Lecture 4 - Medium Access Control

Computer Communication Networks
CS35201 - (001/ 002)
Fall 2022

Kent State University

Department of Computer Science
Betis Baheri
bbaheri@kent.edu

October 10, 2022

Outline I

Channel Allocation Problem

How to divide bandwidth among contending access points?

1. Static Channel Allocation
   - Divides the medium bandwidth among stations statically
     - Time-Division Multiple Access(TDMA)
     - Frequency Division Multiple Access(FDMA)
     - Wave Division Multiple Access(WDMA)
     - Code Division Multiple Access(CDMA)
2. Dynamic Channel Allocation
   - Divides the medium bandwidth among stations dynamically
   - Depends on many factors
   1. Station model ⇒ how many and how much traffic each generates
      - Single/multi channel
      - Collision Assumption ⇒ Concurrent transmissions result in collision
   2. Timing
      - Continuous Time ⇒ Asynchronous transmission
      - Slotted Time ⇒ Synchronous transmission
   3. Sensing ⇒ listening
      - Carrier Sense ⇒ monitor the carrier (medium) for transmission
      - No Carrier Sense

Static Channel Allocation

- N users share the same channel using:
  - Frequency Division Multiplexing (FDM)
  - Time-Division Multiplexing (TDM)
- There is no interference, each user has a private sub-channel $\uparrow$
- It is good for fixed and small number of users
- Large population, bursty traffic, or varying traffic cause problems $\downarrow$
  - Wasting bandwidth (by silent terminals)
  - In most computer systems, data traffic is extremely bursty
  - Most of the channels will be idle most of the time

Dynamic Channel Allocation

- To avoid collisions, dynamic techniques can be used with the following assumptions

1. Station traffic Model ⇒ independent users
    - N independent stations each generates frames
2. Single channel assumption
    - All stations can transmit and receive from one channel
    - All stations are treated equally, although priority could be given to certain stations
3. Collision assumption
    - If two frames are transmitted simultaneously, they overlap in time ⇒ collision
    - The stations can detect collisions

Dynamic Channel Allocation

4. Timing assumption
   - Continuous time in which frames are transmitted at any given time, with no synchronization or a master clock
   - Slotted time in which time is divided into discrete interval (slots) and frames are transmitted at the beginning of each slot
5. Sensing
   - Carrier sense: stations can tell if he channel is in use. If the channel is sensed busy no station attempts to transmit
   - No carrier sense: stations cannot sense the channel

Multiple Access Protocols

Who gets to use the channel next?

1. Fixed/Static assignment
2. Demand assignment $\Rightarrow$ Reservation
3. Contention
4. Turn-Based

Outline I

Contention-Oriented MAC Protocols

- No coordination between hosts
- Control is completely distributed
- Outcome is probabilistic $\Rightarrow$ success or collision
- Examples: ALOHA, CSMA, CSMA/CD (Ethernet)

Advantages

- Short delay for bursty traffic $\Rightarrow$ no wait for access
- Simple (due to distributed control)
- Flexible to fluctuations in the number of hosts
- Fairness
    - Everyone has the same chance to transmit

Contention-Oriented MAC Protocols

Disasdvantages

- Access uncertainty $\Rightarrow$ probabilistic success
  - Not be certain who will acquire the media/channel
- Low channel efficiency with a large number of hosts
  - More collisions
- Not good for continuous (streaming, e.g., voice) traffic
  - Unpredictable delay due to probabilistic success
- Cannot support priority traffic
- High variance in transmission delay
  - Some frame may wait for a long time to acquire the channel

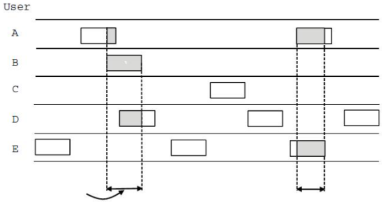
Contention Access Methods

1. ALOHA
    - Pure ALOHA
    - Slotted ALOHA
2. Carrier Sense Multiple Access (CSMA)
    - 1-Persistent CSMA
    - Non-Persistent CSMA
    - p-Persistent CSMA
3. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
    - Etherent $\Rightarrow$ 802.3
4. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
    - WiFi $\Rightarrow$ 802.11
5. Carrier Sense Multiple Access with Collision Elimination (CSMA/CE)

