CEN531 – Computer Networks
4 – Medium Access Control Sublayer

Dr. Mostafa Hassan Dahshan

Department of Computer Engineering

College of Computer and Information Sciences

King Saud University

mdahshan@ksu.edu.sa

http://faculty.ksu.edu.sa/mdahshan

Acknowledgments

These slides are adapted from:

Computer Networks 5E, by Tanenbaum & Wetherall, Pearson Education, 2011.

Computer Networking: A Top Down Approach 6E, by Jim Kurose and Keith Ross, Addison-Wesley, 2012.

Data and Computer Communications, 8E, by William Stallings, Pearson Education, 2007.

Medium Access Control Sublayer

Chapter 4

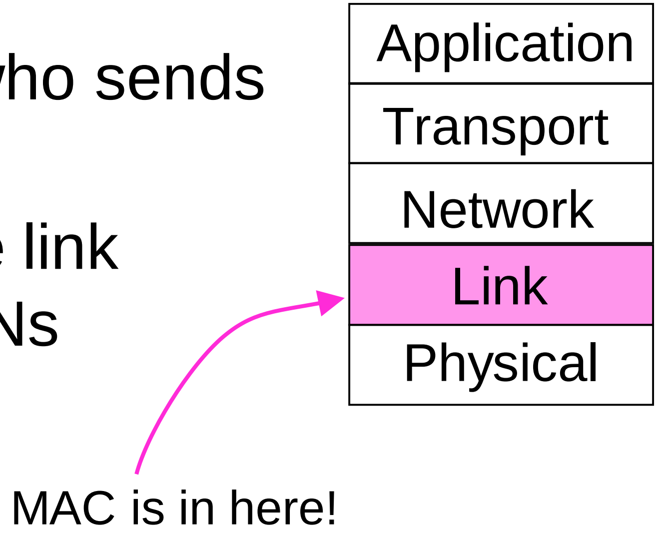
- Channel Allocation Problem
- Multiple Access Protocols
- Ethernet
- Wireless LANs
- ~~Broadband Wireless~~
- ~~Bluetooth~~
- ~~RFID~~
- Data Link Layer Switching

Revised: August 2011

The MAC Sublayer

Responsible for deciding who sends next on a multi-access link

- An important part of the link layer, especially for LANs



Channel Allocation Problem (1)

For fixed channel and traffic from N users

- Divide up bandwidth using FTM, TDM, CDMA, etc.
- This is a static allocation, e.g., FM radio

This static allocation performs poorly for bursty traffic

- Allocation to a user will sometimes go unused

Channel Allocation Problem (2)

Dynamic allocation gives the channel to a user when they need it. Potentially N times as efficient for N users.

Schemes vary with assumptions:

Assumption	**Implication**
Independent traffic	Often not a good model, but permits analysis
Single channel	No external way to coordinate senders
Observable collisions	Needed for reliability; mechanisms vary
Continuous or slotted time	Slotting may improve performance
Carrier sense	Can improve performance if available

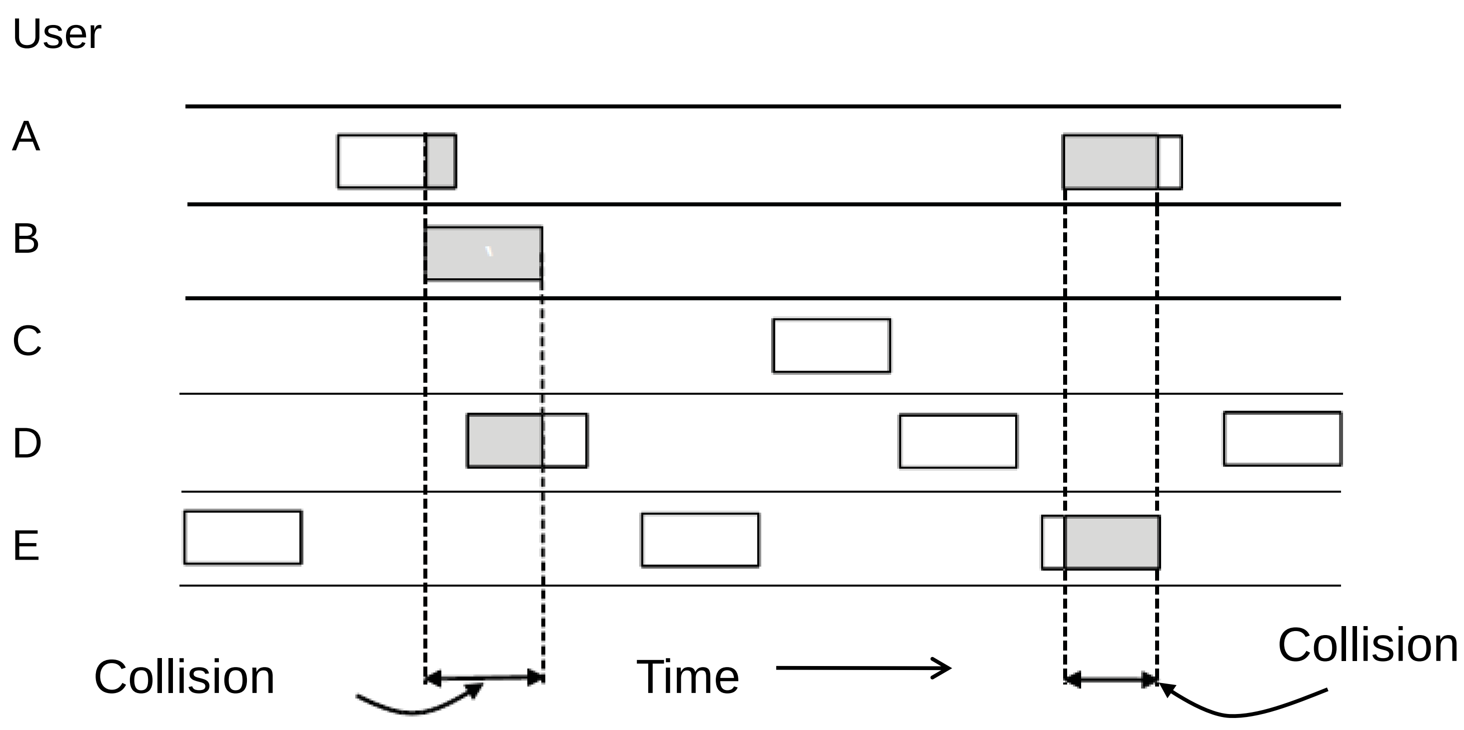
Multiple Access Protocols

- ALOHA »
- CSMA (Carrier Sense Multiple Access) »
- Collision-free protocols »
- Limited-contention protocols »
- Wireless LAN protocols »

ALOHA (1)

In pure ALOHA, users transmit frames whenever they have data; users retry after a random time for collisions

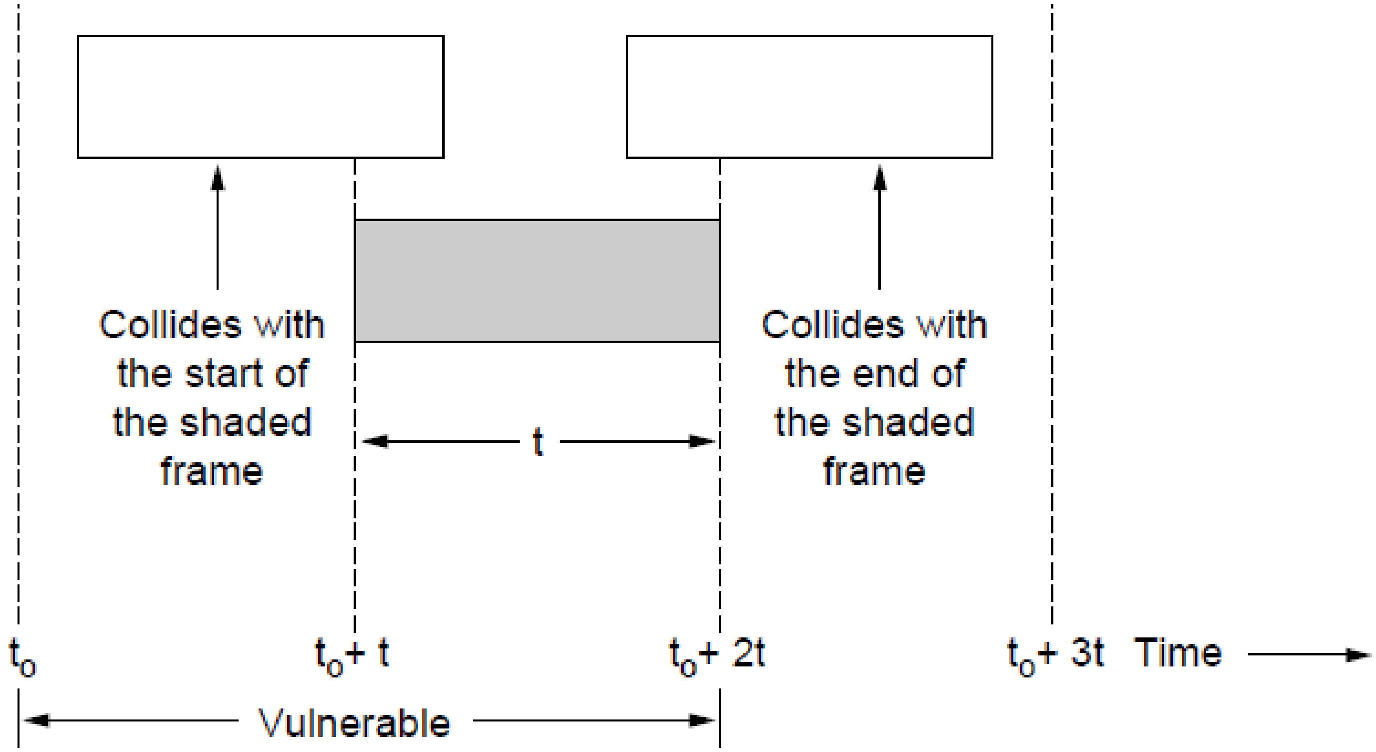
- Efficient and low-delay under low load



ALOHA (2)

Collisions happen when other users transmit during a vulnerable period that is twice the frame time

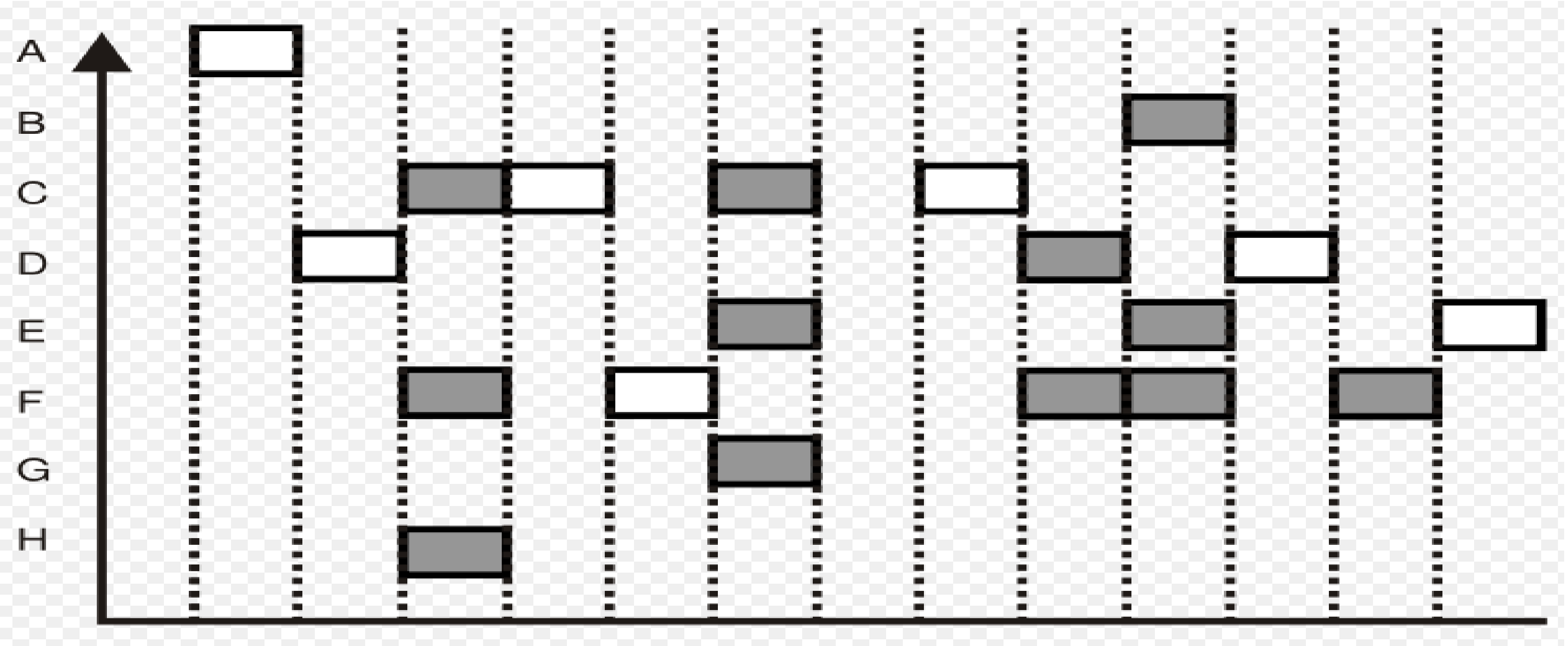
- Synchronizing senders to slots can reduce collisions



