CSMC 417

Computer Networks

Prof. Ashok K Agrawala

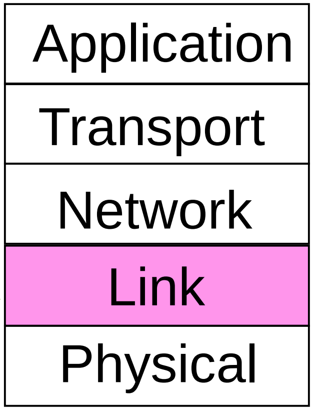
The Medium Access Control Sublayer

Medium Access Control Sublayer

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

The MAC Sublayer

- Responsible for deciding who sends next on a multi-access link
  - An important part of the link layer, especially for



MAC is in here!

The Channel Allocation Problem

- Static Channel Allocation in LANs and MANs
- Dynamic Channel Allocation in LANs and MANs

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

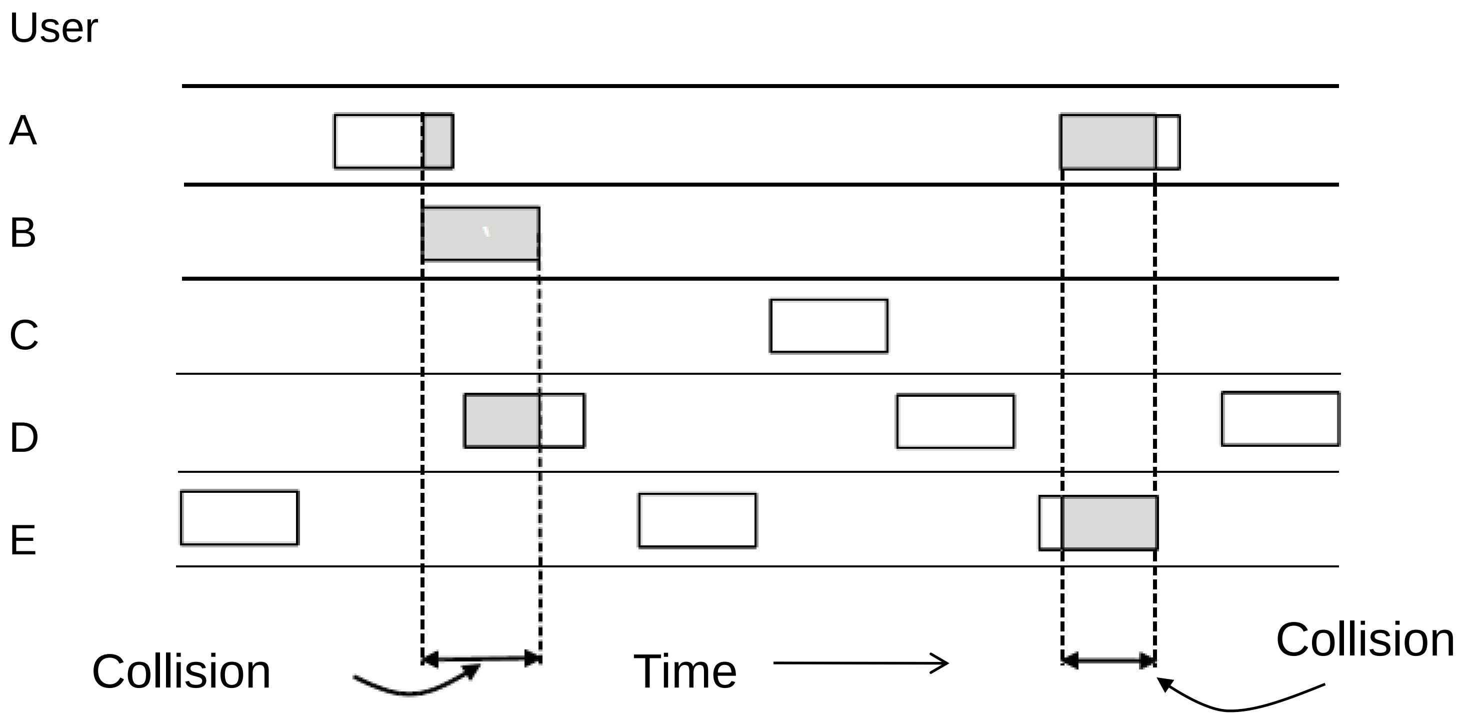
Random Access Protocols

- When node has packet to send
  - Transmit at full channel data rate R.
  - No a priori coordination among nodes