Aloha Protocols

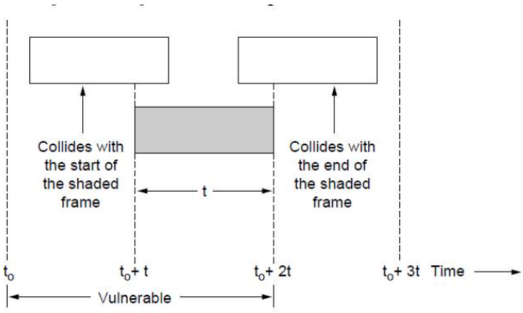
- It was developed in 1970's at the UN. of Hawaii to solve channel allocation problem
- It was based on ground-based radio broadcasting.
- It can be used for any system with shared channel
- Since 1970, several protocols have been proposed
  - Early algorithms were based on Puse ALOHA with $1/2e$ (18%) throughput
  - Later algorithms were based on Slotted ALOHA with $1/e$ (38%) thorughput

Pure Aloha (Un-slotted)



- Random transmission at arbitrary time
- No coordination among stations
- Collision happens if at least one bit overlaps
- Will be detected and after a round trip delay
  - Feed-back ⇒ stations hear their own transmission
  - The checksum cannot distinguish between a total loss and a near miss
  - Very short in LANs but 270 ms in satellite channels
- After each collision, the sender backs off for a random amount of time and then tries again

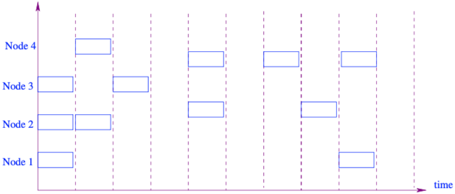
Pure Aloha (Un-slotted)



- Vulnerable period for the shaded frame

Slotted Aloha

- Assumptions
  1. Fixed size frames
  2. Time is divided into equal size slots, each frame fits into one slot
  3. Nodes start to transmit frames only at beginning of slots
  4. Nodes are synchronized
  5. All nodes detect collision when two or more nodes transmit during a slot time



- Collision probability is reduced
- Collisions happen only at the beginning of a time slot
- What is the chance that at least two stations contend at a begining of a lost 1−no station attempts - one station attempts $= 1 - (1-p)^N - p(1-p)^{N-1}$

  P: is probability of an attempt by a station

Slotted ALOHA

Operation

- When a node obtains fresh frame, it transmits in next slot
- If no collision, the node can send new frame in next slot
- If collision, node retransmits frame in each subsequent slot with probability p until success

Pros:

- Single active node can continuously transmit at full rate of channel
- Highly decentralized
  - Only slots in nodes need to be in synchronized, not bits
- Simple to implement

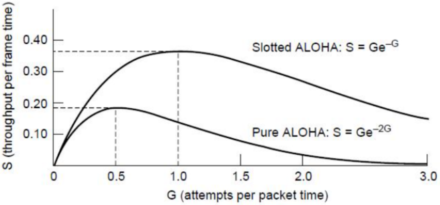
Cons:

- Collisions $\Rightarrow$ wasting time slots
- Also wastes due to idle slots $\Rightarrow$ no one transmits $\Leftarrow$ due to back off
- Nodes may be able to detect collision in less $\tau \Leftarrow$ small distance between
  - τ = transmission time + propagation time
- Clock synchronization is needed

Slotted ALOHA
What is the efficiency of S-ALOHA?