Slotted ALOHA

Divide time into discrete intervals

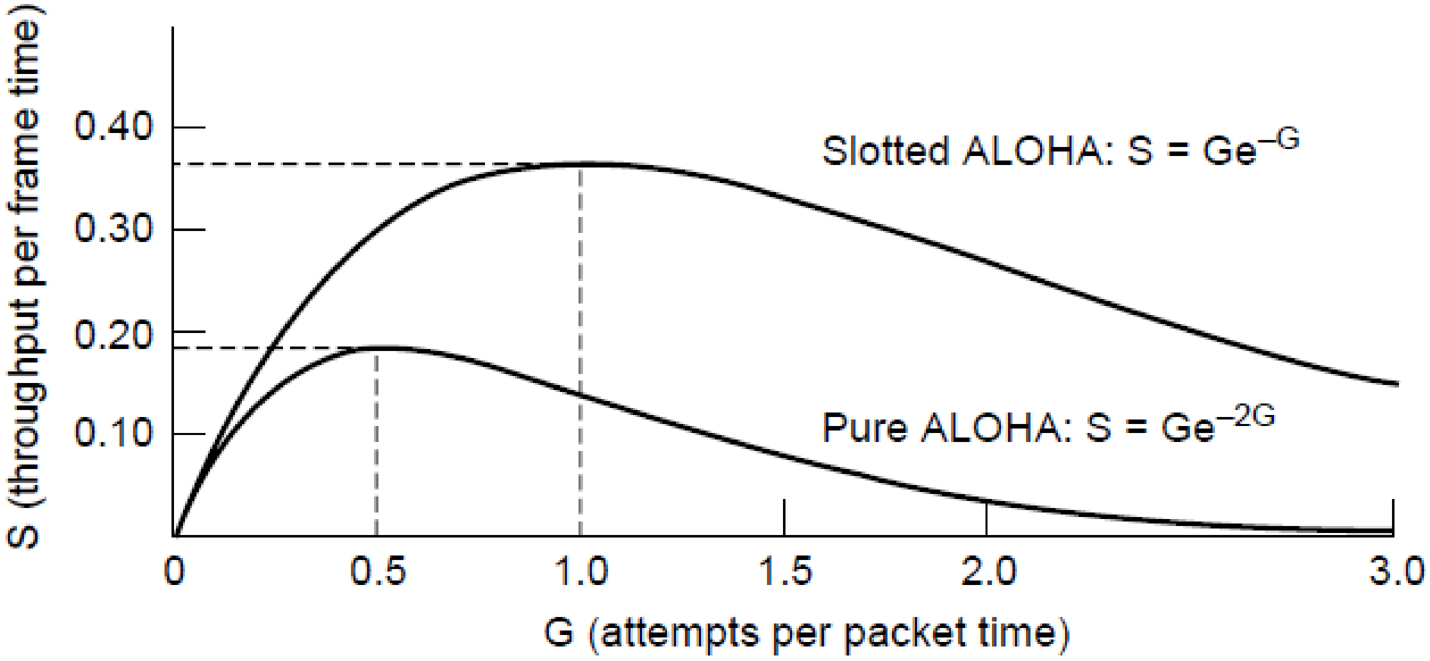
Each interval corresponds to 1 frame



ALOHA (3)

Slotted ALOHA is twice as efficient as pure ALOHA

- Low load wastes slots, high loads causes collisions
- Efficiency up to 1/e (37%) for random traffic models



CSMA (1)

CSMA improves on ALOHA by sensing the channel!

- User doesn’t send if it senses someone else

Variations on what to do if the channel is busy:

- 1-persistent (greedy) sends as soon as idle
- Nonpersistent waits a random time then tries again
- p-persistent sends with probability p when idle

CSMA

stations soon know transmission has started

so first listen for clear medium (carrier sense)

if medium idle, transmit

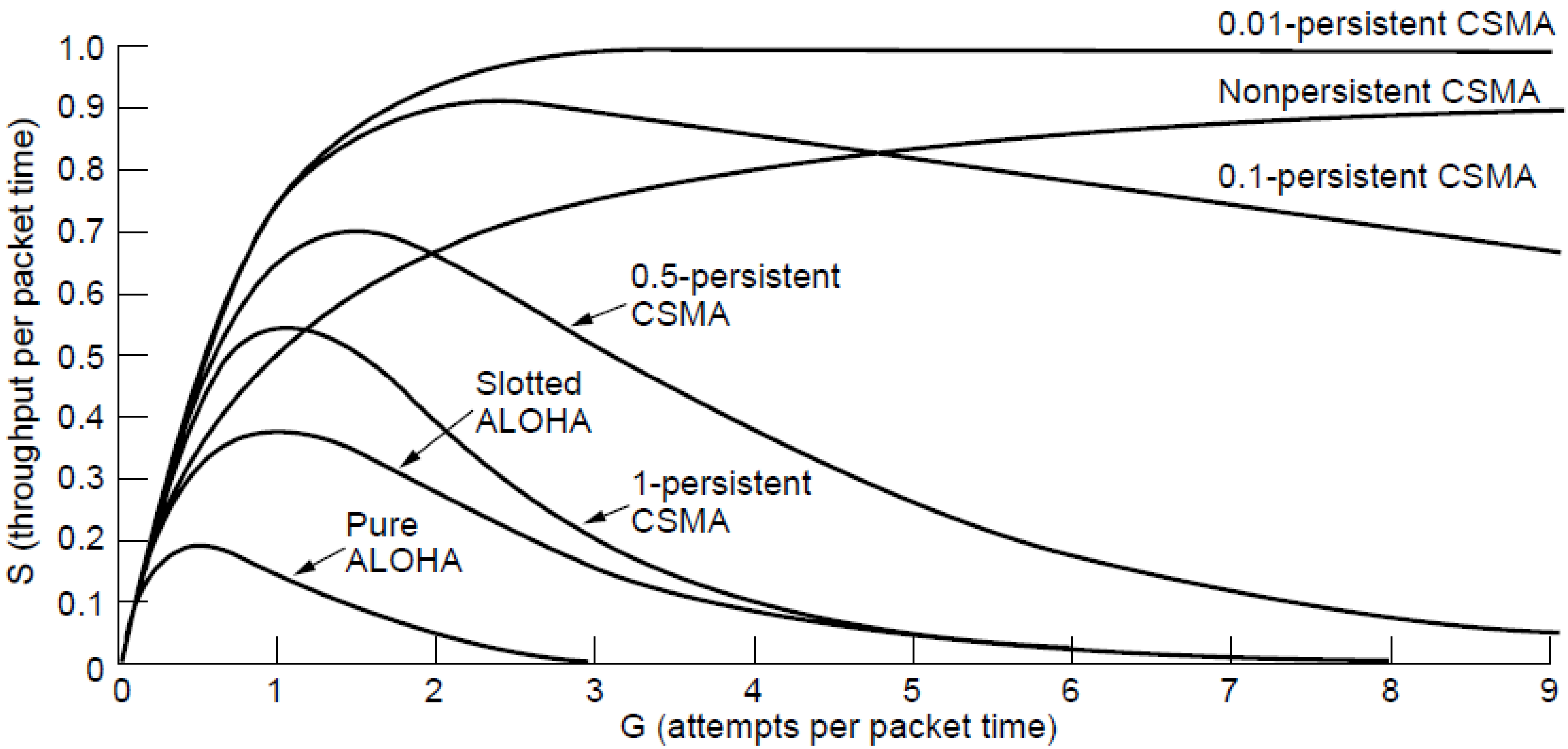
if two stations start at the same instant, collision

- wait reasonable time
- if no ACK then retransmit
- collisions occur occur at leading edge of frame

max utilization depends on propagation time (medium length) and frame length

CSMA (2) – Persistence

CSMA outperforms ALOHA, and being less persistent is better under high load



Nonpersistent CSMA

Nonpersistent CSMA rules:

1. if medium idle, transmit
2. if medium busy, wait amount of time drawn from probability distribution (retransmission delay) & retry

random delays reduces probability of collisions

capacity is wasted because medium will remain idle following end of transmission

nonpersistent stations are deferential

1-persistent CSMA

1-persistent CSMA avoids idle channel time

1-persistent CSMA rules:

1. if medium idle, transmit;
2. if medium busy, listen until idle; then transmit immediately

1-persistent stations are selfish

if two or more stations waiting, a collision is guaranteed

P-persistent CSMA

a compromise to try and reduce collisions and idle time

p-persistent CSMA rules:

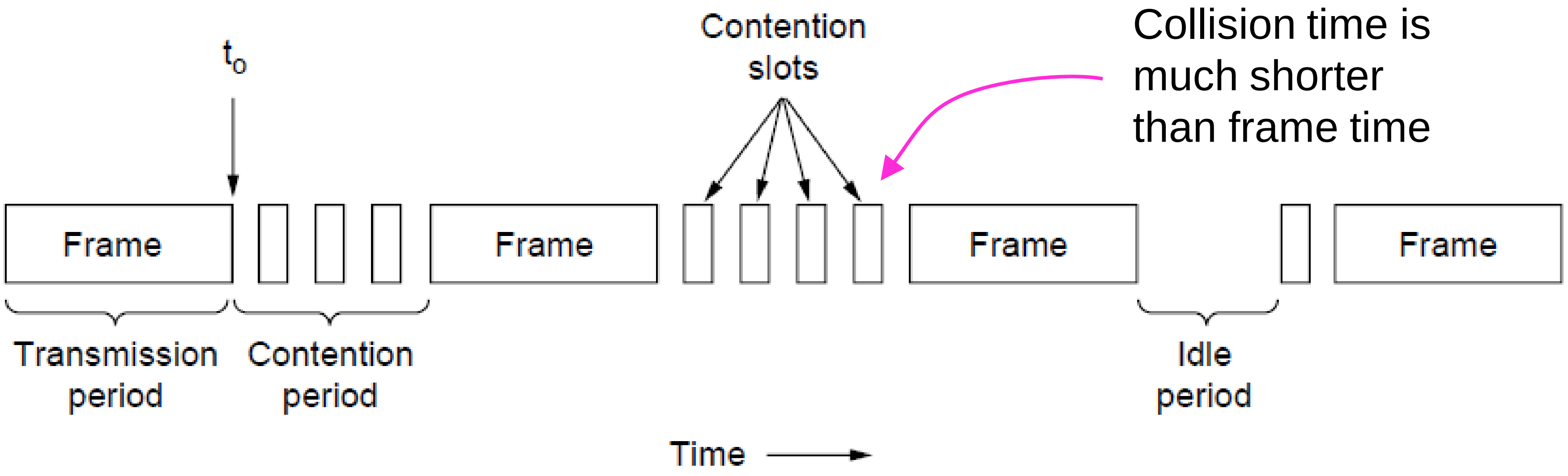
1. if medium idle, transmit with probability p, and delay one time unit with probability (1–p)
2. if medium busy, listen until idle and repeat step 1
3. if transmission is delayed one time unit, repeat step 1

issue of choosing effective value of p to avoid instability under heavy load

CSMA (3) – Collision Detection

CSMA/CD improvement is to detect/abort collisions

- Reduced contention times improve performance



CSMA/CD Description

with CSMA, collision occupies medium for duration of transmission

better if stations listen whilst transmitting

CSMA/CD rules:

1. if medium idle, transmit
2. if busy, listen for idle, then transmit
3. if collision detected, jam and then cease transmission
4. after jam, wait random time then retry

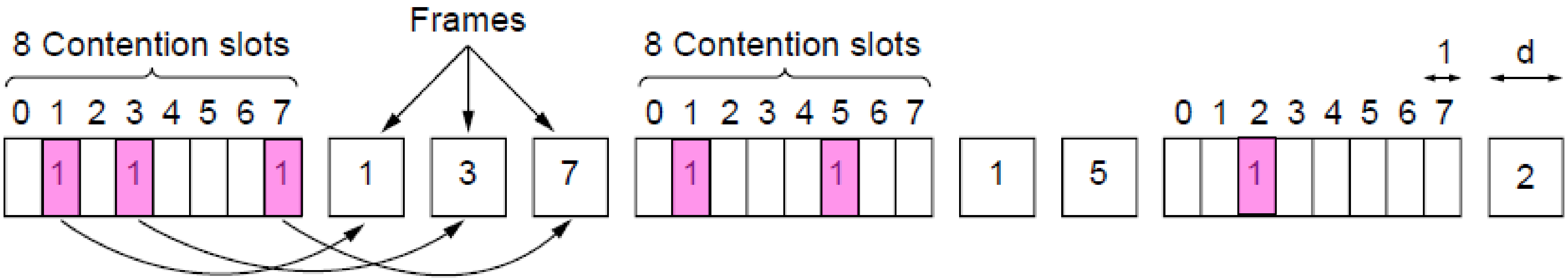
Collision-Free (1) – Bitmap

Collision-free protocols avoid collisions entirely

- Senders must know when it is their turn to send

The basic bit-map protocol:

