18-452/18-750
Wireless Networks and Applications
Lecture 9:
WiFi Header and Management

Peter Steenkiste

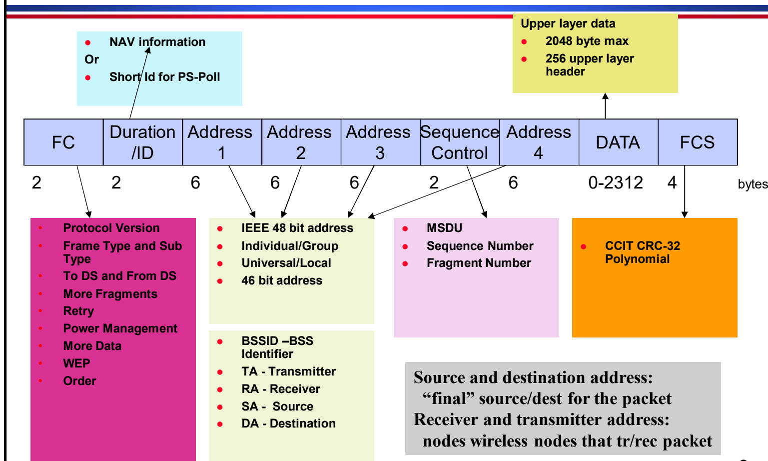
Spring Semester 2020

http://www.cs.cmu.edu/~prs/wirelessS20/

Outline

- 802 protocol overview
- Wireless LANs – 802.11
  - » Overview of 802.11
  - » 802.11 MAC, frame format, operations
  - » 802.11 management
  - » 802.11*
  - » Deployment example
- Personal Area Networks – 802.15

801.11 MAC Frame Format



Detailed 802.11 MAC Frame Format

MAC header

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame control	Duration/ ID	Address 1	Address 2	Address 3	Seq. control	Address 4	Frame body	FCS

	Protocol version	Type	Sub-type	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
bits	2	2	4	1	1	1	1	1	1	1	1

Packet Types

- Type/sub-type field is used to indicate the type of the frame
- Management:
  - » Association/Authentication/Beacon
- Control
  - » RTS, CTS, CF-end, ACK
- Data
  - » Data only, or Data + CF-ACK, or Data + CF-Poll or Data + CF-Poll + CF-ACK

Addressing Fields

To DS	From DS	Message	Address 1	Address 2	Address 3	Address 4
0	0	station-to-station frames in an IBSS (ad hoc); all mgmt/control frames	DA	SA	BSSID	N/A
0	1	From AP to station	DA	BSSID	SA	N/A
1	0	From station to AP	BSSID	SA	DA	N/A
1	1	From one AP to another in same DS	RA	TA	DA	SA

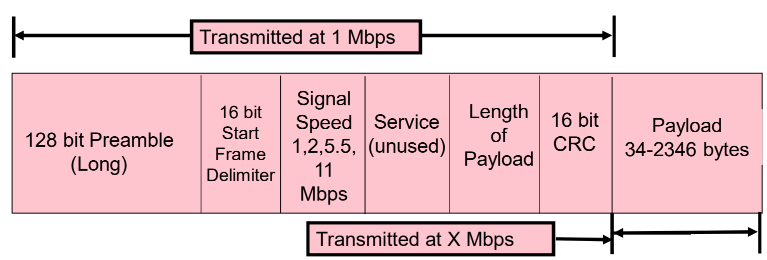
RA: Receiver Address TA: Transmitter Address
DA: Destination Address SA: Source Address
BSSID: MAC address of AP in an infrastructure BSS

Some More Fields

- Duration/ID: Duration in DCF mode/ID is used in PCF mode
- More Frag: 802.11 supports fragmentation of data
- More Data: In polling mode, station indicates it has more data to send when replying to CF-POLL
- RETRY is 1 if frame is a retransmission; WEP (Wired Equivalent Privacy)
- Power Mgmt is 1 if in Power Save Mode; Order = 1 for strictly ordered service

