

---

# Access Networks and Media Access Control #6

MAC 1

## Outline

---

- Why use MAC protocols
- General classes of MAC protocols
  - Deterministic
  - Random Access
- Standard LAN protocols
- Access Networks
  - Wireless LAN
  - Cable
  - Cellular
  - DSL
  - Satellite Networks

*With some detours*

MAC 2

## Media Access Control:

Protocols provide:

---

- Direct access to the media
- Distributed and decentralized control over resource allocation
- Typically broadcast (real or virtual)

## Media Access Control: Advantages

---

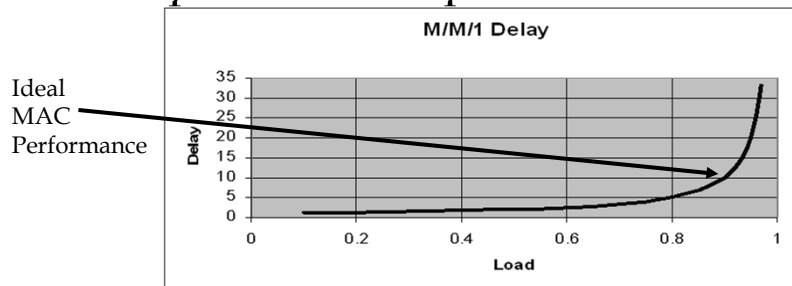
- High data rates  
(open new applications)
- Low cost
- Possible local organizational control
- Wireless is a broadcast media and efficient use of resources is important
- Enable sharing of resources
- Mobility via Wireless

# Media Access Control

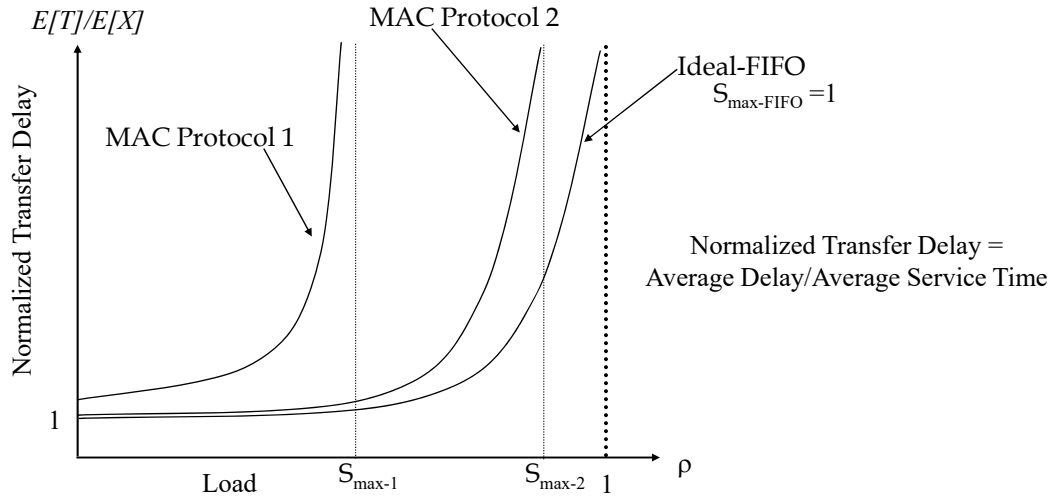
- MAC protocols establish a set of rules that govern who gets to use the shared transmission media.
- Obstacle to perfect channel utilization
  - Finite propagation delay means that each users' **knowledge of the state** of the system is imperfect and thus they can not perfectly schedule transmissions, i.e., some time will be wasted attempting to learn the state of the system and/or learning the fate of transmissions.
  - Lost messages

# Media Access Control

- Perfect Knowledge would lead to FIFO performance.
- Performance of MAC protocols will be compared to FIFO performance.



## Impact of MAC Overhead



Adapted from: Leon-Garcia & Widjaja: *Communication Networks*

MAC 7

## Alternative Media Access Control Strategies

### □ Static Allocation

- FDM
- TDM

#### ➤ Problems

- Management; not easy to add users
  - Requires signaling
- Wasteful in resources for bursty traffic  
(Proved using queueing theory)

#### ➤ Example

- A transmission media has a rate of 10 Mb/s and supports 50 users. The system uses static allocation. A user has a 1 Mbyte file to transmit. The file transfer time is:

$$\frac{1 \times 10^6 \times 8 \text{ bit}}{10^7 \text{ bits/sec} \times 50} = 40 \text{ sec}$$

MAC 8

## Alternative Media Access Control Strategies

---

- Suppose you *send a message* to all the other 49 users saying, *'I need the whole channel for about 1sec, do not use it, please'*
- As long as the overhead incurred in sending the message is less than 39 sec. the user will get better performance.

Are MAC strategies suitable for WANs?

## Alternative Media Access Control Strategies

---

- Deterministic
  - Polling
  - Token networks
- Random Access
  - ALOHA
  - Carrier sense multiple access (CSMA)
  - CSMA with collision detection (CSMA/CD)
  - CSMA with collision avoidance (CSMA/CA)
- Reservation Systems
- Combinations of Random Access and Reservations

## Alternative Media Access Control Strategies:

### Dynamic allocation of resources

---

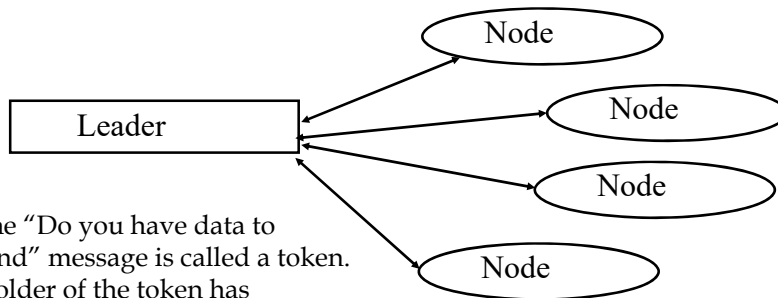
- Deterministic; Polling, Token Ring & Token Bus
  - Advantage: the maximum time between users chances to transmit is deterministically bounded. (assuming a limit on the token holding time)
  - Disadvantage: Time is wasted polling other users if they have no data to send.
  - The technology does not scale

## Deterministic Protocols

---

- Roll Call Polling
  - Leader/Follower arrangement
  - Leader polls each follower (node);
    - Do you have data to send?*
  - If the polled follower (node) has data it is sent otherwise next node is polled.
  - To be fair to the other users, the follower with data is allowed to send for a limited amount of time: called the "Maximum token holding time (MTHT)" After the MTHT the follower must tell Leader it is done transmitting so next station can be polled.

# Deterministic Protocols



The "Do you have data to send" message is called a token. Holder of the token has permission to transmit.

Maximum token holding time (MTHT)= Maximum time a station is allowed to transmit before passing on the permission to transmit, the token.

Example:  
Leader-Node distance 300 m  
or  $1\mu\text{s}$  (free space)  
Link rate = 100Mb/s  
MTHT=100ms

Maximum data burst/node = 10Mbits

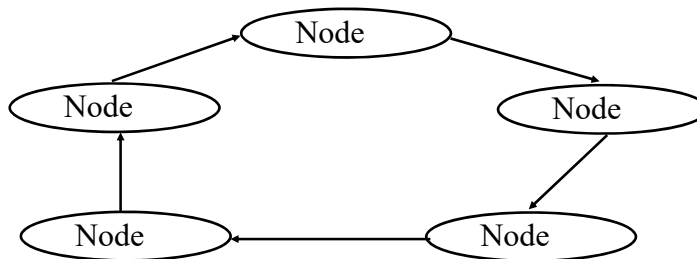
Maximum time between user visits  
~ 400ms

Guaranteed  
(Deterministically) to get to transmit every 400ms

# Deterministic Protocols

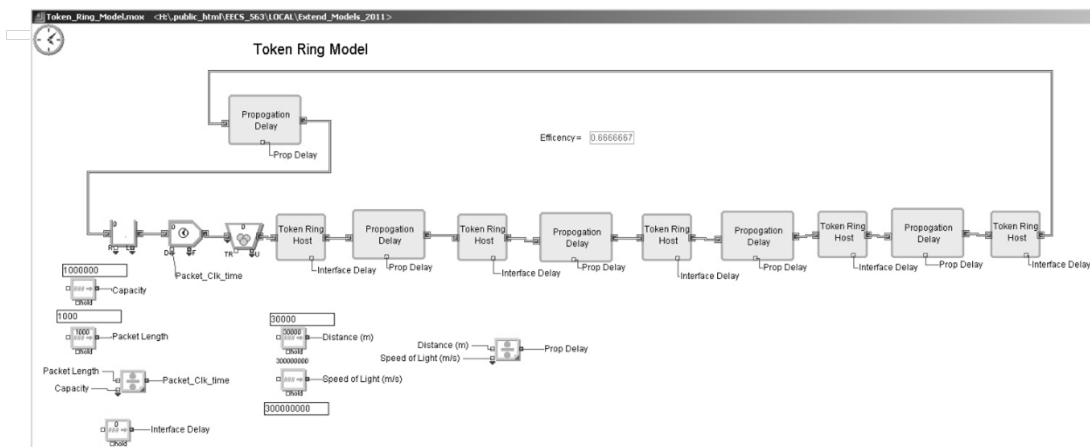
## □ Hub Polling

- No Leader station
- Each nodes polls the next node in turn



# Deterministic Protocols

- Example:
  - # nodes = 10
  - Link rate = 1 Mb/s
  - Packet Size = 1000 bits
  - Assume Low load → no queueing
  - Assume node interface delay = 0
  - 0.1 ms between nodes ( $30 \text{ km} / (3 \times 10^8 \text{ m/s}) = 0.1 \text{ ms}$ )
  - Find the effective transmission rate and efficiency.
    - On average destination is 5 nodes away → 0.5 ms
    - Time to transmit 1000 bits = 0.5 ms + 1 ms = 1.5 ms
    - Effective transmission rate = 1000 bits / 1.5 ms = 666Kb/s
    - Efficiency = (666 Kb/s) / (1000 Kb/s) = 0.66
  - Repeat for link rate = 10 Mb/s
    - On average destination is 5 nodes away → 0.5 ms
    - Time to transmit 1000 bits = 0.5 ms + 0.1 ms = 0.6 ms
    - Effective transmission rate = 1000 bits / 0.6 ms = 1.67 Mb/s
    - Efficiency = (1.67 Mb/s) / (10 Mb/s) = 16.7%
  - Conclusion → Polling does not scale with link rate



## Token Ring Model

[http://www.ittc.ku.edu/~frost/EECS\\_563/LOCAL/Extend\\_Models\\_2019-v10/Token\\_Ring\\_Model-ES10.mox](http://www.ittc.ku.edu/~frost/EECS_563/LOCAL/Extend_Models_2019-v10/Token_Ring_Model-ES10.mox)



## Alternative Media Access Control Strategies:

### Random Access

---

- Each node sends data with *limited* coordination between users:

#### **No explicit permission to transmit**

- Total chaos: Send data as soon as ready
- Limited chaos: Listen before sending data, if the channel is busy do not send.
- Further Limiting chaos: Listen before sending data, continue listening after sending and if collision with another transmission stop sending.

[Carrier Sense Multiple Access with Collision Detection  
CSMA/CD]

## Alternative Media Access Control Strategies:

### Random Access

---

- Advantage: **Simple**
- Disadvantage:
  - No guarantee that you will ever get to send.
  - The MAC protocol technology does not scale

## Random Access Protocols:

### System Assumptions

---

- Overlap in time and space of two or more transmissions causes a collision and the destruction of all packets involved.
  - [ No capture effects]
- One channel
- For analysis no station buffering

## Random Access Protocols:

### Assumptions

---

- Time-Alternatives
  - Synchronization between users (Slotted time)
  - No synchronization between users (unslotted time)
- Knowledge of the channel state-Alternatives
  - Carrier sensing (Listen before talk-LBT)
  - Collision detection

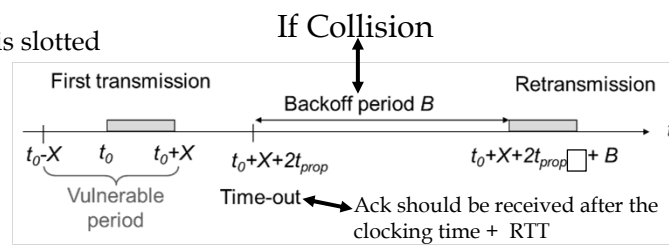
## Random Access Protocols Strategies

- ALOHA (Total chaos)
  - No coordination between users
  - Send a PDU, start timer, wait for acknowledgment, if no acknowledgment (timer fires) then ASSUME collision then **backoff** and try again

*However the PDU could be successfully received but the Ack lost*

- Backoff
  - Select “pseudo-random” time to attempt another transmission
- Slotted ALOHA
  - Same as ALOHA only time is slotted

$X$ =Packet clocking time  
Assume fixed length packets



MAC

21

## Some key general concepts

- Protocols make extensive use of timers
- Protocols make assumptions given local knowledge
- Often protocols need knowledge of the RTT, specifically in setting time-out values
- Protocols “learn” about the fate of their transmissions in a variety of ways; here via expiring of a timeout timer.
- Generation of pseudo-random number generation is needed in some protocols.

MAC

22

## The ALOHAnet

---

- The ALOHAnet, Additive Links On-line Hawaii Area network, a pioneering computer networking system, was developed at the University of Hawaii and implemented in 1971 by Norman Abramson and his colleagues. This wireless data communication system laid the groundwork for modern packet-switched communication networks and played a significant role in the development of the Internet.

See: N. Abramson, "The ALOHA System - Another Alternative for Computer Communications," in Proceedings of the Fall Joint Computer Conference, 1970, pp. 281-285.

## Random Access Protocols Strategies

---

- $p$ -persistent CSMA
  - Listen to channel, on transition from busy to idle transmit with probability  $p$
  - After sending the PDU, wait for acknowledgment, if no acknowledgment before timer fires then **backoff** and retransmit
- Non-persistent, if channel busy then reschedule transmission
- 1-persistent, Transmit as soon as idle

## Random Access Protocols Strategies

---

### □ CSMA/CD

- 1-persistent but continue to sense the channel, if collision detected then stop transmission and backoff (more details later).
- CSMA/CD is used in 10, 100 Mb/s, and 1 Gb/s Ethernet within a collision domain.
- A collision domain is a segment of a network where the network nodes contend for access to the network medium. It is the part of a network where data packets can collide with each other if two or more devices attempt to send data simultaneously.
- Ethernet is often used without a collision domain (more later).