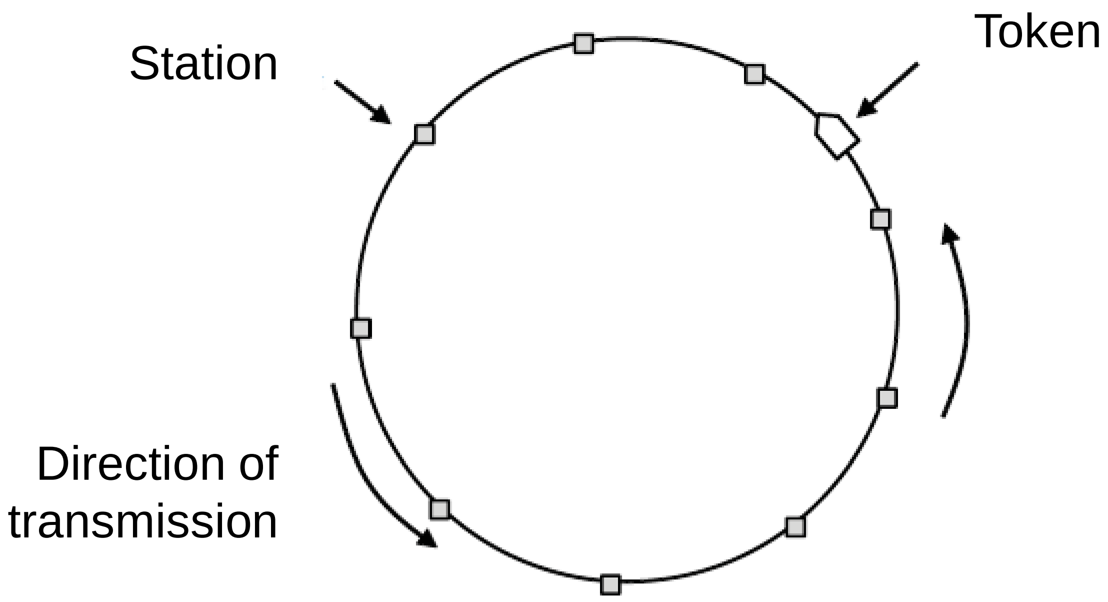
- Sender set a bit in contention slot if they have data
- Senders send in turn; everyone knows who has data



Collision-Free (2) – Token Ring

Token sent round ring defines the sending order

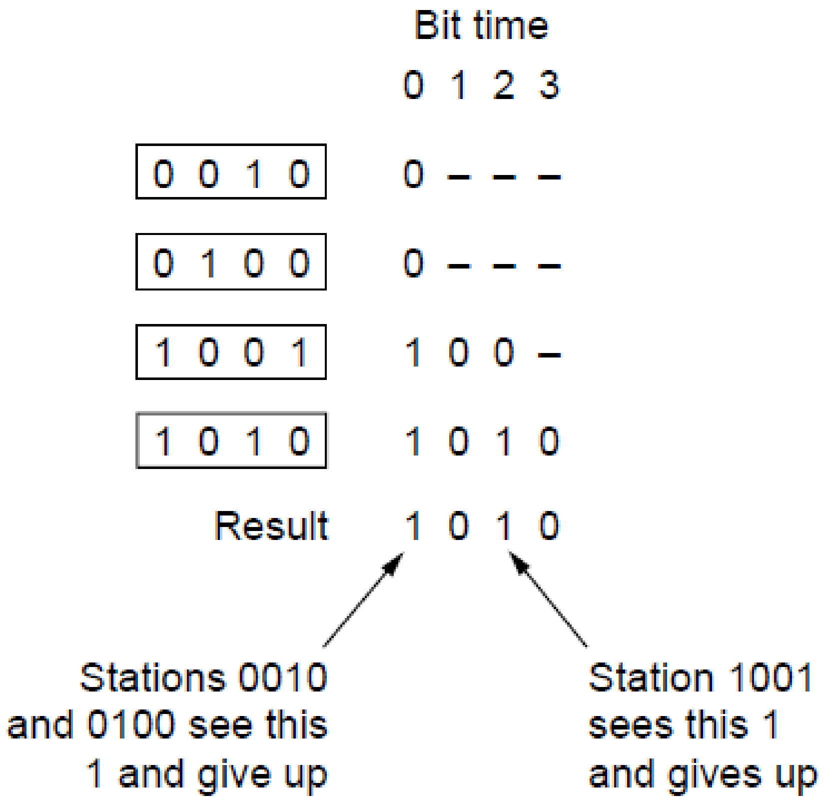
- Station with token may send a frame before passing
- Idea can be used without ring too, e.g., token bus



Collision-Free (3) – Countdown

Binary countdown improves on the bitmap protocol

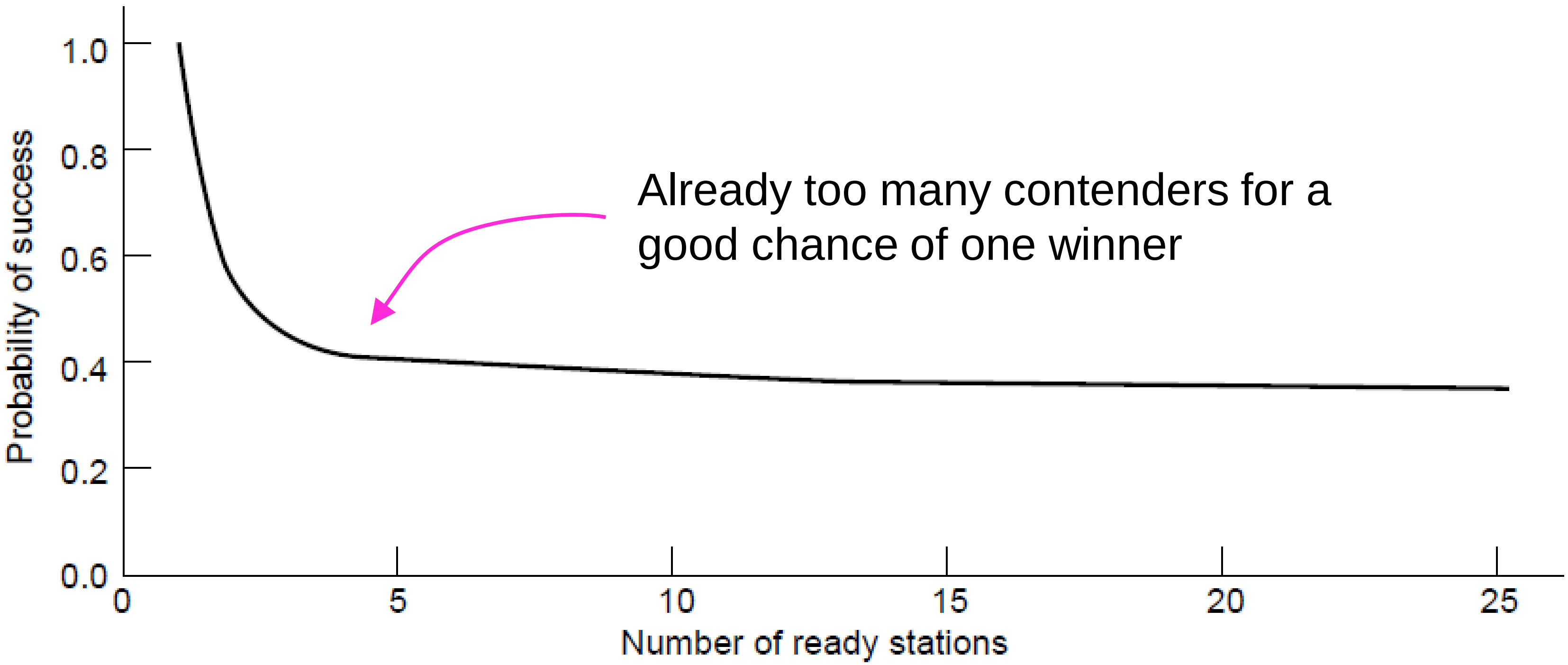
- Stations send their address in contention slot (log N bits instead of N bits)
- Medium ORs bits; stations give up when they send a "0" but see a "1"
- Station that sees its full address is next to send



Limited-Contention Protocols (1)

Idea is to divide stations into groups within which only a very small number are likely to want to send

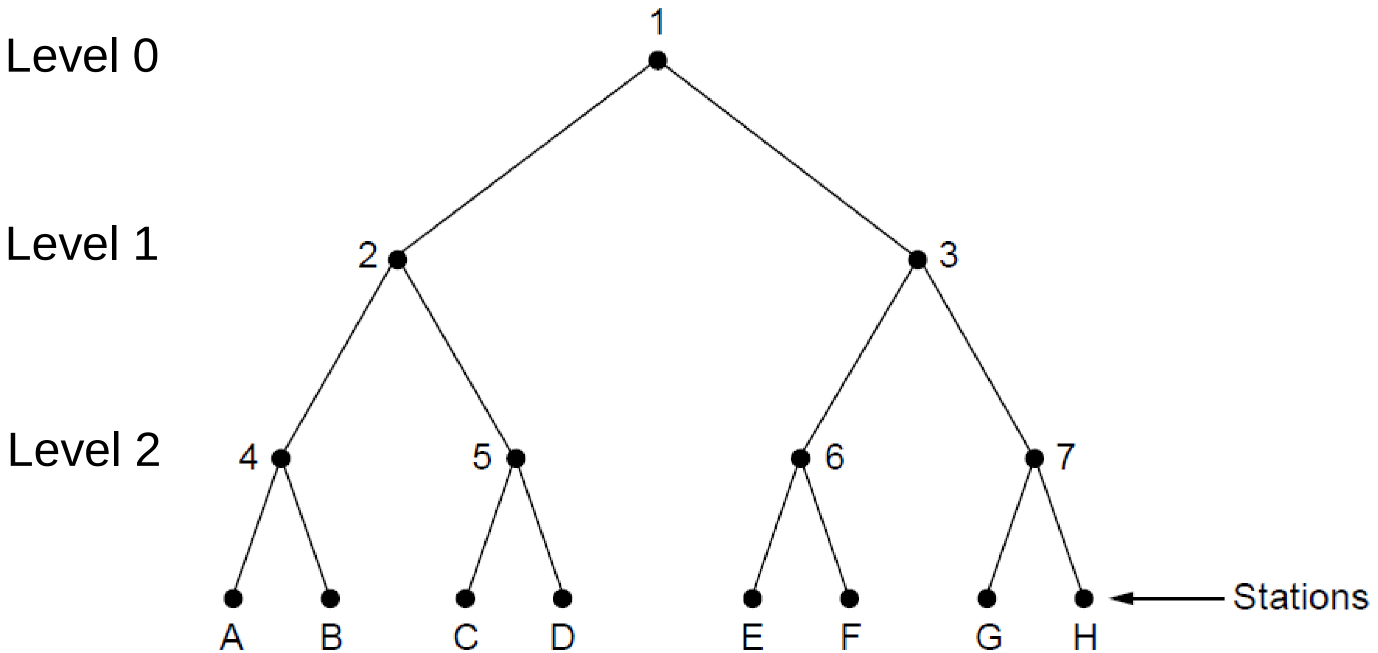
- Avoids wastage due to idle periods and collisions



Limited Contention (2) –Adaptive Tree Walk

Tree divides stations into groups (nodes) to poll

- Depth first search under nodes with poll collisions
- Start search at lower levels if >1 station expected



Wireless LAN Protocols (1)

Wireless has complications compared to wired.

Nodes may have different coverage regions

- Leads to <u>hidden</u> and <u>exposed</u> terminals

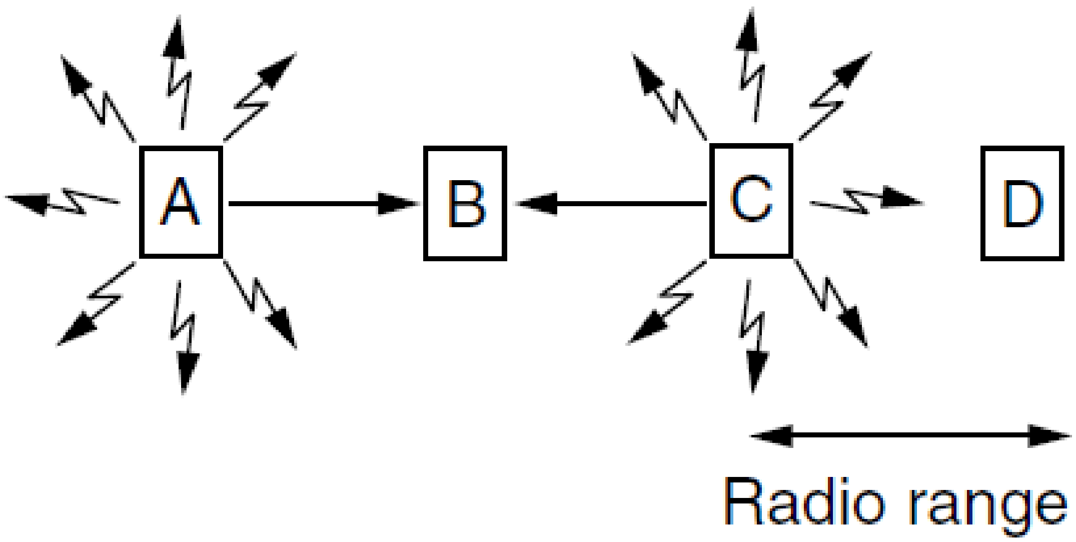
Nodes can't detect collisions, i.e., sense while sending

- Makes collisions expensive and to be avoided

Wireless LANs (2) – Hidden terminals

Hidden terminals are senders that cannot sense each other but nonetheless collide at intended receiver