PLCP: Long Preamble (802.11b)

- PLCP: Physical Layer Convergence Procedure
- Long Preamble = 144 bits
  - Interoperable with older 802.11 devices
  - Entire Preamble and 48 bit PLCP Header sent at *1 Mbps*



PLCP: Short Preamble

- Short Preamble = 72 bits
  - Preamble transmitted at 1 Mbps
  - PLCP Header transmitted at 2 Mbps
  - More efficient than long preamble
- Different formats for later (OFDM) standards

Transmitted at 1 Mbps		Transmitted at 2 Mbps				Transmitted at X Mbps
56 bit Preamble	16 bit Start Frame Delimiter	Signal Speed 1,2,5.5, 11 Mbps	Service (unused)	Length of Payload	16 bit CRC	Payload 34-2346 bytes

Multi-bit Rate

- 802.11 allows for multiple bit rates
  - » Allows for adaptation to channel conditions
  - » Specific rates dependent on the version
- Algorithm for selecting the rate is not defined by the standard – left to vendors
  - » Still a research topic!
  - » More later in the semester
- Packets have multi-rate format
  - » Different parts of the packet are sent at different rates
  - » Why?

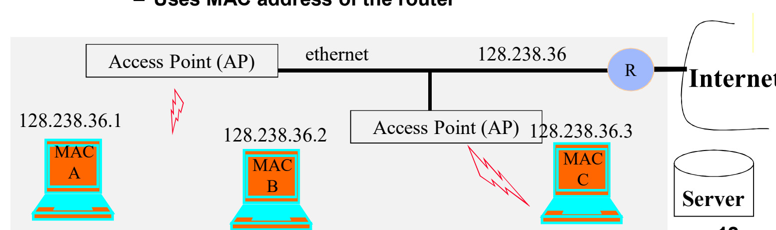
Data Flow Examples

- Case 1: Packet from a station under one AP to another in same AP's coverage area
- Case 2: Packet between stations in an IBSS
- Case 3: Packet from an 802.11 station to a wired server on the Internet
- Case 4: Packet from an Internet server to an 802.11 station

Some Background: Forwarding Logic

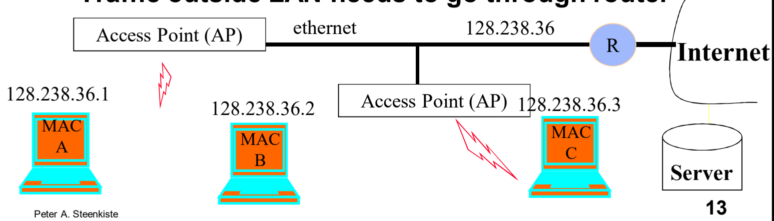
- When node needs to send an IP packet:
  - » In the same IP network?
    - – Check destination IP address
  - » Yes: forward based on MAC address
    - – Uses ARP protocol to map IP to MAC address
  - » No: forward packet to "gateway" router
    - – Uses MAC address of the router

Application
Presentation
Session
Transport
Network
Data link
Physical

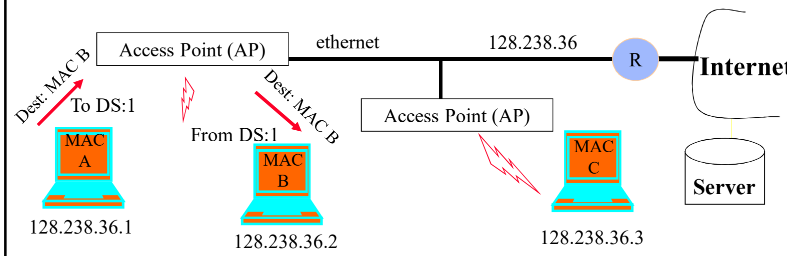


Communication in LANs

- Every interface to the network has a IEEE MAC and an IP address associated with it
  - » True for both end-points and routers
- IP address inside a LAN share a prefix
  - » Prefix = first part of the IP address, e.g., 128.238.36
  - » Can be used to determine whether devices are on same LAN
- Traffic outside LAN needs to go through router

