18-452/18-750
Wireless Networks and Applications
Lecture 10:
WiFi Header and Management

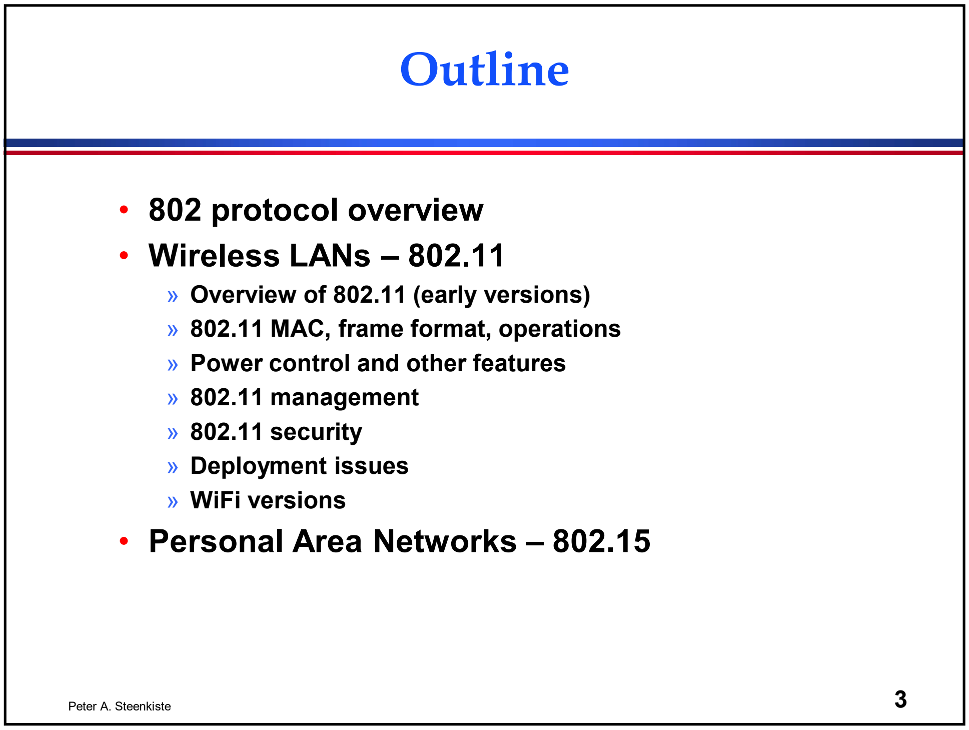
Peter Steenkiste

Spring Semester 2024

http://www.cs.cmu.edu/~prs/wirelessS24/

Announcements

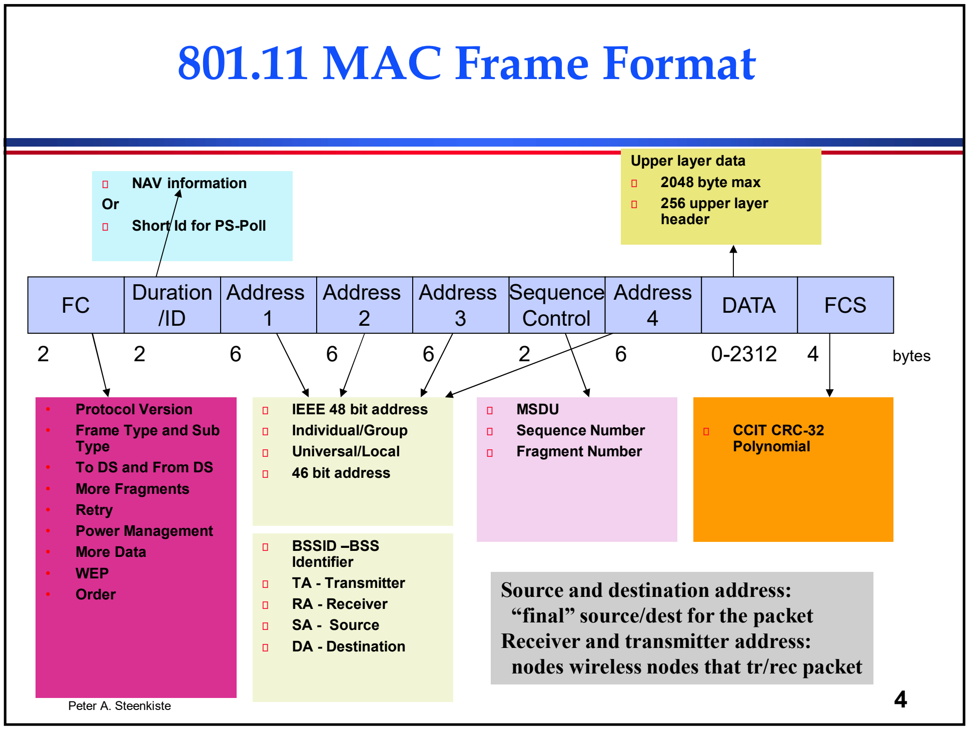
- Project handouts and homeworks are posted on Canvas
- You submit your assignments through Canvas as well (except for P2)
- If you have trouble setting up Wireshark, please attend Sofia's office hours
- For Windows users with a "bad" adapter
  - » I have a second USB adapter
  - » I have a MAC OS system if you want to try it