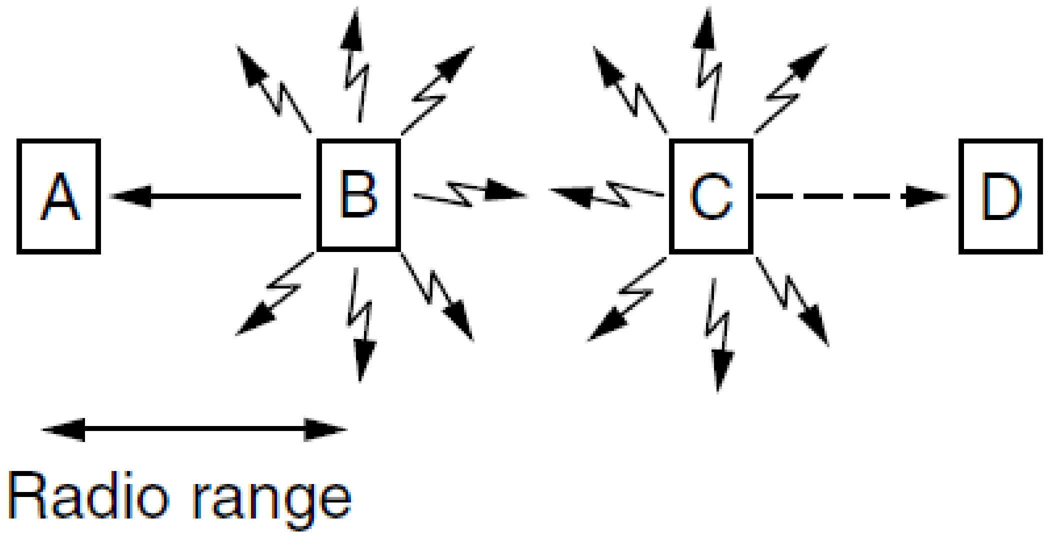
- Want to prevent; loss of efficiency
- A and C are hidden terminals when sending to B



Wireless LANs (3) – Exposed terminals

Exposed terminals are senders who can sense each other but still transmit safely (to different receivers)

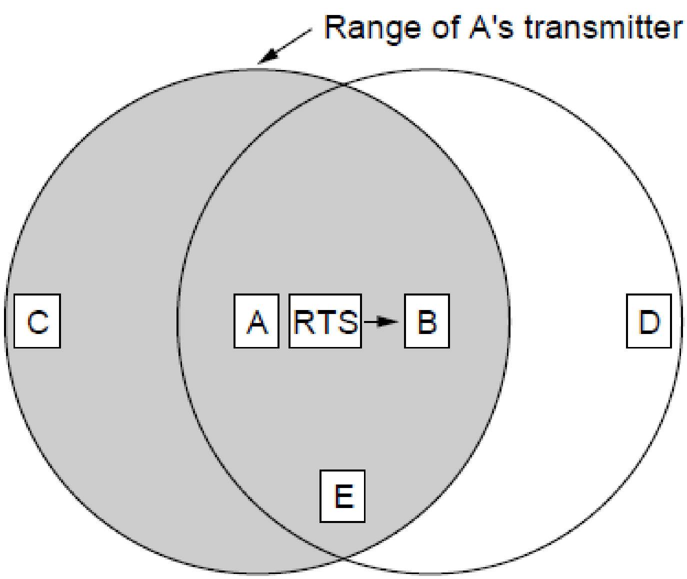
- Desirably concurrency; improves performance
- B → A and C → D are exposed terminals



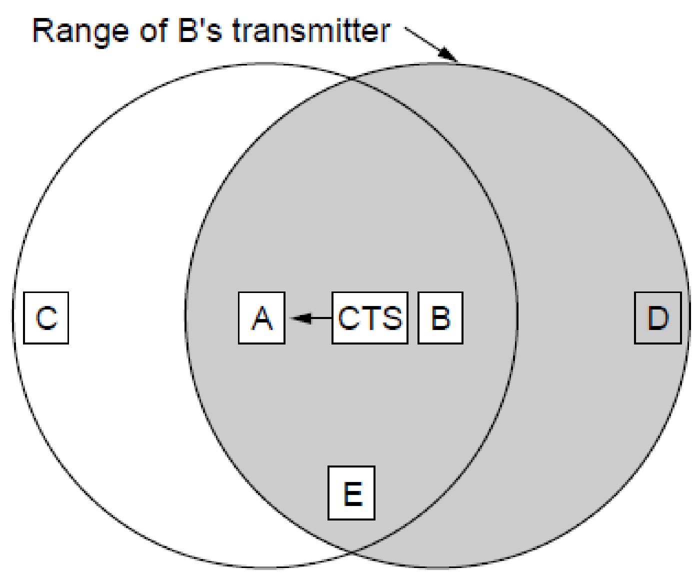
Wireless LANs (4) – MACA

MACA protocol grants access for A to send to B:

- A sends RTS to B [left]; B replies with CTS [right]
- A can send with exposed but no hidden terminals



A sends RTS to B; C and E hear and defer for CTS



B replies with CTS; D and E hear and defer for data

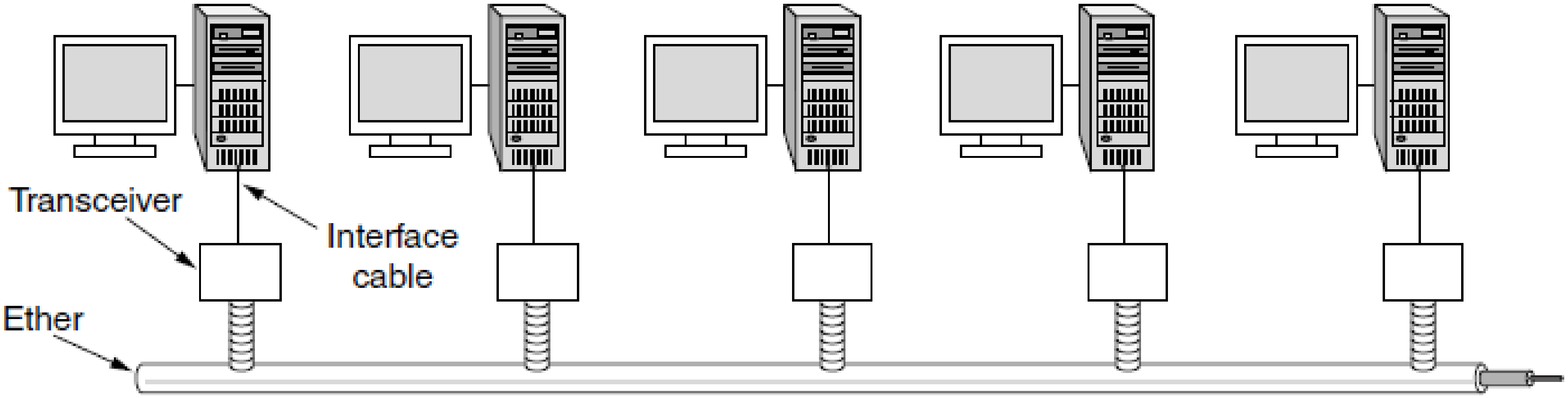
Ethernet

- Classic Ethernet »
- Switched/Fast Ethernet »
- Gigabit/10 Gigabit Ethernet »

Classic Ethernet (1) – Physical Layer

One shared coaxial cable to which all hosts attached

- Up to 10 Mbps, with Manchester encoding
- Hosts ran the classic Ethernet protocol for access



Classic Ethernet (2) – MAC

MAC protocol is 1-persistent CSMA/CD (earlier)

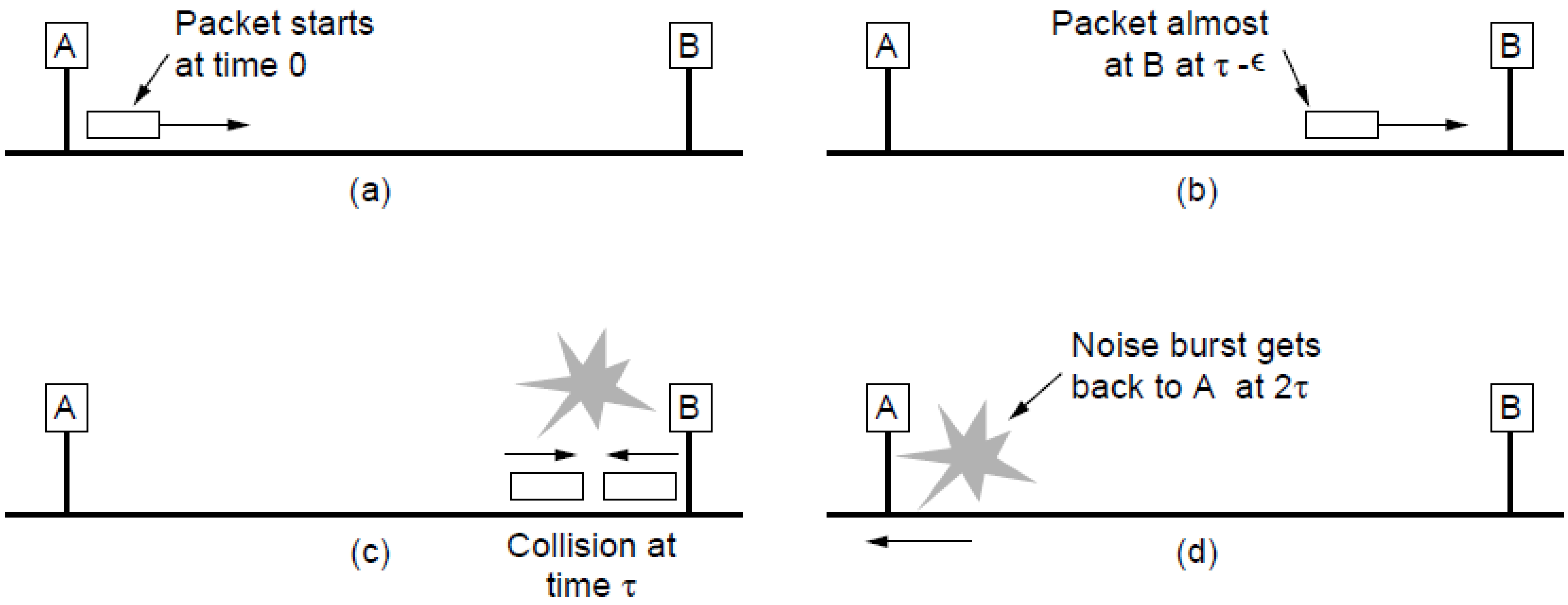
- Random delay (backoff) after collision is computed with BEB (Binary Exponential Backoff)
- Frame format is still used with modern Ethernet.

Bytes	8		6	6	2	0-1500	0-46	4
Ethernet (DIX)	Preamble		Destination address	Source address	Type	Data	Pad	Check-sum
IEEE 802.3	Preamble	SoF	Destination address	Source address	Length	Data	Pad	Check-sum

Classic Ethernet (3) – MAC

Collisions can occur and take as long as 2τ to detect

- τ is the time it takes to propagate over the Ethernet
- Leads to minimum packet size for reliable detection



Binary Exponential Backoff

for backoff stability, IEEE 802.3 and Ethernet both use binary exponential backoff

stations repeatedly resend when collide

- on first 10 attempts, mean random delay doubled
- value then remains same for 6 further attempts
- after 16 unsuccessful attempts, station gives up and reports error

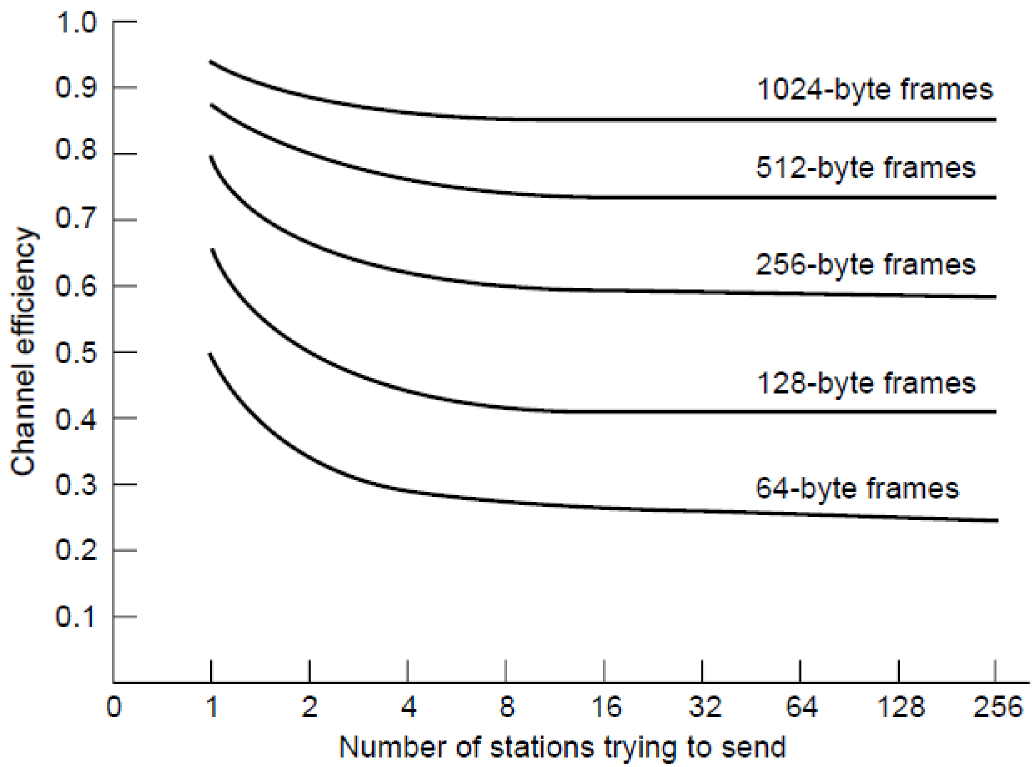
1-persistent algorithm with binary exponential backoff efficient over wide range of loads

