
251-0292: A Hand-on Introduction to Wireless Networks

Lectures 6 and 7: Protocols

Peter Steenkiste

Thomas Gross

Computer Science Department

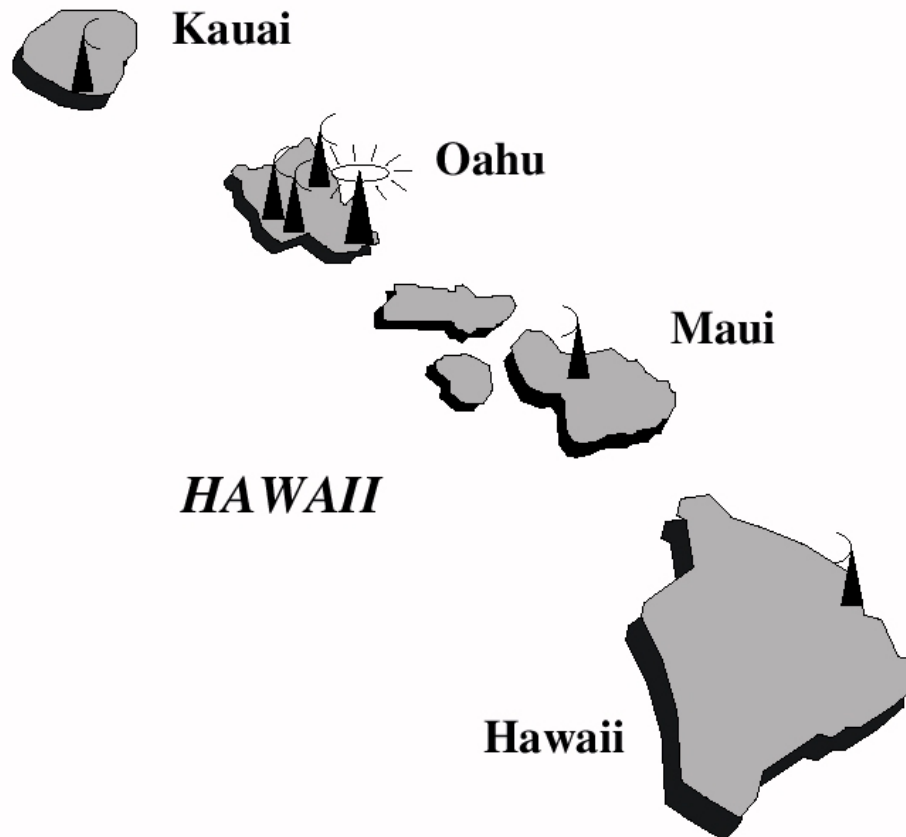
ETH Zürich

Spring Semester 2007

Outline

- **Brief history**
- **802 protocol overview**
- **Wireless LANs – 802.11**
- **Wireless Access – 802.16**
- **Personal Area Networks – 802.15**
- **Special topics**

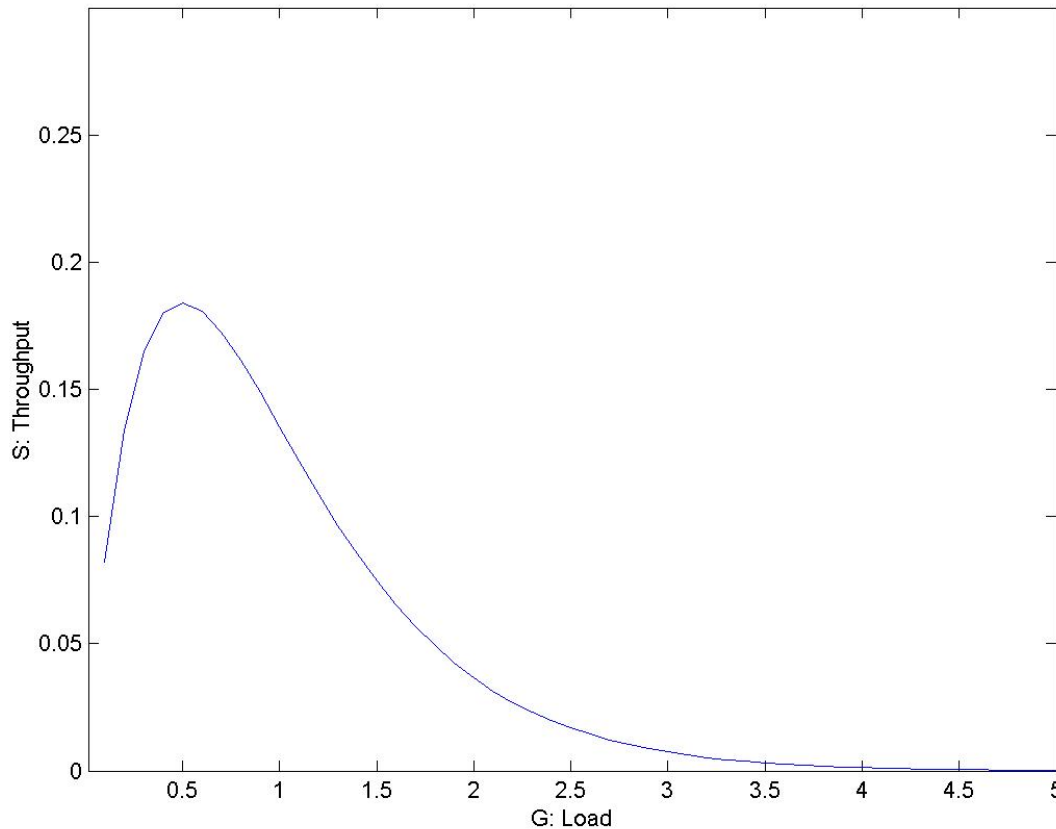
Why ALOHA



ALOHA

- **True free-for-all**
 - » When a node needs to send, it does so.
 - » It listens for an amount of time equal to the maximum round trip delay plus a fixed increment.
 - » If it hears an acknowledgment, fine;
 - » Otherwise it resends after waiting a random amount of time.
 - » After several attempts, it gives up.
- **Low delay if light load**
- **Max. utilization: 18%**

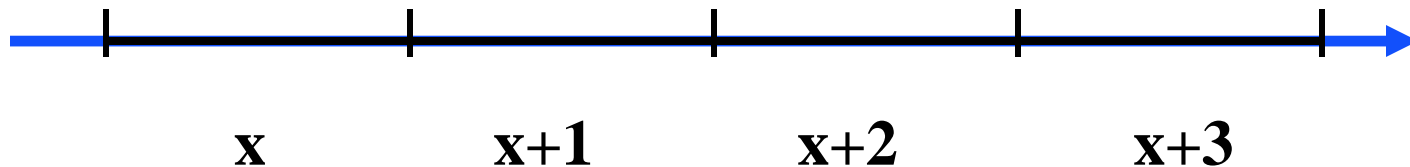
ALOHA throughput



**Maximum
throughput
is 18% at
 $G = 0.5$**

Slotted ALOHA

- **Competition to send only occurs at the start of each slot of length T**
- **Vulnerable period is T**
 - » Period is $2 \times T$ in Aloha
- **Doubles maximum throughput.**
 - » Result based on many assumptions



Multiple Access with Collision Avoidance (MACA)

- **RTS/CTS handshake to reduce chances of hidden terminal collision**
- **Sender sends brief Request-to-Send (RTS)**
 - » RTS includes the length of the data packets
- **Receiver returns Clear-to-Send (CTS)**
 - » Also includes the data length
- **All other transmitters stay off channel long enough so the sender can finish data transmit**
- **Collisions can still occur on RTS messages**
 - » But RTS message are small