Outline

- 802 protocol overview
- Wireless LANs – 802.11
  - Overview of 802.11 (early versions)
  - 802.11 MAC, frame format, operations
  - Power control and other features
  - 802.11 management
  - 802.11 security
  - Deployment issues
  - WiFi versions
- Personal Area Networks – 802.15

Peter A. Steenkiste



801.11 MAC Frame Format

FC	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	DATA	FCS	
2	2	6	6	6	2	6	0-2312	4	bytes

- NAV information

Or

- Short Id for PS-Poll

Upper layer data

- 2048 byte max
- 256 upper layer header

- Protocol Version
- Frame Type and Sub Type
- To DS and From DS
- More Fragments
- Retry
- Power Management
- More Data
- WEP
- Order

- IEEE 48 bit address
- Individual/Group
- Universal/Local
- 46 bit address

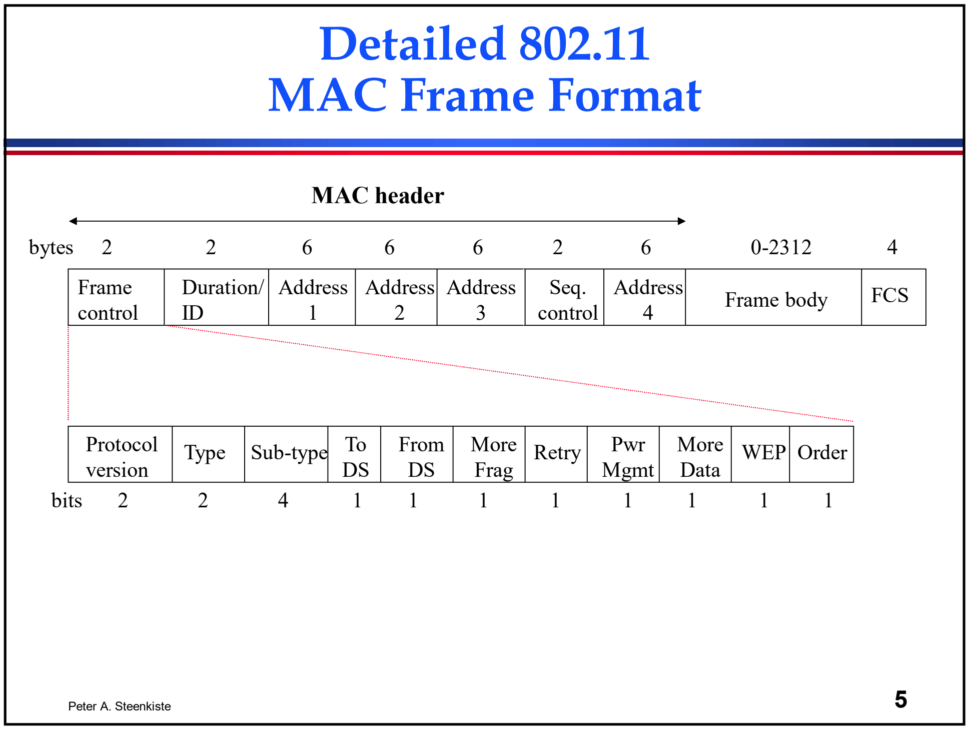
- BSSID –BSS Identifier
- TA - Transmitter
- RA - Receiver
- SA - Source
- DA - Destination

- MSDU
- Sequence Number
- Fragment Number

- CCIT CRC-32 Polynomial

Source and destination address:
"final" source/dest for the packet
Receiver and transmitter address:
nodes wireless nodes that tr/rec packet