- Similar to pure Aloha

$$Efficiency = \frac{1}{e} \approx 0.38$$

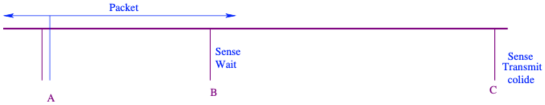


Throughput versus offered traffic for ALOHA systems

Outline I

Carrier Sense Multiple Access (CSMA)

- We can achieve a better throughput if we can listen to the channel before transmitting a packet and avoid collisions *How?*



- For that we make some assumptions

1. Constant length packets ⇒ Each fits into a time slot
2. No errors, except those caused by collisions
3. No capture effect
   - A station holds the channel for a long time white others starving
4. Each station can sense traffic transmission of others
5. The propagation delay is small compared to the transmission delay

$$\Rightarrow \frac{T_p}{T_f} \ll 1$$

Types of CSMA

Algorithm 1: 1-Persistent CSMA

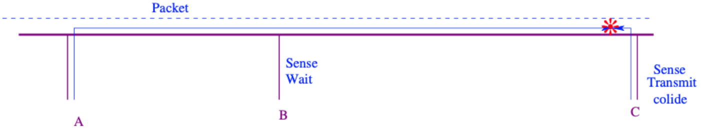
```
repeat
    Sense the channel;
    if the channel is idle then
        transmit immediately ;                                  // with probability 1
    else
        delay transmission, but keep sensing (step 2)
    end
until Transmission completed;
```

Algorithm 2: Non-Persistent CSMA

```
repeat
    Sense the channel;
    if the channel is idle then
        transmit immediately ;                                  // with probability 1
    else
        wait a random amount and then sense again (step 2) ;    // can save energy
    end
    if Collision occurs then
        wait a random amount and then sense again (step 2)
    end
until Transmission completed;
```

Tradeoff between 1- and Non- Persistent CSMA

- If B and C become ready in the middle of A's transmission,
  - 1-Persistent: B and C collide *Why?*
  - Non-Persistent: B and C probably do not collide *Why?*
- If only B becomes ready in the middle of A's transmission,
  - 1-Persistent: B succeeds as soon as A ends
  - Non-Persistent: B may have to wait *How?*



- CSMA Collision
  - Despite sensing, two nodes may not hear each other's transmission
  - Collision cause wasting the entire transmission time
  - Distance and transmission delay directly affect collision probability
- Collision Detection Time
  - How long does it take to realize there has been a collision?
    - Worst case: 2 $\times$ end-to-end delay $=2T_p + T_f$ *Why?*

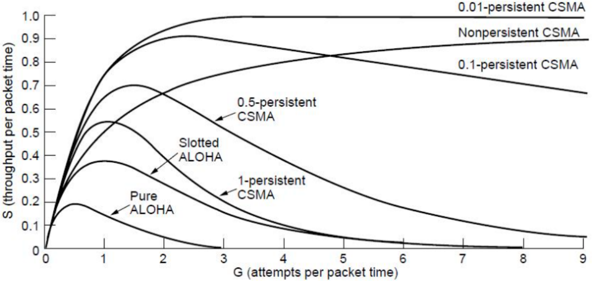
p-Persistent CSMA

- An optimal strategy $\Rightarrow$ attempting with probability p
  - p could be fixed or variable
- Assumptions
  - Channels are slotted
  - One slot = contention period (i.e., one round trip propagation delay)

Algorithm 3: p-Persistent CSMA

```
1  repeat
2      Sense the channel;
3      if the channel is idle then
4          transmit the packet with probability p, otherwise wait one slot and then goto 2;
5          if successful transmission then goto 2;
6          ;
7          else if collision then
8              wait for a random amount of time and then goto 2
9          else
10             wait one slot and then goto 2
11         end
12     else if the channel is busy then
13         wait one slot and then goto 2
14     end
15 until Transmission completed;
```

Comparing Contention-oriented Protocols



Comparison of the channel utilization versus load for various random access protocols

Question 4.1

Can we conclude that that p-persistent protocols are really good as $p \longrightarrow 0$?