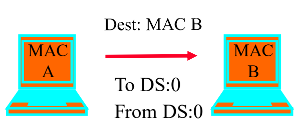


Case 1: Communication Inside BSS



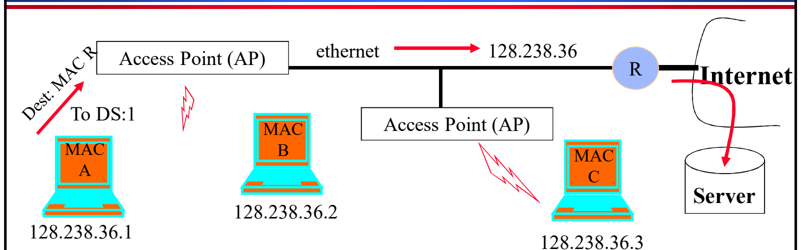
- AP knows which stations are registered with it so it knows when it can send frame directly to the destination
- Frame can be set directly to the destination by AP

Case 2: Ad Hoc



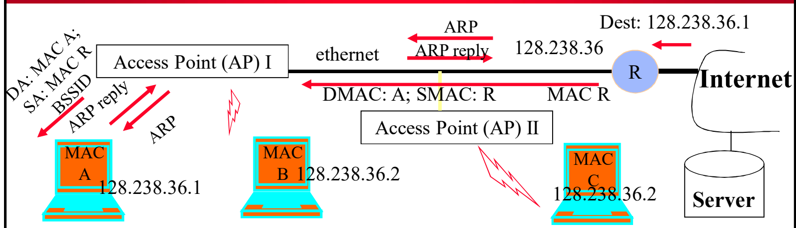
- Direct transmit only in IBSS (Independent BSS), i.e., without AP
- Note: in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B

Case 3: To the Internet



- MAC A determines IP address of the server (using DNS)
- From the IP address, it determines that server is in a different subnet
- Hence it sets MAC R as DA;
  - » Address 1: BSSID, Address 2: MAC A; Address 3: DA
- AP will look at the DA address and send it on the ethernet
  - » AP is an 802.11 to ethernet bridge
- Router R will relay it to server

Case 4: From Internet to Station



- Packet arrives at router R – uses ARP to resolve destination IP address
  - » AP knows nothing about IP addresses, so it will simply broadcast ARP on its wireless link
  - » DA = all ones – broadcast address on the ARP
- MAC A host replies with its MAC address (ARP reply)
  - » AP passes on reply to router
- Router sends data packet, which the AP simply forwards because it knows that MAC A is registered
- Will AP II broadcast the ARP request on the wireless medium? How about the data packet?

Summary

- Wifi packets have 4 MAC addresses
- Needed to support communication inside a LAN, across access points connected by a wired LAN
- WiFi frames have a multi-rate format, i.e., different parts are sent at different rates
  - » The header is sent at a lower rate to improve chances it can be decoded by receivers
  - » Contains critical information such as virtual carrier sense, and the bit rate used for the data

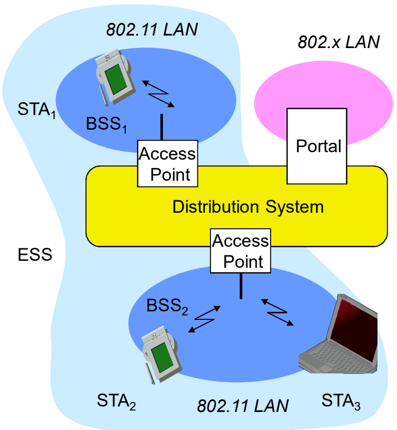
Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

Management and Control Services

- Association management
- Handoff
- Security: authentication and privacy
- Power management
- QoS