## Limitations on Random Access Protocols

---

### □ Distance

- Time to learn channel state → Propagation time

### □ Speed

- Time to learn channel state → Clocking speed

## Random Access Protocols

### Analysis of ALOHA:

---

- Goal: Find  $S_{\max}$
- Protocol Operation
  - Packet of fixed length  $L$  (sec) arrives at station  $i$ 
    - Station  $i$  transmits immediately
    - Station  $i$  starts an acknowledgment timer
  - If no other station transmits while  $i$  is transmitting then *success*
  - Else a collision occurred
  - Station  $i$  learns that a collision occurred if the acknowledgment timer fires before the acknowledgment arrives

## Random Access Protocols

### Analysis of ALOHA

---

- If collision detected then station  $i$  retransmits at a later time, this time is pseudo-random and is determined by a **backoff** algorithm
- Design Issue:
  - Determine the maximum normalized throughput for an Aloha system

## Random Access Protocols

### Analysis of ALOHA

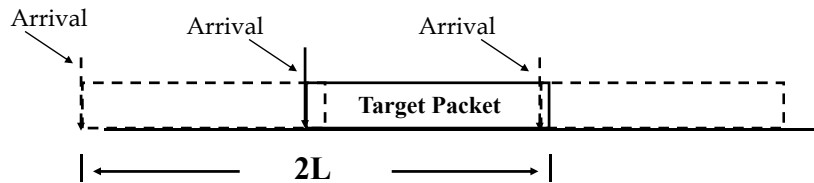
#### Assumptions

1.  $\lambda$  = Average rate of **new** message arrivals to the system
2.  $\Lambda$  = Average rate arrivals to the system, i.e.,  
new arrivals + retransmissions Incoming load  $S = \lambda L \leq 1$
3. The total arrival process is Markov, i.e., time between arrivals has exponential pdf
4. Fixed Length Packets, here L in sec

## Random Access Protocols

### Analysis of ALOHA

#### Collision Mechanism



**Target packet is vulnerable to collision for 2L Sec.**

## Random Access Protocols:

### Analysis of Aloha

Total packet interarrival times,  $T_a$ , are exponentially distributed - Markov Process

Arrival Rate (packets/sec) =  $\Lambda$

With exponentially interarrival times the probability mass function for the number of arrivals,  $k$ , in  $t$  sec is a Poisson pmf of the form:

$$\text{Prob}[k,t] = \frac{(\Lambda t)^k e^{-\Lambda t}}{k!}$$

$$\text{Probability of no arrivals in } 2L \text{ sec} = \text{Prob}[0,2L] = \frac{(\Lambda 2L)^0 e^{-\Lambda 2L}}{0!} = e^{-\Lambda 2L}$$

## Analysis of Aloha

Goal: Find  $S_{\max}$  = Maximum incoming load

$$\begin{aligned} \text{Probability of Collision} &= 1 - \text{Prob}[\text{no arrivals in } 2L \text{ sec}] \\ &= 1 - e^{-2\Lambda L} \end{aligned}$$

But

$$\Lambda = \lambda + \Lambda(1 - e^{-2\Lambda L})$$

Let

$$G = \Lambda L = \text{Offered load (incoming load } S = \lambda L)$$

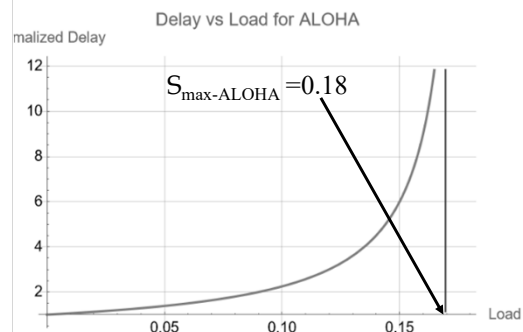
Then

$$G = S + G(1 - e^{-2\Lambda L}) \text{ or } S = G e^{-2\Lambda L}$$

Find  $S_{\max}$

$$\frac{dS}{dG} = 0 \text{ when } G = \frac{1}{2} \text{ or } S_{\max} = \frac{1}{2e} = 0.18$$

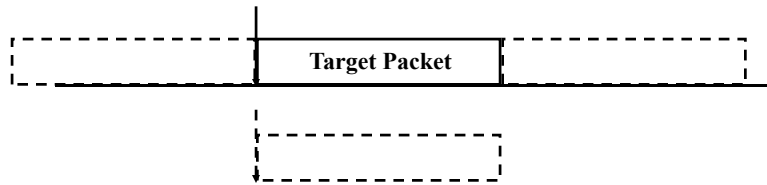
The Maximum throughput for Aloha is 18%





## Random Access Protocols

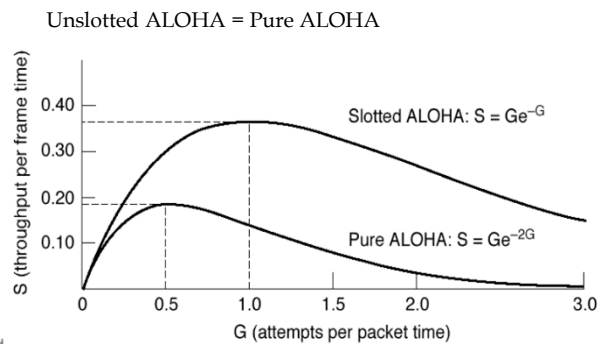
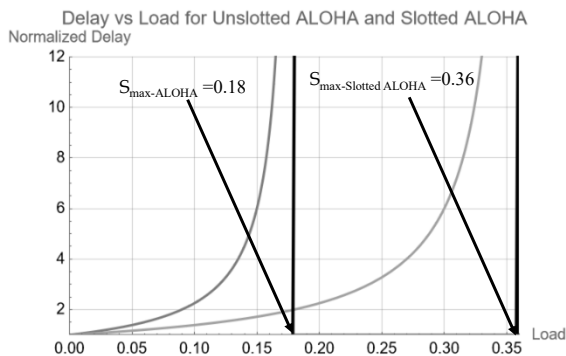
### Analysis of Slotted ALOHA



Synchronization reduces the vulnerable period from  $2L$  to  $L$  so the maximum throughput is increases to 36%

## Random Access Protocols

### Performance of Unslotted and Slotted ALOHA



From: "Computer Networks, 3rd Edition, A.S. Tanenbaum. Prentice Hall, 1996

## Random Access Protocols

### CSMA Protocols

- Listen to the channel before transmitting to reduce the vulnerable period
  - Let  $D$  = maximum distance between nodes (m)
  - Let  $R$  = the transmission rate (b/s)
  - Let  $c$  = speed of light =  $3 \times 10^8$  m/s
  - $v$  = propagation speed in media (m/s)
  - The propagation time =  $\tau$  (sec) =  $D/v$   
k is a constant for the physical media:  
k = .66 for fiber, k=.88 for coax
- Example: 1 km
- Free space propagation time = 3.33 us
  - Fiber propagation time = 5.05 us
  - Coax propagation time = 3.79 us

## CSMA (carrier sense multiple access)

simple CSMA: listen before transmit:

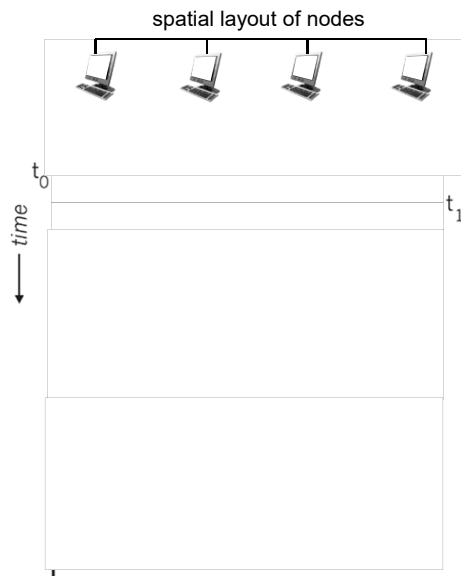
- if channel sensed idle: transmit entire frame
- if channel sensed busy: defer transmission
- human analogy: don't interrupt others!

CSMA/CD: CSMA with *collision detection*

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- collision detection easy in wired, difficult with wireless
- human analogy: the polite conversationalist

## CSMA: collisions

- collisions *can* still occur with carrier sensing:
  - propagation delay means two nodes may not hear each other's just-started transmission
- collision: entire packet transmission time wasted
  - distance & propagation delay play role in determining collision probability



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-37

## Random Access Protocols

### CSMA Protocols

- Assume node A transmits at time  $t$  and node B at  $t - \varepsilon$ ,  
where  $\varepsilon \rightarrow 0$   
(That is, Node B transmits right before it hears A)
- If after  $2\tau$  sec. no collision occurred, then none will occur and sender should receive ACK (but ACK's can be lost)
- Define  $a = \tau / (L/R) = (\text{Maximum propagation time}) / (\text{clocking time})$   
 $= (D/v) / (L/R)$   
 $= DR/Lv$
- $a = \text{normalized length (size) of the network}$
- As  $a \rightarrow 1$ , CSMA performance approaches ALOHA performance

# Random Access Protocols

## CSMA Protocols

□ Limits on  $a$ =normalized size of the network

➤ Want  $a$  small to keep vulnerable period short by having:

- Short bus
- Lower speeds
- Long packets

$$a = \tau / (L/R) = DR/Lv$$

where  
L= packet length in bits  
v= propagation speed m/s

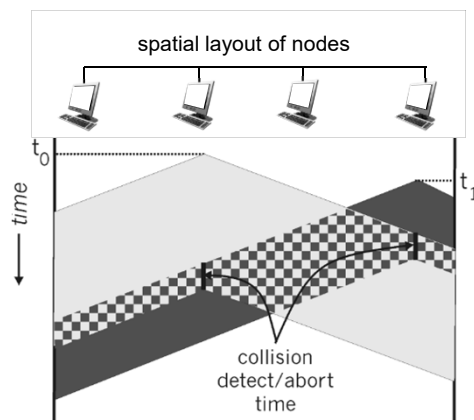
□ Lower limit (Minimum) packet length to upper bound  $a$

Reason for Minimum/Maximum Packet Size in the Internet

□ Maximum packet length to be **fair** → New Concept

## CSMA/CD:

- CSMA/CD reduces the amount of time wasted in collisions
  - transmission aborted on collision detection



# Approximations for the Maximum Throughput for CSMA/CD

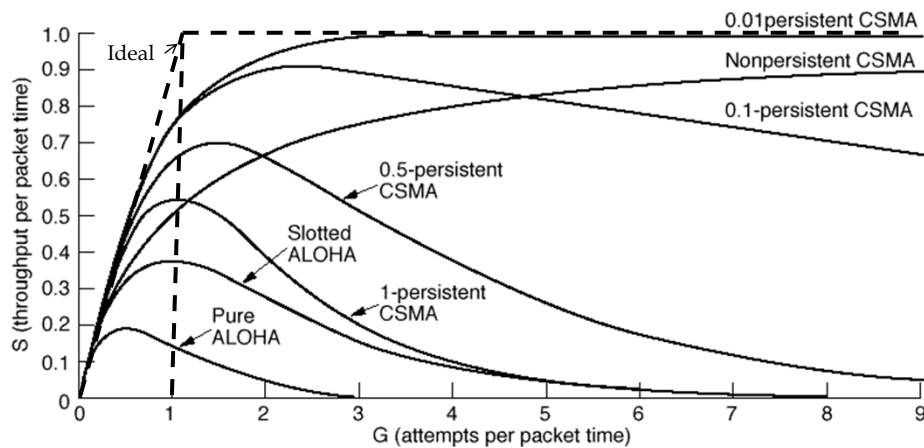
$$\text{Maximum Throughput for CSMA-CD} = \frac{1}{1 + 6.44 a}$$

Note: Book has maximum throughput =  $\frac{1}{1 + 5a}$

$$a = \tau / (L/R) = (\text{Maximum propagation time}) / (\text{clocking time})$$

See: Average Normalized Delay for a CSMA/CD Network as a function of load as the packet length, size of network and link rate and  
Maximum Normalized Throughput for CSMA-CD Networks as a function of packet length, size of the network, and link rate

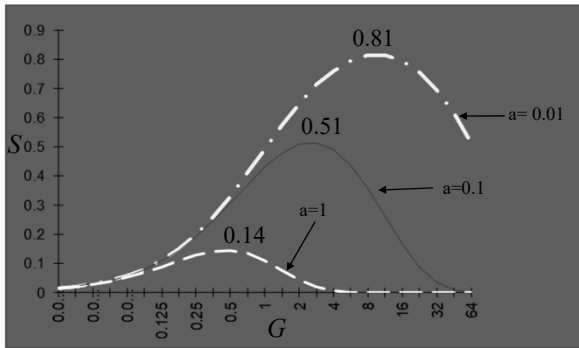
## Random Access Protocols Performance



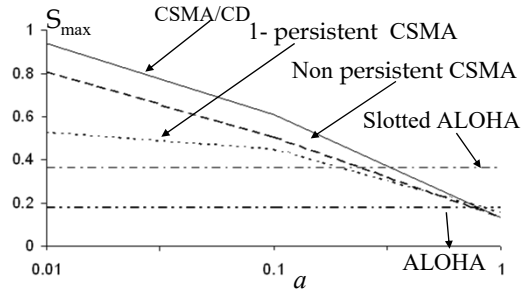
Modified from: "Computer Networks, 3rd Edition, A.S. Tanenbaum. Prentice Hall, 1996

# Random Access Protocols

Performance:

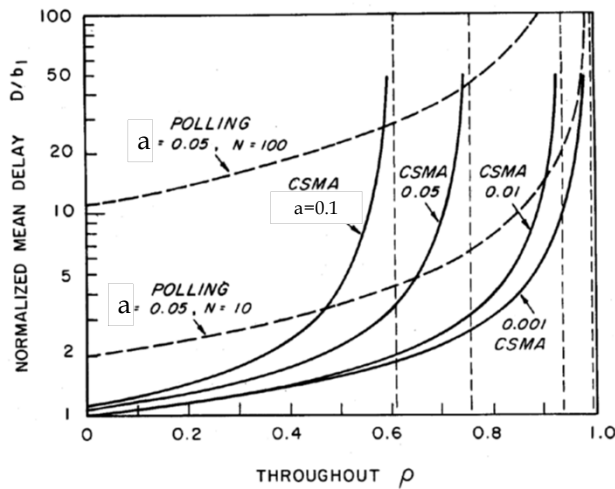


Performance of Nonpersistent CSMA



Modified from: Leon-Garcia & Widjaja: *Communication Networks*

# Polling vs Random Access Performance



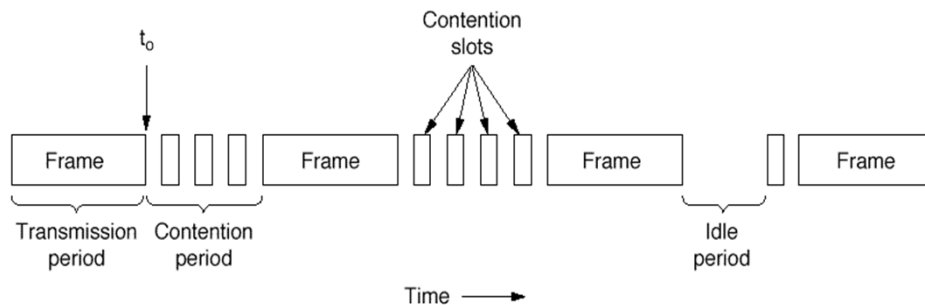
N = # Nodes

From: A Carrier Sense Multiple Access Protocol for Local Networks  
Simon S. Lam, Computer Networks 1979

## Random Access Protocols

### CSMA Protocols: States

- Transmission
- Contention
- Idle



From: "Computer Networks, 3rd Edition, A.S. Tanenbaum.  
Prentice Hall, 1996

MAC 45

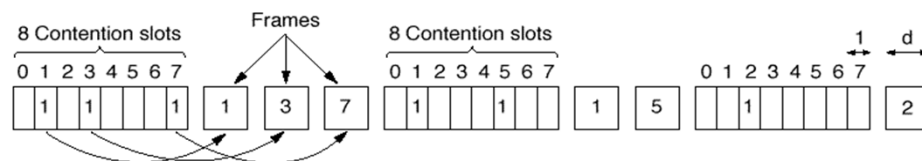
## Data Packet Collision Free Protocols Reservations

- Data packet collision free protocols establish rules to determine which stations send after a successful transmission.
- Assume there are  $N$  stations with unique addresses  $0$  to  $N-1$ .
- A contention *interval* is a period after a successful transmission that is divided into  $N$  time slots, one for each station.

MAC 46

## Data Packet Collision Free Protocols Reservations

- If a station has a PDU to send it sets a bit to 1 in its time slot in the contention interval.
- At the end of the contention interval all nodes know who has data to send and the order in which it will be sent.



From: "Computer Networks, 3rd Edition, A.S. Tanenbaum.  
Prentice Hall, 1996

MAC 47

## Data Packet Collision Free Protocols Reservations

- Problems:
  - Fairness
  - Flexibility
- Many systems use this technique as a basis for their approach to collision free protocols

MAC 48



## Random Access and Reservations

---

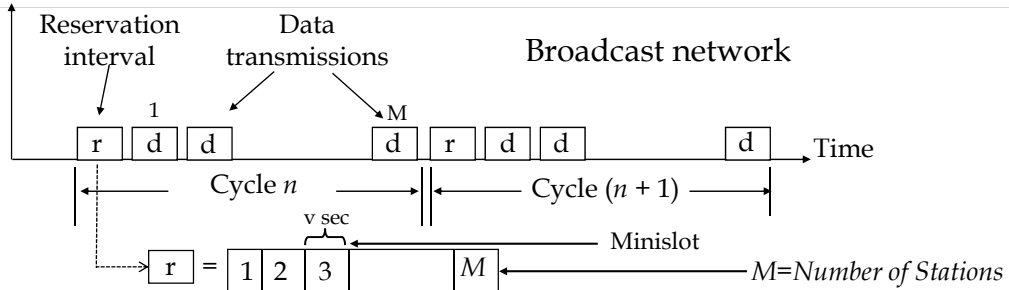
- *Distributed systems*: Stations implement a decentralized algorithm to determine transmission order, e.g., reservation Aloha
- *Centralized systems*: A central controller accepts requests from stations and issues grants to transmit
- The centralized reservation system is used in many access technologies, e.g.,
  - DOCSIS: cable modems
  - Cellular Networks - Long Term Evolution (LTE) & 4G/5G

## Reservation System

---

- System Characteristics
  - Asymmetric
    - Upstream/Uplink
      - Minislots with requests for resources
      - Access Minislots via random access protocol
    - Downstream/Downlink
      - Accepts minislots and includes grants for transmission on the upstream
      - Grants control the flow on the upstream link
      - Order of grants established via a “scheduling” algorithm

# Reservation Systems



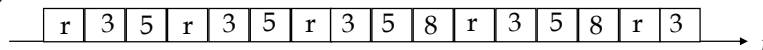
- Transmissions organized into cycles (or frames, e.g. time/frequency slots, as in OFDMA)
- Cycle: reservation interval + frame transmissions
- Reservation interval has a minislot for *each* station to request reservations for frame transmissions; minislot can carry other information, e.g., number of frame to TX, station backlog, channel quality indicator (CQI)

Adapted from: Leon-Garcia & Widjaja: *Communication Networks*

# Example

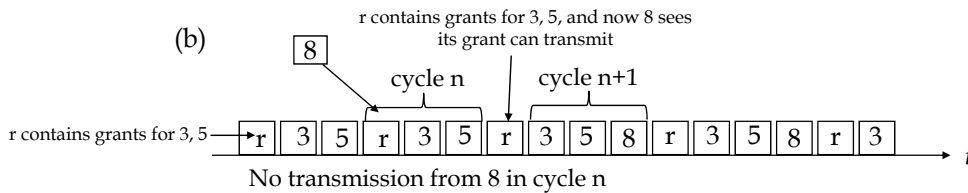
- Initially stations 3 & 5 have reservations to transmit frames

(a)



- Station 8 becomes active and makes reservation
- Cycle now also includes frame transmissions from station 8

(b)



Adapted from: Leon-Garcia & Widjaja: *Communication Networks*

## Central controller issues grants to transmit

- Algorithms in the central controller (base station or headend) are used to grant permission to UE to transmit on upstream can be based on:
  - station backlog (queue length),
  - channel quality indicator (CQI)
    - Leads to Opportunistic Scheduling
  - Other.....