Later Developments

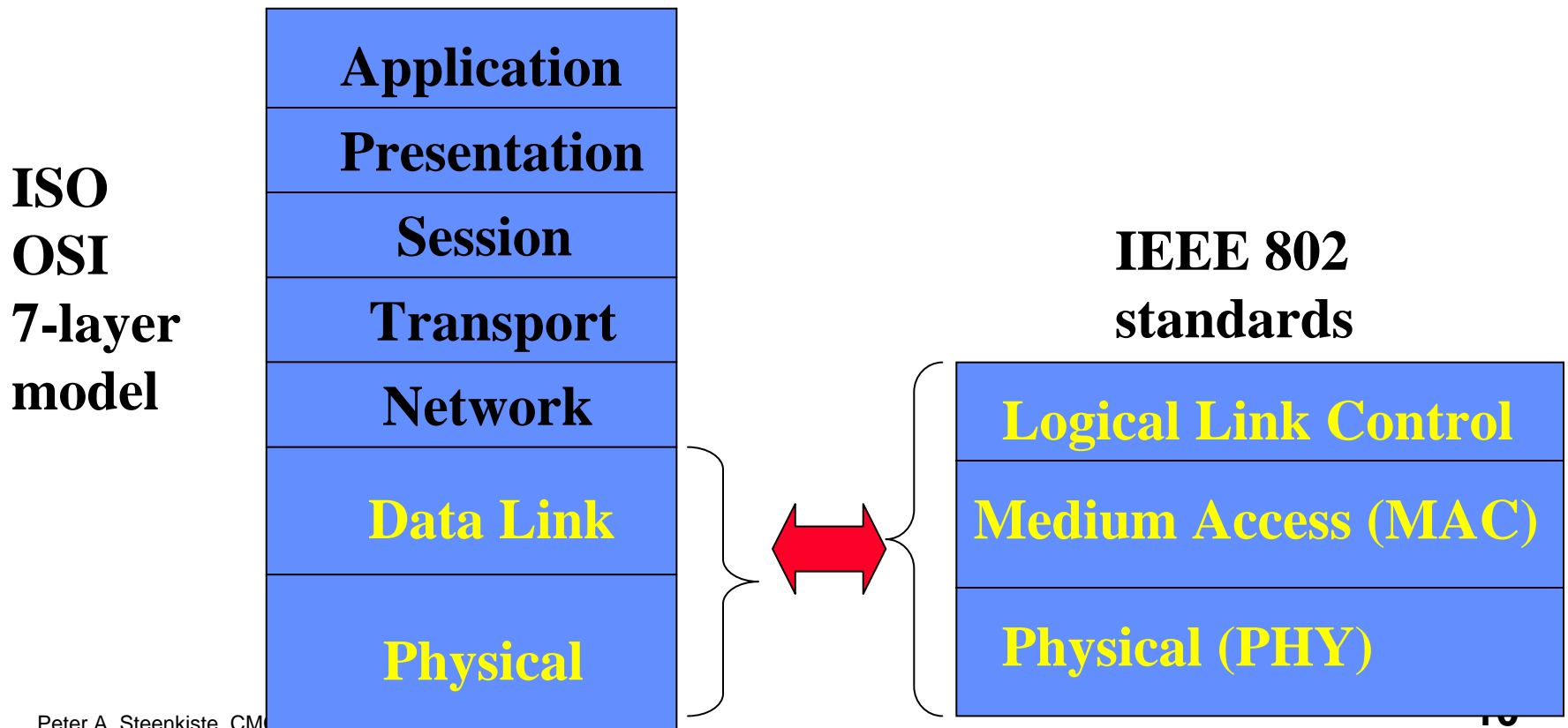
- **Car phones**
 - » Big and heavy “portable” phones
 - » Limited battery life time
 - » But introduced people to “mobile networking”
 - » Later turned into truly portable cell phones
- **Wireless LANs**
 - » Originally in the 900 MHz band
 - » Later evolved into the 802.11 standard
 - » Later joined by the 802.15 and 802.16 standards
- **Cellular data networking**
 - » Data networking over the cell phone
 - » Many standards – throughput is the challenge

Overview of Technologies

	PAN	LAN	MAN	MAN
<i>Access speed</i>	1-2Mb	11Mb	Mbs	>56kb
<i>Range</i>	10m	100- 400m	kms	global
<i>Standard</i>	IEEE 802.15	IEEE 802.11	IEEE 802.16	GPRS 1xRTT
<i>Scalability</i>	Low device specific	Medium ethernet	Infra structure	High regional Infrastructure
<i>Architecture</i>	FHSS	DSSS	cellular	cellular

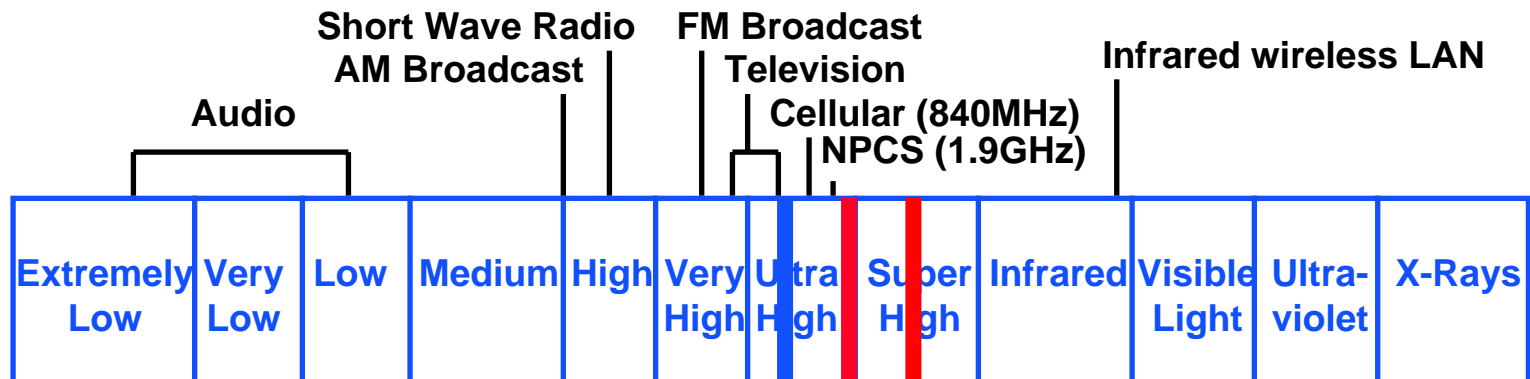
Standardization of Wireless Networks

- Wireless networks are standardized by IEEE.
- Under 802 LAN MAN standards committee.



Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Unlicensed, 22 MHz channel bandwidth



902 - 928 MHz
26 MHz

2.4 - 2.4835 GHz
83.5 MHz
(IEEE 802.11)