Answer: *Not really, the delay approaches* ∞

CSMA/CD
Ethernet

1. CSMA protocols
   - When two stations begin transmitting at the same time, each will transmit its complete packet,
   - This wastes the channel for an entire packet time
2. CSMA/CD protocols
   - Transmission is terminated immediately upon the detection of a collision

How to Detect Collisions

- Easy in wired LANS
  - Measure and compare signal strengths can send/receive at the same time
    - Transmitted
    - Received
  - Difficult in wireless LANs   Either sends or receives at the same time
    - Receivee shuts off while transmitting

$\Rightarrow$ Carrier sensing + collision detection (terminating transmission) allow faster access to the channel and hence better throughput than %38 of S-Aloha

Question 4.2

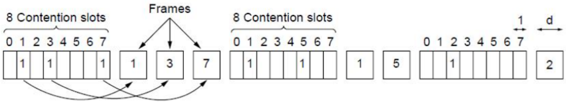
How long should the contention period be?

Answer: *The minimum time to detect a collision is* $2T_p - \epsilon$

Outline I

Collision-Free Protocols
Basic-Bit Map

- Interleaved scheduling and transmission periods
  - Reservation followed by a transmission period
- Contention is moved from data packets to control packets
- The contention period is divided into mini-slots, 1 bit-wide each
- A host attempting to transmit sets its contention slot equal to 1
- The Basic Bit Map

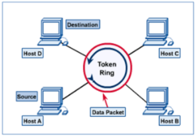


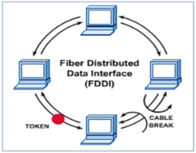
Problems

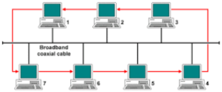
- Scalability:
  - Large large number of hosts $\Rightarrow$ long contention period $\Rightarrow$ leading to inefficiency
- Is it Fair?

Token Passing

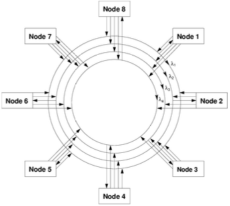
- Stations form a logical ring ⇒ single, double, triple, etc.
- Each station knows the identity of its preceding and following stations
- A control packet known as the token provides the right of access
- The protocol consists of alternating data transmission and token passing phases
- This protocol requires considerable maintenance







IEEE 802.4



WDM

Comparison

Contention-oriented vs. Contention-free Protocols

1. Contention protocols are good when:
   - Traffic load is light ⇒ $\rho = \frac{\lambda}{\mu} \ll 1$
     - λ : arrival rate μ : departure rate rate ρ : traffic load
   - A station can immediately transmit a frame
   - Can recover fast from a collision or failure
2. Collision-free systems are good when:
   - Traffic load is relatively high ⇒ $0.5 \leq \rho = \frac{\lambda}{\mu} < 1$
   - A station can get the channel explicitly before transmission
   - A lot of work can be done to avoid collisions ⇒ scheduling/resrevation

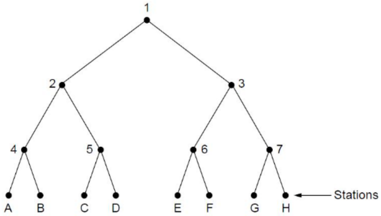
- What is needed is a contention strategy during light loads, and collision-free strategy during rush hours   *How?*
  - Dynamically regulate the number of competing stations during a contention period

Limited Contention Protocols

- If there is a collision during the k^{th} slot, then
  - Divide the contenders into two groups
- The first group gets to try it again during the next slot $(k+1)$
  - If no collisions occur then, the second group gets a try during the slot after that $(k+2)$
  - Otherwise, the first group is split up again
- With a lot of traffic, the strategy reduces to the bit-map protocol *How?*

Adaptive Tree Protocol

- Stations are organized as leaves of a binary tree
- All stations are allowed to attempt on slot 1.
- If there is a collision during this time slot, only stations belonging to left sub-tree are allowed to compete for next time slot.
- In general the tree is searched in depth first fashion, to locate all ready stations



- During slot 0, all stations can try to transmit
- If a collision occurs, in slot 1 only nodes falling under node 2 may compete