Peter A. Steenkiste



Detailed 802.11 MAC Frame Format

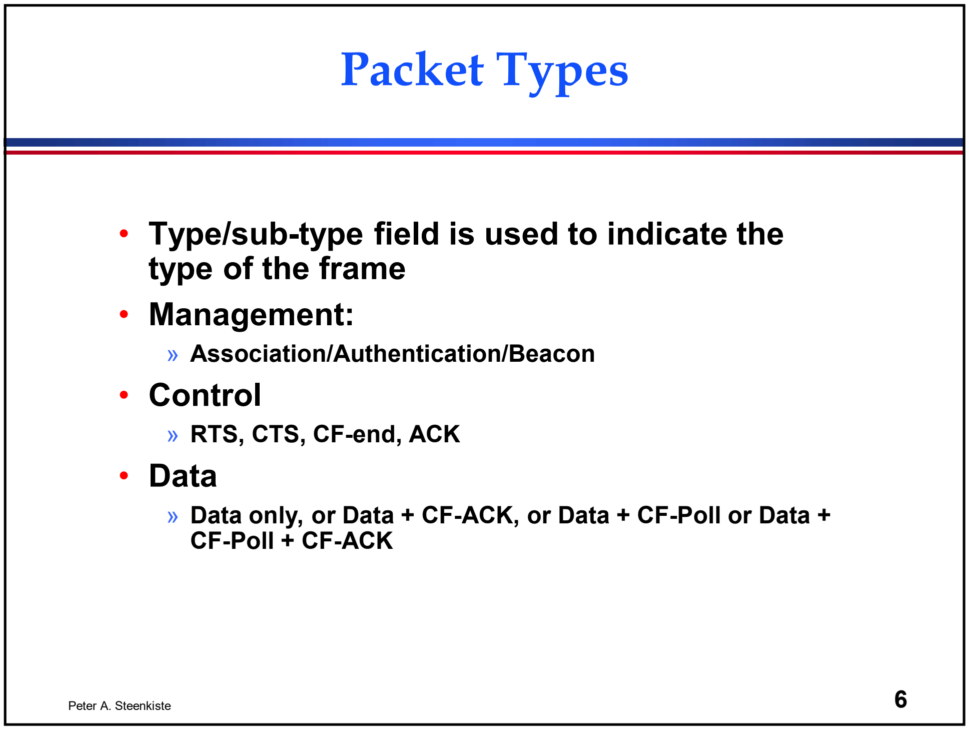
MAC header

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

Peter A. Steenkiste

5

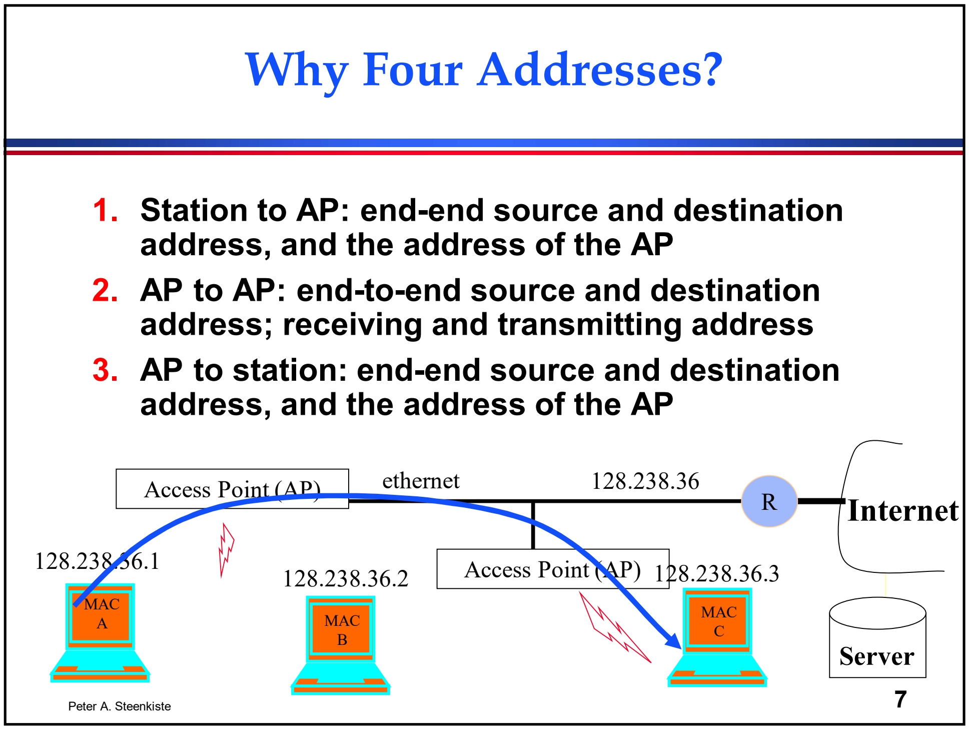


Packet Types

- 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

Peter A. Steenkiste

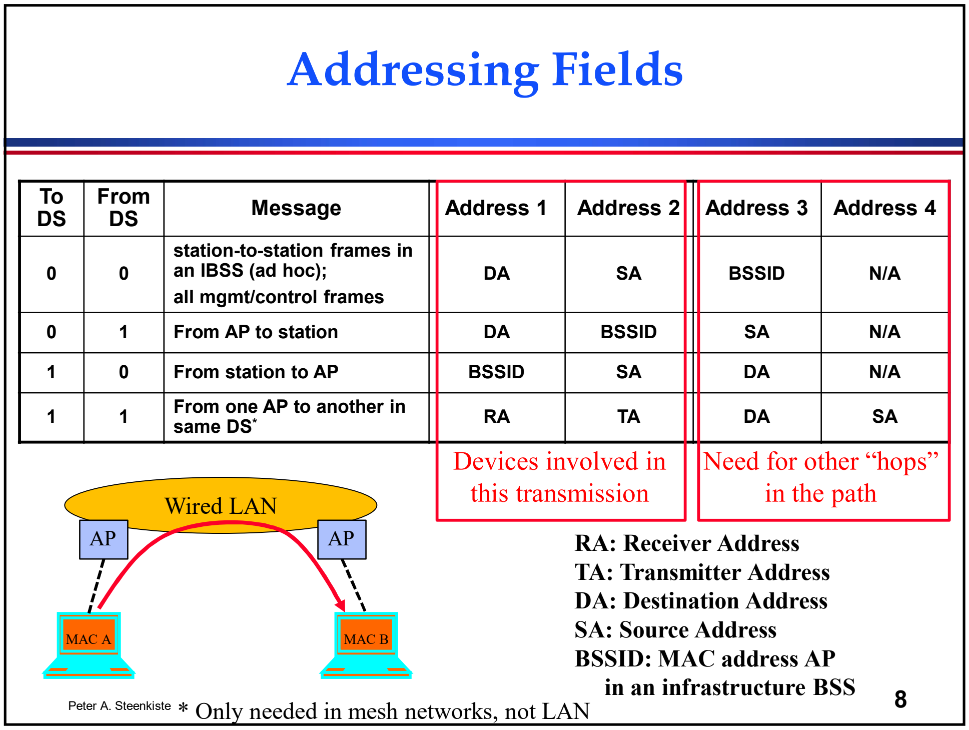
6



Why Four Addresses?

1. Station to AP: end-end source and destination address, and the address of the AP
2. AP to AP: end-to-end source and destination address; receiving and transmitting address
3. AP to station: end-end source and destination address, and the address of the AP

Access Point (AP)
ethernet
128.238.36
R
Internet
128.238.36.1
MAC A
128.238.36.2
MAC B
Access Point (AP)