802.11: Infrastructure Reminder



- Station (STA)
  - » terminal with access mechanisms to the wireless medium and radio contact to the access point
- Access Point
  - » station integrated into the wireless LAN and the distribution system
- Basic Service Set (BSS)
  - » group of stations using the same AP
- Portal
  - » bridge to other (wired) networks
- Distribution System
  - » interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

Service Set Identifier - SSID

- Mechanism used to segment wireless networks
  - » Multiple independent wireless networks can coexist in the same location
  - » Effectively the name of the wireless network
- Each AP is programmed with a SSID that corresponds to its network
- Client computer presents correct SSID to access AP
- Security Compromises
  - » AP can be configured to "broadcast" its SSID
  - » Broadcasting can be disabled to improve security
  - » SSID may be shared among users of the wireless segment

Association Management

- Stations must associate with an AP before they can use the wireless network
  - » AP must know about them so it can forward packets
  - » Often also must authenticate
- Association is initiated by the wireless host – involves multiple steps:
  1. Scanning: finding out what access points are available
  2. Selection: deciding what AP (or ESS) to use
  3. Association: protocol to "sign up" with AP – involves exchange of parameters
  4. Authentication: needed to gain access to secure APs – manyoptions possible
- Disassociation: station or AP can terminate association

Association Management: Scanning

- Stations can detect AP using scanning
- Passive Scanning: station simply listens for Beacon and gets info of the BSS
  - » Beacons are sent roughly 10 times per second
  - » Power is saved
- Active Scanning: station transmits Probe Request; elicits Probe Response from AP
  - » Saves time + is more thorough
  - » Wait for 10-20 msec for response
- Scanning all available channels can become very time consuming!
  - » Especially with passive scanning
  - » Cannot transmit and receive frames during most of that time – not a big problem during initial association

Association Management: Selecting an AP and Joining

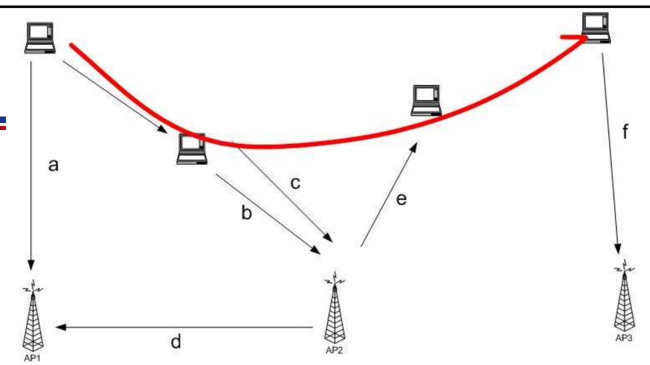
- Selecting a BSS or ESS typically must involve the user
  - » What networks do you trust? Are you willing to pay?
  - » Can be done automatically based on stated user preferences (e.g., the "automatic" list in Windows)
- The wireless host selects the AP it will use in an ESS based on vendor-specific algorithm
  - » Uses the information from the scan
  - » Typically simply joins the AP with the strongest signal
- Associating with an AP
  - » Synchronization in Timestamp Field and frequency
  - » Adopt PHY parameters
  - » Other parameters: BSSID, WEP, Beacon Period, etc.

Association Management: Roaming

- Reassociation: association is transferred from active AP to a new target AP
  - » Supports mobility in the same ESS – layer 2 roaming
- Reassociation is initiated by wireless host based on vendor specific algorithms
  - » Implemented using an Association Request Frame that is sent to the new AP
  - » New AP accepts or rejects the request using an Association Response Frame
- Coordination between APs is defined in 802.11f
  - » Allows forwarding of frames in multi-vendor networks
  - » Inter-AP authentication and discovery typically coordinated using a RADIUS server
  - » "Fast roaming" support (802.11r) also streamlines authentication and QoS, e.g. for VoIP