- Two or more transmitting nodes → “collision”,
- Random access MAC protocol specifies:
  - How to detect collisions
  - How to recover from collisions
- Examples
  - ALOHA and Slotted ALOHA
  - CSMA, CSMA/CD, CSMA/CA

Key Ideas of Random Access

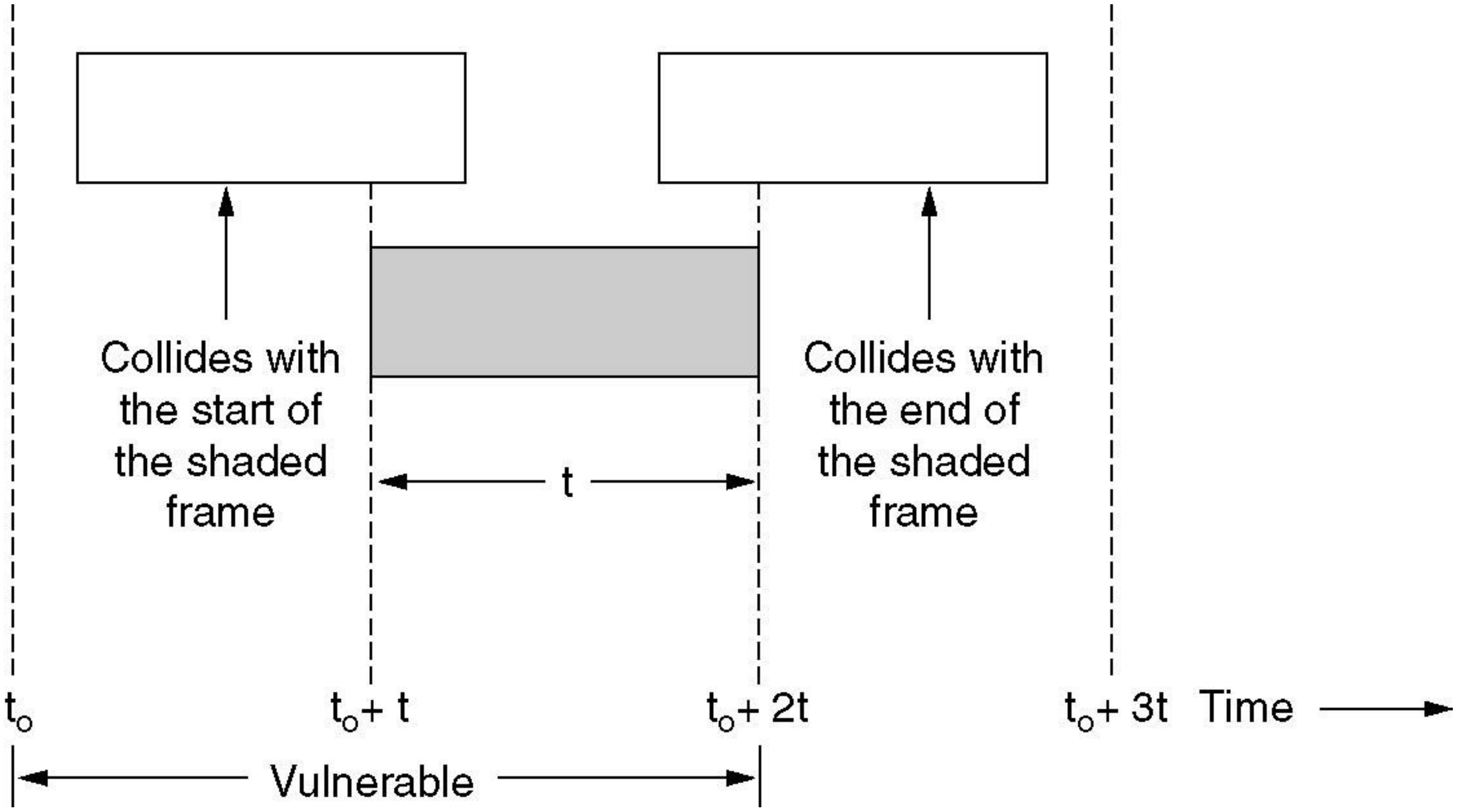
- Carrier sense
  - *Listen before speaking, and don’t interrupt*
  - Checking if someone else is already sending data
  - … and waiting till the other node is done
- Collision detection
  - *If someone else starts talking at the same time, stop*
  - Realizing when two nodes are transmitting at once
  - …by detecting that the data on the wire is garbled
- Randomness
  - *Don’t start talking again right away*
  - Waiting for a random time before trying again