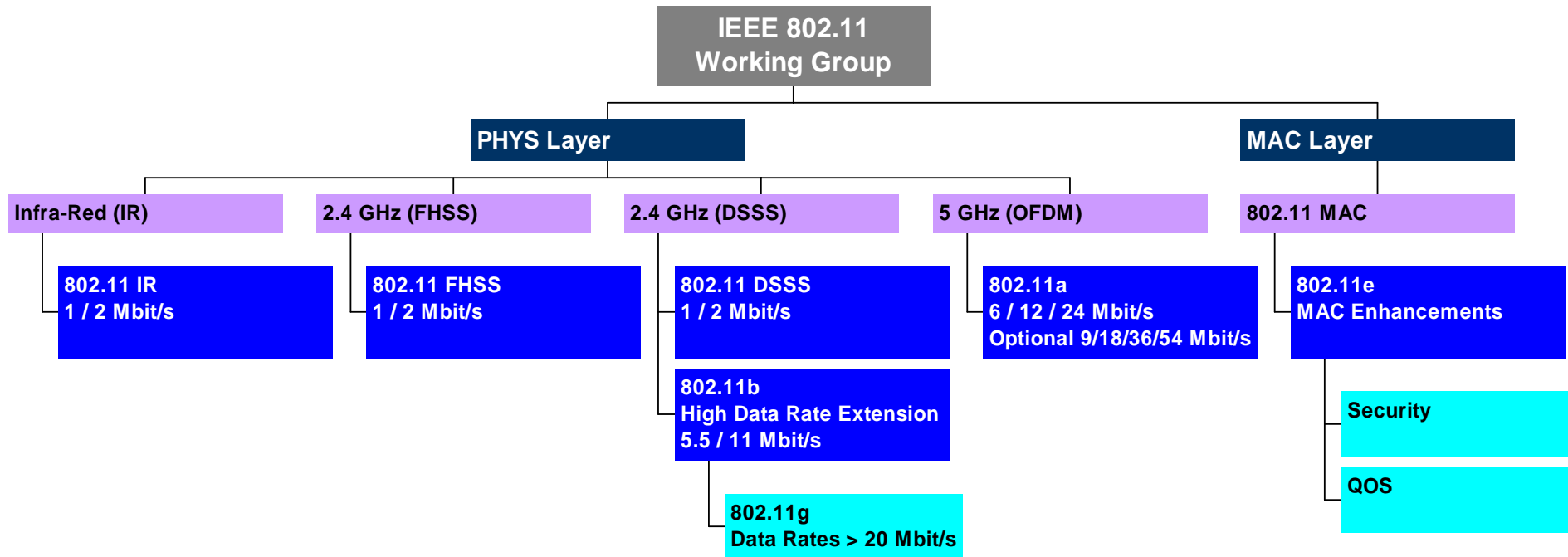
5 GHz
(IEEE 802.11)
HyperLAN
HyperLAN2

The 802 Class of Standards

- **List on next slide**
- **Some standards apply to all 802 technologies**
 - » E.g. 802.2 is LLC
 - » Important for inter operability
- **Some standards are for technologies that are dated**
 - » Not actively deployed anymore
 - » E.g. 802.6

- 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
- 802.1 b Specification for LAN Traffic Prioritization
- 802.1 q Virtual Bridged LANs
- 802.2 Logical Link Control
- 802.3 Contention Bus Standard 1 Obase 5 (Thick Net)
 - » 802.3a Contention Bus Standard 10base 2 (Thin Net)
 - » 802.3b Broadband Contention Bus Standard 10broad 36
 - » 802.3d Fiber-Optic InterRepeater Link (FOIRL)
 - » 802.3e Contention Bus Standard 1 base 5 (Starlan)
 - » 802.3i Twisted-Pair Standard 10base T
 - » 802.3j Contention Bus Standard for Fiber Optics 10base F
 - » 802.3u 100-Mb/s Contention Bus Standard 100base T
 - » 802.3x Full-Duplex Ethernet
 - » 802.3z Gigabit Ethernet
 - » 802.3ab Gigabit Ethernet over Category 5 UTP
- 802.4 Token Bus Standard
- 802.5 Token Ring Standard
 - » 802.5b Token Ring Standard 4 Mb/s over Unshielded Twisted-Pair
 - » 802.5f Token Ring Standard 16-Mb/s Operation
- 802.6 Metropolitan Area Network DQDB
- 802.7 Broadband LAN Recommended Practices
- 802.8 Fiber-Optic Contention Network Practices
- 802.9a Integrated Voice and Data LAN
- 802.10 Interoperable LAN Security
- 802.11 Wireless LAN Standard
- 802.12 Contention Bus Standard 1 OOVG AnyLAN
- 802.15 Wireless Personal Area Network
- 802.16 Wireless MAN Standard

IEEE 802.11 Organization Tree



Outline

- **Brief history**
- **802 protocol overview**
- **Wireless LANs – 802.11**
 - » Overview of 802.11
 - » 802.11 MAC, frame format, operations
 - » 802.11*
 - » 802.11 security discussion
 - » Deployment example
- **Wireless Access – 802.16**
- **Personal Area Networks – 802.15**
- **Special topics**

IEEE 802.11 Overview

- **Adopted in 1997**

Includes:

- **MAC sublayer**
- **MAC management protocols and services**
- **Physical (PHY) layers**
 - » IR
 - » FHSS
 - » DSSS

Goals is to

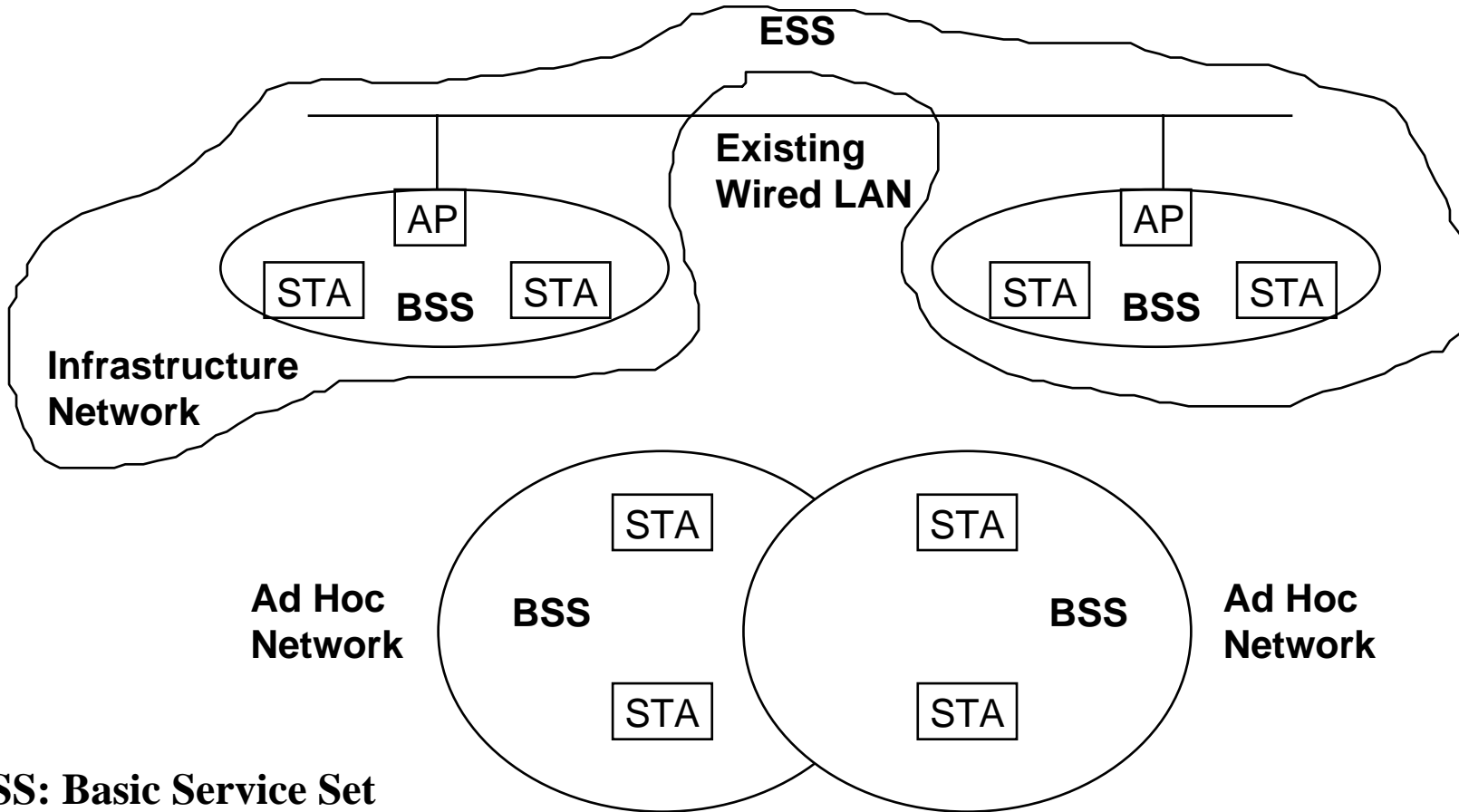
- give access to services in wired networks
- achieve high throughput
- achieve highly reliable data delivery
- achieve continuous network connection.