## Throughput

- Let
  - R = Link rate (b/s)
  - L = packet size (bits) assume fixed length
  - v = minislot size (sec)
  - M = Number of stations
  - X = L/R (sec) = clocking time
- Assume
  - Propagation delay  $\ll$  X=L/R (sec)  $\rightarrow$  Access network
  - Heavy load  $\rightarrow$  stations have packets to send
  - All requests are granted
  - One minislot needed for each packet/station
- Time to transmit M packets = Mv+MX

$$S_{\max} = \frac{MX}{Mv + MX} = \frac{1}{1 + \frac{v}{X}}$$

Example:  
L=1000 Bytes  
R=100Mb/s  
v=10us

X= 80us  
S<sub>max</sub> = 87.5%

## Throughput

- If  $k$  frame transmissions can be reserved with ONE reservation message and if there are  $M$  stations, as many as  $Mk$  frames can be transmitted in  $XM(k+v)$  seconds

$$S_{\max} = \frac{MkX}{Mv + MkX} = \frac{1}{1 + \frac{v}{Xk}}$$

Example:  
L=1000 Bytes  
R=100Mb/s  
v=10us  
k= 4

X= 80us  
S<sub>max</sub> = ~97%

Adapted from: Leon-Garcia & Widjaja: *Communication Networks*

MAC

55

## Throughput:

### Random access contention for Minislots

- Real systems have too many nodes for each to get a fixed minislot.
- Therefore a random access protocol, typically slotted ALOHA, is used to transmit in a minislot.
  - A station attempts to obtain a grant by transmitting in a minislot.
  - If successful the station will see their reservation in the next reservation interval (cycle)
  - Therefore station learns about collision by observing next next reservation interval, not by time-out.
  - If unsuccessful, then assume collision, backoff and retry.
  - Unsuccessful means collision in the minislot and then backoff and try again

MAC

56

## Throughput:

### Random access contention for Minislots

- Assume slotted Aloha is used for contention for minislots.
- On average, each reservation takes at least  $e = 2.71$  minislot attempts

$$S_{\max} = \frac{1}{1 + 2.71v/X}$$

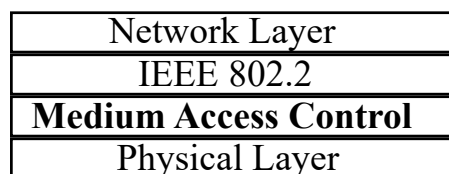
- Effect is just to make the minislots seem longer  $\rightarrow$  reducing  $S_{\max}$

Example:  
L=1000 Bytes  
R=100Mb/s  
v=10us

X= 80us  
 $S_{\max} = \sim 75\%$

## Standard IEEE 802 LANs

All are broadcast or emulated broadcast



IEEE 802.2 = Logical Link Control Protocol

IEEE 802.3  
IEEE 802.4  
IEEE 802.5  
IEEE 802.6  
IEEE 802.11 Wireless  
IEEE 802.12  
IEEE 802.16  
Others.....

•[Why Li-Fi Might Be Better Than Wi-Fi](#) From: IEEE Institute Jan 9, 2024

[How Li-Fi Could Revolutionize Wireless Communications](#)

IEEE 802.11bb Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Light Communications

## Random Access Protocols

### CSMA Protocols

---

- Example: Ethernet (IEEE 802.3)
  - Original Rate = 10 Mb/s
  - Minimum packet size = 512 bits (64B)
  - Maximum packet size = 12144 bits (1518B)
  - D (max per segment) = 500 m
  - $a \rightarrow [0.001, 0.03]$
- CSMA networks do not scale
  - Increase D (therefore  $\tau$  increases) performance degrades
  - Increase R performance degrades

## Ethernet

---

- Unslotted 1-persistent CSMA/CD
- Procedure
  - Frame\_to\_transmit and idle
    - wait *interframe\_gap* (prevents back-to-back transmission)
    - transmit
  - Listen to channel and if collision
    - stop sending
    - send *jam* signal (makes sure all nodes hear collision)
    - schedule retransmission

## Ethernet: Schedule retransmission

(the binary exponential backoff algorithm)

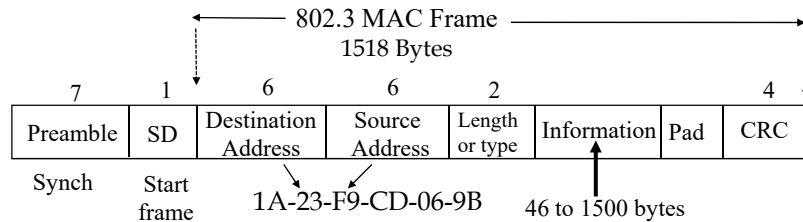
- N = number of retransmission attempts
- Upon collision
  - N = N+1
  - If N > *attempt limit* then trash the PDU (*attempt limit* is a parameter of the algorithm)
    - Else calculate the backoff time
      - k = Min[N, *backoff\_limit*] (*backoff\_limit* is a parameter of the algorithm)
      - R ~ Uniform [0, 2<sup>k</sup>]
      - retransmit at time t<sub>now</sub> + R\**slot\_time* (*slot\_time* is a parameter of the algorithm)
- Collision, node enters binary (exponential) backoff:
  - after m<sup>th</sup> collision, NIC chooses k at random from {0,1,2, ..., 2<sup>backoff\_limit-1</sup>}. NIC waits k·512 bit times, retransmits
  - more collisions: longer backoff interval and better chance next transmission will be successful

## Ethernet: Parameters

- Slot time = 512 bit times
- Interframe gap = 9.6us
- Attempt limit = 16
- Backoff limit = 10
- Jam time = 32 bits/rate
- Maximum frame size = 8\*(1518) bits
- Minimum frame size = 8\*(64) bits

# Ethernet

## Packet structure



Preamble: 7 bytes of 10101010

Start Of Frame: 1 byte, thus: 10101011

Source and Destination Address: Each 6 bytes and are globally unique. <https://www.macvendorlookup.com/>

Example: Look up manufacture for 34-17-EB-AE-45-41

Length: this field gives the length (in bytes) of the data field.

Data field: From 46 to 1500 bytes.

Overhead = 26 bytes

CRC=cyclic redundancy check is an error-detecting code

MAC 63

## More on addressing: Ethernet addresses

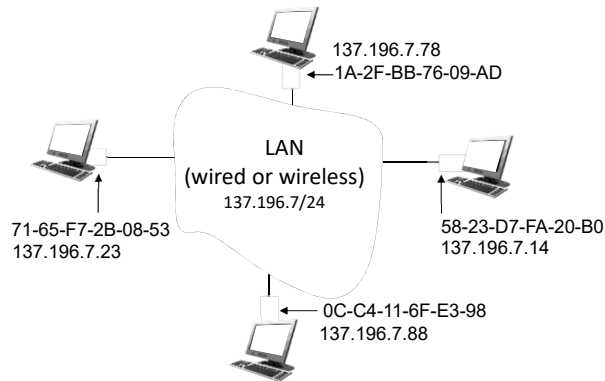
- 32-bit IP address:
  - *network-layer* address for interface
  - used for layer 3 (network layer) forwarding
  - e.g.: 128.119.40.136
- MAC (or LAN or physical or Ethernet) address:
  - function: used “locally” to get frame from one interface to another physically-connected interface (same subnet, in IP-addressing sense)
  - 48-bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable (Do not change your MAC address!)
  - e.g.: 1A-2F-BB-76-09-AD

*hexadecimal (base 16) notation  
(each “numeral” represents 4 bits)*



## More on addressing: Ethernet addresses each interface on LAN

- has unique 48-bit MAC address
- has a locally unique 32-bit IP address (as we've seen)
- ARP used to associate MAC with IP Address



Show ARP in action

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-65

## More on addressing: Ethernet addresses

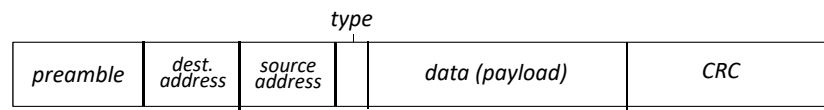
- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- analogy:
  - MAC address: like Social Security Number
  - IP address: like postal address
- MAC flat address: portability
  - can move interface from one LAN to another
  - recall IP address *not* portable: depends on IP subnet to which node is attached

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-66

# Ethernet frame structure

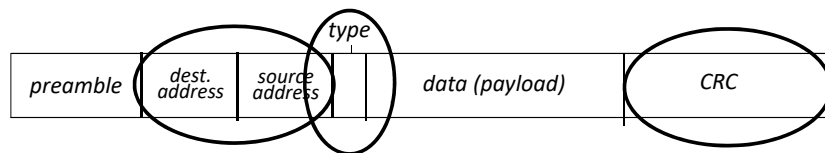
sending interface encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame



*preamble:*

- used to synchronize receiver, sender clock rates
- 7 bytes of 10101010 followed by one byte of 10101011

# Ethernet frame structure (more)



- addresses: 6 byte source, destination MAC addresses
  - if adapter receives frame with matching destination address, or with broadcast address (e.g., ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame
- type: indicates higher layer protocol
  - mostly IP but others possible, e.g., Novell IPX, AppleTalk
  - used to demultiplex up at receiver
- CRC: cyclic redundancy check at receiver
  - error detected: frame is dropped

## Ethernet: unreliable, connectionless

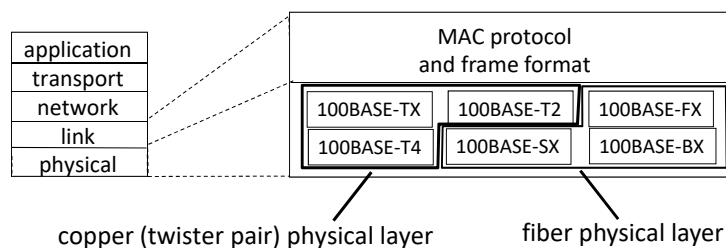
- connectionless: no handshaking between sending and receiving NICs
- unreliable: receiving NIC doesn't send ACKs or NAKs to sending NIC
  - data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: unslotted CSMA/CD with binary backoff

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-69

## 802.3 Ethernet standards: link & physical layers

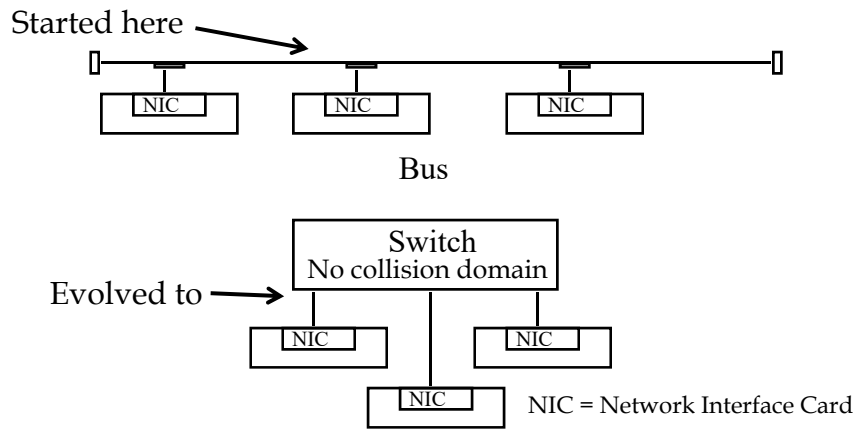
- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps
  - different physical layer media: fiber, cable



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-70

# Ethernet: Typical Configurations

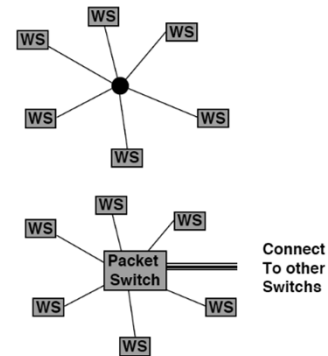


MAC 71

# Migration to switched LANs

WS=Workstation,  
aka, host, aks, PC

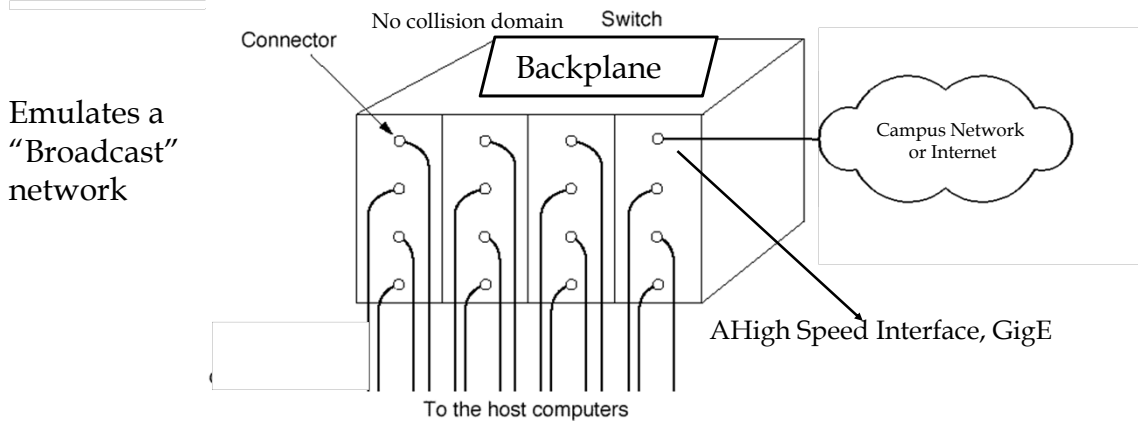
- **Traditional Ethernet**
  - Nodes connected with coax
    - Long “runs” of wire everywhere
  - CSMA/CD protocol
- **“Hub” Ethernet or Bridge**
  - Nodes connected to hub
    - Hub acts as a broadcast repeater
    - Shorted cable “runs”, Useful for 100 Mbps
  - CSMA/CD protocol
  - Easy to add/remove users
  - Easy to localize faults
  - Cheap cabling (twisted pair, 10baseT)
- **Switched Ethernet**
  - No CSMA/CD
    - Easy to increase data rate (e.g., Gbit Ethernet)
  - Nodes transmit when they want
  - Switch queues the packets and transmits to destination
  - Typical switch capacity of 20-40 ports
  - Each node can now transmit at the full rate of 10/100/Gbps
  - **Modularity:** Switches can be connected to each other using high rate ports
  - No collision domain



Modified from: Lectures 12: CSMA, CSMA/CD and Ethernet, Eytan Modiano  
<http://web.mit.edu/modiano/www/6.263/L12.pdf>

MAC 72

# Switched Ethernet



For nonblocking backplane speed = sum of port speeds

Example: for a switch with 8 1-GigE ports the backplane runs at 8 Gb/s

From: "Computer Networks, 3rd Edition, A.S. Tanenbaum.  
Prentice Hall, 1996

MAC 73

# Gigabit Ethernet

- Allows half- and full-duplex operation at speeds of 1000 Mb/s
- Uses the 802.3 Ethernet frame format
- Can use the CSMA/CD access method with support for one repeater per collision domain: Half-duplex
- Common use is with Gigabit Ethernet switches in Full-duplex mode  
→ No CSMA/CD
- Addresses compatibility with 10 Mb/s, 100 Mb/s, and 10-Gigabit Ethernet technologies

From: Whitepaper: Gigabit Ethernet Overview,  
Gigabit Ethernet Alliance, May, 1997, <http://www.gigabitEthernet.org/technology/whitepapers>