128.238.36.3
MAC C
Server



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

Devices involved in this transmission

Need for other "hops" in the path

Wired LAN
AP
AP
MAC A
MAC B

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

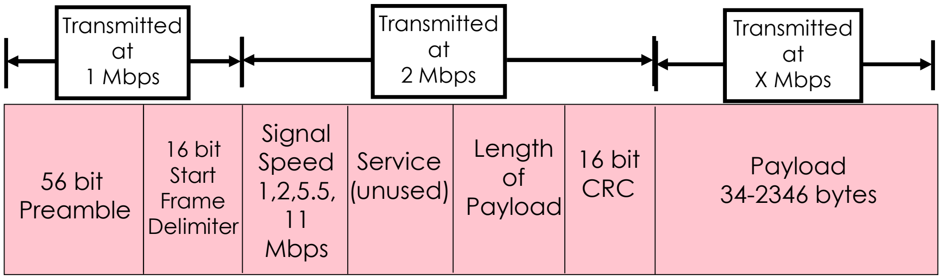
* Only needed in mesh networks, not LAN

Some More Fields

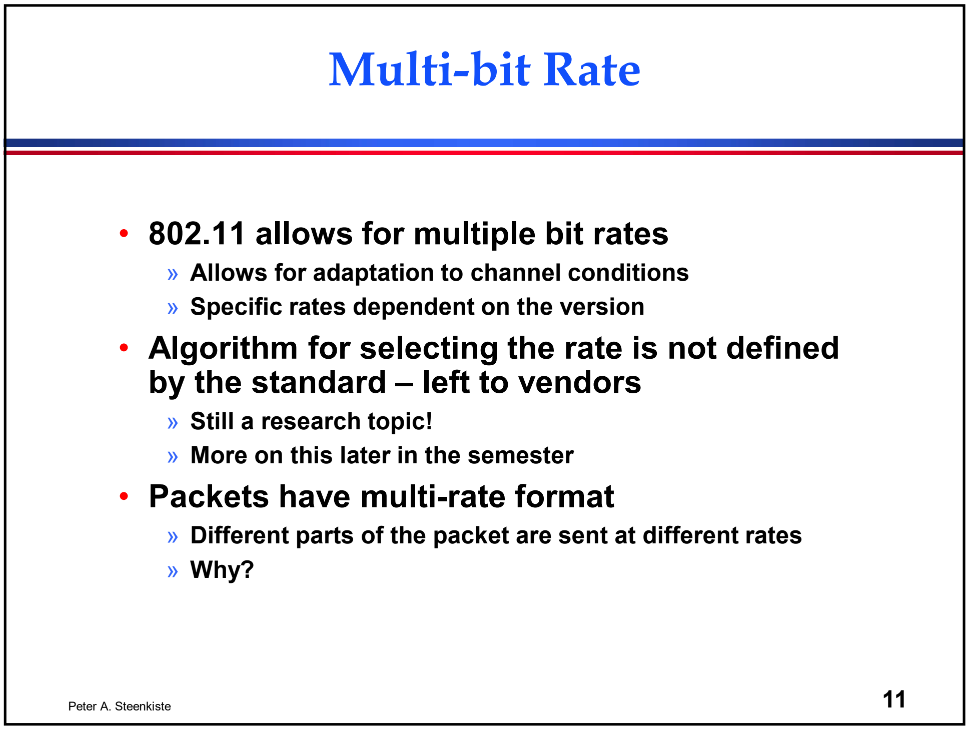
- Duration/ID: SIFS+ACK in DCF mode/ID is used in PCF mode (discussed later)
- More Frag: 802.11 supports fragmentation of data
- More Data: In polling mode, station indicates it has more data to send when replying to CF-POLL (PCF)
- RETRY is 1 if frame is a retransmission; WEP (Wired Equivalent Privacy)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