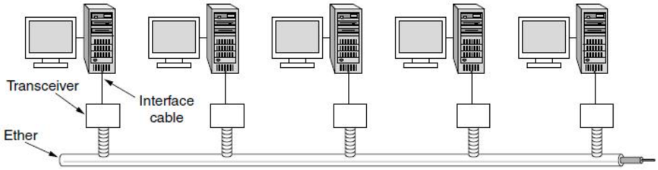
Ethernet

- Near implementation of the IEEE 802.3 protocol
- CSMA/CD based
  - Ethernet format

Bytes	8		6	6	2	0-1500	0-46	4
(a)	Preamble		Destination address	Source address	Type	Data	Pad	Check-sum
(b)	Preamble	SoF	Destination address	Source address	Length	Data	Pad	Check-sum

  - 802.3 format
    - Preamble: Seven 10101010 used to synchronize For synchronization
    - SoF (start of the frame) to tell that the real info is now coming
    - Address: Generally 48-bit fields. Leftmost bit indicates ordinary or group addresses (multicast / broadcast). Second bit indicates global or local address
    - Length: Ranges from 0-1500. Frames should always be at least 64 bytes useful for collision detection
    - Pad: used to fill out the frame to the minimum size
    - Checksum: Calculated over the data field. CRC-based Paolo Costa 04 - MAC Sub-layer

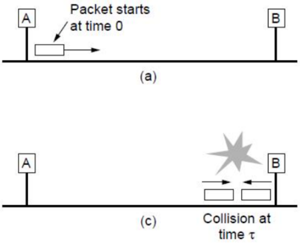
Architecture of classic Ethernet



Name	Cable	Max. dist.	Nodes/Seg.
10Base5	Thick coax	500 m	100
10Base2	Thin coax	200 m	30
10Base-T	Twisted pair	100 m	1024
10Base-F	Fiber optics	2000 m	1024

Collision Detection

Collision detection can take as long as $2\tau = 2T_p$



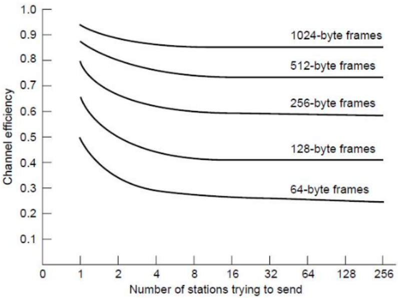
Exponential Backoff distributed

1. After the first collision, each station waits either 0 or 1 slot times before trying again
2. After i collisions, each station waits a random number between 0 and $2^i - 1$ slot times

- It dynamically adapts to the number of stations trying to send

Ethernet Performance

- Efficiency of Ethernet at 10 Mbps with 512-bit slot times

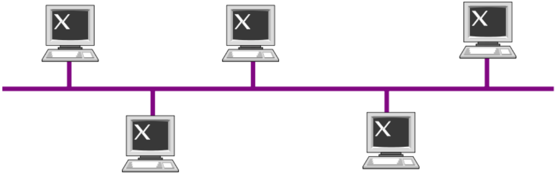


- Throughput degraded faster
- Problem:
  - As more stations are added, traffic will go up, and so will the possibility of collisions
    - The network will saturate
- Solution:
  - Divide the network into separate sub-LANs and connect them through a switch
  - Each has its own collision domain

Ethernet Evolution

History: Initial Idea

- Shared media
- CSMA/CD MAC
- Half duplex
- Low latency $\Rightarrow$ no networking node (distributed control)
- One collision domain



10 Mbps shared bus

Fast Ethernet

- 100 Mbps
- Data formats, interfaces, and protocols are all the same

Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps (Cat 5 UTP)
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