MAC 74

## Gigabit Ethernet: Distance

---

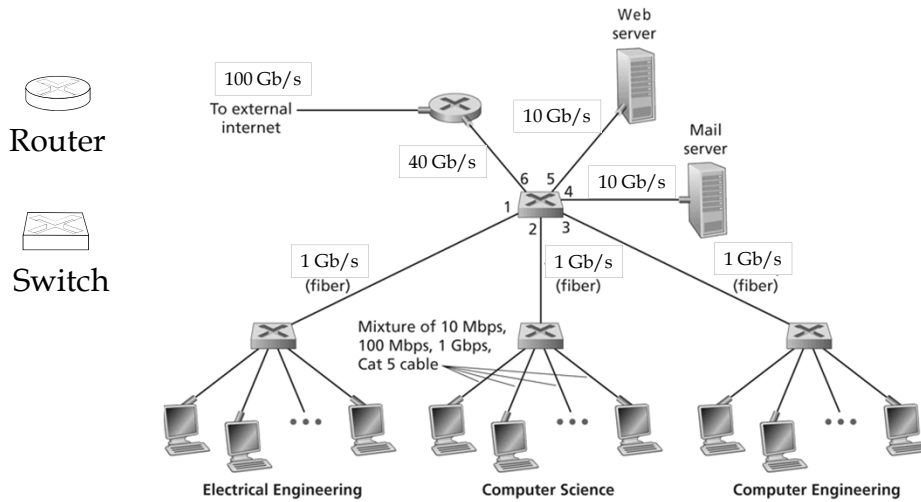
- Multimode fiber-optic link with a maximum length of 550m
- Single-mode fiber-optic link with a maximum length of 3km
- Copper based link with a maximum length of at least 25m
  - Category 5 unshielded twisted pair (UTP) wiring link 100m

## Ethernet

---

- 40 Gb/s Ethernet 40GbE
- 100 Gb/s Ethernet 100GbE
- Provide support for optical transport network(OTN)
- Carrier Grade Ethernet
  - Ethernet services to end customers
  - Ethernet technology in carrier networks

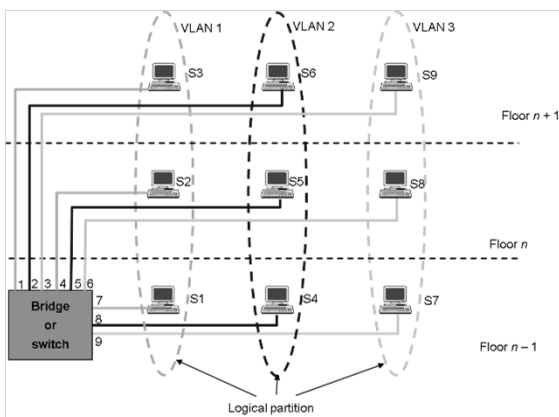
# Example: Switched Based Campus Network



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

MAC 77

# VLANS



## Virtual LAN

Virtual LAN emulates a broadcast network for that set of end nodes

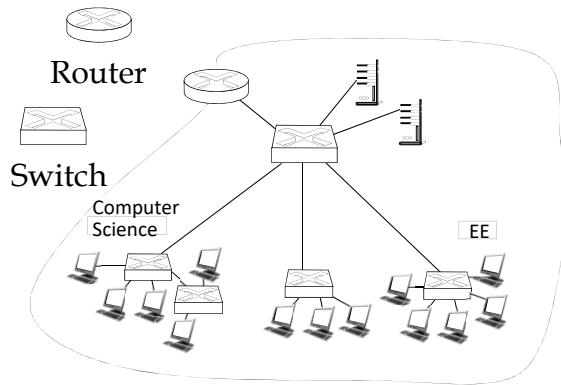
Forwarding between VLANs: done via routing

Adapted from: Leon-Garcia & Widjaja: *Communication Networks*

MAC 78

## Virtual LANs (VLANs): motivation

Q: what happens as LAN sizes scale, users change point of attachment?



single broadcast domain:

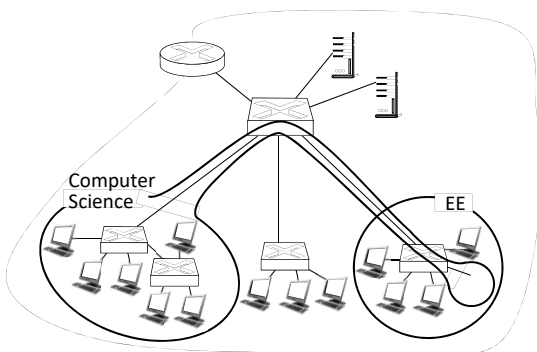
- *scaling*: all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy issues

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-79

## Virtual LANs (VLANs): motivation

Q: what happens as LAN sizes scale, users change point of attachment?



single broadcast domain:

- *scaling*: all layer-2 broadcast traffic (ARP, DHCP, unknown MAC) must cross entire LAN
- efficiency, security, privacy, efficiency issues

administrative issues:

- CS user moves office to EE - *physically* attached to EE switch, but wants to remain *logically* attached to CS switch

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-80



# Advantages of VLANs

---

- Virtual LANs (VLANs)
- A primary advantages of VLANs is their ability to logically segment a physical network into multiple virtual networks.
- Other advantages of using VLANs:
  - Network Segmentation: VLANs allow you to divide a physical network into multiple logical segments without the need for separate physical hardware. This segmentation provides isolation and enhances network security. Different departments, projects, or functions can be separated into their own VLANs, which helps prevent broadcast storms and limits the scope of network breaches.

# Advantages of VLANs

---

- Improved Network Security: By segregating network traffic into VLANs, you can control which devices can communicate with each other. This enhances security by restricting unauthorized access and limiting the potential attack surface. For example, sensitive data on a finance VLAN can be isolated from other parts of the network.
- Broadcast Control: In a traditional flat network, broadcast traffic can consume a significant amount of bandwidth. With VLANs, broadcast domains are smaller, reducing the impact of broadcasts on the network and improving overall network performance.

## Advantages of VLANs

---

- **Scalability:** VLANs make it easier to scale your network as your organization grows. You can add new VLANs or expand existing ones without needing to reconfigure the physical network infrastructure.
- **Simplified Network Management:** Managing a network with VLANs is more efficient, as it allows you to group and administer devices logically. This simplifies tasks like assigning IP addresses, implementing Quality of Service (QoS) policies, and monitoring network traffic.
- **Optimized Traffic Flow:** You can apply QoS policies to VLANs to prioritize certain types of traffic. This ensures that critical applications receive the necessary network resources, leading to better performance for important services.



## Advantages of VLANs

---

- **Guest Networking:** VLANs are commonly used to create isolated guest networks. Guests can access the internet while remaining separate from the internal corporate network, enhancing security.
- **Flexibility:** VLANs can be reconfigured and adjusted as needed, making it easier to adapt to changing network requirements and topologies.
- **Redundancy and Failover:** VLANs can be used to set up redundant network paths and failover mechanisms to increase network availability. This can be important for critical applications.
- **Compliance and Regulatory Requirements:** VLANs can help organizations meet compliance requirements by isolating sensitive data and ensuring that it is only accessible to authorized users.

## Definitions of Network Elements

---

- Repeaters
- Bridges
- Switches   
Switch
  
- Routers   
Router
  - Routing
  - Forwarding

## Repeaters & Bridges

---

- Repeaters forwards electrical signals from one Ethernet to another
- Bridges (sometimes called hubs)
  - Interconnects multiple access LANs to form *Extended LANs*
  - Only forwards frames destined for other LANs
  - Link layer forwarding based on MAC address
  - Bridges are devices that forward link-level frames from one physical LAN to another
  - Bridging forwarding rules prevent loops

# Switches & Routers



## ➤ Switches

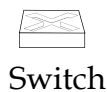
- Forwards packets, based on MAC (link layer) address
- Star topology
- New hosts can be added without degrading the performance of the existing hosts
- Scales by adding additional switches and virtualization



## ➤ Routers

- Forwards packets, based on network address (IP)
- Interconnects two or more networks (maybe owned by different organizations)
- Forwarding → take packet from input port then use routing table to find an output port then forward packet to that port.
- Routing → process of filling in the routing table

# Switches & Routers



- Layer 2 switching is performed by looking at a destination MAC address within a frame. Layer 2 switching builds and maintains a switching table that keeps track of which MAC addresses belong to each port or interface, e.g., Ethernet switches

## Switches & Routers

---



Router

- Layer 3 switching (routers) operates at the network layer. It examines packet information and forwards packets based on their network-layer destination addresses.
  - IP Switches, aka routers
- Layer 4 Switching operates at the transport layer makes forwarding decision based on IP address and TCP/UDP application port
  - Firewalls, Policy Based Networks (PBN), Directory Enabled Networks (DEN)

## Generalized Forwarding

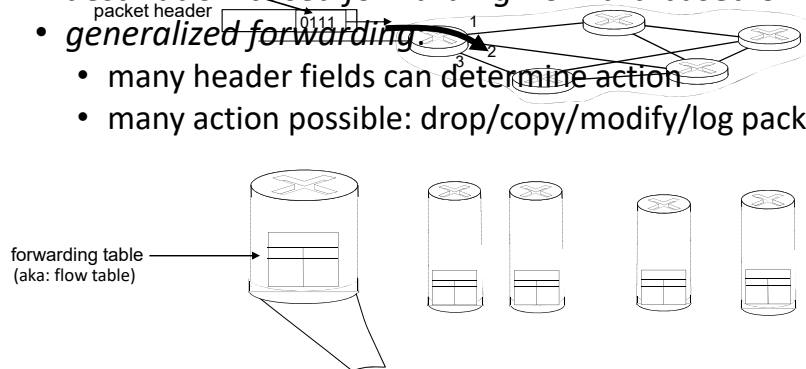
---

- In general the “box” does a match function, e.g., lookup the address and then an action function,
- Actions include:
  - Send packet to selected output port (physical)
  - Drop the packet
  - Modifying a field in the header (there are restrictions)
- Action is based on any fields in the packet header
- Generalized forwarding is used in Software Defined Networks (SDNs)

# Generalized forwarding: match plus action

*Review:* each router contains a forwarding table (aka: flow table)

- “match plus action” abstraction: match bits in arriving packet, take action
  - ~~destination-based forwarding~~: forward based on dest. IP address
  - **generalized forwarding**:
    - many header fields can determine action
    - many action possible: drop/copy/modify/log packet

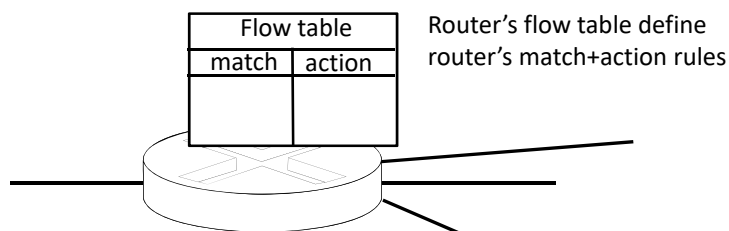


Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-91

# Flow table abstraction

- flow: defined by header field values (in link-, network-, transport-layer fields)
- generalized forwarding: simple packet-handling rules
  - match: pattern values in packet header fields
  - actions: for matched packet: drop, forward, modify, matched packet or send matched packet to controller
  - counters: #bytes and #packets

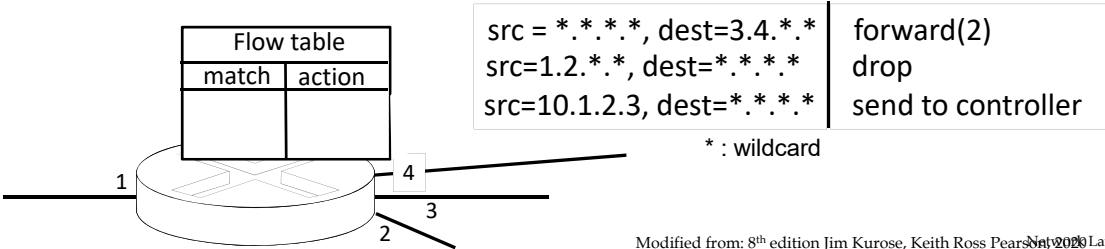


Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-92

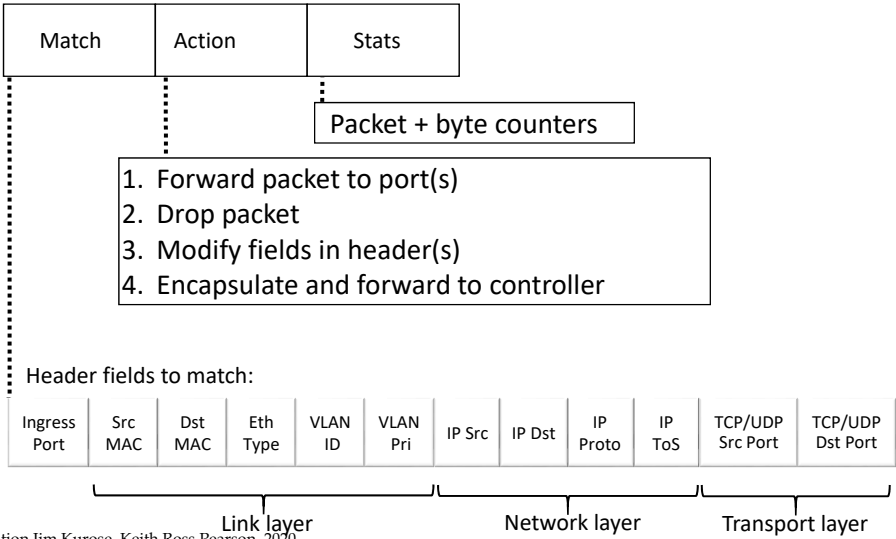
# Flow table abstraction

- flow: defined by header fields
- generalized forwarding: simple packet-handling rules
  - match: pattern values in packet header fields
  - actions: for matched packet: drop, forward, modify, matched packet or send matched packet to controller
  - priority: disambiguate overlapping patterns
  - counters: #bytes and #packets



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020 Layer: 4-93

# OpenFlow: flow table entries



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-94

# OpenFlow: examples

Destination-based forwarding:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	VLAN Pri	IP Src	IP Dst	IP Prot	IP ToS	TCP s-port	TCP d-port	Action
*	*	*	*	*	*	*	51.6.0.8	*	*	*	*	port6

IP datagrams destined to IP address 51.6.0.8 should be forwarded to router output port 6

Firewall:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	VLAN Pri	IP Src	IP Dst	IP Prot	IP ToS	TCP s-port	TCP d-port	Action
*	*	*	*	*	*	*	*	*	*	*	22	drop

Block (do not forward) all datagrams destined to TCP port 22 (ssh port #)

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	VLAN Pri	IP Src	IP Dst	IP Prot	IP ToS	TCP s-port	TCP d-port	Action
*	*	*	*	*	*	128.119.1.1	*	*	*	*	*	drop

Block (do not forward) all datagrams sent by host 128.119.1.1

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-95

# OpenFlow: examples

Layer 2 destination-based forwarding:

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	VLAN Pri	IP Src	IP Dst	IP Prot	IP ToS	TCP s-port	TCP d-port	Action
*	*	22:A7:23: 11:E1:02	*	*	*	*	*	*	*	*	*	port3

layer 2 frames with destination MAC address 22:A7:23:11:E1:02 should be forwarded to output port 3