802.11b PLCP: Short Preamble

- PLCP: Physical Layer Convergence Procedure
- Short Preamble = 72 bits
  - Preamble and PLCP header transmitted at 1 and 2 Mbps
  - Longer preamble: interoperable with older WiFi versions
- Different formats for later (OFDM) standards



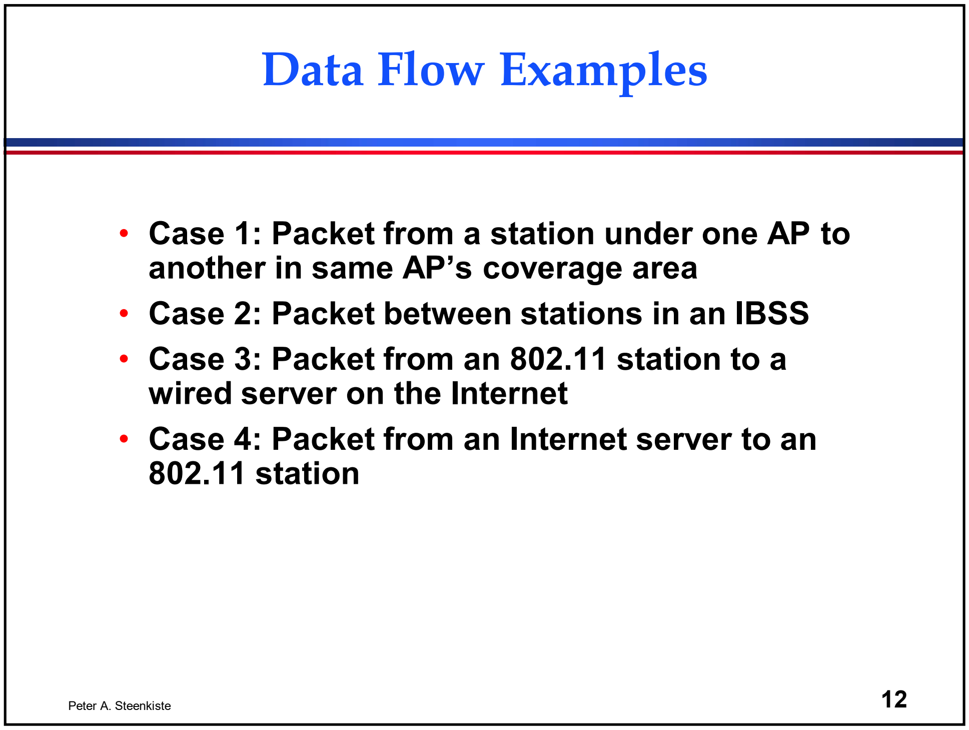
56 bit Preamble	16 bit Start Frame Delimiter	Signal Speed 1,2,5.5, 11 Mbps	Service (unused)	Length of Payload	16 bit CRC	Payload 34-2346 bytes



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 on this later in the semester
- Packets have multi-rate format
  - » Different parts of the packet are sent at different rates
  - » Why?