Infrastructure and Ad Hoc Mode

- **Infrastructure mode: stations communicate with one or more access points which are connected to the wired infrastructure**
 - » What is deployed in practice
- **Two modes of operation:**
 - » Distributed Control Functions - DCF
 - » Point Control Functions – PCF
 - » PCF is rarely used - inefficient
- **Alternative is “ad hoc” mode: multi-hop, assumes no infrastructure**
 - » Rarely used, e.g. military
 - » Hot research topic!



802.11 Architecture



BSS: Basic Service Set

ESS: Extended Service Set

Terminology for DCF

- **Stations and access points**
- **BSS - Basic Service Set**
 - » One access point that provides access to wired infrastructure
 - » Infrastructure BSS
- **ESS - Extended Service Set**
 - » A set of infrastructure BSSs that work together
 - » APs are connected to the same infrastructure
 - » Tracking of mobility
- **DS – Distribution System**
 - » AP communicates with another
 - » Thin layer between LLC and MAC sublayers

MAC Functions

Functionality:

- **Reliable data delivery**
- **Fair control access**
- **Protection of data**

Deals with:

- **Noisy and unreliable medium**
- **Frame exchange protocol - ACK**
- **Overhead to IEEE 802.3**
- **Hidden Node Problem – RTS/CTS**
- **Participation of all stations**
- **Reaction to every frame**

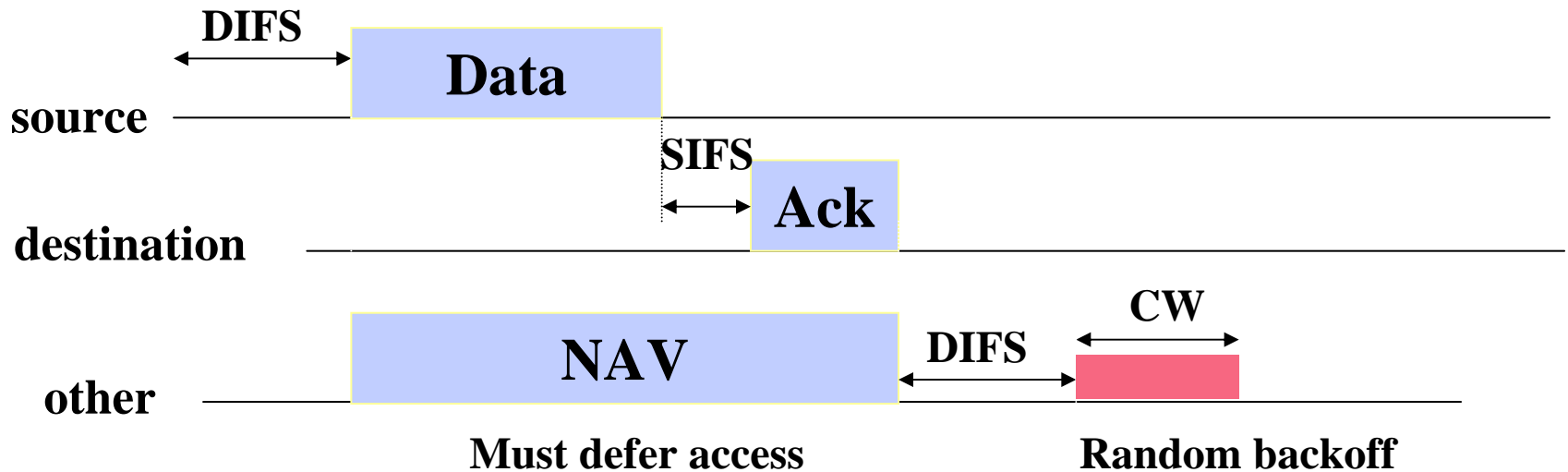
Features of 802.11 MAC protocol

- **Supports MAC functionality**
 - » Addressing
 - » CSMA/CA
- **Error detection (FCS)**
- **Error correction (ACK frame)**
- **Flow control: stop-and-wait**
- **Fragmentation (More Frag)**

Carrier Sense Multiple Access

- **Before transmitting a packet, sense carrier**
- **If it is idle, send**
 - » After waiting for one DCF inter frame spacing (DIFS)
- **If it is busy, then**
 - » Wait for medium to be idle for a DIFS (DCF IFS) period
 - » Go through exponential backoff, then send
 - » Want to avoid that several stations waiting to transmit automatically collide
- **Wait for ack**
 - » If there is one, you are done
 - » If there isn't one, assume there was a collision, retransmit using exponential backoff

DCF mode transmission without RTS/CTS

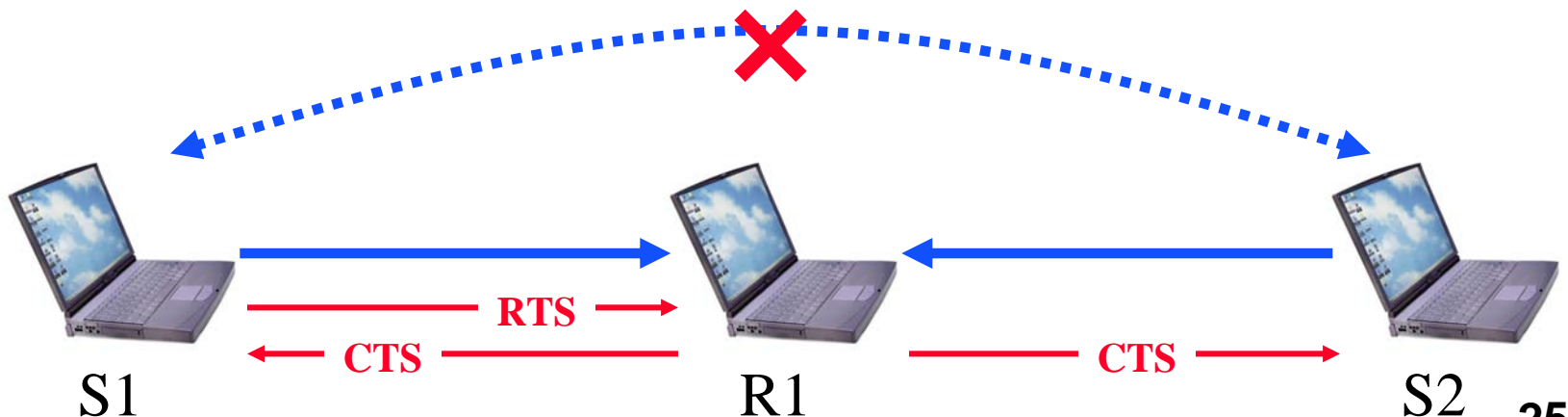


Exponential Backoff

- **Force stations to wait for random amount of time to reduce the chance of collision**
 - » Backoff period increases exponential after each collision
 - » Similar to Ethernet
- **If the medium is sensed it is busy:**
 - » Wait for medium to be idle for a DIFS (DCF IFS) period
 - » Pick random number in contention window (CW) = backoff counter
 - » Decrement backoff timer until it reaches 0
 - But freeze counter whenever medium becomes busy
 - » When counter reaches 0, transmit frame
 - » If two stations have their timers reach 0; collision will occur;
- **After every failed retransmission attempt:**
 - » increase the contention window exponentially
 - » $2^i - 1$ starting with CW_{\min} up to CW_{\max} e.g., 7, 15, 31, ...