Association Management: Reassociation Algorithms

- Failure driven: only try to reassociate after connection to current AP is lost
  - » Typically efficient for stationary clients since it not common that the best AP changes during a session
  - » Mostly useful for nomadic clients
  - » Can be very disruptive for mobile devices
- Proactive reassociation: periodically try to find an AP with a stronger signal
  - » Tricky part: cannot communicate while scanning other channels
  - » Trick: user power save mode to "hold" messages
  - » Throughput during scanning is still affected though
    - – Mostly affects latency sensitive applications



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

Outline

- Brief history
- 802 protocol overview
- Wireless LANs – 802.11 – overview
- 802.11 MAC, frame format, operations
- 802.11 management
- 802.11 security
- 802.11 power control
- 802.11*
- 802.11 QoS

WLAN Security Requirements

- Authentication: only allow authorized stations to associate with and use the AP
- Confidentiality: hide the contents of traffic from unauthorized parties
- Integrity: make sure traffic contents is not modified while in transit

WLAN Security Exploits

- Insertion attacks: unauthorized Clients or AP
  - » Client: reuse MAC or IP address –free service on “secured” APs
  - » AP: impersonate an AP, e.g., use well known name
- Interception and unauthorized monitoring
  - » Packet Analysis by “sniffing” – listening to all traffic
- Brute Force Attacks Against AP Passwords
  - » Dictionary Attacks Against SSID
- Encryption Attacks
  - » Exploit known weaknesses of WEP
- Misconfigurations, e.g., use default password
- Jamming – denial of service
  - » Cordless phones, baby monitors, leaky microwave oven, etc.

Security in 802.11

- 802.1x: port-based authentication for LANs
  - » Port-based authentication for LANs
- WEP: Wired Equivalent Privacy
  - » Achieve privacy similar to that on LAN through encryption
  - » Intended to provide both privacy and integrity
  - » RC4 and CRC32
  - » Has known vulnerabilities
- WPA: Wi-Fi Protected Access
  - » Larger, dynamically changed keys
- 802.11i (WPA2)
  - » Builds on WPA but fixes various vulnerability
  - » Uses AES for encryption (TKIP version is deprecated)
    - – Pre-shared keys (PSK) versus Enterprise options

MAC Filtering

- Each client is identified by its 802.11 Mac Address
- Each AP can be programmed with the set of MAC addresses it accepts ("white list")
- Combine this filtering with the AP's SSID
- Very simple solution
  - » Some overhead to maintain list of MAC addresses
- But it is possible to forge MAC addresses …
  - » Unauthorized client can "borrow" the MAC address of an authenticated client
  - » Built in firewall will discard unexpected packets

Wired Equivalent Privacy WEP

- Original standard for WiFi security
- Very weak standard: key could be cracked with a couple of hours of computing (much faster today)
  - » Too much information is transmitted in the clear
  - » No protocol for encryption key distribution
  - » Clever optimizations can reduce time to minutes
- All data then becomes vulnerable to interception
  - » WEP typically uses a single shared key for all stations
- The CRC32 check is also vulnerable so that the data could be altered as well
  - » Can makes changes without even decrypting!
- Not recommended

Wi-Fi Protected Access WPA

- Introduced by Wi-Fi Alliance as an interim solution after WEP flaws were published
  - » Uses a different Message Integrity Check
  - » Encryption still based on RC4, but uses 176 bit key (48bit IV) and keys are changed periodically
  - » Also frame counter in MIC to prevent replay attacks.
- Can be used with 802.1x authentication (optional)
  - » It generates a long WPA key that is randomly generated, uniquely assigned and frequently changed.
  - » Attacks are still possible since people sometimes use short, poorly random WPA keys that can be cracked
- 802.11i is a "permanent" security fix
  - » Builds on the interim WPA standard (i.e. WPA2)
  - » Replaces RC4 by the more secure Advanced Encryption Standard (AES) block encryption
  - » Better key management and data integrity
  - » Uses 802.1x for authentication.

Authentication in WLAN Hotspots

- Upon association with the AP, only authentication traffic can pass through, as defined by IEEE 802.1x

- The protocol used to transport authentication traffic is the Extensible Authentication Protocol (EAP - RFC3748)

Dual SSID Approach