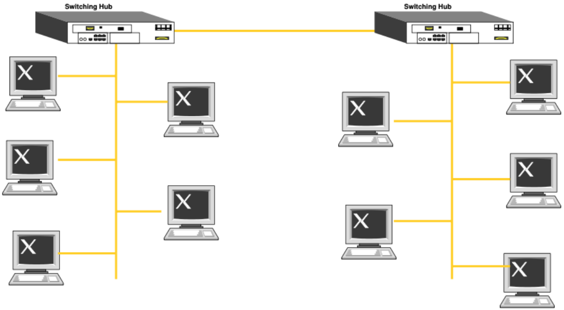
The original fast Ethernet cabling

Multi-port Repeater

- Demand for structured cabling
  - Voice grade twisted pair
  - 10BaseT (Cat3, cat4, ...)
- Multiport repeater (hub) created
- Still one collision domain
- CSMA/CD in a box

Ethernet Bridging

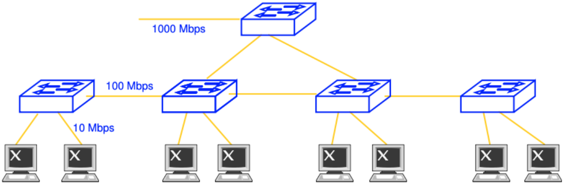
- Store and forward according to destination MAC address
  - Learning bridges
- Separated collision domains
- Improved network performance *Why?*
- Still one broadcast domain *Why?*



Three collision domains

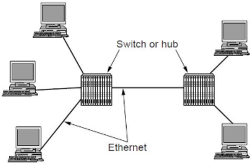
Ethernet Switches

- Switch = Multiport bridge with hardware acceleration
- Full duplex $\Rightarrow$ collision-free Ethernet $\Rightarrow$ No CSMA/CD
- Different data rates



Collision-free plug&play scalable Ethernet

Gigabit Ethernet



A two-station Ethernet

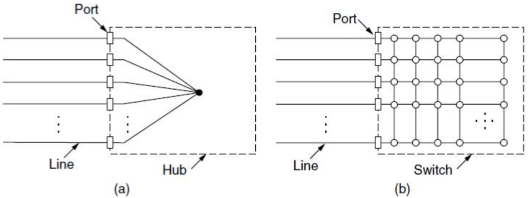
Gigabit Ethernet Cabling

Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 µ) or multimode (50, 62.5 µ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

10 Gigabit Ethernet Cabling

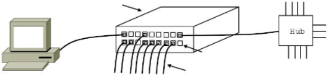
Name	Cable	Max. segment	Advantages
10GBase-SR	Fiber optics	Up to 300 m	Multimode fiber (0.85µ)
10GBase-LR	Fiber optics	10 km	Single-mode fiber (1.3µ)
10GBase-ER	Fiber optics	40 km	Single-mode fiber (1.5µ)
10GBase-CX4	4 Pairs of twinax	15 m	Twinaxial copper
10GBase-T	4 Pairs of UTP	100 m	Category 6a UTP

Hubs vs. Switches



(a) Hub, (b) Switch

10 Gigabit Ethernet Cabling



An Ethernet Switch

History: Today

- No collision ⇒ no distance limitation
- Gigabit Ethernet becomes WAN
- Links span over 100 km

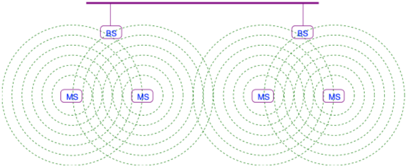
1-10 Gbps long reach connection

Outline I

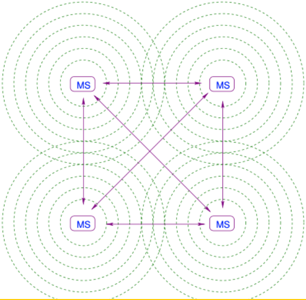
Wireless LAN Protocols

Two Architecture

1. Infrastructure ⇒ Base station (BA) plus wireless clients



2. Ad hoc ⇒ A group of wireless mobile stations(MS) get together

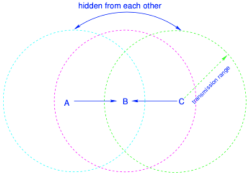


Hidden and Exposed Node Problems

Hidden Nodes:

A and C are hidden from each other when transmitting to B

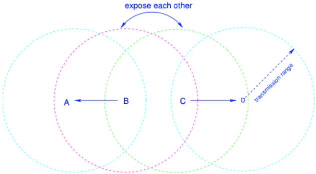
- They don't hear each other
- Results in collision



Exposed Nodes:

B and C are exposed when transmitting to A and D

- They hear each other
- Results in not transmitting



Question 4.3

How to solve these problems?