Collision Avoidance

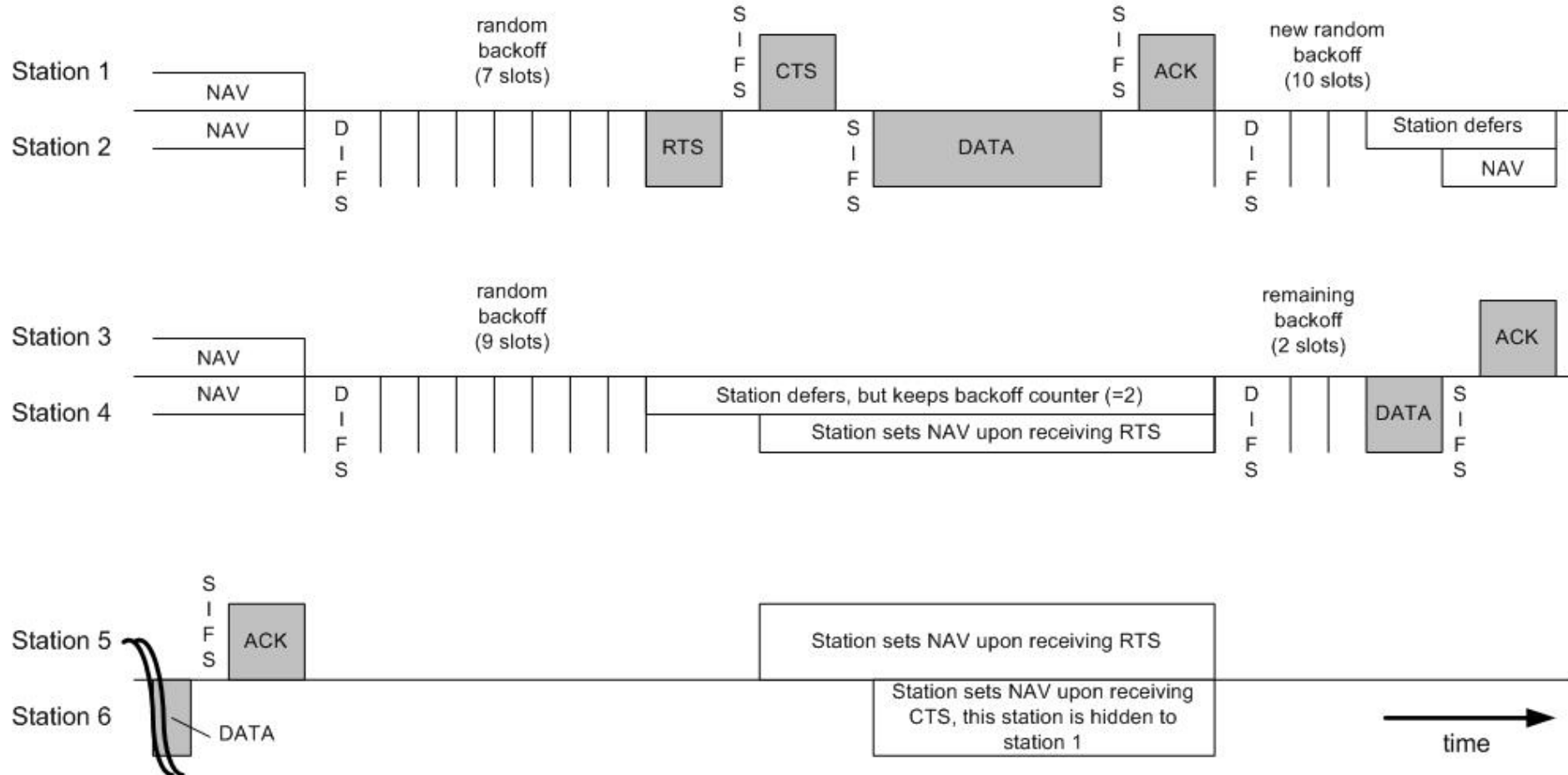
- **Difficult to detect collisions in a radio environment**
 - » While transmitting, a station cannot distinguish incoming weak signals from noise – its own signal is too strong
- **Why do collisions happen?**
 - » Near simultaneous transmissions
 - Period of vulnerability: propagation delay
 - » Hidden node situation: two transmitters cannot hear each other and their transmission overlap at a receiver



Request-to-Send and Clear-to-Send

- **Before sending a packet, first send a station first sends a RTS.**
- **The receiving station responds with a CTS.**
 - » RTS and CTS are smaller than data packets
 - » RTS and CTS use shorter IFS to guarantee access
- **Stations that hear either the RTS or the CTS “remember” that the medium will be busy for the duration of the transmission**
 - » Based on a Duration ID in the RTS and CTS
- **Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)**
 - » Time that must elapse before a station can sample channel for idle status

Use of RTS/CTS

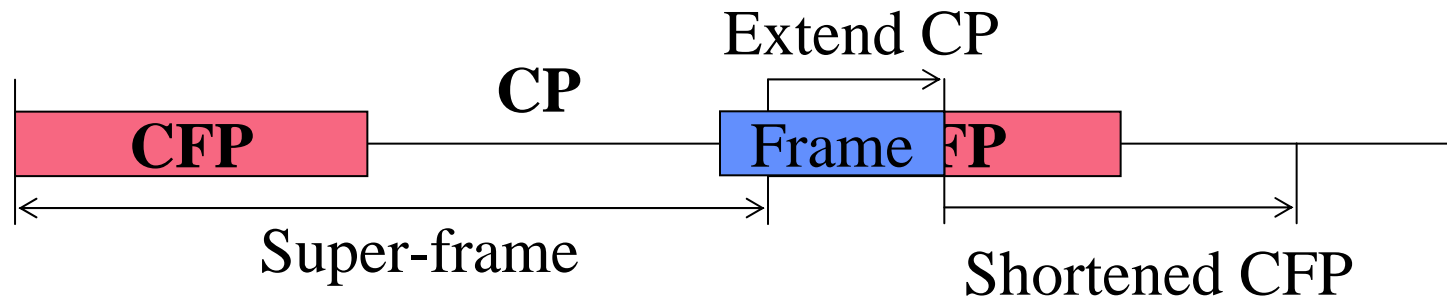


Some More MAC Features

- **Use of RTS/CTS is controlled by an RTS threshold**
 - » RTS/CTS is only used for data packets longer than the RTS threshold
 - » Pointless to use RTS/CTS for short data packets – high overhead!
- **Number of retries is limited by a Retry Counter**
 - » Short retry counter: for packets shorter than RTS threshold
 - » Long retry counter: for packets longer than RTS threshold
- **Packets can be fragmented.**
 - » Each fragment is acknowledged
 - » But all fragments are sent in one sequence
 - » Sending shorter frames can reduce impact of bit errors
 - » Lifetime timer: maximum time for all fragments of frame

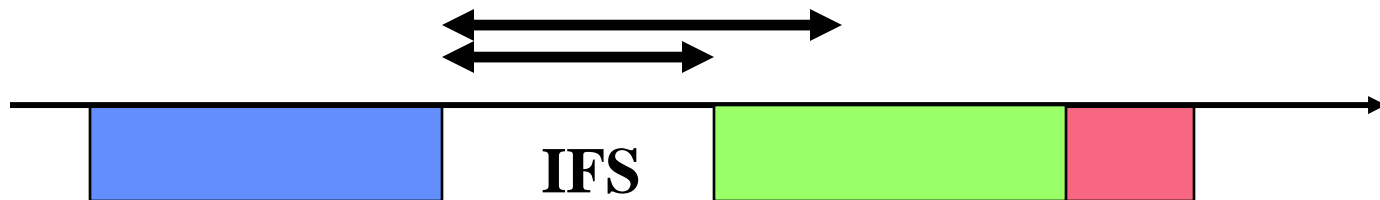
Now What about PCF?