but backoff algorithm has last-in, first-out effect

Classic Ethernet (4) – Performance

Efficient for large frames, even with many senders

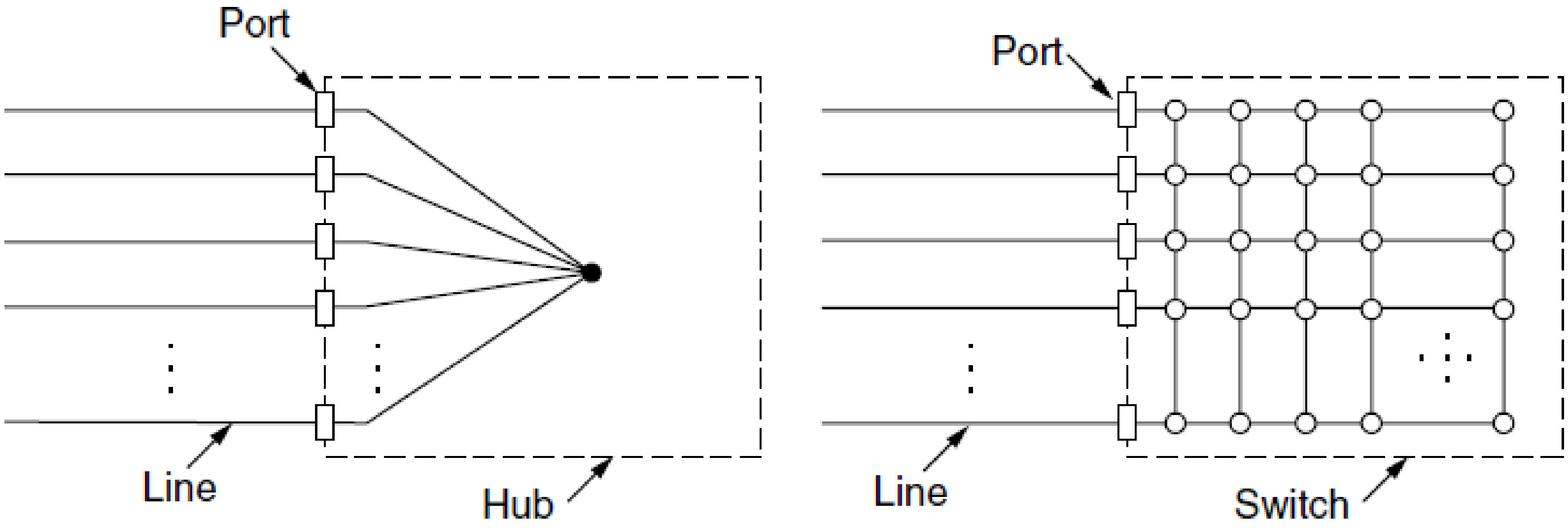
- Degrades for small frames (and long LANs)



10 Mbps Ethernet,
64 byte min. frame

Switched/Fast Ethernet (1)

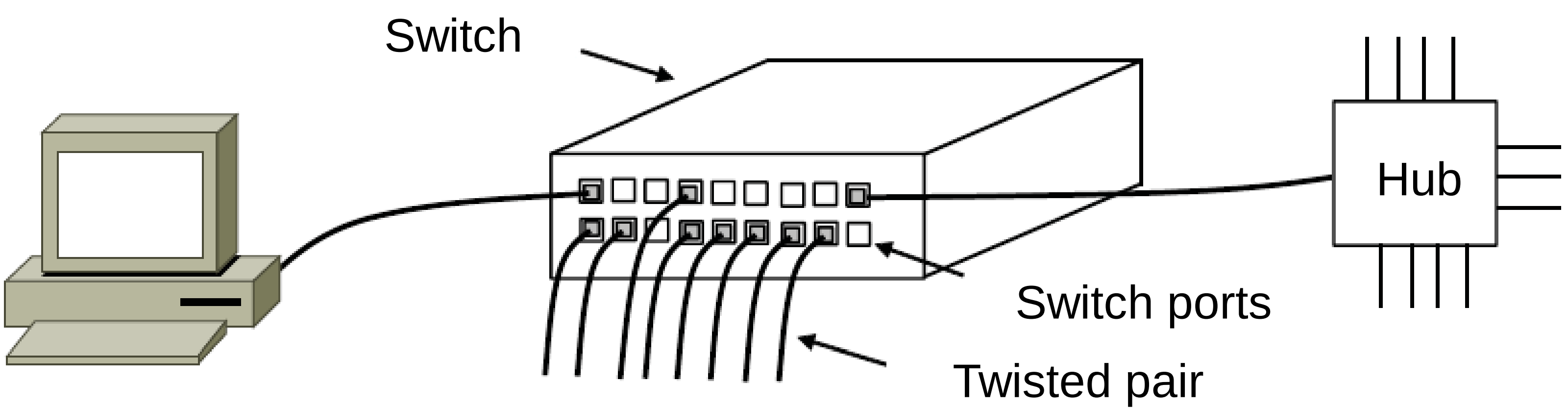
- Hubs wire all lines into a single CSMA/CD domain
- Switches isolate each port to a separate domain
  - Much greater throughput for multiple ports
  - No need for CSMA/CD with full-duplex lines



Switched/Fast Ethernet (2)

Switches can be wired to computers, hubs and switches

- Hubs concentrate traffic from computers
- More on how to switch frames the in 4.8



Switched/Fast Ethernet (3)

Fast Ethernet extended Ethernet from 10 to 100 Mbps

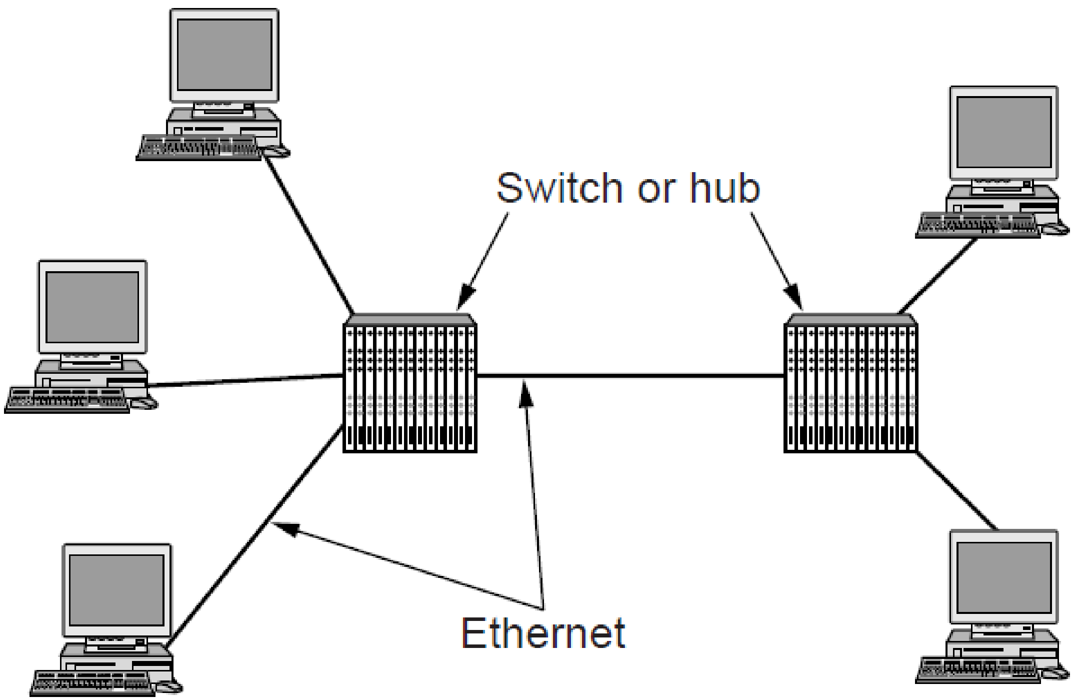
- Twisted pair (with Cat 5) dominated the market

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

Gigabit / 10 Gigabit Ethernet (1)

Switched Gigabit Ethernet is now the garden variety

- With full-duplex lines between computers/switches



Gigabit / 10 Gigabit Ethernet (1)

- Gigabit Ethernet is commonly run over twisted pair

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 is being deployed where needed

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

- 40/100 Gigabit Ethernet is under development

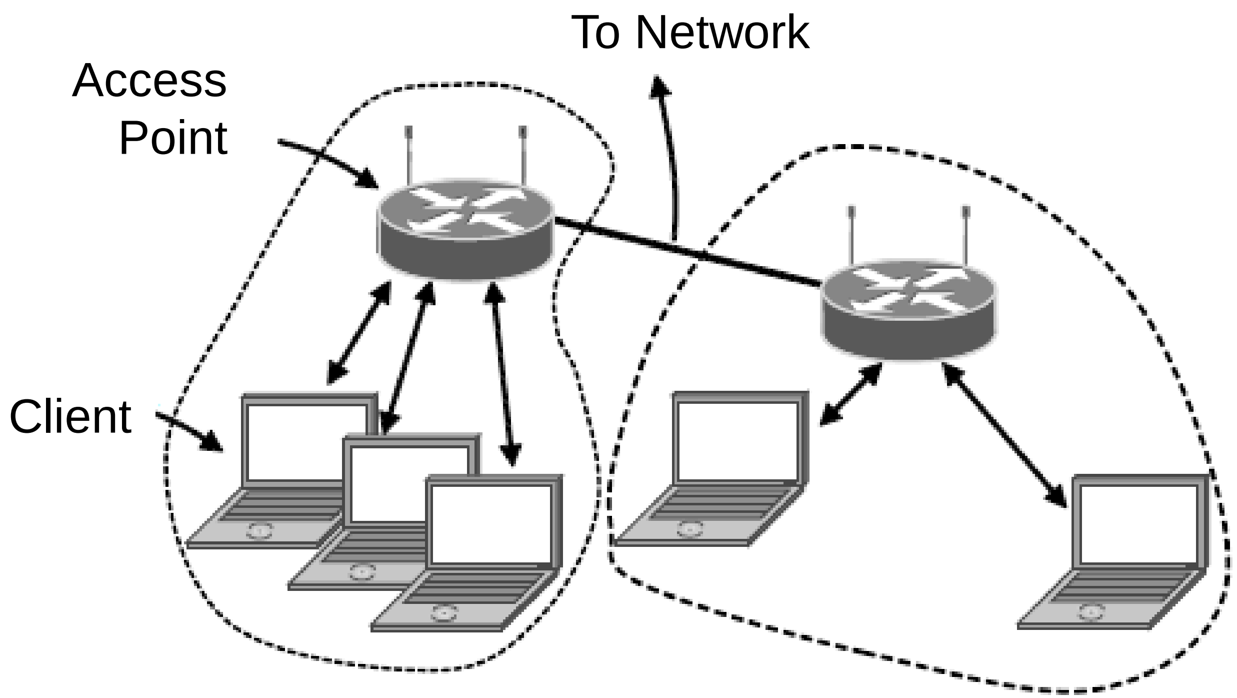
Wireless LANs

- 802.11 architecture/protocol stack »
- 802.11 physical layer »
- 802.11 MAC »
- 802.11 frames »

802.11 Architecture/Protocol Stack (1)

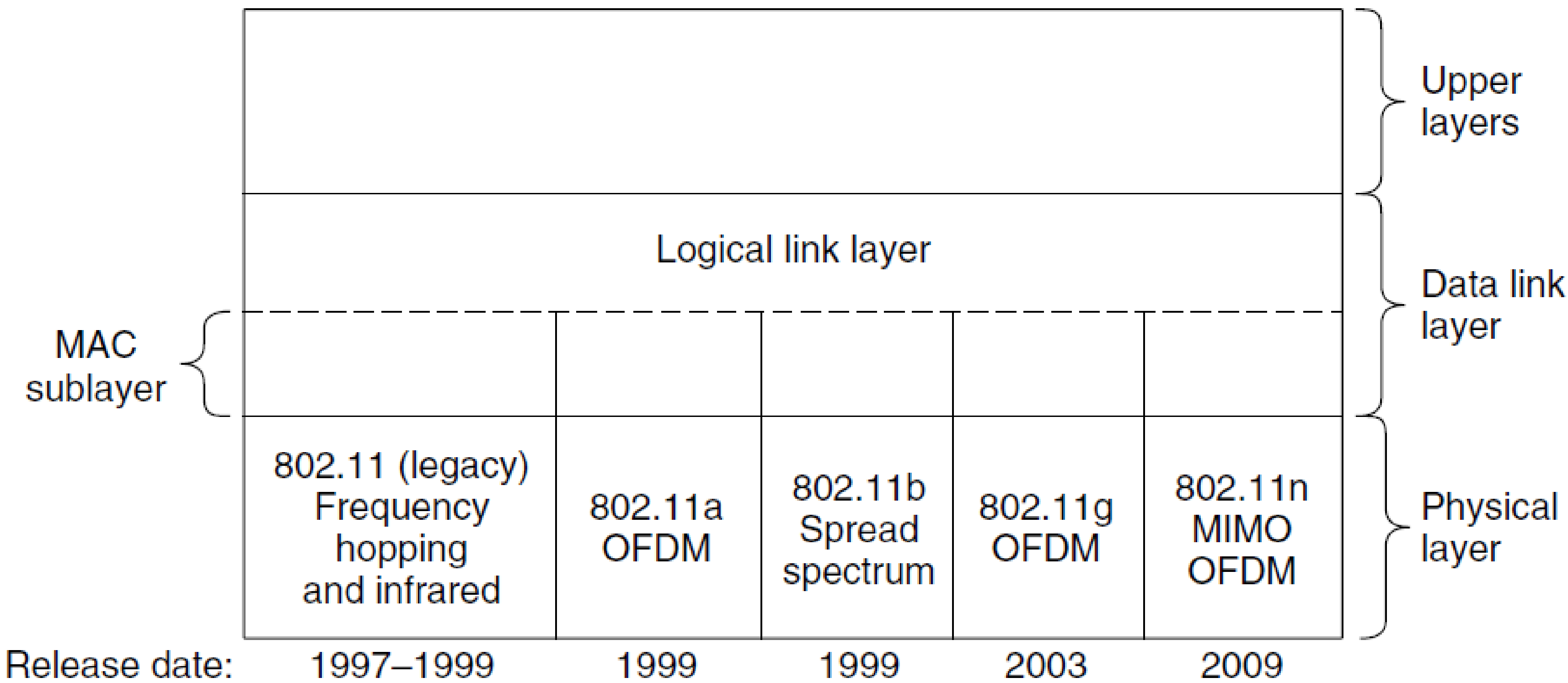
Wireless clients associate to a wired AP (Access Point)

- Called infrastructure mode; there is also ad-hoc mode with no AP, but that is rare.