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-96



# OpenFlow abstraction

- match+action: abstraction unifies different kinds of devices

## Router

- *match*: longest destination IP prefix
- *action*: forward out a link

## Switch

- *match*: destination MAC address
- *action*: forward or flood

## Firewall

- *match*: IP addresses and TCP/UDP port numbers
- *action*: permit or deny

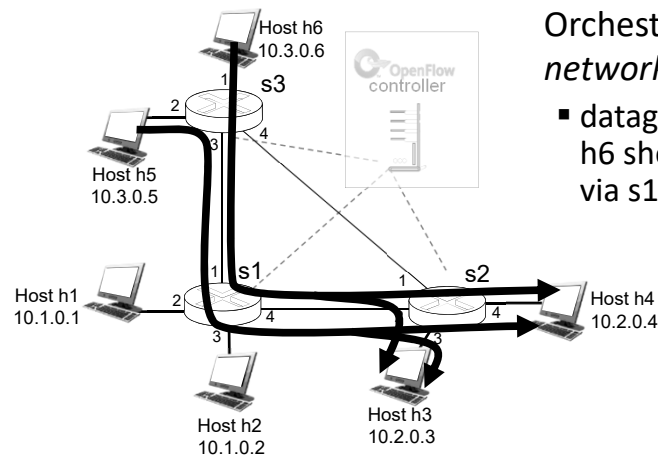
## NAT

- *match*: IP address and port
- *action*: rewrite address and port

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-97

# OpenFlow example



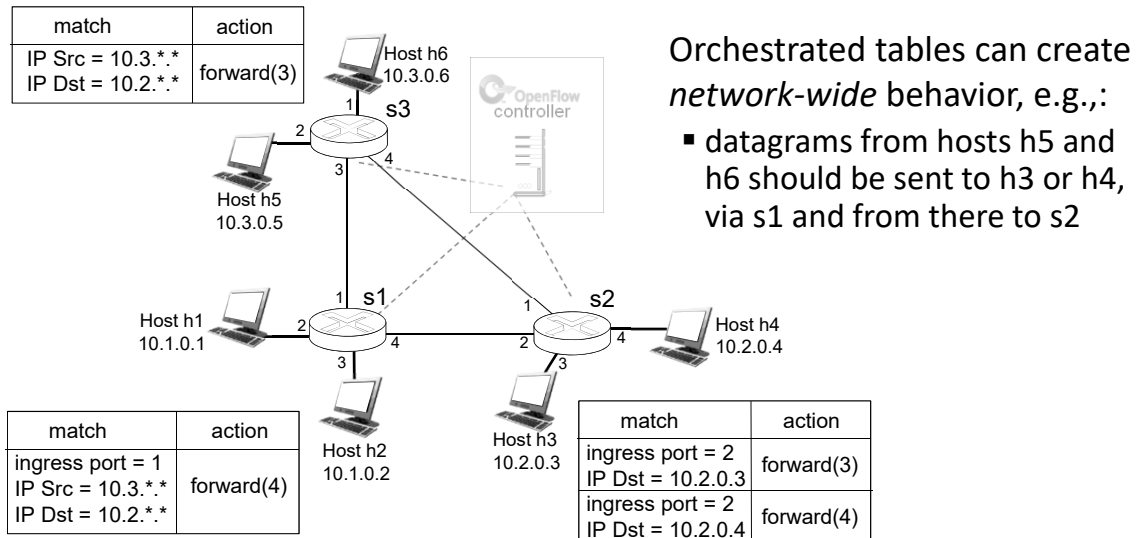
Orchestrated tables can create *network-wide* behavior, e.g.,:

- datagrams from hosts h5 and h6 should be sent to h3 or h4, via s1 and from there to s2

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-98

# OpenFlow example



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-99

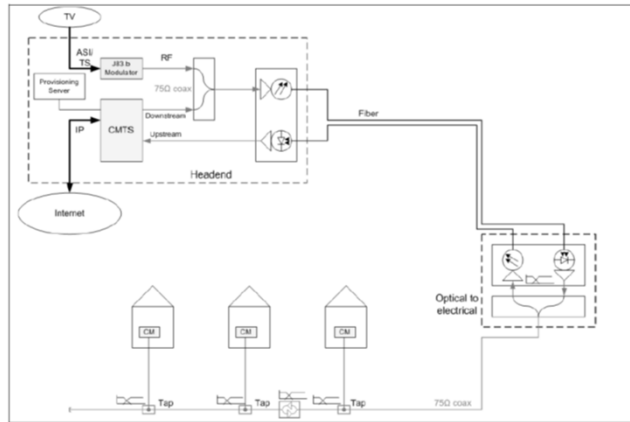
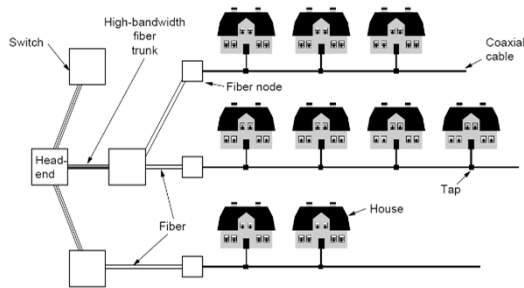
# Generalized forwarding: summary

- “match plus action” abstraction: match bits in arriving packet header(s) in any layers, take action
  - matching over many fields (link-, network-, transport-layer)
  - local actions: drop, forward, modify, or send matched packet to controller
  - “program” *network-wide* behaviors
- simple form of “network programmability”
  - programmable, per-packet “processing”
  - *historical roots*: active networking
  - *today*: more generalized programming: P4 (see p4.org).

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Network Layer: 4-100

# Broadband Access Technologies: Cable Modems



FDM on the Cable

DOCSIS 3.1 Frequency Plan



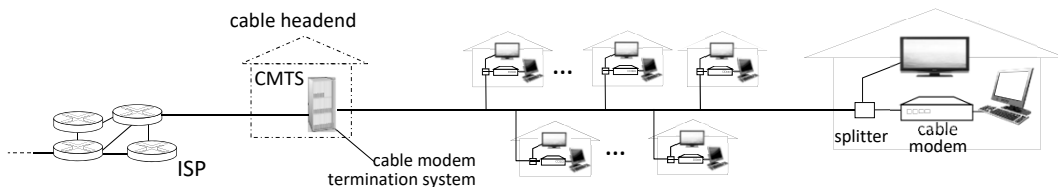
MoCA-Multimedia over Coax, another home networking technology

From: "Computer Networks, 3rd Edition, A.S. Tanenbaum, Prentice Hall, 1996  
And White Paper: DOCSIS 3.1: Cable Tackles the Gigabit Challenge, Alan Breznick, Feb 2016  
And DOCSIS 3.1 Application Note, Rohde and Schwarz

MAC 101

## Cable access network:

Internet frames, TV channels, control transmitted downstream at different frequencies



- multiple downstream (broadcast) FDM channels: up to 1.6 Gbps/channel
  - single CMTS transmits into channels
- multiple upstream channels (up to 1 Gbps/channel)
  - multiple access: all users contend (random access) for certain upstream channel time slots; others assigned TDM

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Link Layer: 6-102

## Broadband Access Technologies: Cable Modems - Terms

---

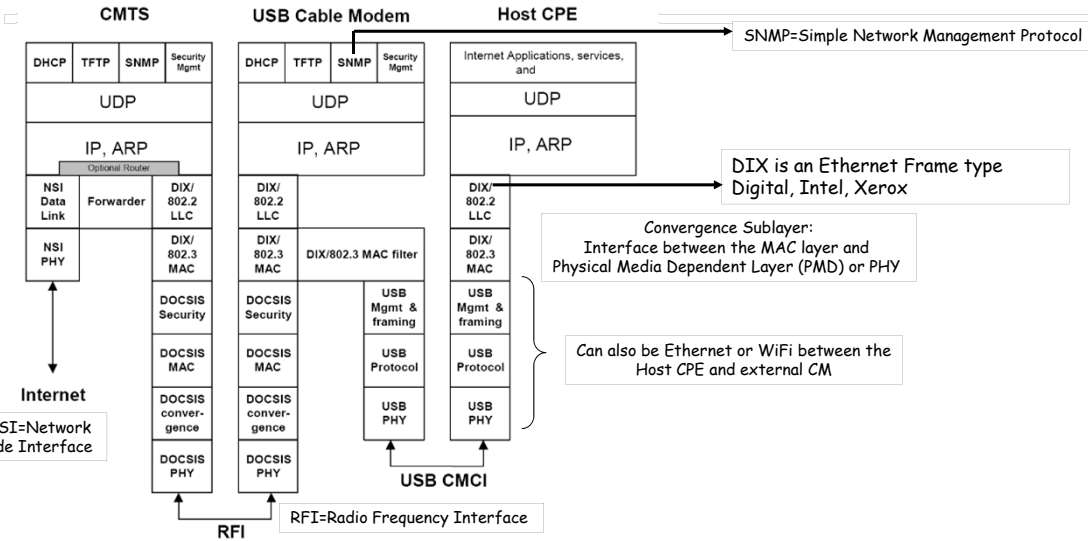
- Data Over Cable Service Interface Specification (DOCSIS)
  - CableLabs sets the standard for the cable industry (see <https://www.cablelabs.com/>)
- CMTS: Cable Modem Termination System. Central device for connecting the cable TV network to a data network like the internet. Normally placed in the headend of the cable TV system.
- Headend: Central distribution point for a CATV system. Video signals are received here from satellites and maybe other sources, frequency converted to the appropriate channels, combined with locally originated signals, and rebroadcast onto the Hybrid fiber/coax (HFC) plant.
- Upstream: The data flowing from the Cable Modem to the CMTS.
- Downstream: The data flowing from the CMTS to the cable modem.

## Broadband Access Technologies: Cable Modems-MAC

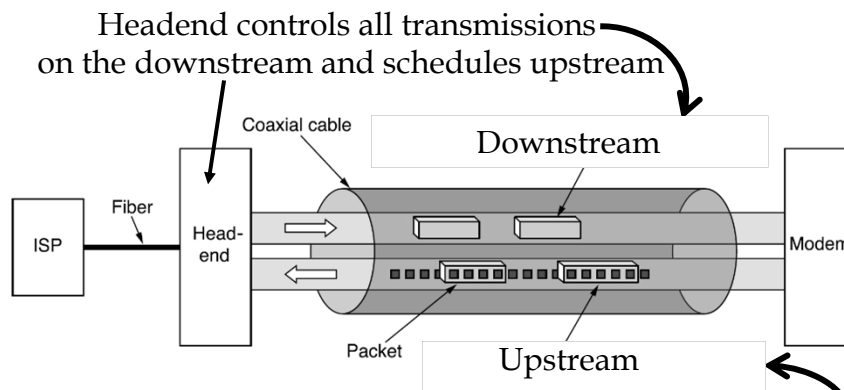
---

- Ranging
  - Calibrate transmit power levels
  - Calibrate time reference
- Frequency data rate assignments
- Request transmissions (Upstream)
- Allocates time slots (grants) for transmission (downstream)
- Forward Error Control (FEC)
- Aggregate Data Rates shared by 500 to 2000 homes today

# DOCSIS Protocol Stack



# Broadband Access Technologies: Cable Modems - Terms

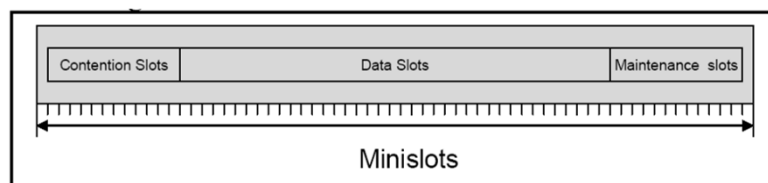


Request for use of upstream made using random access (contention) in specific upstream time slots

# DOCSIS MAC

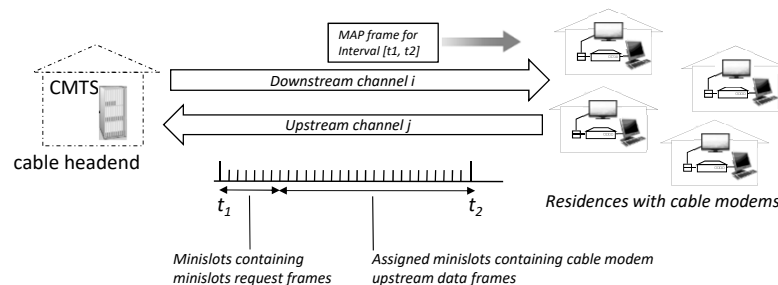
## □ Upstream Bandwidth Allocation Protocol

- MAP is a MAC management message transmitted by the CMTS in the downstream which describes the use of the next upstream mini-slots (up to 4096)
- A MAP describes some slots as grants for particular stations to transmit data in, some for contention transmission and some as an opportunity for new CMs to join the link



MAC 107

## Cable access network:

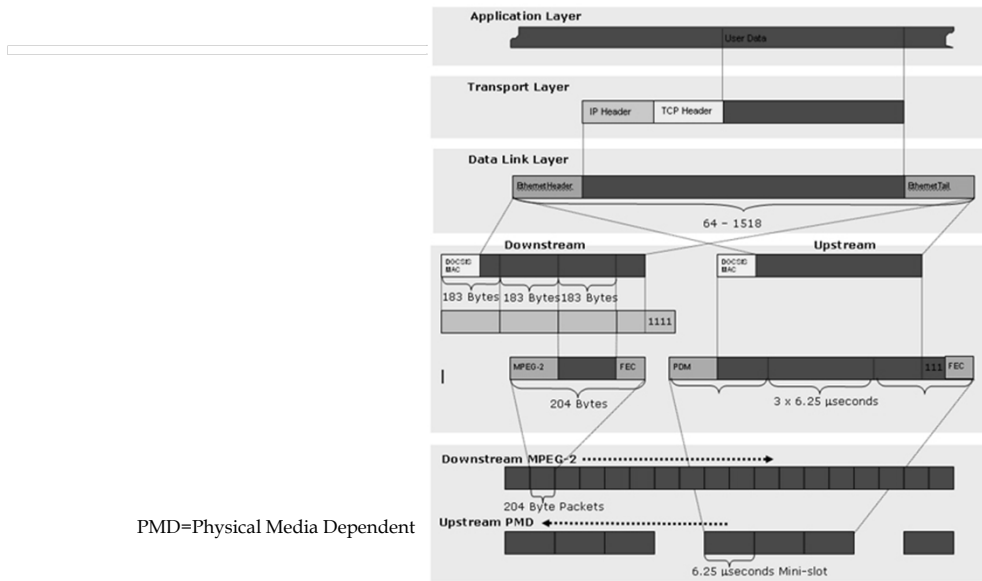


## DOCSIS: data over cable service interface specification

Upstream: some slots assigned, some have contention

- downstream MAP frame: assigns upstream slots
- request for upstream slots (and data) transmitted random access (binary backoff) in selected slots
- Learn if collision if no grant for transmission in next downstream MAP frame (not wait for ack to determine a collision)

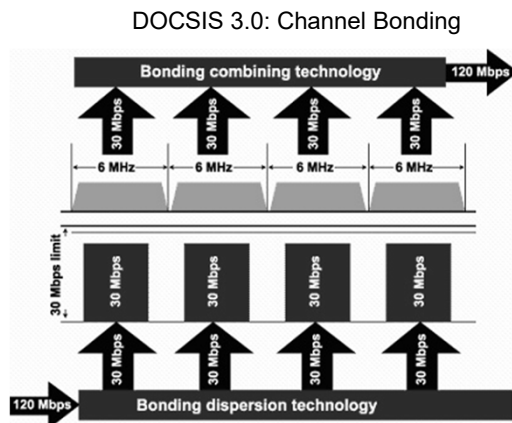
# DOCSIS MAC



PMD=Physical Media Dependent

From: [http://www.jlsnet.co.uk/index.php?page=projects\\_docsis\\_chap3c](http://www.jlsnet.co.uk/index.php?page=projects_docsis_chap3c)

# DOCSIS 3.0 & 3.1



From: <http://www.fttxtra.com/hfc/docsis/docsis-3-0-tutorial/>

## DOCSIS 3.1

- 10Gb/s Downstream
- 1 Gb/s UpStream
- Orthogonal Frequency Division Multiplexing(OFDM) in the downstream channel
- Orthogonal Frequency Division Multiple Access(OFDMA) in the upstream channel.
- Note: LTE and 802.11 also use OFDM

See: DOCSIS 3.1: scaling broadband cable to Gigabit speeds  
 Belal Hamzeh ; Mehmet Toy ; Yunhui Fu ; James Martin IEEE  
 Communications Magazine  
 Vol: 53 , Issue: 3 , March 2015

# Wireless Networking

## □ Some general problems

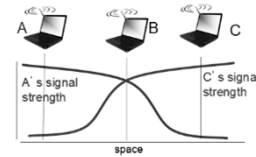
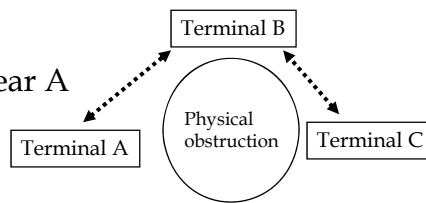
- Noise (likelihood of bit errors)

e.g., BER of 1 in 1000

- Hidden Terminal

(Removes advantage of carrier sensing)

- B Hears A
- B Hears C
- C can not hear A



Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

# Wireless Networking

## (Some problems continued)

### □ Average received signal strength

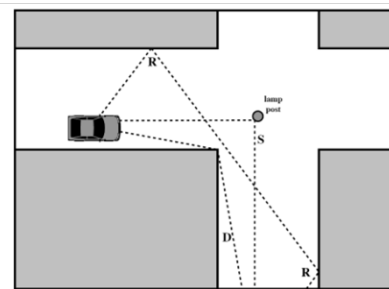
- Falls off with distance between tx and rec
- Is a function of
  - Reflection
  - Diffraction
  - Scattering

### □ Changing received signal strength

→ Signal fading

- Mobility
- Weather

- Interference from other sources: wireless network frequencies shared by many devices (e.g., WiFi, cellular, motors)



Propagation mechanisms → R=Reflection  
S=Scattering  
D=Diffraction

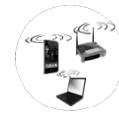
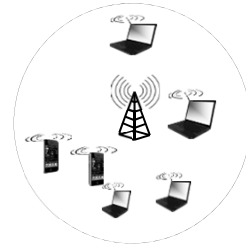


# Wireless link characteristics

*important* differences from wired link ....