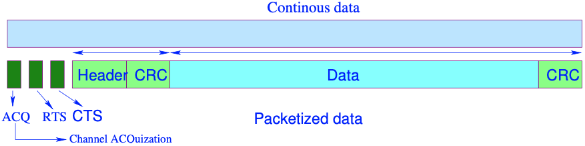
Answer: *Multiple Access with* *Collision Avoidance*

CSMA/CA
WiFi

⇒ Sometimes called Media Access with Collision Avoidance (MACA)

Communication from A to B

1. A sends a Request To Send (RTS)
   - B answers with Clear To Send (CTS)
   - C hears only the CTS, knows someone in its transmission range is communication
     - Stays quiet to prevent interference with B
     - Solves the hidden problem
2. B sends a Request To Send (RTS)
   - C hears only the RTS, knows the receiver is not in its transmission range
     - Can freely transmits to D
     - Solves the exposed problem



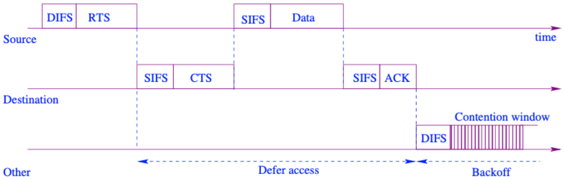
WiFi

802.11x

- 802.11

802.2			Data link
802.11 MAC			
FH	DSSS	IR	Phy Layer

  - FR: Frequency hopping at 2.4 GHz band
  - DSSS: Direct Sequence Spread Spectrum at 2.4 GHz band
  - IR: Infrared



DIFS: Distributed interframe space
SIFS: Short interframe space
RTS: Request to send
CTS: Clear to send
ACK: Acknowlegement

WiFi

DCF vs. PCF

- IEEE 802.11 standard defines two variations of CSMA/CA
  1. Distributed Coordination Function (DCF)
     - Fundamental medium access control (MAC) (including Wi-Fi)
     - Employs CSMA/CA with binary exponential backoff algorithm
     - BackofTime= random() $\times$ SlotTime
     - DCF does not solve the hidden/exposed terminal problem completely
     - It moves contention from data to control (Request to Send (RTS) and Clear to Send (CTS))
  2. Point Coordination Function (PCF)
     - It coordinate the communication via the access point (AP)
     - PCF is located directly above the DCF
- IEEE 802.11e amendment to the standard enhances the DCF and the PCF, through a new coordination function called Hybrid Coordination Function (HCF) Hybrid Coordination Function (HCF).

IEEE 802.11x

WiFi

- 802.11
  - Family of specifications for wireless local area network (WLAN) use
  - Employs phase-shift keying
  - Provides a wireless alternative to wired Ethernet LANs
  - Several enhancements as defined below
- 802.11a
  - Enhancement to 802.11 that applies to wireless ATM systems
  - Used in access hubs
  - Enhanced data speed
  - Frequency range 5.725 GHz to 5.850 GHz
- 802.11b
  - Enhancement to 802.11 that employs complementary code keying (CCK)
  - High data speed
  - Low susceptibility to multi-path-propagation interference
  - Frequency range 2.400 GHz to 2.4835 GHz
- 802.11d
  - Enhancement to 802.11 that allows for global Roaming
  - Attributes similar to 802.11b
  - Particulars can be set at Media Access Control (MAC) layer

IEEE 802.11x

- 802.11e
  - Enhancement to 802.11 that includes Quality of Service (QoS) features
  - Facilitates prioritization of data, voice, and video transmissions
- 802.11g
  - Enhancement to 802.11 that offers wireless transmission over relatively short distances
  - Operates at up to 54 megabits per second (Mbps)
- 802.11h
  - Enhancement to 802.11a that resolves interference issues
  - Dynamic frequency selection (DFS)
  - Transmit power control (TPC)
- 802.11i
  - Enhancement to 802.11 that offers additional security for WLAN applications
- 802.11j
  - Japanese regulatory extensions to 802.11a specification
  - Frequency range 4.9 GHz to 5.0 GHz