802.11 Architecture/Protocol Stack (2)

MAC is used across different physical layers



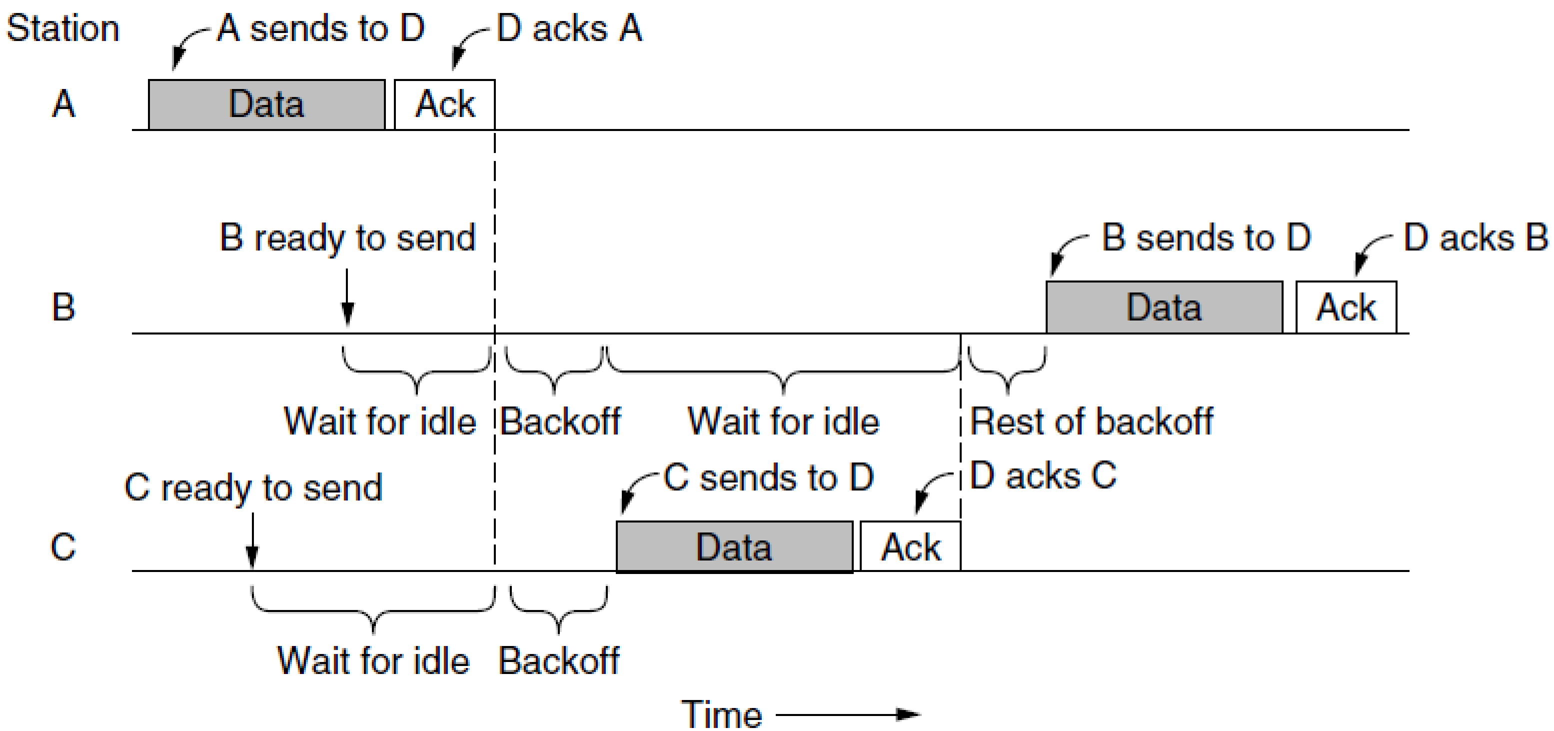
802.11 physical layer

- NICs are compatible with multiple physical layers
  - E.g., 802.11 a/b/g

Name	Technique	Max. Bit Rate
802.11b	Spread spectrum, 2.4 GHz	11 Mbps
802.11g	OFDM, 2.4 GHz	54 Mbps
802.11a	OFDM, 5 GHz	54 Mbps
802.11n	OFDM with MIMO, 2.4/5 GHz	600 Mbps

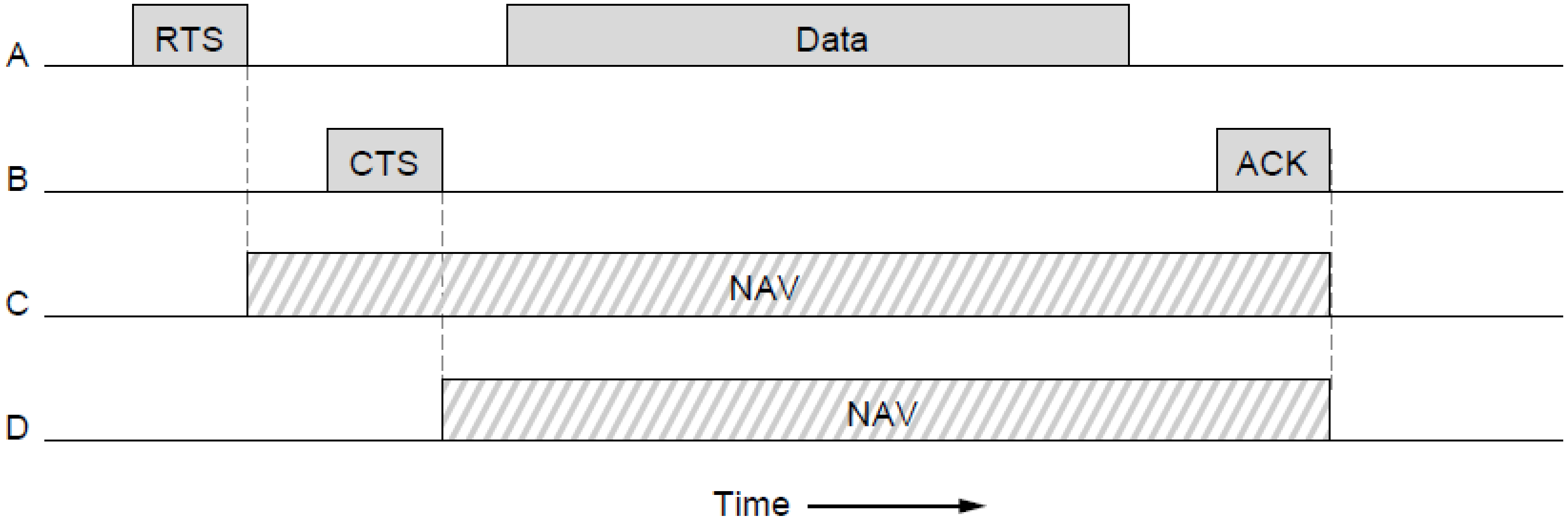
802.11 MAC (1)

- CSMA/CA inserts backoff slots to avoid collisions
- MAC uses ACKs/retransmissions for wireless errors



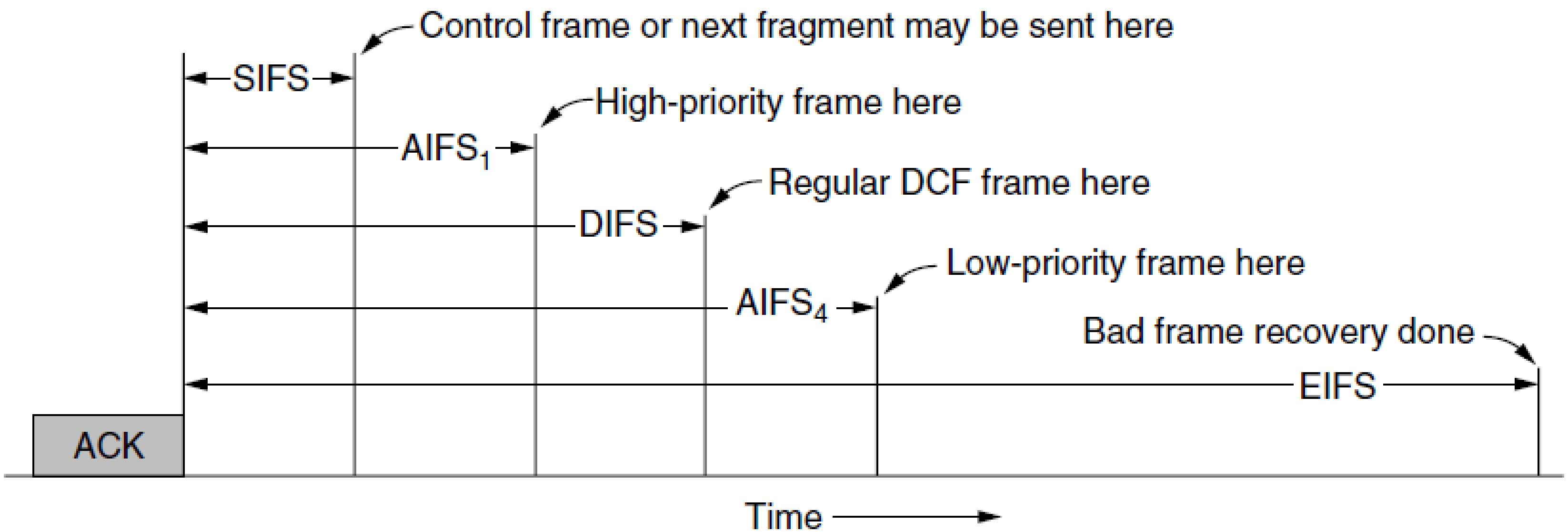
802.11 MAC (2)

Virtual channel sensing with the NAV and optional RTS/CTS (often not used) avoids hidden terminals



802.11 MAC (3)

- Different backoff slot times add quality of service
  - Short intervals give preferred access, e.g., control, VoIP
- MAC has other mechanisms too, e.g., power save



Distributed Coordination Function

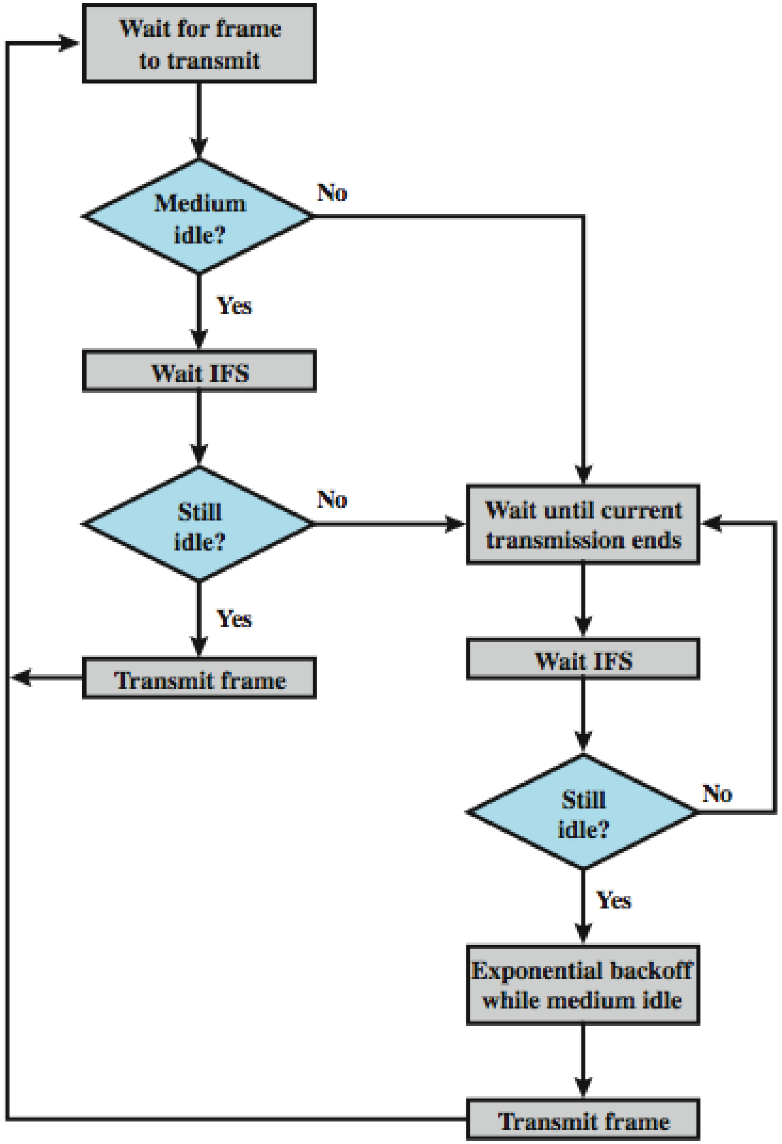
DCF sublayer uses CSMA

- if station has frame to send it listens to medium
- if medium idle, station may transmit
- else waits until current transmission complete

no collision detection since on wireless network

DCF includes delays that act as a priority scheme

IEEE 802.11 Medium Access Control Logic



Priority IFS Values

SIFS (short IFS)