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: wireless network frequencies (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
- multipath propagation: radio signal reflects off objects ground, arriving at destination at slightly different times

... make communication across (even a point to point) wireless link much more “difficult”

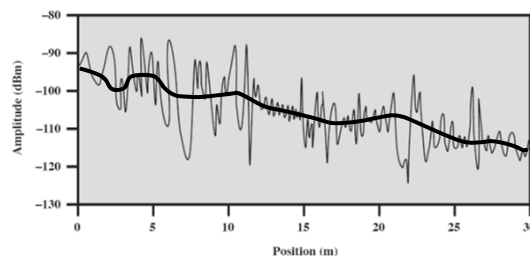


Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 113

# Propagation Effects

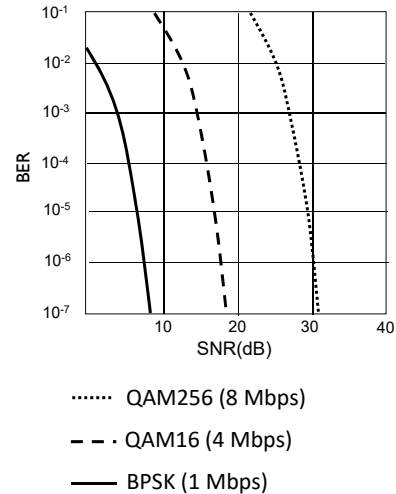
- Signal strength at a distance varies due to Multipath
- Large scale models predicts the average signal strength  
→ Red line
- Small scale (fading) models characterize the short term fluctuations  
→ Black line



Modified from: W. Stallings, Wireless Communications & Networks, Pearson 2005

# Wireless link characteristics

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a “good thing”)
- SNR versus BER tradeoffs
  - *given physical layer*: increase power -> increase SNR->decrease BER
  - *given SNR*: choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



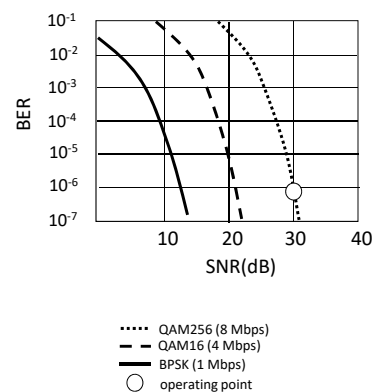
Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 115

# Advanced capabilities

## Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies
  1. SNR decreases, BER increase as node moves away from base station
  2. When BER becomes too high, switch to lower transmission rate but with lower BER



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 116

# Evolution of Wireless IEEE 802.11 LAN Technology

Wi-Fi generations

Generation	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
Wi-Fi 7	802.11be	(2024)	1376 to 46120	2.4/5/6
Wi-Fi 6E	802.11ax	2020	574 to 9608 <sup>[3]</sup>	6 <sup>[4]</sup>
Wi-Fi 6		2019		2.4/5
Wi-Fi 5	802.11ac	2014	433 to 6933	5 <sup>[5]</sup>
Wi-Fi 4	802.11n	2008	72 to 600	2.4/5
(Wi-Fi 3)*	802.11g	2003	6 to 54	2.4
(Wi-Fi 2)*	802.11a	1999	6 to 54	5
(Wi-Fi 1)*	802.11b	1999	1 to 11	2.4
(Wi-Fi 0)*	802.11	1997	1 to 2	2.4

\* (Wi-Fi 0, 1, 2, 3, are unbranded common usage)<sup>[6][7][8][9]</sup>

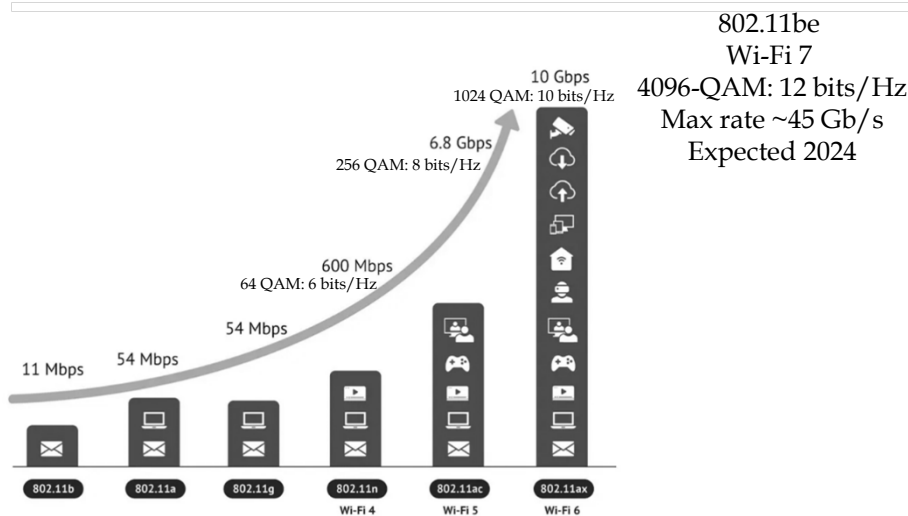
## Wi-Fi Alliance® introduces Wi-Fi CERTIFIED 7™

January 8, 2024

See: <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-7>

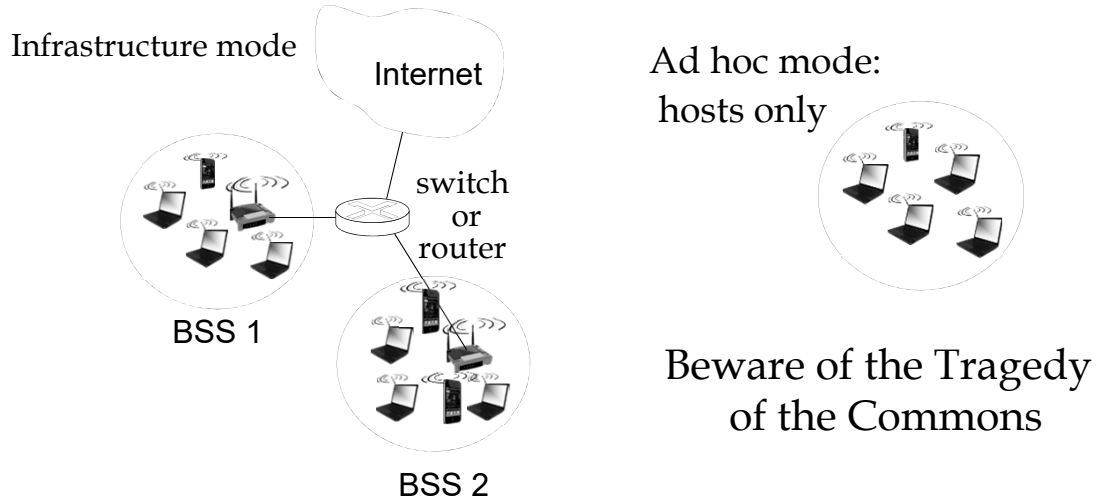
From: <https://en.wikipedia.org/wiki/Wi-Fi>

# Evolution of WiFi



Modified from: <https://www.wevolver.com/article/the-evolution-of-wi-fi-networks-from-ieee-80211-to-wi-fi-6e> MAC

# 802.11 LAN architecture



\* Modified From: Computer Networking, Kurose and Ross, 8<sup>th</sup> Edition, Pearson, 2020

MAC

119

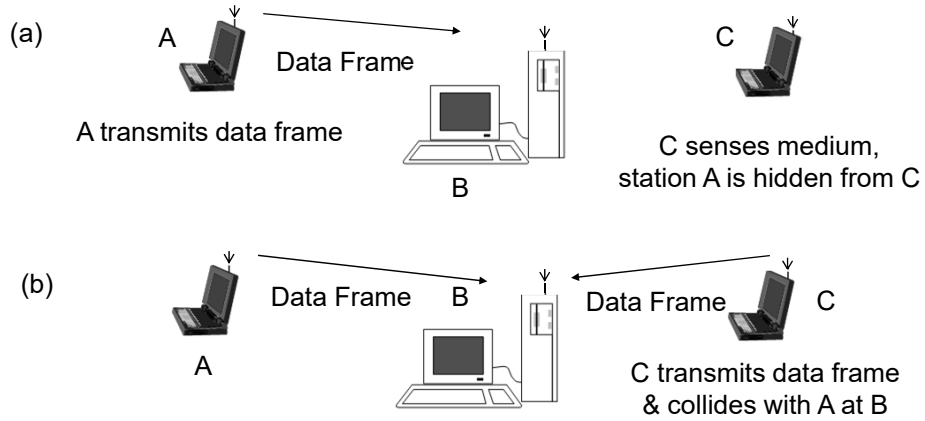
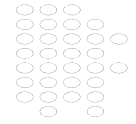
# IEEE 802.11

- MAC- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Sense channel if idle the send → *Request to Send (RTS)* PDU
  - Receiver responds with a → *Clear to Send (CTS)* PDU
  - If receive CTS then all other nodes know the channel is captured and will not send, original sources sends without collision
  - If RTS PDUs collide then use random access backoff algorithm
  - RTS/CTS deals with the hidden terminal problem
- *Access Points (AP)* are the wireless/wired gateways:  
Infrastructure mode
- Ad hoc mode-peer-to-peer

MAC

120

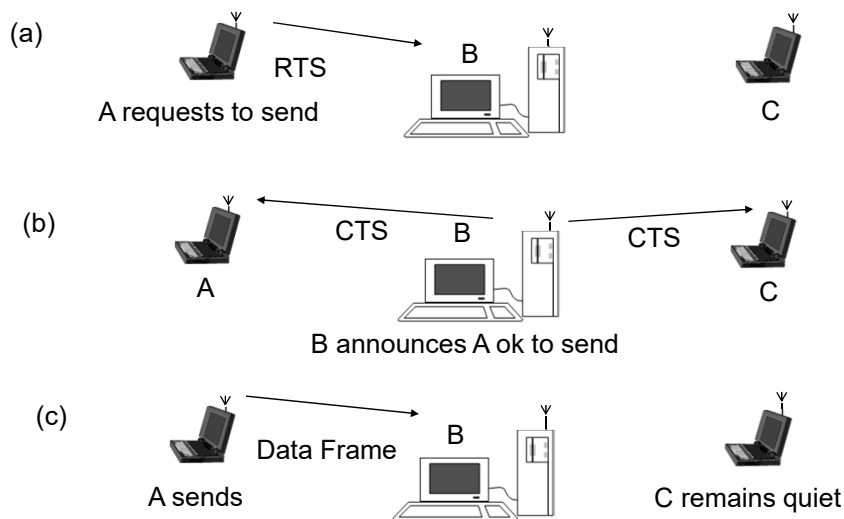
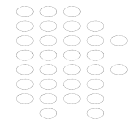
# Hidden Terminal Problem



- New MAC: CSMA with *Collision Avoidance* CSMA/CA

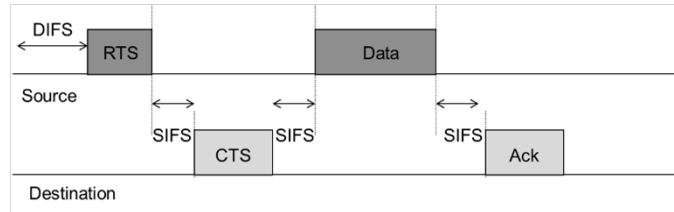
Adapted from: Leon-Garcia & Widjaja: *Communication Networks*

# CSMA with Collision Avoidance



Adapted from: Leon-Garcia & Widjaja: *Communication Networks*

# Transmission with RTS/CTS

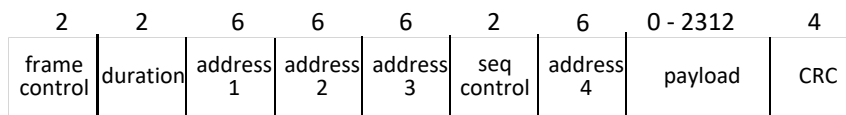


- Distributed Coordination Function (DCF) provides basic access service
  - Asynchronous best-effort data transfer
  - All stations contend for access to medium
- CSMA-CA
  - Ready stations wait for completion of transmission
  - All stations must wait *Interframe Space (IFS)*

DIFS = Distributed Inter-Frame Space. DIFS represents the time interval that a station must wait after the medium becomes idle before it can initiate a transmission.

SIFS = Short Inter-Frame Space time that a station must wait after receiving or transmitting a frame before it can start transmitting its own frame. SIFS is shorter than DIFS

# 802.11 frame: addressing



Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

## 802.11: advanced capabilities

### power management

- node-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 125

## 802.11e

---

- Supplementary to the MAC layer to provide CoS support for LAN applications.
- Applies to 802.11 physical standards a, b and g.
- 802.11e provides some features for differentiating data traffic streams.

# WiFi 6 aka IEEE 802.11ax

- Backwards compatible with 802.11a/b/g/n/ac
- Increase 4X the average throughput per user in high-density scenarios, such as train stations, airports and stadiums.
- Better power management for longer battery life
- Specified for downlink and uplink multi-user operation by means of Orthogonal Frequency Division Multiple Access (OFDMA) technology (and MU-MIMO).
- MU-MIMO
  - MU= Multi-User;
  - MIMO=Multiple Input/Multi Output;
  - MIMO is an antenna technology providing directionality to support multiple Spatial Streams (SS),
  - Spatial streams are a fundamental concept in MIMO technology,

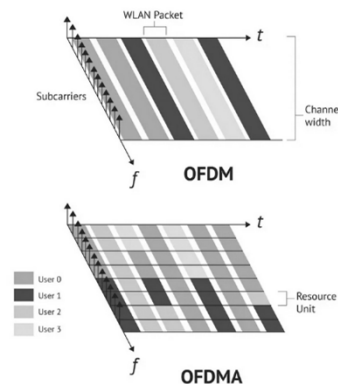
From: <https://www.ni.com/en/solutions/semiconductor/wireless-connectivity-test/introduction-to-802-11ax-high-efficiency-wireless.html>

MAC

127

# WiFi 6 aka IEEE 802.11ax

- Specified for downlink and uplink multi-user operation by means of Orthogonal Frequency Division Multiple Access (OFDMA) technology (and MU-MIMO).
- Previous version of IEEE 802.11 used CSMA/CA, not efficient as rates and number of users increase
- 802.11ax uses OFDMA and schedule-based resource allocation.
  - Like DOCSIS
  - 4G/5G
- Supports the transmission of multiple streams to a single client or multiple clients simultaneously.



Modified from: <https://www.wevolver.com/article/the-evolution-of-wi-fi-networks-from-ieee-80211-to-wi-fi-6e> MAC

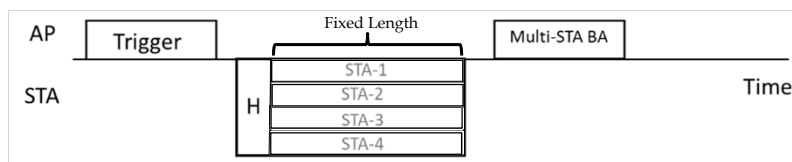
128



# WiFi 6 aka IEEE 802.11ax

## □ Uplink (UL) Procedure

- AP=Access Point
- STA = Station
- Trigger: assigns each station Resource Units (RU's)
- Multi-STA BA = Acknowledge UL transmissions from multiple stations (BA=Block Ack)
- AP initiates UL transmissions by mean of a trigger frame
- H=Header



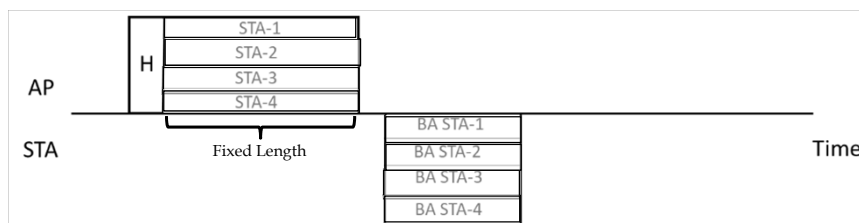
Modified from: IEEE 802.11ax - An Overview, Osama Aboul-Magd, Huawei Technologies, Canada, July 2019

MAC

129

# WiFi 6 aka IEEE 802.11ax

- Downlink (DL) Procedure
- STAs send BA's back to AP
  - BA's include status station status information, e.g., buffer status report (BSR)
  - BSR used by AP to make resource scheduling decisions



Modified from: IEEE 802.11ax - An Overview, Osama Aboul-Magd, Huawei Technologies, Canada, July 2019

MAC

130

## 4G/5G cellular networks

- *the* solution for wide-area mobile Internet
- widespread deployment/use:
- transmission rates up to 100's Mbps
- technical standards: 3rd Generation Partnership Project (3GPP)
  - [www.3gpp.org](http://www.3gpp.org)
  - 4G: Long-Term Evolution (LTE) standard

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

## 4G/5G cellular networks

### *similarities* to wired Internet

- edge/core distinction, but both below to same carrier
- global cellular network: a network of networks
- widespread use of protocols: HTTP, DNS, TCP, UDP, IP, NAT, separation of data/control planes, SDN, Ethernet, tunneling
- interconnected to wired Internet

### *differences* from wired Internet

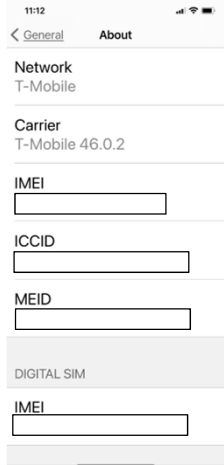
- different wireless link layer
- mobility as a 1<sup>st</sup> class service
- user "identity" (via SIM card)
- business model: users subscribe to a cellular provider
  - strong notion of "home network" versus roaming on visited nets
  - global access, with authentication infrastructure, and inter-carrier settlements

### *differences* from WiFi

- different wireless link layer
- WiFi range ~50m to 100m
- Cellular range ~ 100's of m to few km
- user "identity" (via MAC address)
- business model: owned by local organization, e.g., home or campus

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

# Cellular Networks: Addressing



**Wi-Fi Address**  
B4:56:E3:0E:7A:D1

**Bluetooth**  
B4:56:E3:09:42:31

**Modem Firmware**  
1.80.02

**SEID**

**EID**

**Bluetooth Device Address** - Unique 48-bit address to each Bluetooth device by the manufacturer.

**EID** - Embedded Identity Document. Built-in SIM card identifier in the phone. Allows you to use the services of a mobile operator without the need for an external Sim card.