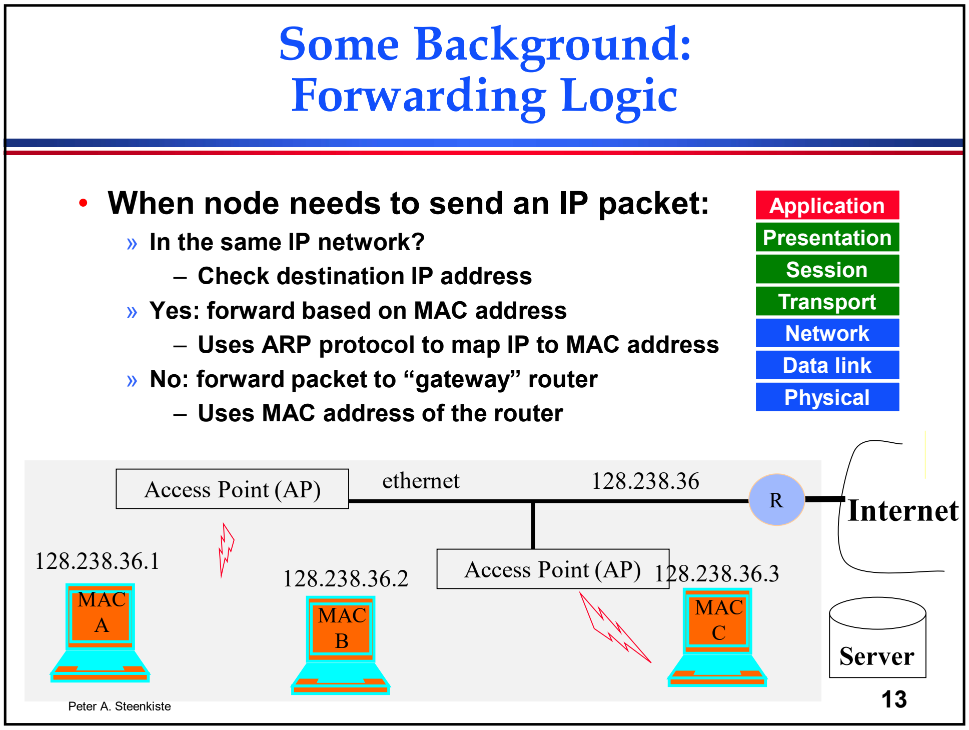
11



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

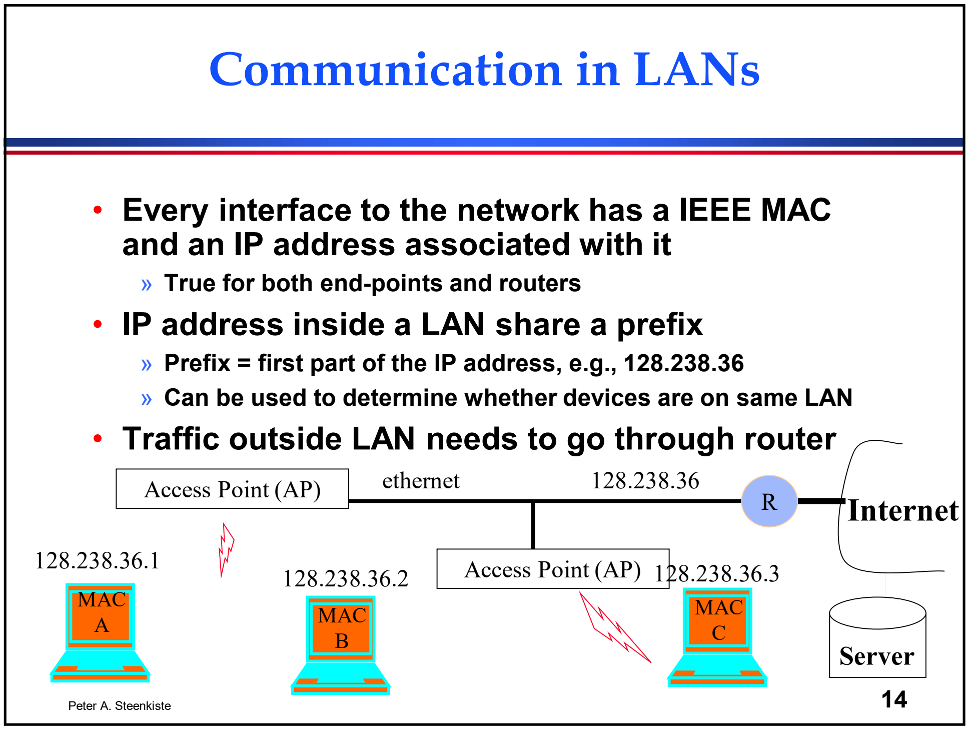
12



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

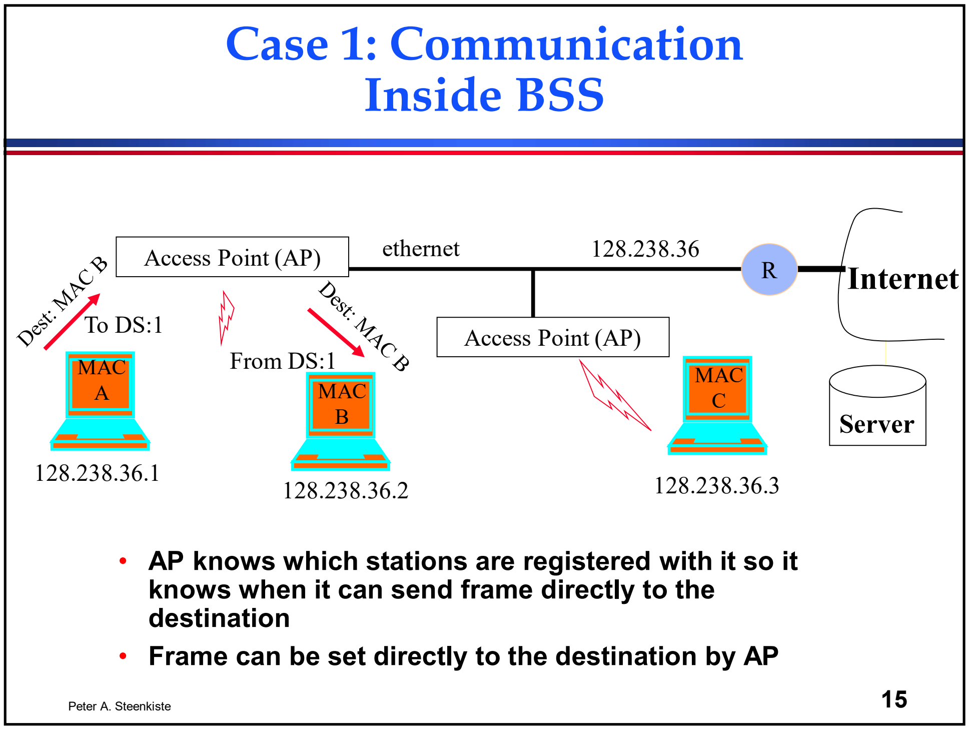
Application
Presentation
Session
Transport
Network
Data link
Physical
Access Point (AP)
ethernet
128.238.36
R
Internet
128.238.36.1
MAC A
128.238.36.2
MAC B
Access Point (AP)
128.238.36.3
MAC C
Server