- **IEEE 802.11 combines random access with a “taking turns” protocol**
 - » **DCF (Distributed Coordination Mode) – Random access**
 - **CP (Contention Period): CSMA/CA is used**
 - » **PCF (Point Coordination Mode) – Polling**
 - **CFP (Contention-Free Period): AP polls hosts**



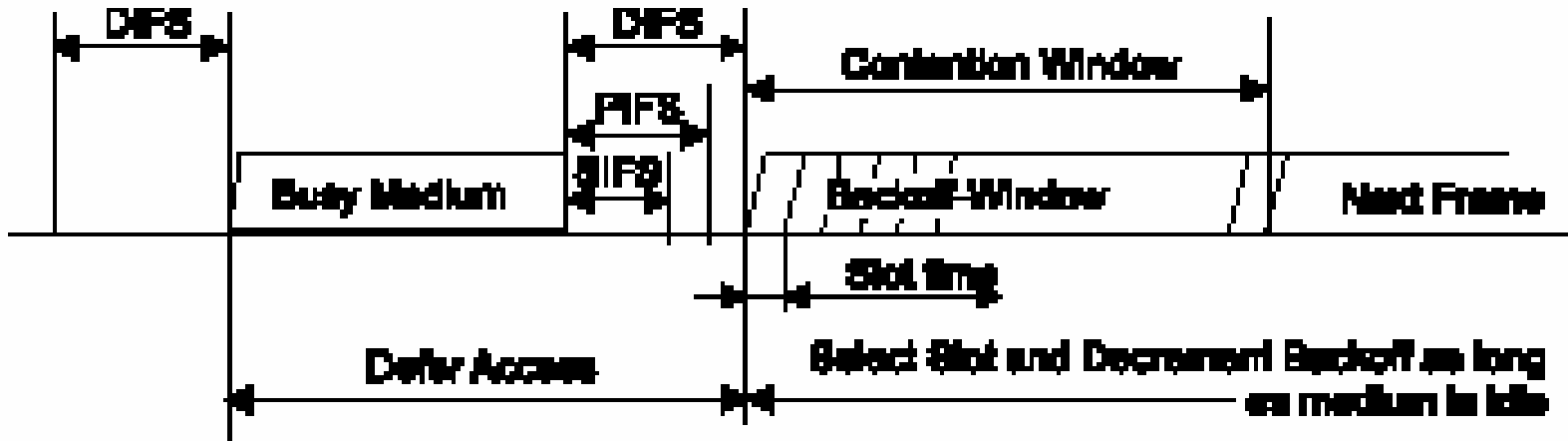
Playing Games with Inter Frame Spacing

- Assigning different IFS effectively provides a mechanism for prioritizing packets and events
- SIFS - short IFS: for high priority transmissions
- PIFS – PCF IFS: used by PCF during contention-free period
- DIFS – DCF IFS: used for contention-based services
- EIFS – extended IFS: used when there is an error



Effect of Different IFS

Immediate access when medium is free \Rightarrow DIFS



- PCF transmissions effectively get priority over DCF transmission because they use a shorter IFS

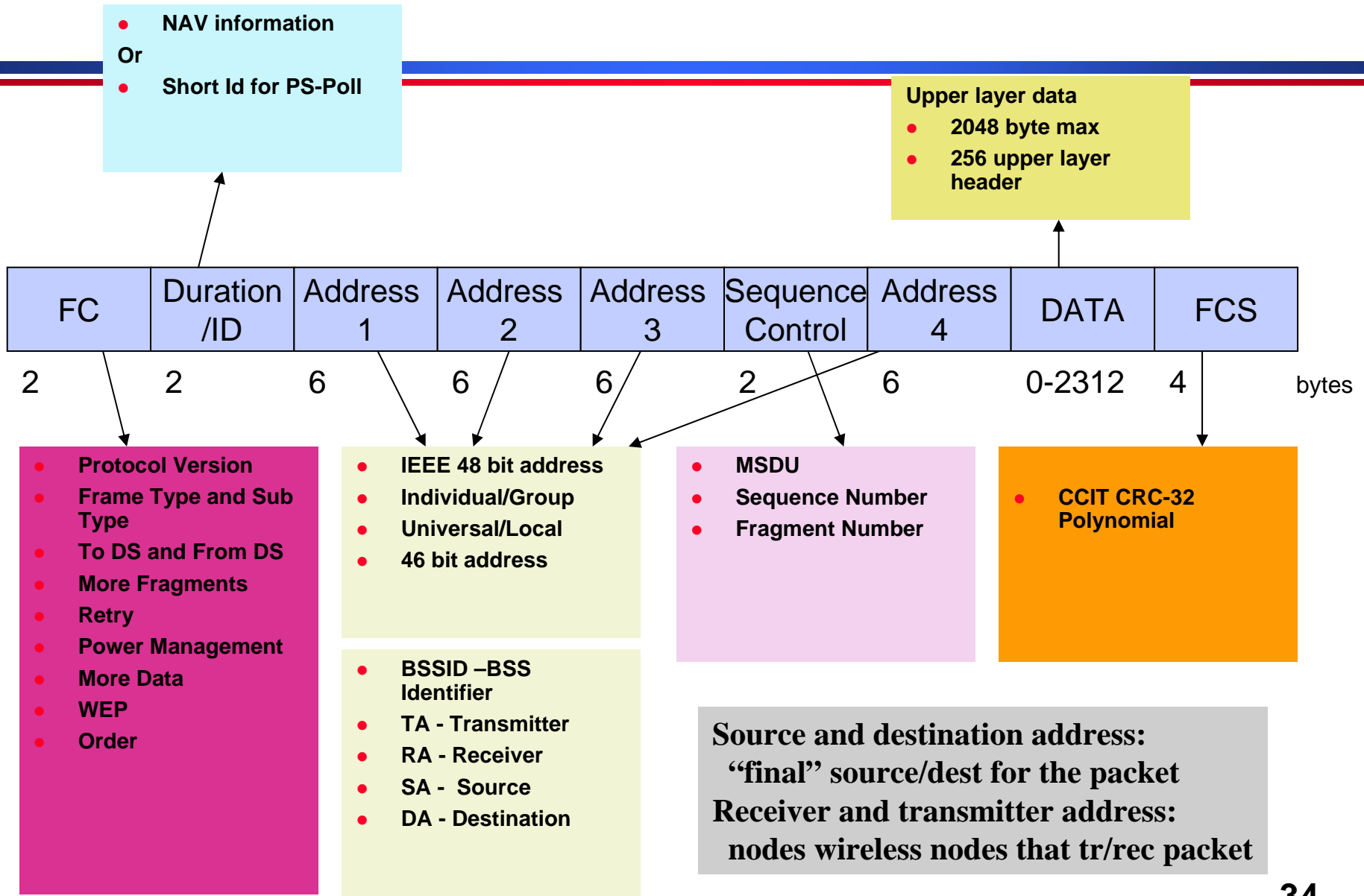
PCF Operation Summary

- **PC – Point Coordinator**
 - » Uses polling – eliminates contention
 - » Uses polling list to ensure access
 - » Over DCF but uses a PIFS instead of a DIFS – gets priority
- **CFP – Contention Free Period**
 - » Alternate with DCF
- **Periodic Beacon – contains length of CFP**
- **CF-Poll – Contention Free Poll**
- **NAV prevents transmission during CFP**
- **CF-End – resets NAV**