IEEE 802.11x

- 802.11k
  - Radio resource measurements for networks using 802.11 family specifications
- 802.11m
  - Maintenance of 802.11 family specifications
  - Corrections and amendments to existing documentation
- 802.11x
  - Generic term for 802.11 family specifications under development
  - General term for all 802.11 family specifications
- Wi-Fi
  - Originally created to ensure compatibility among 802.11b products
  - Can run under any 802.11 standard
  - Indicates interoperability certification by Wi-Fi Alliance
- 802.15
  - A communications specification for wireless personal area networks (WPANs)

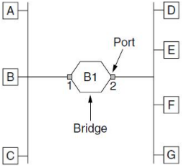
802.15, 802.16, 802.3, 802.4, 802.5

- 802.16
  - A group of broadband wireless communications standards for metropolitan area networks (MANs)
- 802.16a
  - Enhancement to 802.16 for non-line-of-sight extensions in the 2-11 GHz spectrum
  - Delivers up to 70 Mbps at distances up to 31 miles
- 802.16e
  - Enhancement to 802.16 that enables connections for mobile devices
- 802.1X
  - Designed to enhance the security of wireless local area networks (WLANs) that follow the IEEE 802.11 standard
  - Provides an authentication framework for wireless LANs
  - The algorithm that determines user authenticity is left open
  - Multiple algorithms are possible
- 802.3
  - A standard specification for Ethernet
  - Specifies the physical media and the working characteristics of the network
- 802.5
  - Standard specification for Token Ring networks

Outline I

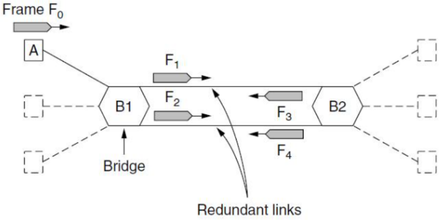
Data Link Layer Switching
Learning Bridges

- Bridges (and a hub) connecting seven point-to-point stations
- Bridges learn and records which MAC address is on which side of the bridge
  - Caching MAC address

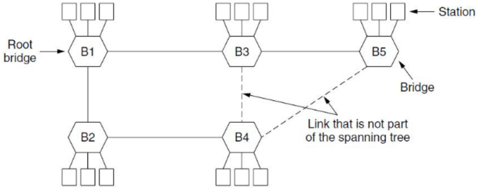


Protocol processing at a bridge

Two logical connections between two bridges



Spanning Tree Bridges



A spanning tree connecting five bridges. The dotted lines are links that are not part of the spanning tree

Outline I

What is the efficiency of P-ALOHA?

- How to find the maximum efficiency?
  - Find p^* that maximizes the the expected transmission *How?*

$$\begin{aligned}\frac{d}{dp}p(1-p)^{2(N-1)} &= (1-p)^{2(N-1)} - 2(N-1)p(1-p)^{2(N-1)-1} \\ &= (1-p)^{2(N-1)-1}[1-p-2(N-1)p] = 0\end{aligned}$$

- Solving for p, $\Rightarrow\ p^* = \frac{1}{2N}$

What is the efficiency of P-ALOHA?

$$\begin{aligned} E(p^*) &= 2N \times p(1-p)^{2(N-1)} = 2N \times \frac{1}{2N}(1-\frac{1}{2N})^{2(N-1)} \\ &= (1-\frac{1}{2N})^{2(N-1)} \end{aligned}$$

$$\lim_{N\to\infty} E(p^*) = \frac{1}{2e} \approx 0.18$$

Outline I

References

[Tanenbaum and Wetherall, 2011] Tanenbaum, A. S. and Wetherall, D. J. (2011). Computer Networks: 5th Edition. Prentice Hall PTR.