Communication in LANs

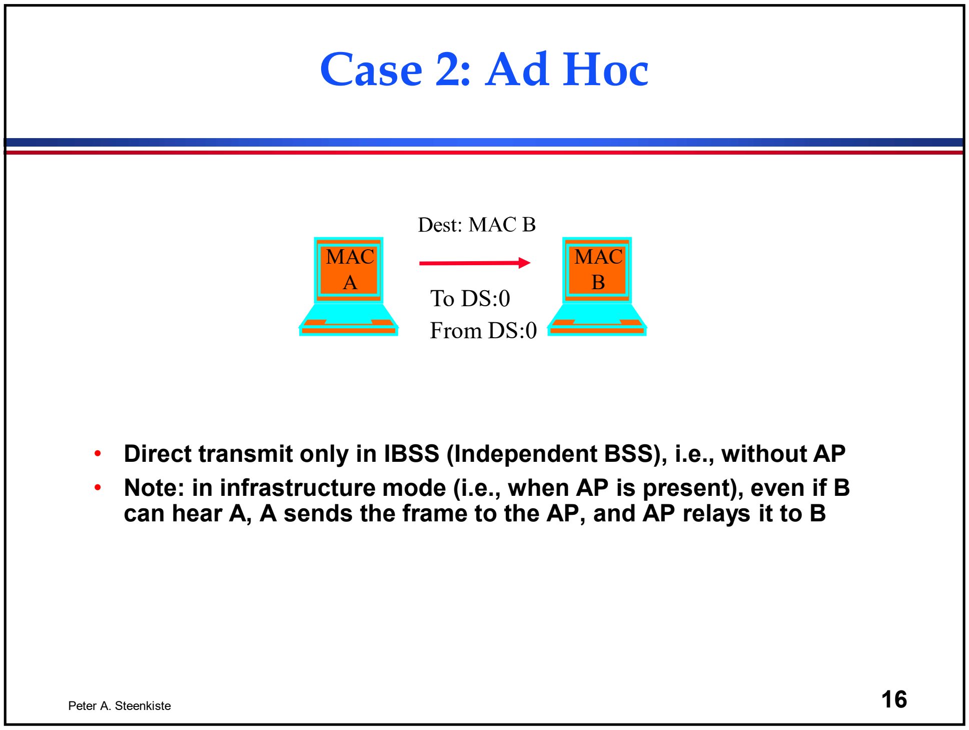
- Every interface to the network has a IEEE MAC and an IP address associated with it
  - » True for both end-points and routers
- IP address inside a LAN share a prefix
  - » Prefix = first part of the IP address, e.g., 128.238.36
  - » Can be used to determine whether devices are on same LAN
- Traffic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

Access Point (AP)
ethernet
128.238.36
R
Internet
128.238.36.1
MAC A
128.238.36.2
MAC B
Access Point (AP)
128.238.36.3
MAC C
Server