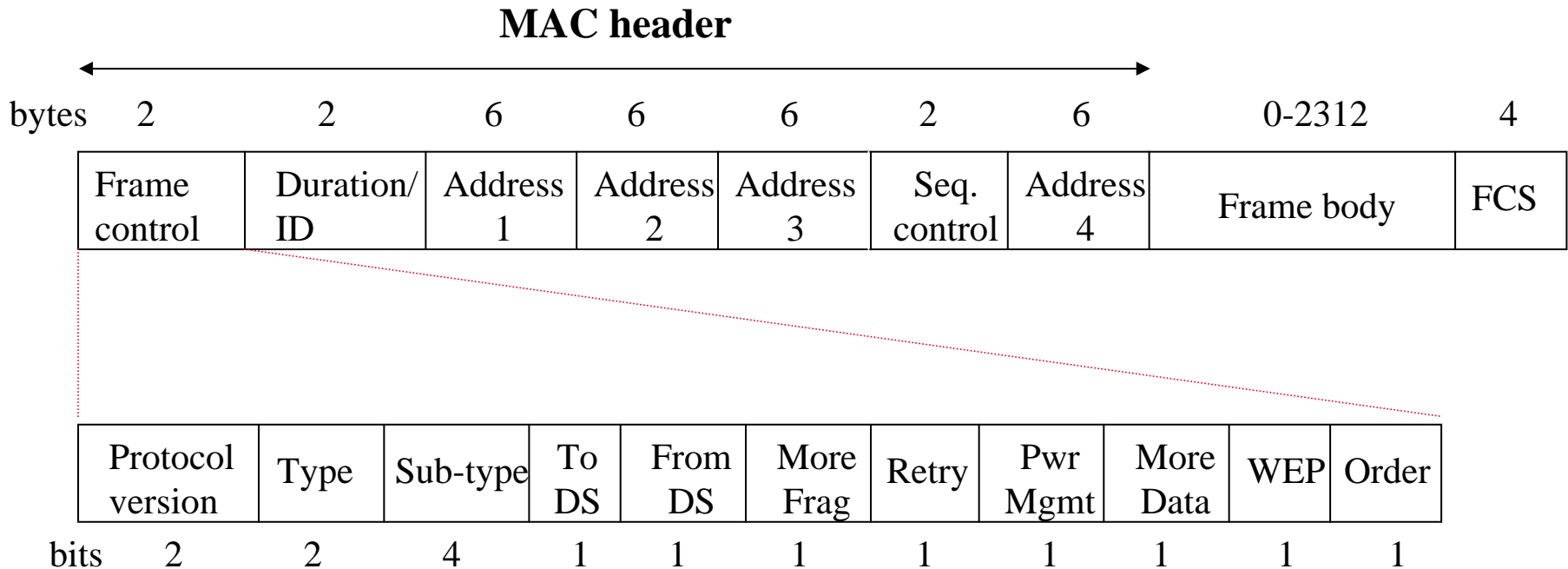
And What about Ad Hoc?

- **Infrastructure mode: access points relay packets**
 - » Based on an Infrastructure BSS
 - » APs are connected through a distribution system
- **Ad-hoc mode: no fixed network infrastructure**
 - » Based on an Independent BSS
 - » A wireless endpoint sends and all nodes within range can pick up signal
 - » Each packet carries destination and source address
 - » Effectively need to implement a “network layer”
 - How do know who is in the network?
 - Routing?
 - Security?
 - » Research area – discussed later in the course

Frame Format



Detailed 802.11 MAC Frame Format



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

To DS and From DS Fields

To DS	From DS	Message
0	0	station-to-station frames in an IBSS; all mgmt/control frames
0	1	From AP to station
1	0	From station to AP
1	1	From one AP to another on DS

Addressing Fields

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	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

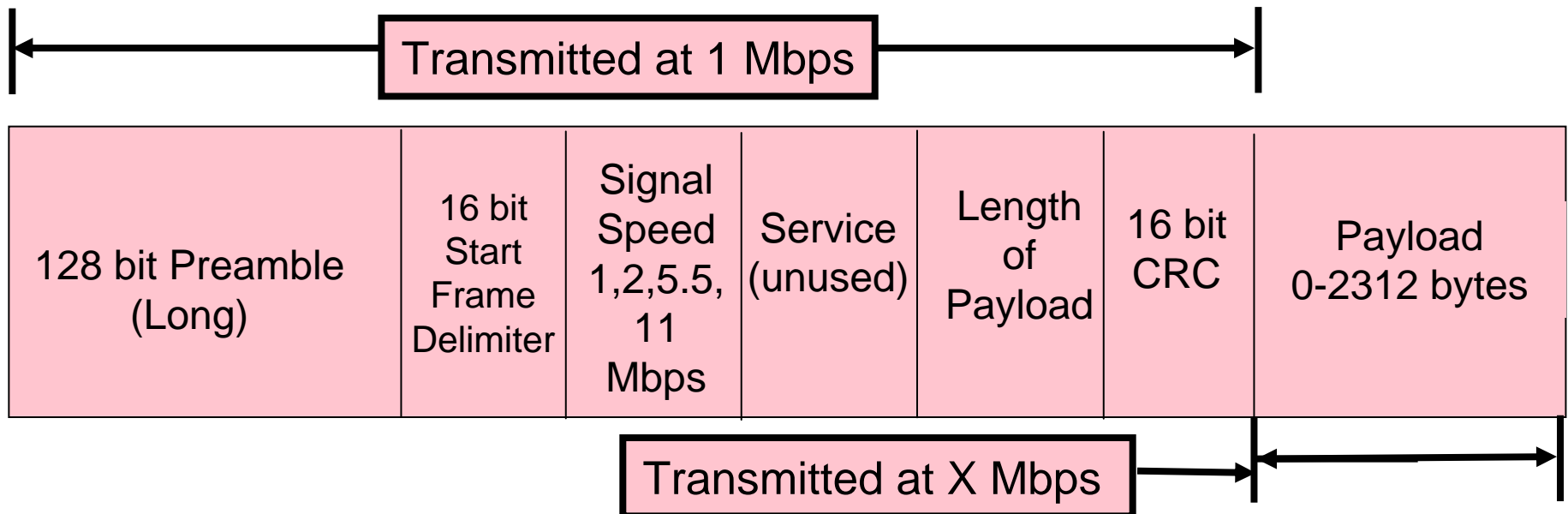
Multi-bit Rate

- **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**
- **Packets have multi-rate format**
 - » Different parts of the packet are sent at different rates

Long Preamble

Long Preamble = 144 bits

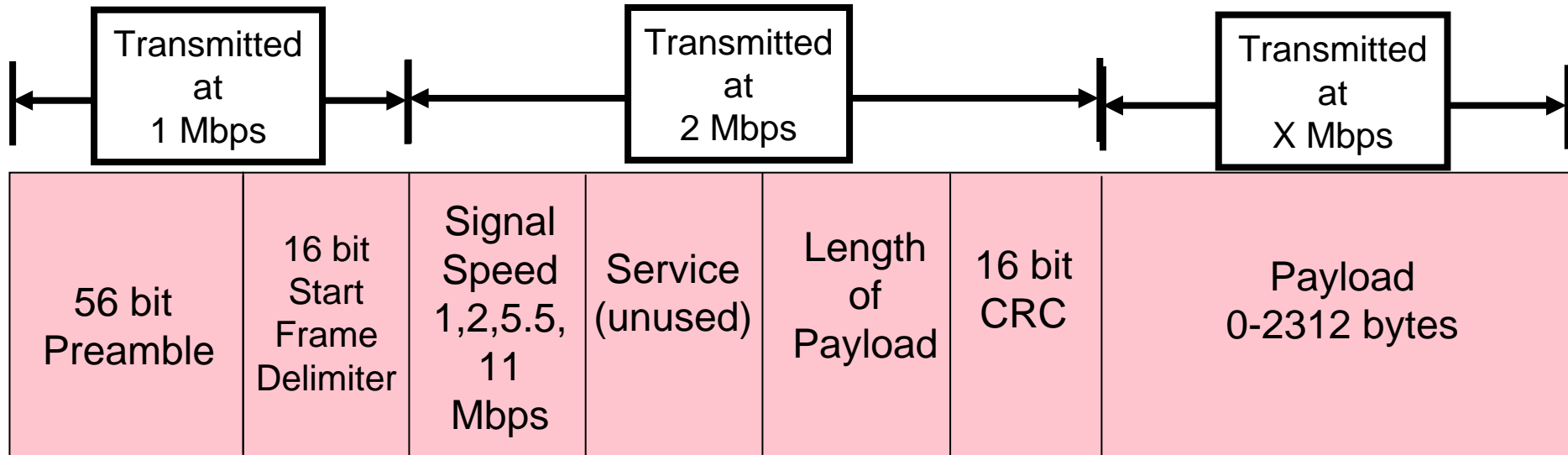
- Interoperable with older 802.11 devices
- Entire Preamble and 48 bit PLCP Header sent at *1 Mbps*