**IMEI** - International Mobile Equipment Identity number is a unique identification or serial number that all mobile phones and smartphones have.

**ICCID** - Globally unique serial number – a one-of-a-kind signature that identifies the SIM card itself.

**MEID** - Globally unique number identifying a physical piece of CDMA2000 mobile station equipment.

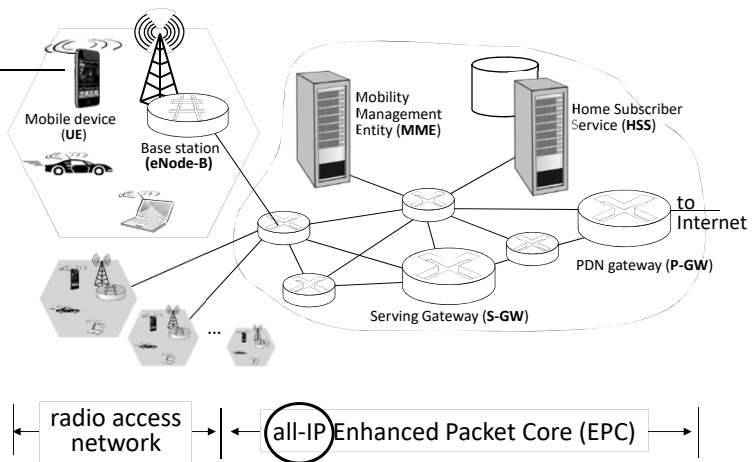
**SEID** - Security Element Identifier is a long identifier of the Security Element chip, which works together with the NFC (Near Field Communication).

**IMSI** - 64-bit International Mobile Subscriber Identity stored on SIM (not commonly displayed to user)

## Elements of 4G LTE architecture

Mobile device:

- smartphone, tablet, laptop, IoT, ... with 4G LTE radio
- 64-bit International Mobile Subscriber Identity (IMSI), stored on SIM (Subscriber Identity Module) card
- IMSI is the primary identifier of a subscriber used for signaling
- LTE jargon: User Equipment (UE)

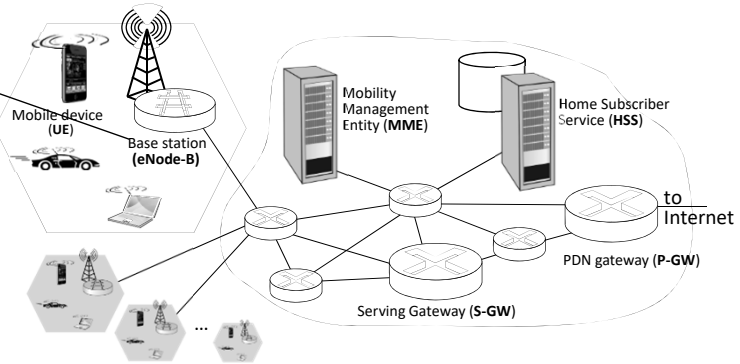


Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

# Elements of 4G LTE architecture

## Base station:

- at “edge” of carrier’s network
- manages wireless radio resources, mobile devices in its coverage area (“cell”)
- coordinates device authentication with other elements
- similar to WiFi AP but:
  - active role in user mobility
  - coordinates with nearby base stations to optimize radio use
- LTE jargon: eNode-B

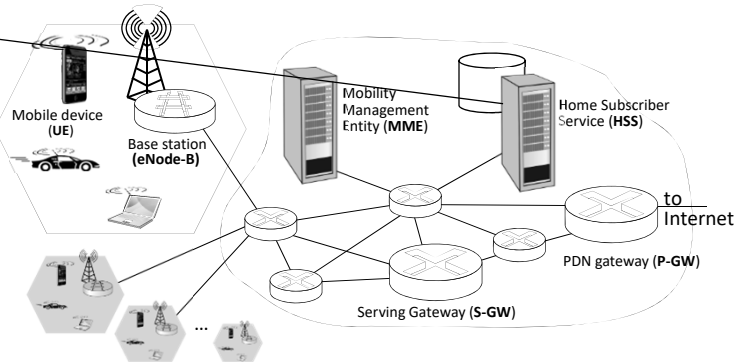


Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

# Elements of 4G LTE architecture

## Home Subscriber Service

- stores info about mobile devices for which the HSS’s network is their “home network”
- works with MME in device authentication

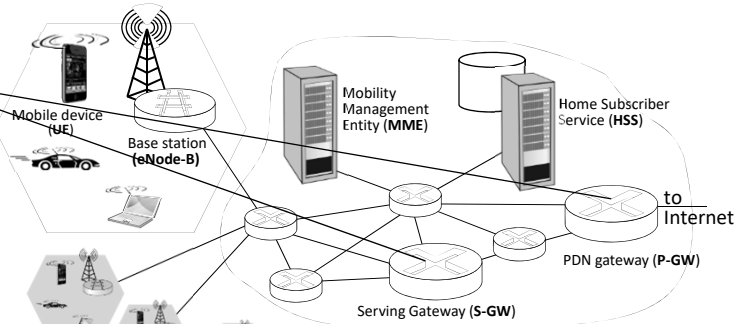


Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

# Elements of 4G LTE architecture

## Serving Gateway (S-GW), PDN Gateway (P-GW)

- lie on data path from mobile to/from Internet
- S-GW
  - responsible for routing data packets between the UE and the P-GW
- P-GW
  - gateway to mobile cellular network
  - Looks like any other internet gateway router
  - provides NAT services
- other routers:
  - extensive use of tunneling



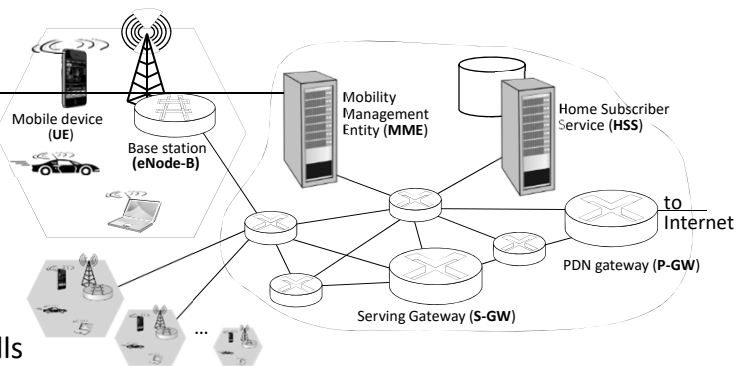
Servicing Gateway = S-GW  
Packet Data Network Gateway = P-GW

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

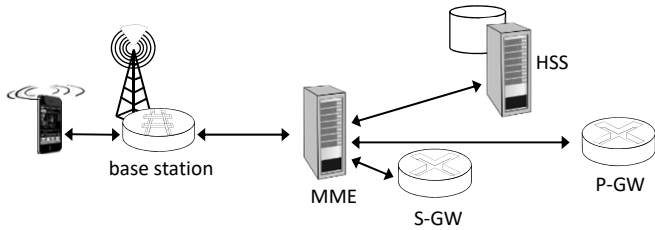
# Elements of 4G LTE architecture

## Mobility Management Entity

- device authentication (device-to-network, network-to-device) coordinated with mobile home network HSS
- mobile device management:
  - device handover between cells
  - tracking/paging device location
- path (tunneling) setup from mobile device to P-GW

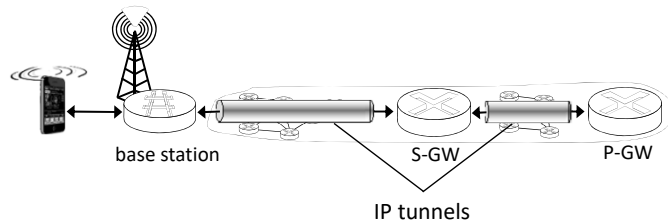


# LTE: data plane/control plane separation



## control plane

- new protocols for mobility management , security, authentication (later)

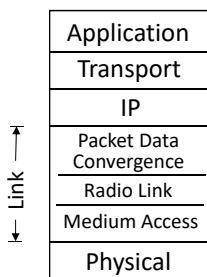


## data plane

- new protocols at link, physical layers
- extensive use of tunneling to facilitate mobility

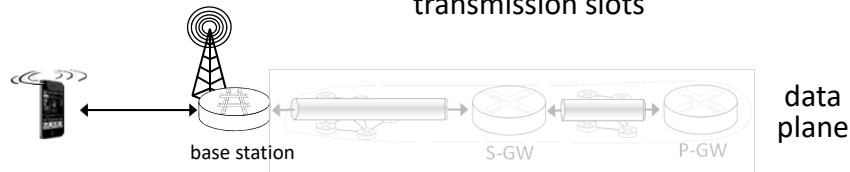
Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

# LTE data plane protocol stack: first hop



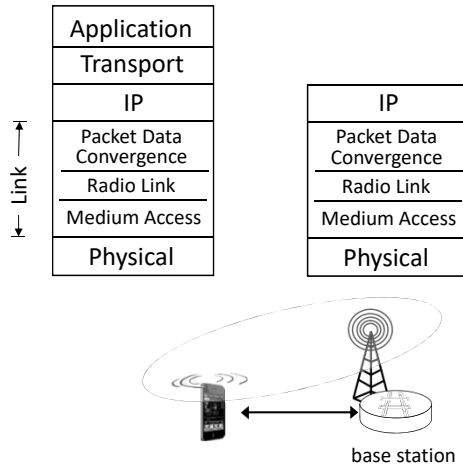
## LTE link layer protocols:

- Packet Data Convergence: header compression, encryption
- Radio Link Control (RLC) Protocol: fragmentation/reassembly, reliable data transfer
- Medium Access: requesting, use of radio transmission slots



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

## LTE data plane protocol stack: first hop



### LTE radio access network:

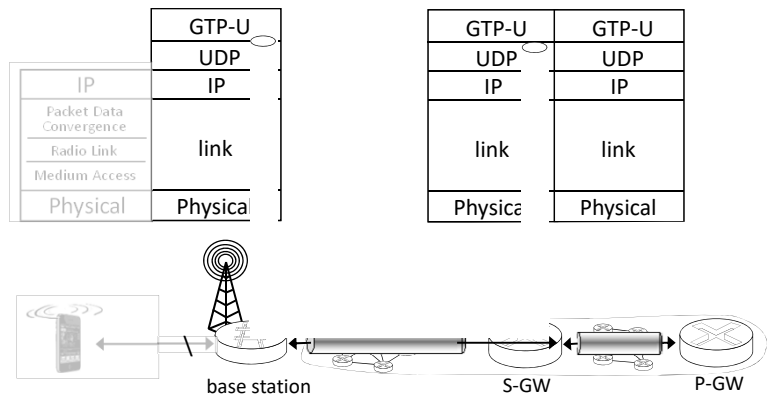
- downstream channel: FDM, TDM within frequency channel (OFDM - orthogonal frequency division multiplexing)
  - upstream: FDM, TDM similar to OFDM
- each active mobile device allocated two or more 0.5 ms time slots over 12 frequencies
  - scheduling algorithm not standardized – up to operator
  - 100's Mbps per device possible

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

## Some advanced mechanisms

- Adaptive Modulation and Coding (AMC)
  - Dynamically adjusts the modulation scheme and coding rate of transmitted data based on the channel conditions.
  - Using feedback the observed signal-to-noise ratio (SNR), an appropriate modulation scheme and coding rate is selected.
- Hybrid Automatic Repeat Request (HARQ)
  - If the receiver detects errors in the received packet, it sends a NACK message to the transmitter, requesting the retransmission of the packet.
  - The receiver stores the erroneous packets and waits for the retransmission. Once the retransmission arrives, the receiver combines the previously stored and newly received packets to recover the original data.
  - More on ARQ later

# LTE data plane protocol stack: packet core



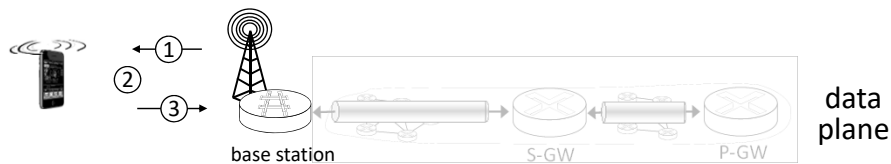
## tunneling:

- mobile datagram encapsulated using GPRS Tunneling Protocol (GTP), sent inside UDP datagram to S-GW
- S-GW re-tunnels datagrams to P-GW
- supporting mobility: only tunneling endpoints change when mobile user moves

- GPRS= General Packet Radio Service
- GPRS Tunneling Protocol-User plane =GTP-U

Wireless and Mobile Networks: 7- 143

# LTE data plane: associating with a BS



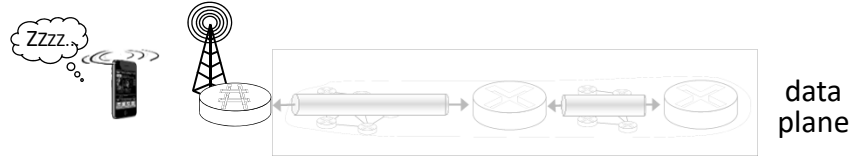
- ① BS broadcasts primary synch signal every 5 ms on all frequencies
  - BSs from multiple carriers may be broadcasting synch signals
- ② mobile finds a primary synch signal, then locates 2<sup>nd</sup> synch signal on this freq.
  - mobile then finds info broadcast by BS: channel bandwidth, configurations; BS's cellular carrier info
  - mobile may get info from multiple base stations, multiple cellular networks
- ③ mobile selects which BS to associate with (*e.g.*, preference for home carrier)
- ④ more steps still needed to authenticate, establish state, set up data plane

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 144



# LTE mobiles: sleep modes



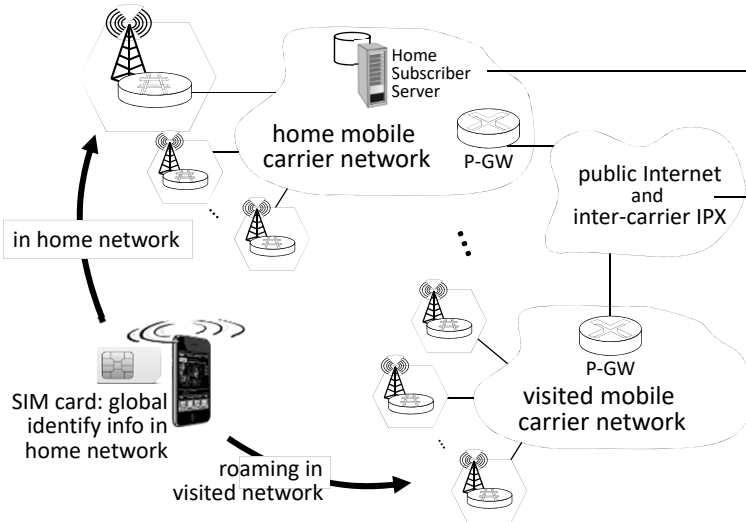
as in WiFi, Bluetooth: LTE mobile may put radio to “sleep” to conserve battery:

- light sleep: after 100’s msec of inactivity
  - wake up periodically (100’s msec) to check for downstream transmissions
- deep sleep: after 5-10 secs of inactivity
  - mobile may change cells while deep sleeping – need to re-establish association

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 145

# Global cellular network: a network of IP networks



home network HSS:

- identify & services info, while in home network and roaming

all IP:

- carriers interconnect with each other, and public internet at exchange points
- legacy 2G, 3G: not all IP, handled otherwise

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 146

## On to 5G!

- goal: 10x increase in peak bitrate, 10x decrease in latency, 100x increase in traffic capacity over 4G
- 5G NR (new radio):
  - two frequency bands: FR1 (450 MHz–6 GHz) and FR2 (24 GHz–52 GHz): millimeter wave frequencies
  - not backwards-compatible with 4G
  - MIMO: multiple directional antennae
- millimeter wave frequencies: much higher data rates, but over shorter distances
  - pico-cells: cells diameters: 10-100 m
  - massive, dense deployment of new base stations required

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 147

## Mobility

---

### □ Handoff

- In cellular networks, handoff (aka handover) is the process of transferring an ongoing call or data session from one base station (cell) to another, as the user moves out of range of the current base station and into the coverage area of another.
- Handoff enables uninterrupted communication and data transfer while the user is on the move. Without handoff, calls or data sessions would be dropped whenever a user moves out of range of the current cell.
- The mobile device continuously monitors the signal strength and quality of neighboring cells, and when the signal from a neighboring cell is stronger than the current cell, the mobile device initiates a handoff to the neighboring cell. The handoff process involves signaling between the mobile device, the current base station, and the target base station, to transfer the call or data session seamlessly from one cell to another.
- Handoff process should be fast and seamless to avoid dropping the call or data session.