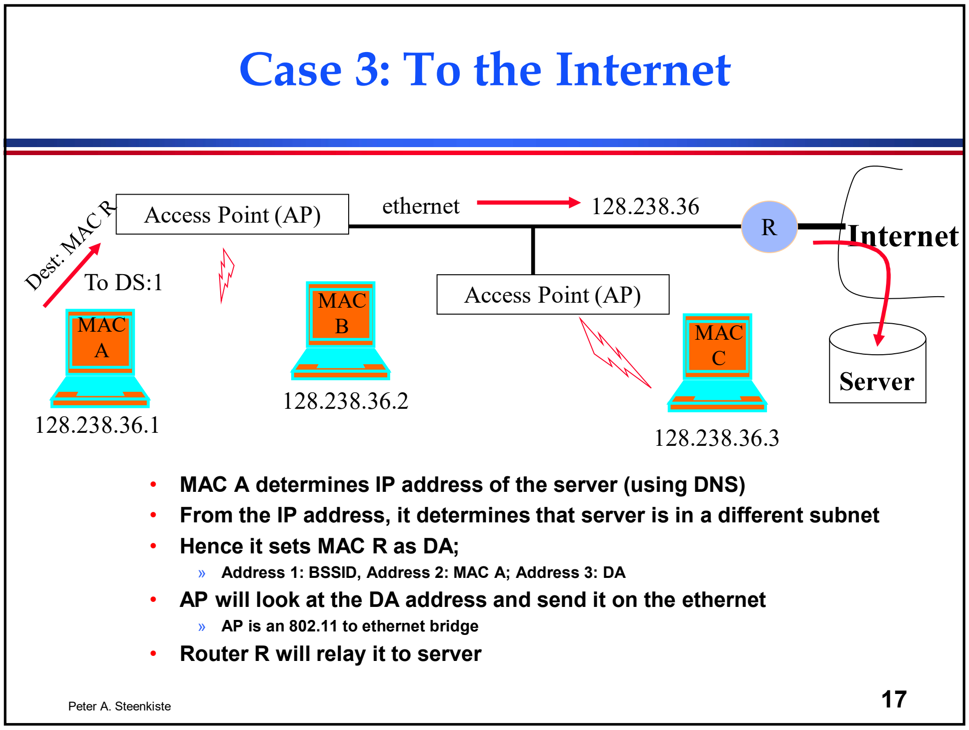
Case 1: Communication Inside BSS

- 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



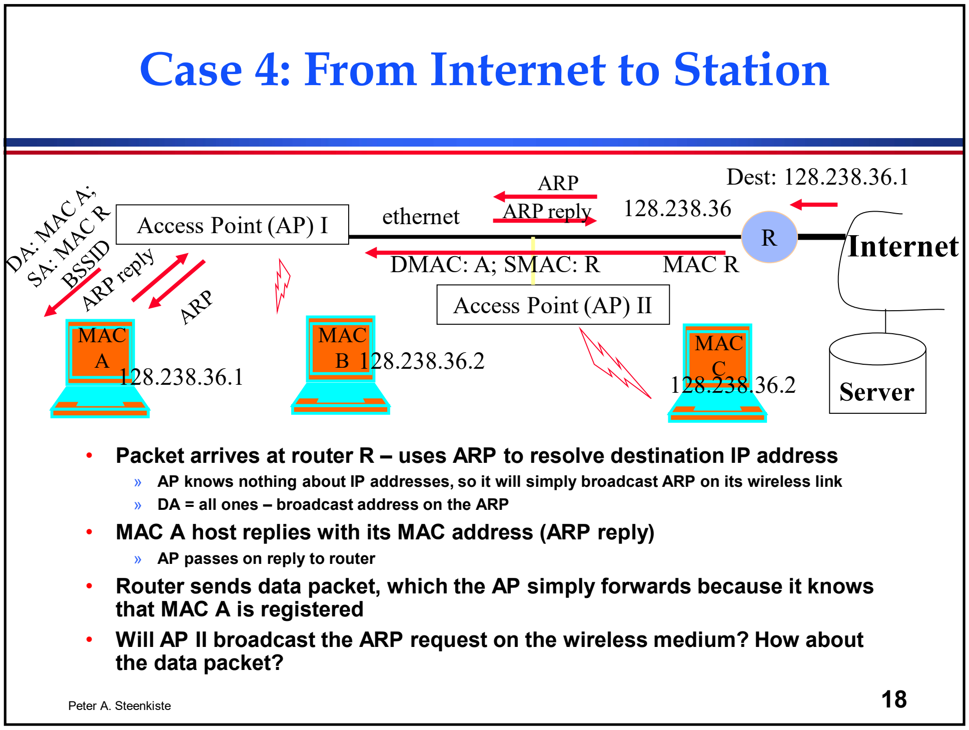
Case 2: Ad Hoc

- 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



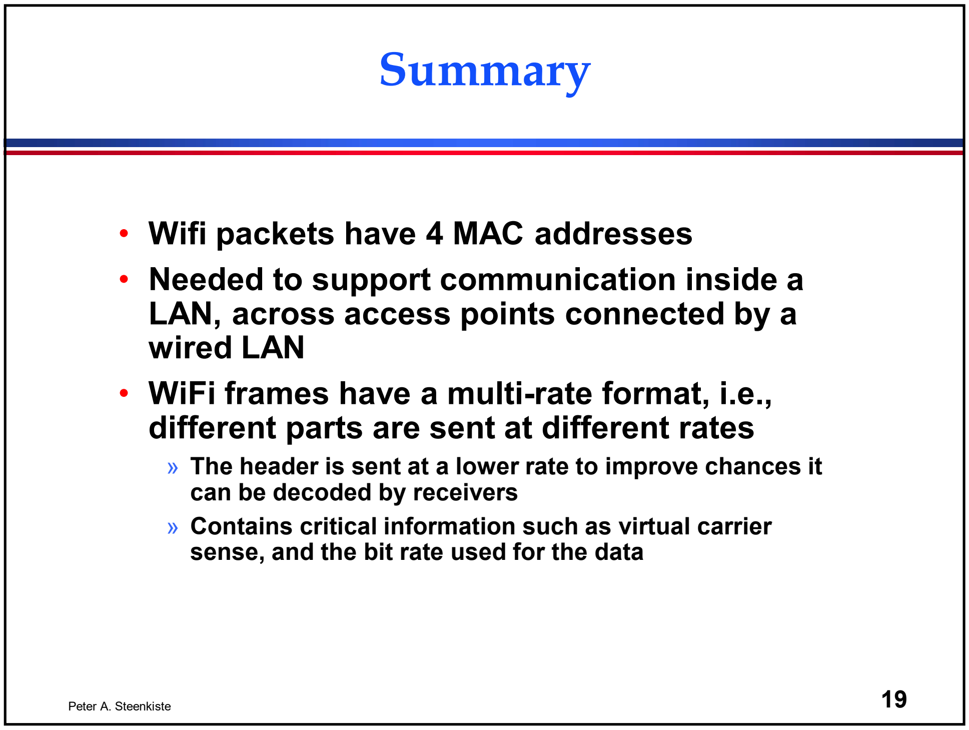
Case 3: To the Internet

- 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