- for all immediate response actions (see later)

PIFS (point coordination function IFS)

- used by the centralized controller in PCF scheme when issuing polls

DIFS (distributed coordination function IFS)

- used as minimum delay for asynchronous frames contending for access

SIFS Use

SIFS gives highest priority

- over stations waiting PIFS or DIFS time

SIFS used in following circumstances:

- Acknowledgment (ACK)
  - station responds with ACK after waiting SIFS gap
  - for efficient collision detect & multi-frame transmission
- Clear to Send (CTS)
  - station ensures data frame gets through by issuing RTS
  - and waits for CTS response from destination
- Poll response
  - see Point coordination Function (PCF) discussion next

PIFS and DIFS Use

PIFS used by centralized controller

- for issuing polls
- has precedence over normal contention traffic
- but not SIFS

DIFS used for all ordinary asynchronous traffic

802.11 Frames

- Frames vary depending on their type (Frame control)
- Data frames have 3 addresses to pass via APs

Bytes	2	2	6	6	6	2	0–2312	4
	Frame control	Duration	Address 1 (recipient)	Address 2 (transmitter)	Address 3	Sequence	Data	Check sequence

	Version = 00	Type = 10	Subtype = 0000	To DS	From DS	More frag.	Retry	Pwr. mgt.	More data	Protected	Order
Bits	2	2	4	1	1	1	1	1	1	1	1

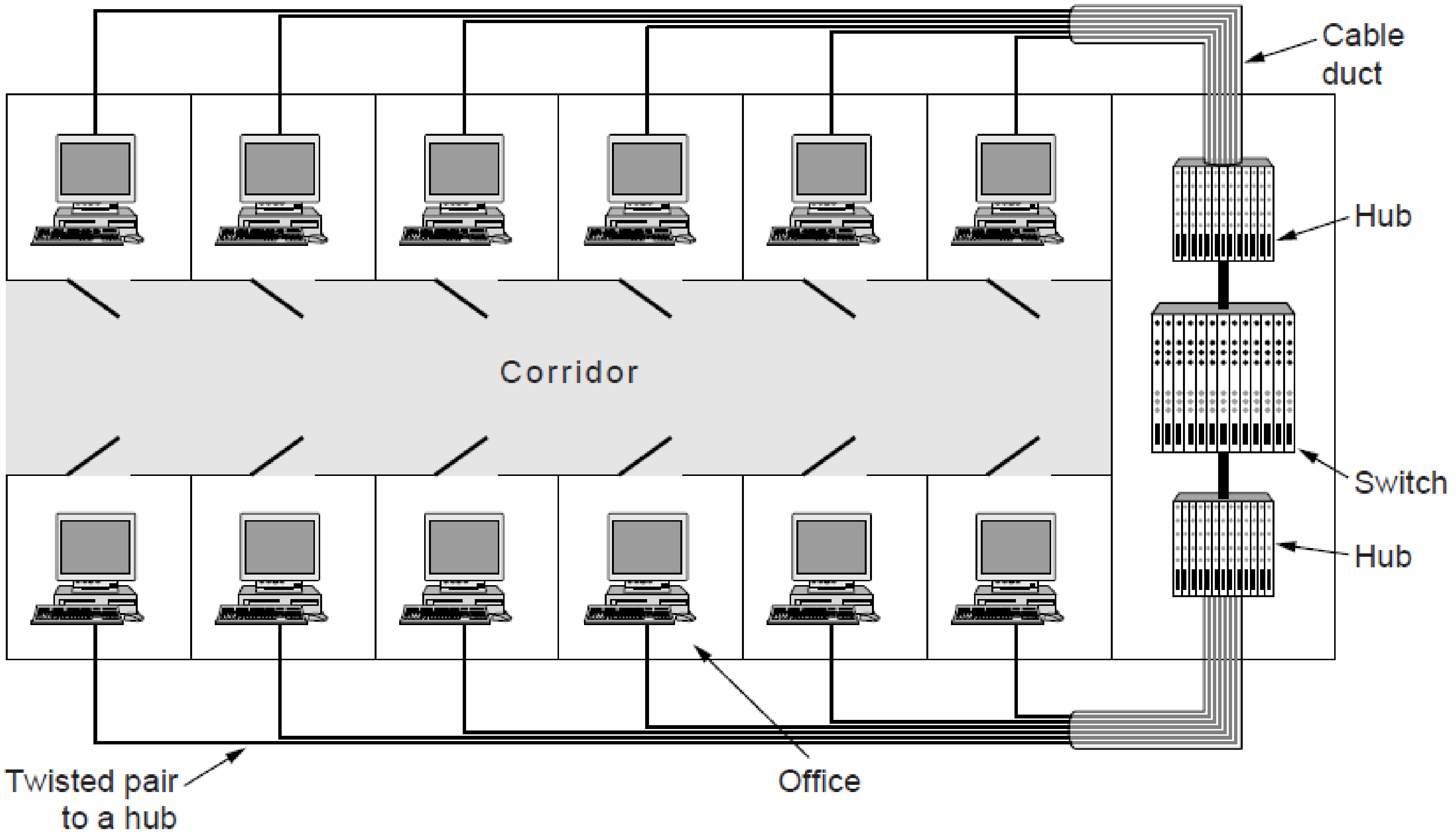
Data Link Layer Switching

- Uses of Bridges »
- Learning Bridges »
- Spanning Tree »
- Repeaters, hubs, bridges, .., routers, gateways »
- Virtual LANs »

Uses of Bridges

Common setup is a building with centralized wiring

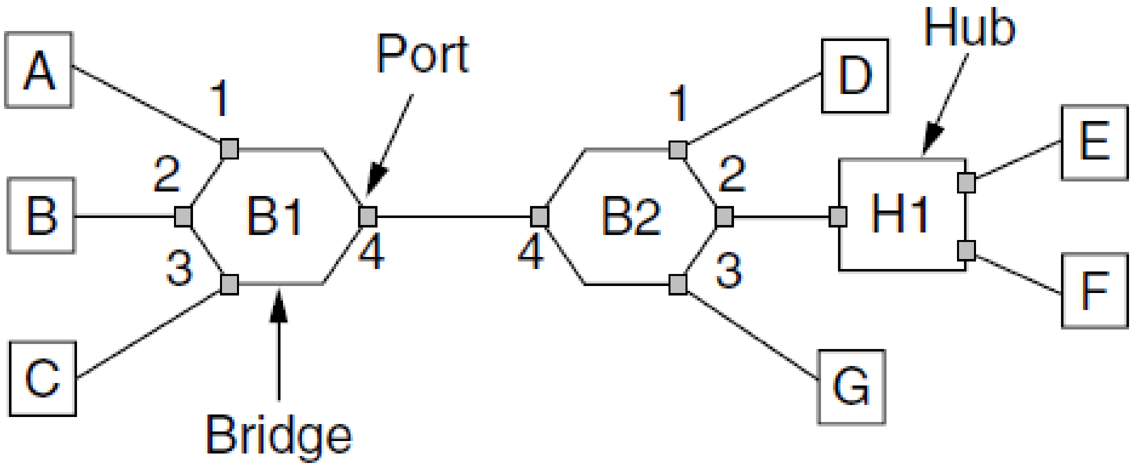
- Bridges (switches) are placed in or near wiring closets



Learning Bridges (1)

A bridge operates as a switched LAN (not a hub)

- Computers, bridges, and hubs connect to its ports



Learning Bridges (2)

Backward learning algorithm picks the output port:

- Associates source address on frame with input port
- Frame with destination address sent to learned port
- Unlearned destinations are sent to all other ports

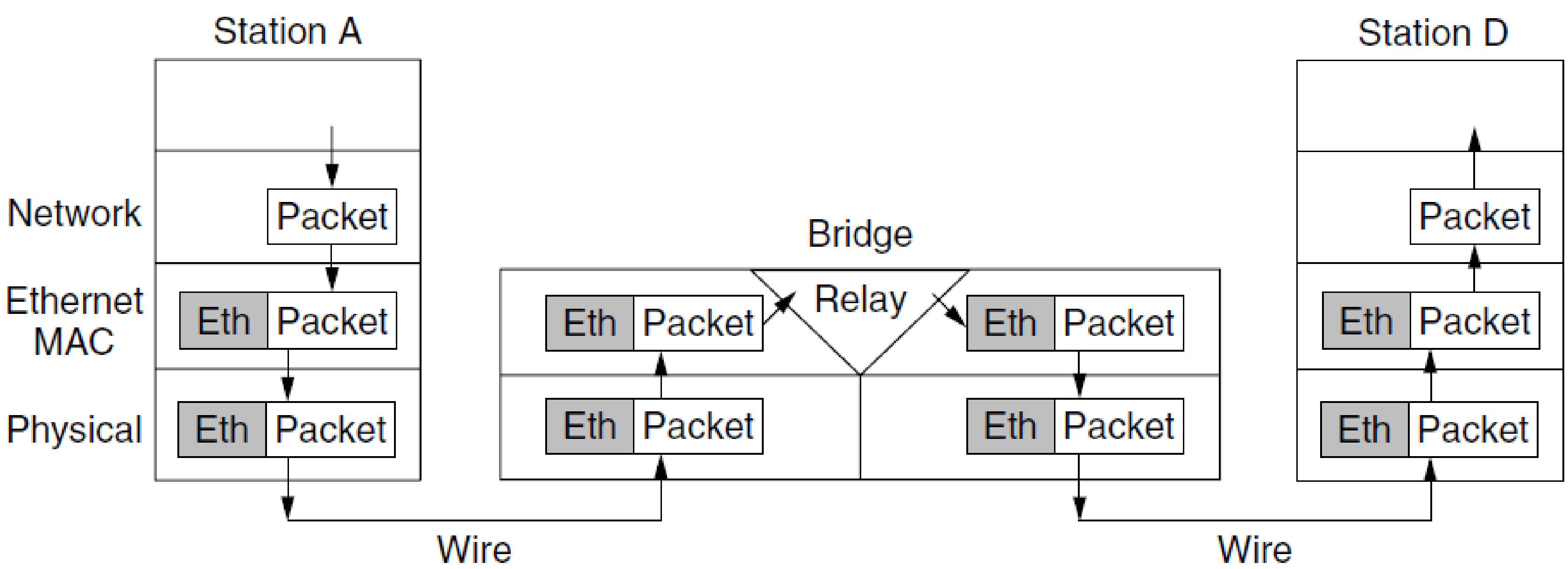
Needs no configuration

- Forget unused addresses to allow changes
- Bandwidth efficient for two-way traffic

Learning Bridges (3)

Bridges extend the Link layer:

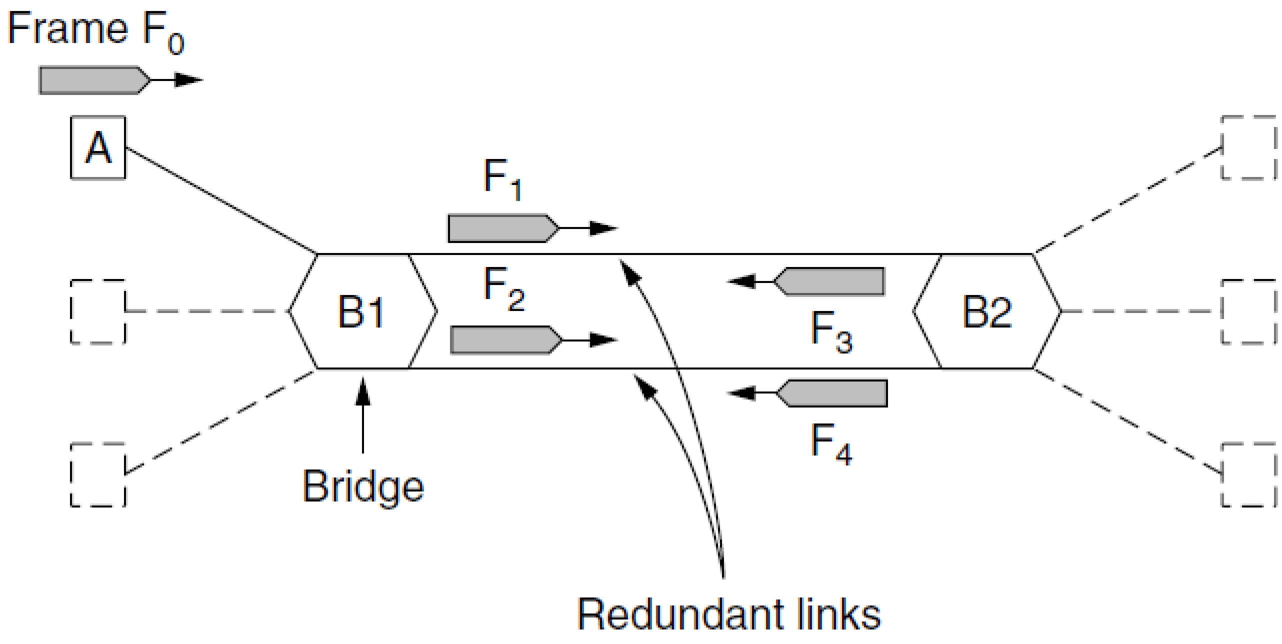
- Use but don't remove Ethernet header/addresses
- Do not inspect Network header