Short Preamble

Short Preamble = 72 bits

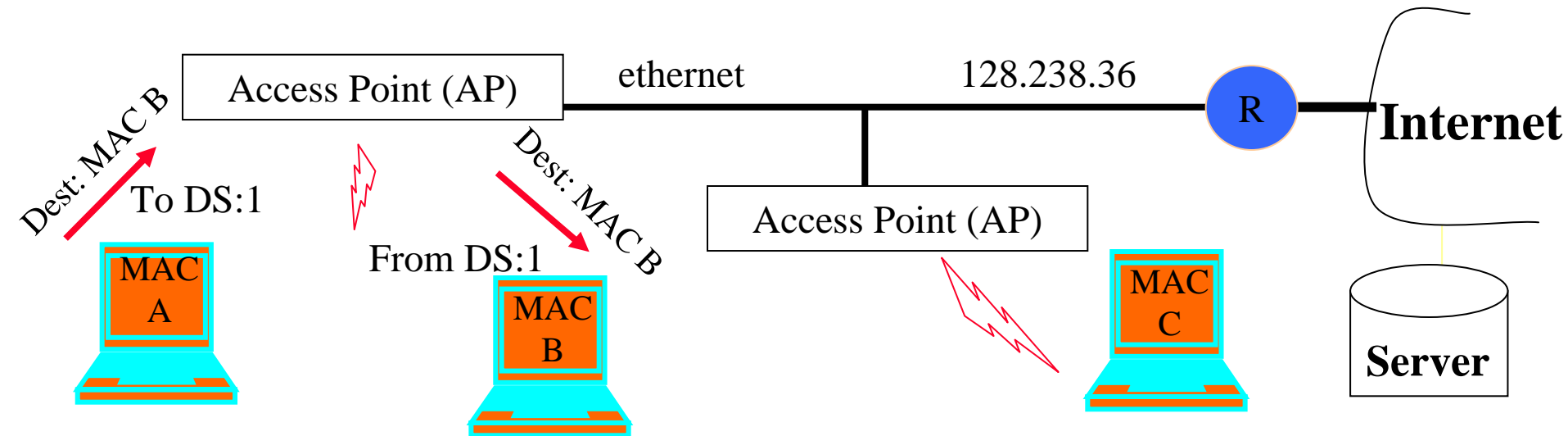
- Preamble transmitted at 1 Mbps
- PLCP Header transmitted at 2 Mbps
- more efficient than long preamble



Data Flow Examples

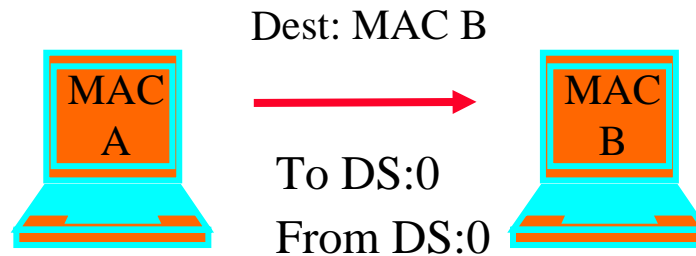
- **Case 1: Packet from a station under one AP to another in same AP's coverage area**
- **Case 2: Packet between stations in an IBSS**
- **Case 3: Packet from an 802.11 station to a wired server on the Internet**
- **Case 4: Packet from an Internet server to an 802.11 station**

Case 1: Communication Inside BSSS



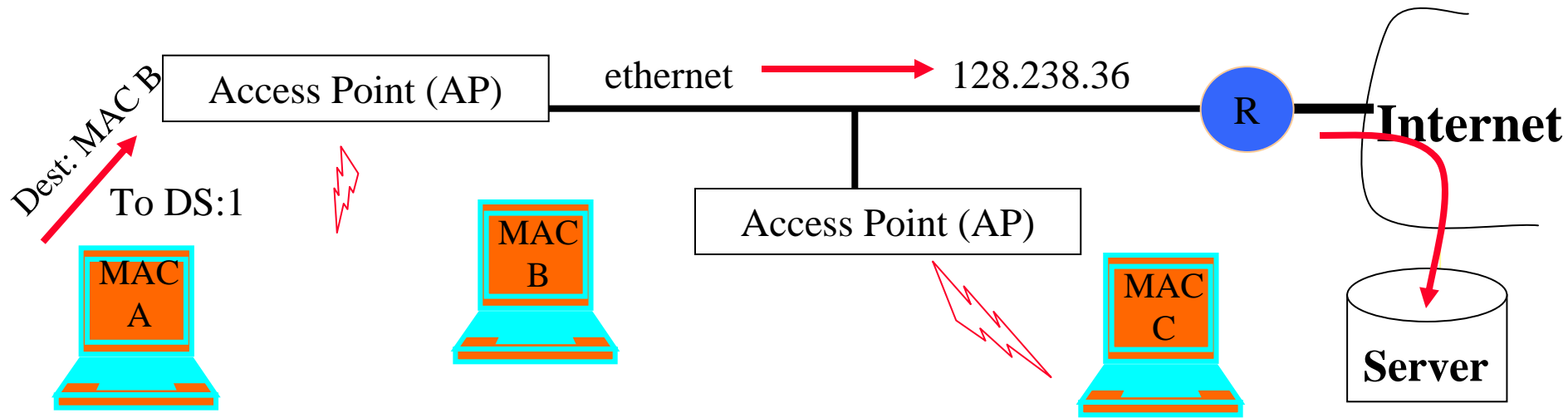
- AP knows which stations are registered with it so it know when it can send frame directory to destination

Case 2: Ad Hoc



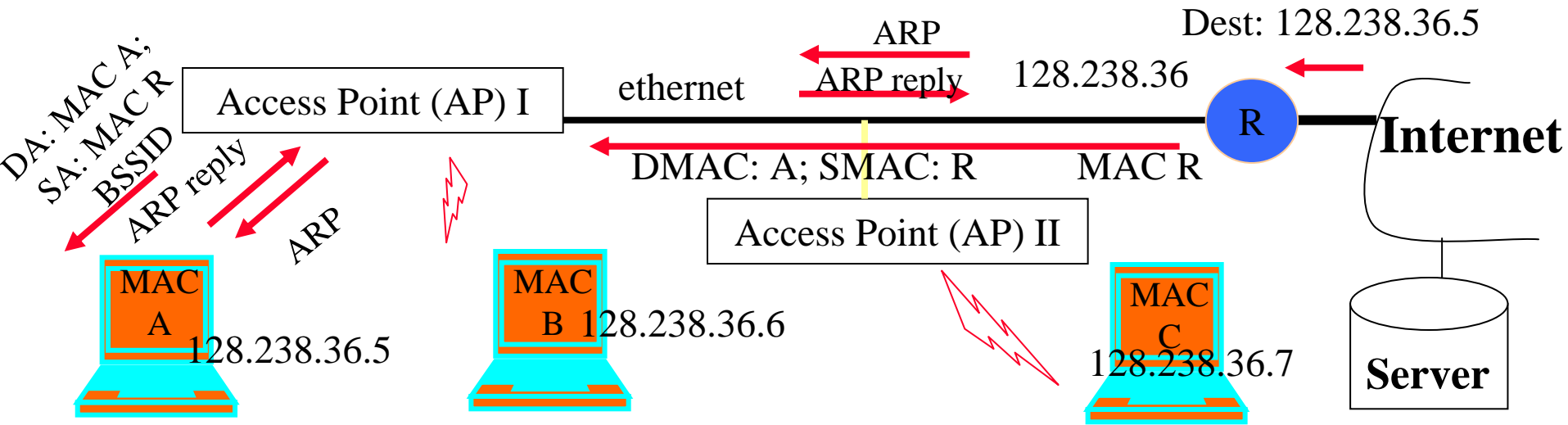
- Direct transmit only in IBSS (Independent BSS), i.e., without AP
- When AP is present, even if B can hear A, A sends the frame to the AP, and AP relays it to B
- What is the exchange in an IBSS that lets A know that B is in range?

Case 3: To the Internet data flow



- **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



- AP knows nothing of 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?

Management and Control Services

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