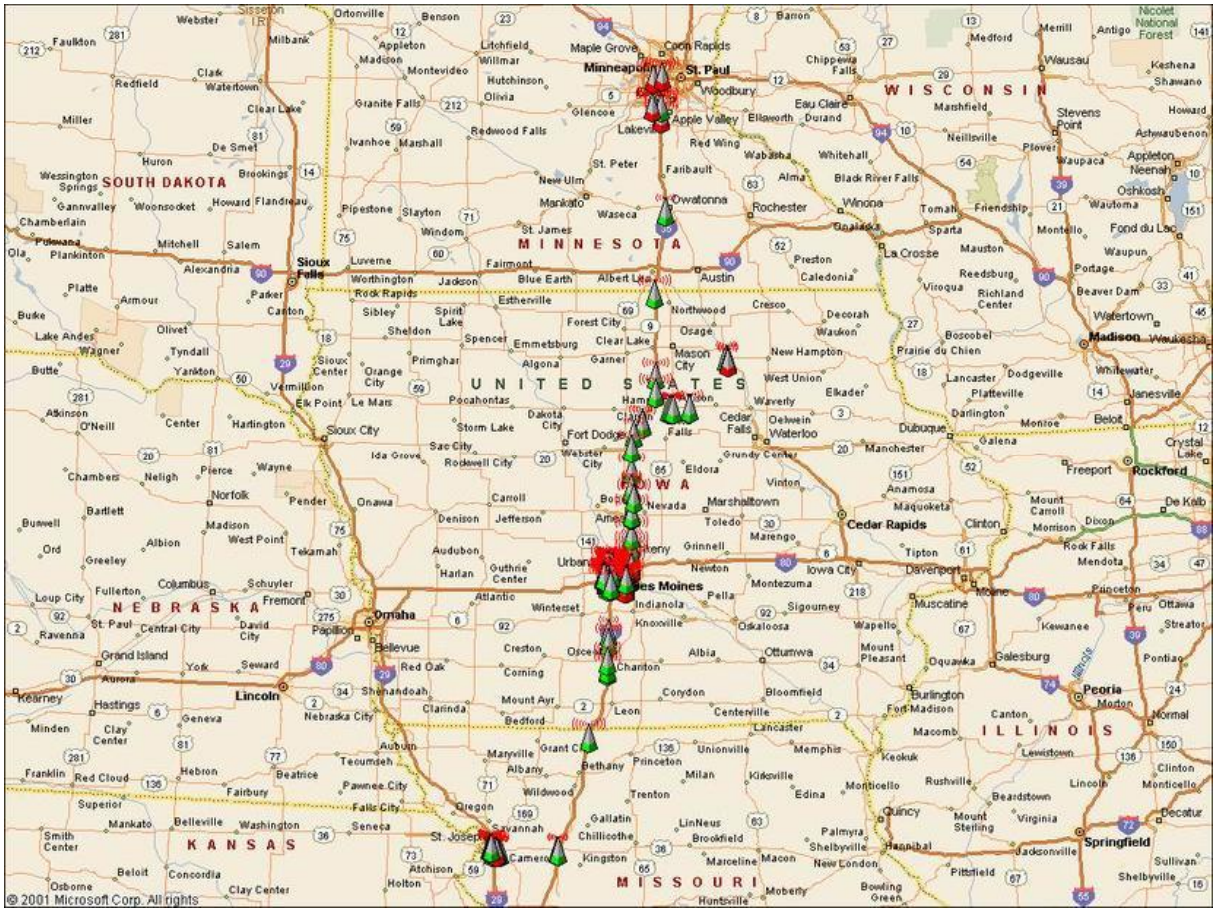
- Protocol is simple and is in hardware
- Can transmit packets to cause Denial of service
- Jamming of signals by ignoring the protocol
- Very hard to stop

Protocol-Based

- Access point can broadcast its SSID
  - Wardriving
- www.wardriving.com
- www.worldwidewardrive.org

Wardriving How easy

- One laptop with wireless
- Free software
- GPS optional



Wardriving

Mitigation:

- Do we need to mitigate it?
- Turn off broadcast of SSID
- Use encryption or Network Access Control (NAC) (make it an authentication problem)

SSID discovery

- Sometimes additional information is provided by the SSID that could help an attacker
- Business name
- Home address or user's last name