Spanning Tree (1) – Problem

Bridge topologies with loops and only backward learning will cause frames to circulate for ever

- Need spanning tree support to solve problem



Spanning Tree (2) – Algorithm

- Subset of forwarding ports for data is use to avoid loops
- Selected with the spanning tree distributed algorithm by Perlman

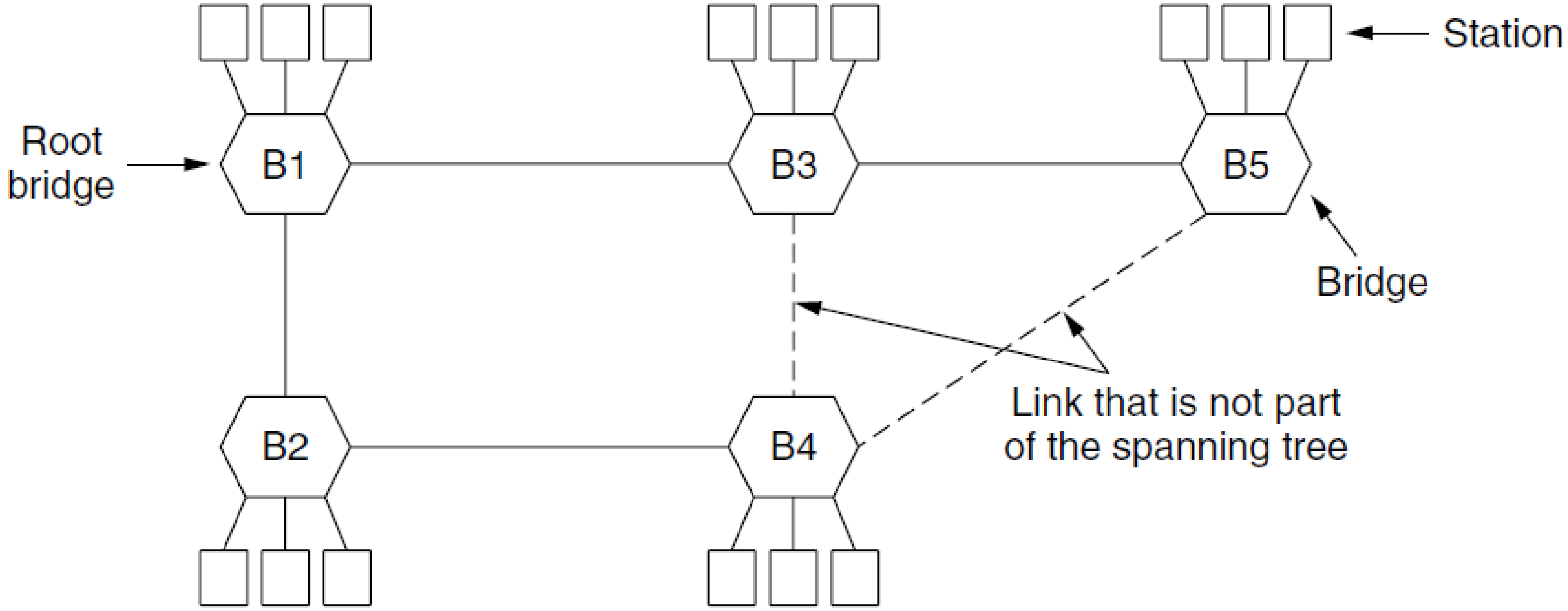
I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths are placed.
A mesh is made by folks like me
Then bridges find a spanning tree.

– Radia Perlman, 1985.

Spanning Tree (3) – Example

After the algorithm runs:

- B1 is the root, two dashed links are turned off
- B4 uses link to B2 (lower than B3 also at distance 1)
- B5 uses B3 (distance 1 versus B4 at distance 2)



Repeaters, Hubs, Bridges, Switches, Routers, & Gateways

Devices are named according to the layer they process

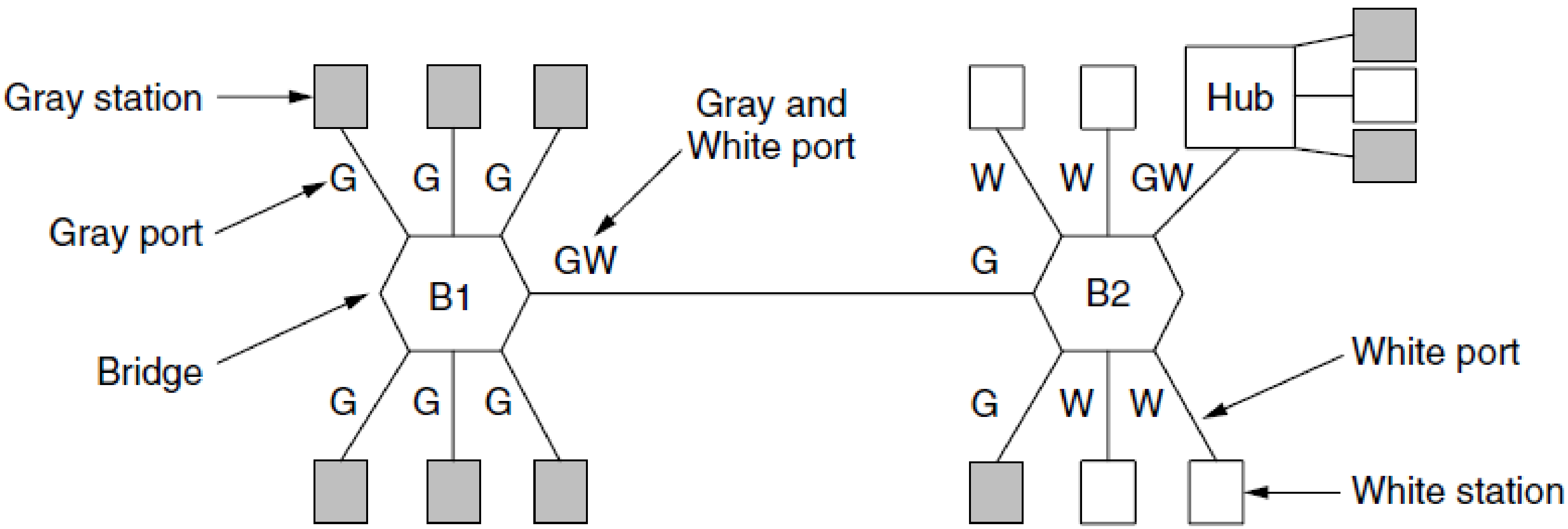
- A bridge or LAN switch operates in the Link layer

Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, switch
Physical layer	Repeater, hub

Virtual LANs (1)

VLANs (Virtual LANs) splits one physical LAN into multiple logical LANs to ease management tasks

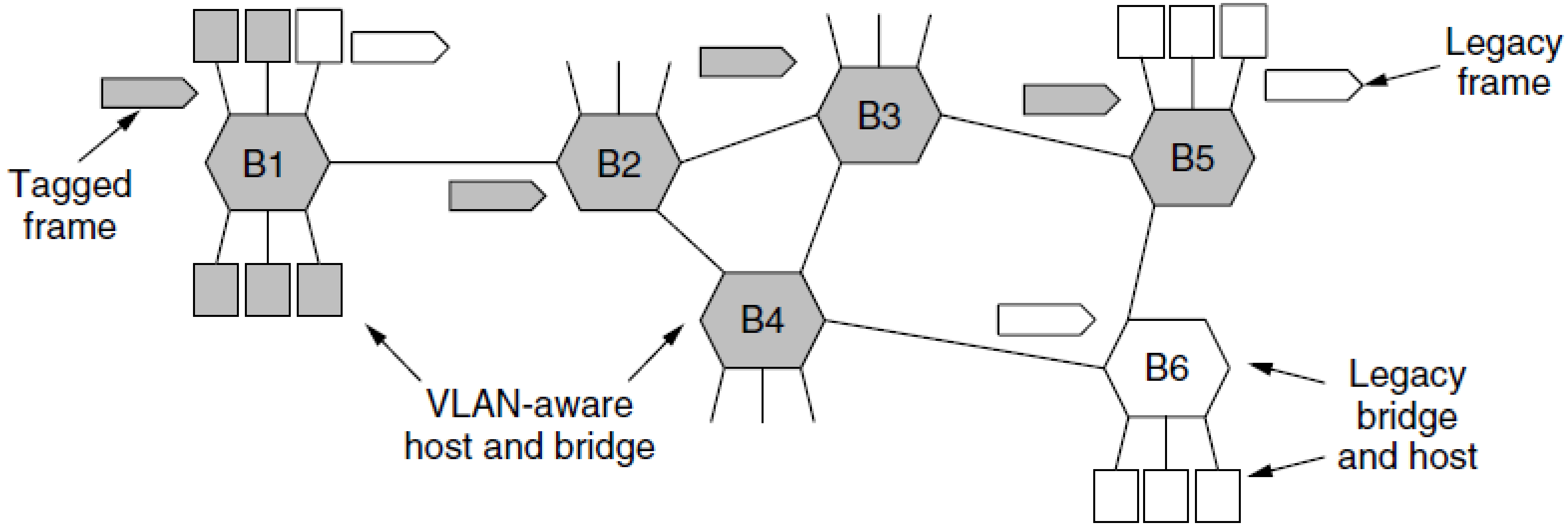
- Ports are “colored” according to their VLAN



Virtual LANs (2) – IEEE 802.1Q

Bridges need to be aware of VLANs to support them

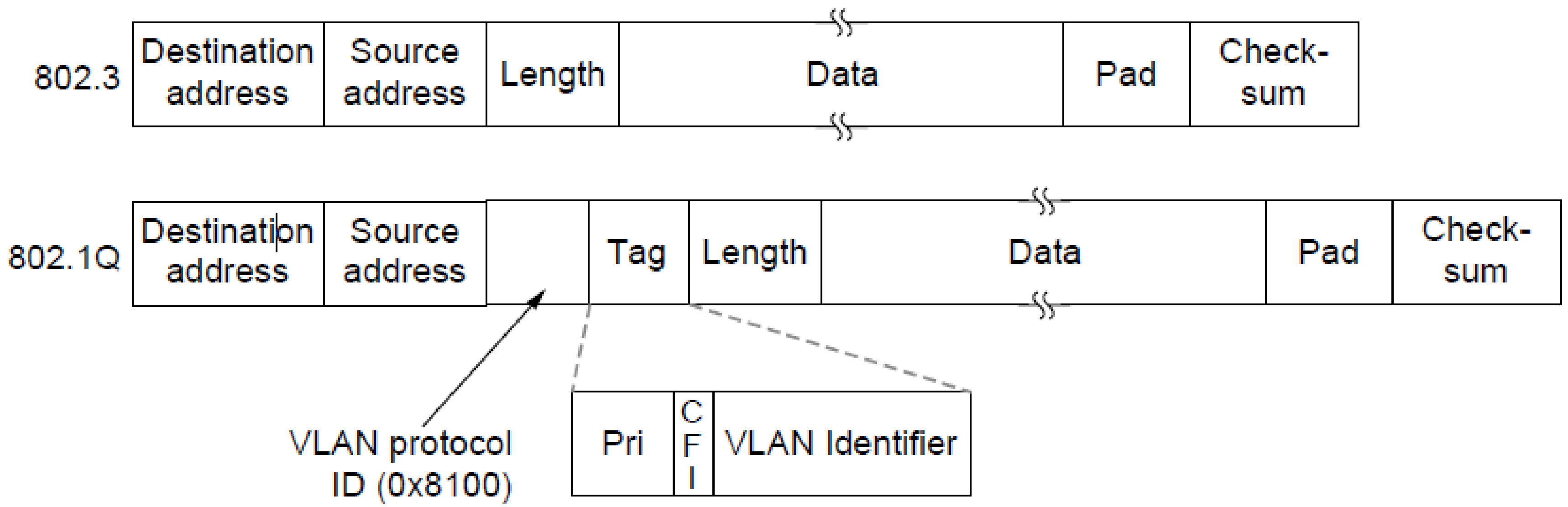
- In 802.1Q, frames are tagged with their “color”
- Legacy switches with no tags are supported



Virtual LANs (3) – IEEE 802.1Q

802.1Q frames carry a color tag (VLAN identifier)

- Length/Type value is 0x8100 for VLAN protocol



End

Chapter 4