# Mobility

---

- Visiting “other” networks
- A person want to talk to you but you are not “home”
- The person is called the “correspondent” knows your home address, e.g., your IP address
- “Home” means your home network

## Mobility approaches

- let network (routers) handle it:
  - routers advertise well-known name, address (e.g., permanent 32-bit IP address), or number (e.g., cell #) of visiting mobile node via usual routing table exchange
  - Internet routing could do this already *with no* changes! Routing tables indicate where each mobile located via longest prefix match!

## Mobility approaches

- let network (routers) handle it:
  - routers advertise well-known address (e.g., permanent 32-bit IP address), or number (not scalable to billions of mobiles) of visiting mobile node via usual routing table exchange
  - Internet routing could do this *with no changes!* Routing tables indicate where each mobile located via longest prefix match!
- let end-systems handle it: functionality at the “edge”
  - *indirect routing*: communication from correspondent to mobile goes through home network, then forwarded to remote mobile
  - *direct routing*: correspondent gets foreign address of mobile, send directly to mobile

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 151

## Contacting a mobile friend:

Consider friend frequently changing locations, how do you find him/her?

- search all phone books?
- expect her to let you know where he/she is?

- call the parents?
- Facebook!

The importance of having a “home”:

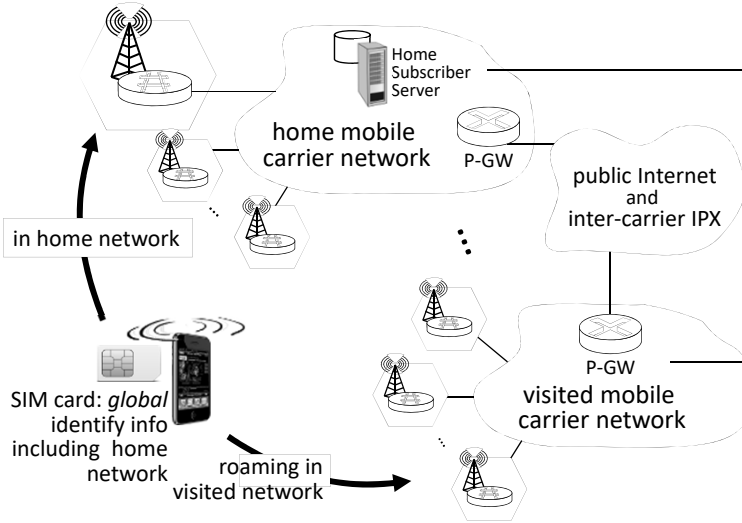
- a definitive source of information about you
- a place where people can find out where you are



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 152

# Home network, visited network: 4G/5G



## home network:

- (paid) service plan with cellular provider, e.g., Verizon, Orange
- home network HSS stores identify & services info

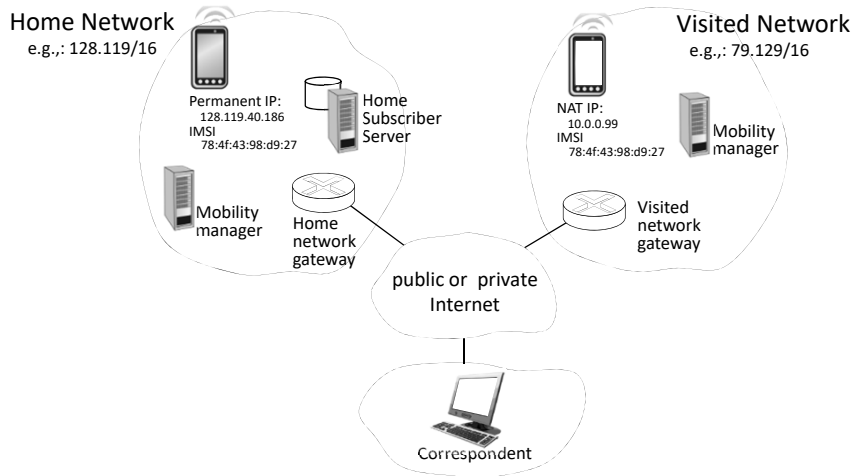
## visited network:

- any network other than your home network
- service agreement with other networks: to provide access to visiting mobile

Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 153

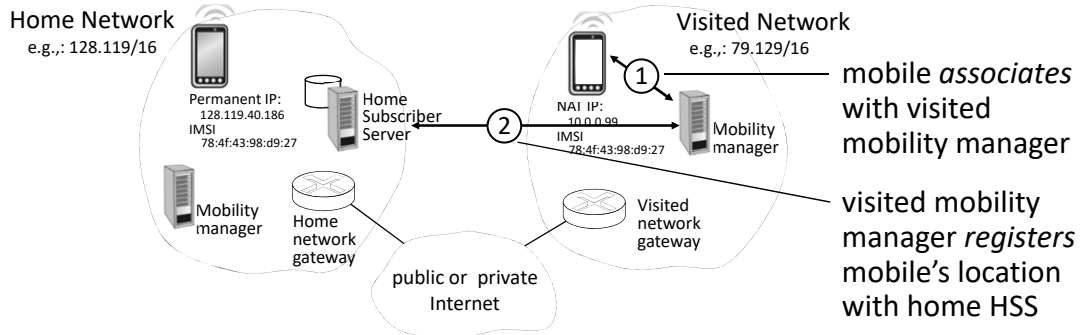
# Home network, visited network: generic



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 154

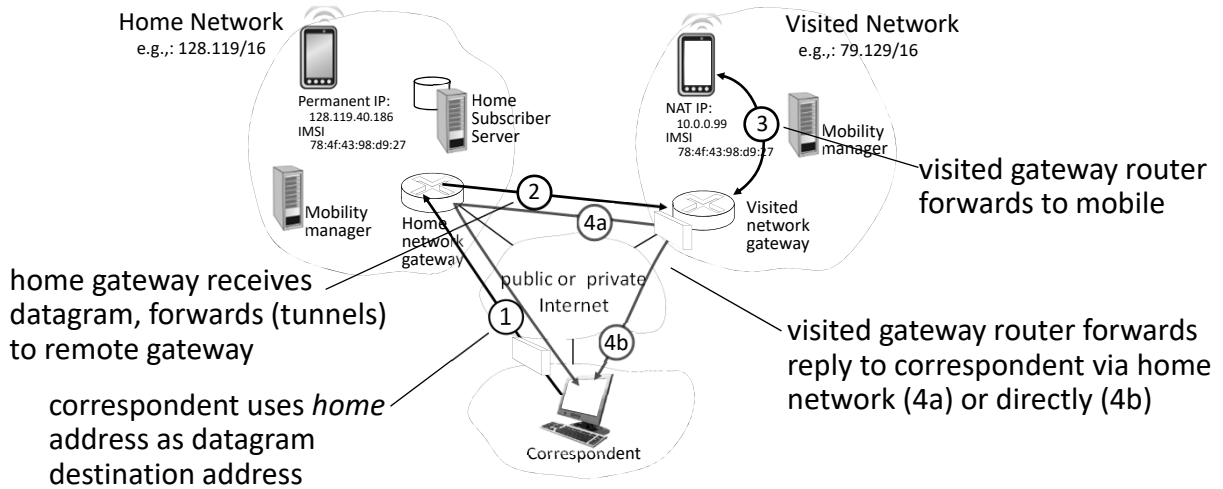
# Registration: home needs to know where you are!



end result:

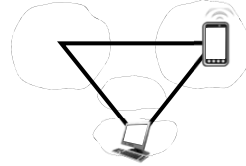
- visited mobility manager knows about mobile
- home HSS knows location of mobile

# Mobility with indirect routing



## Mobility with indirect routing: comments

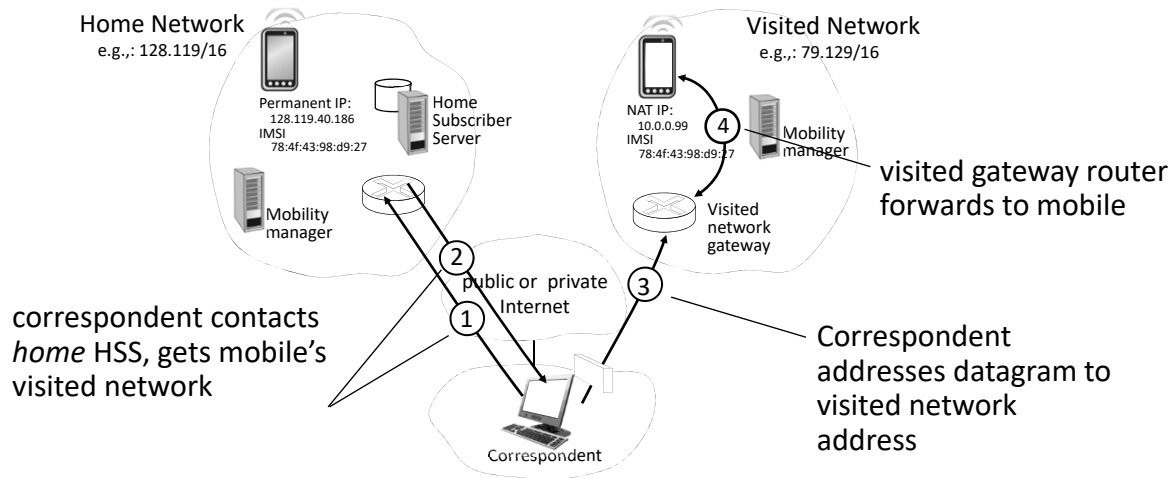
- triangle routing:
  - inefficient when correspondent and mobile are in same network
- mobile moves among visited networks: transparent to correspondent!
  - registers in new visited network
  - new visited network registers with home HSS
  - datagrams continue to be forwarded from home network to mobile in new network
  - *on-going (e.g., TCP) connections between correspondent and mobile may be maintained, however, the time to setup the new path may result in TCP timeouts*



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 157

## Mobility with direct routing



Modified from: 8<sup>th</sup> edition Jim Kurose, Keith Ross Pearson, 2020

Wireless and Mobile Networks: 7- 158

## Mobility with direct routing: comments

- overcomes triangle routing inefficiencies
- *non-transparent to correspondent*: correspondent must get care-of-address from home agent
- what if mobile changes visited network?
  - can be handled, but with additional complexity

## Wireless, mobility: impact on higher layer protocols

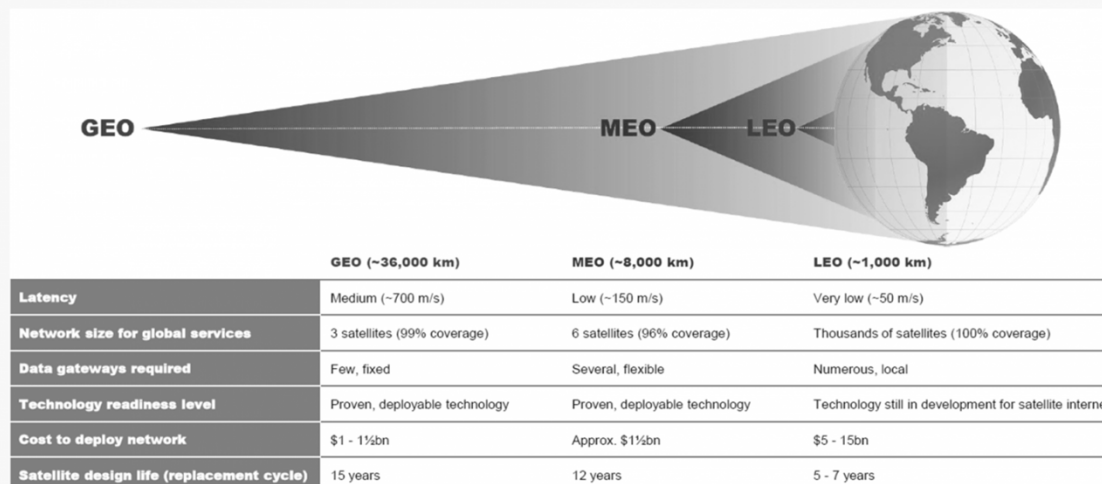
- logically, impact *should* be minimal ...
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- ... but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handover loss
  - TCP interprets loss as congestion, will decrease congestion window unnecessarily
  - delay impairments for real-time traffic
  - bandwidth a scarce resource for wireless links



# Satellite Networks: GEO, MEO, LEO

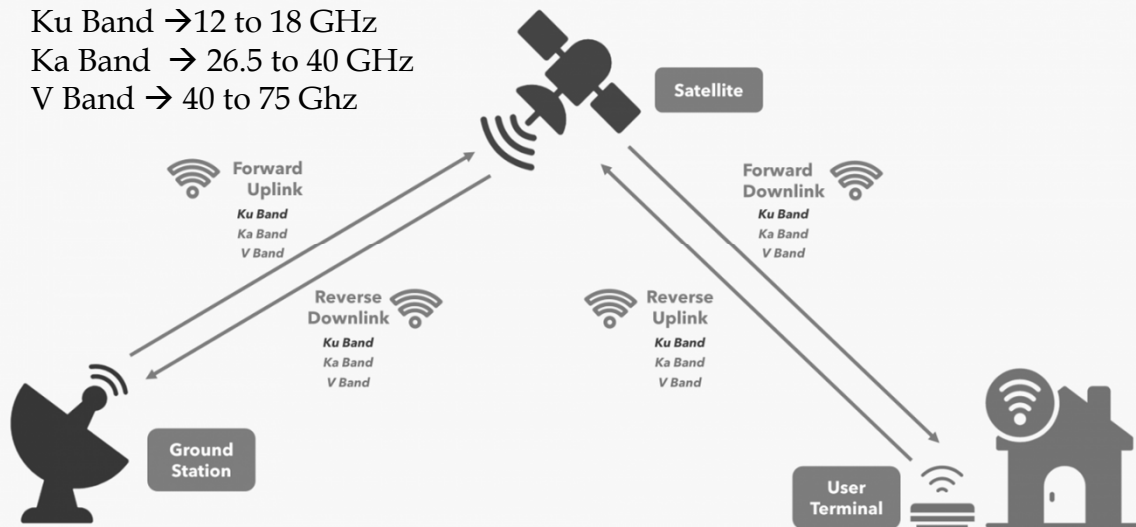
- Geostationary earth orbit
- 37,700 km
- Power--> increased cost
- Propagation delay
- Limited orbital slots ~ 180
  - Properties
    - > Large delay ~ 270 ms (Geosynchronous)
    - > Up and down links are on different frequencies (full duplex)
  - CSMA/CD will not work because of long delay
  - Token networks are not applicable because of long delays, e.g., 100 nodes will have a 27 sec. token return time.
- Medium earth orbit
- 5,000 - 15,000 km
- Period ~ 4-9 hours
- Fewer satellites
- Low earth orbit
- Below 2000 km
- Periods up to 2 hours
- More satellites
- Cheaper to launch

## GEO, MEO and LEO Satellites



## How Does Starlink Work?

Ku Band → 12 to 18 GHz  
Ka Band → 26.5 to 40 GHz  
V Band → 40 to 75 GHz



3

## Example: Starlink

- Video from Mark Handley
- “The early SpaceX Starlink satellites lack inter-satellite links planned for later versions. Can they still provide low latency wide-area communications? In this video I look at what might be possible using ground relays to hop from satellite to satellite around the world.”
- <https://www.youtube.com/watch?v=m05abdGSOxY>

## Other LAN technologies

---

- Bluetooth
- Passive Optical Networks
- Sensor networks
- Ad-hoc networks