ALOHA (1)

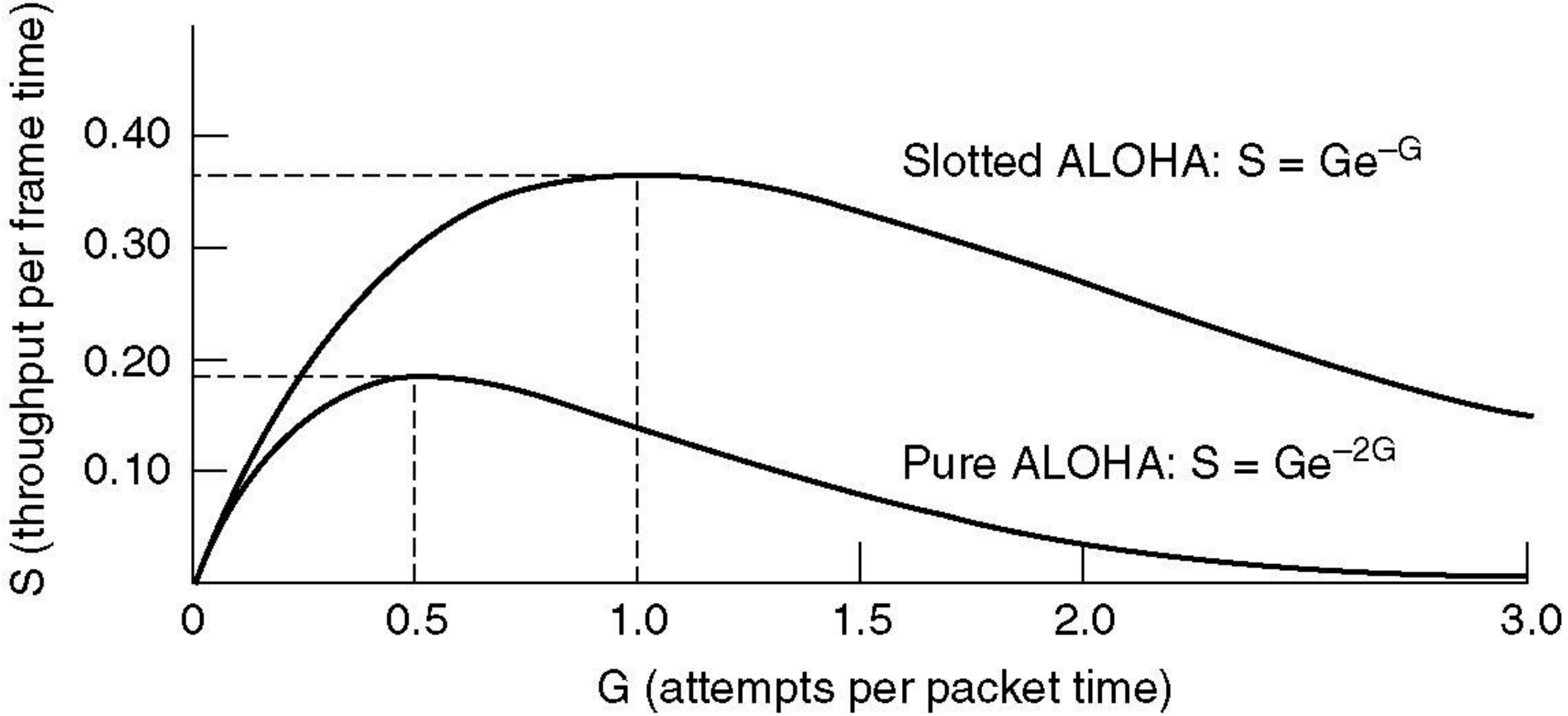


In pure ALOHA, frames are transmitted at completely arbitrary times

Pure ALOHA (2)


Collides with the start of the shaded frame
Collides with the end of the shaded frame
t
t_o
t_o+ t
t_o+ 2t
t_o+ 3t
Time
Vulnerable

Pure ALOHA (3)


S (throughput per frame time)
0.40
0.30
0.20
0.10
Slotted ALOHA: $S = Ge^{-G}$
Pure ALOHA: $S = Ge^{-2G}$
0
0.5
1.0
1.5
2.0
3.0
G (attempts per packet time)

Slotted ALOHA

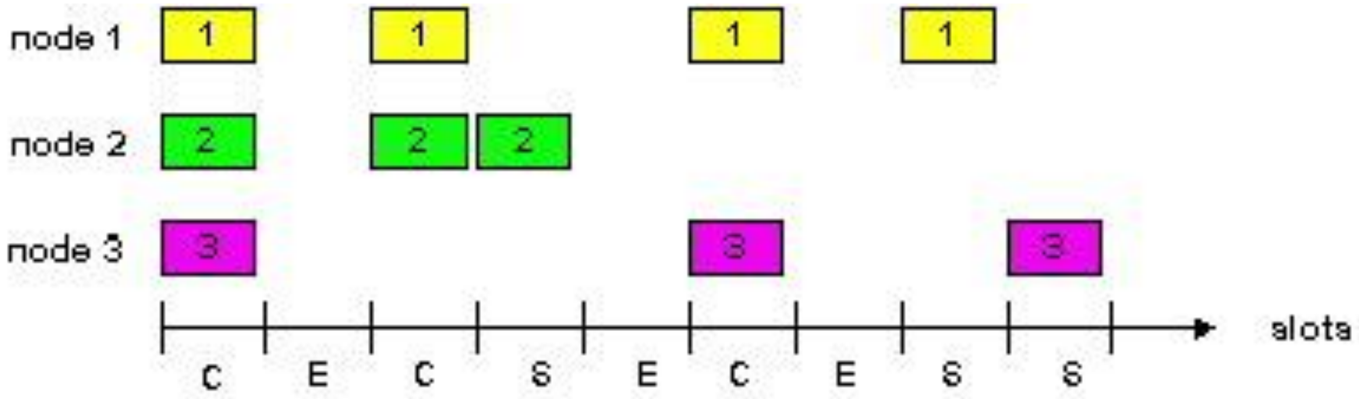
Assumptions

- All frames same size
- Time divided into equal slots (time to transmit a frame)
- Nodes start to transmit frames only at start of slots
- Nodes are synchronized
- If two or more nodes transmit, all nodes detect collision

Operation

- When node obtains fresh frame, transmits in next slot
- No collision: node can send new frame in next slot
- Collision: node retransmits frame in each subsequent slot with probability p until success

Slotted ALOHA



Pros

- Single active node can continuously transmit at full rate of channel
- Highly decentralized: only slots in nodes need to be in sync
- Simple

Cons

- Collisions, wasting slots
- Idle slots
- Nodes may be able to detect collision in less than time to transmit packet
- Clock synchronization

CSMA (Carrier Sense Multiple Access)

- Collisions hurt the efficiency of ALOHA protocol
  - At best, channel is useful 37% of the time

- CSMA: listen before transmit
  - If channel sensed idle: transmit entire frame
  - If channel sensed busy, defer transmission

- Human analogy: don’t interrupt others!

CSMA (1)

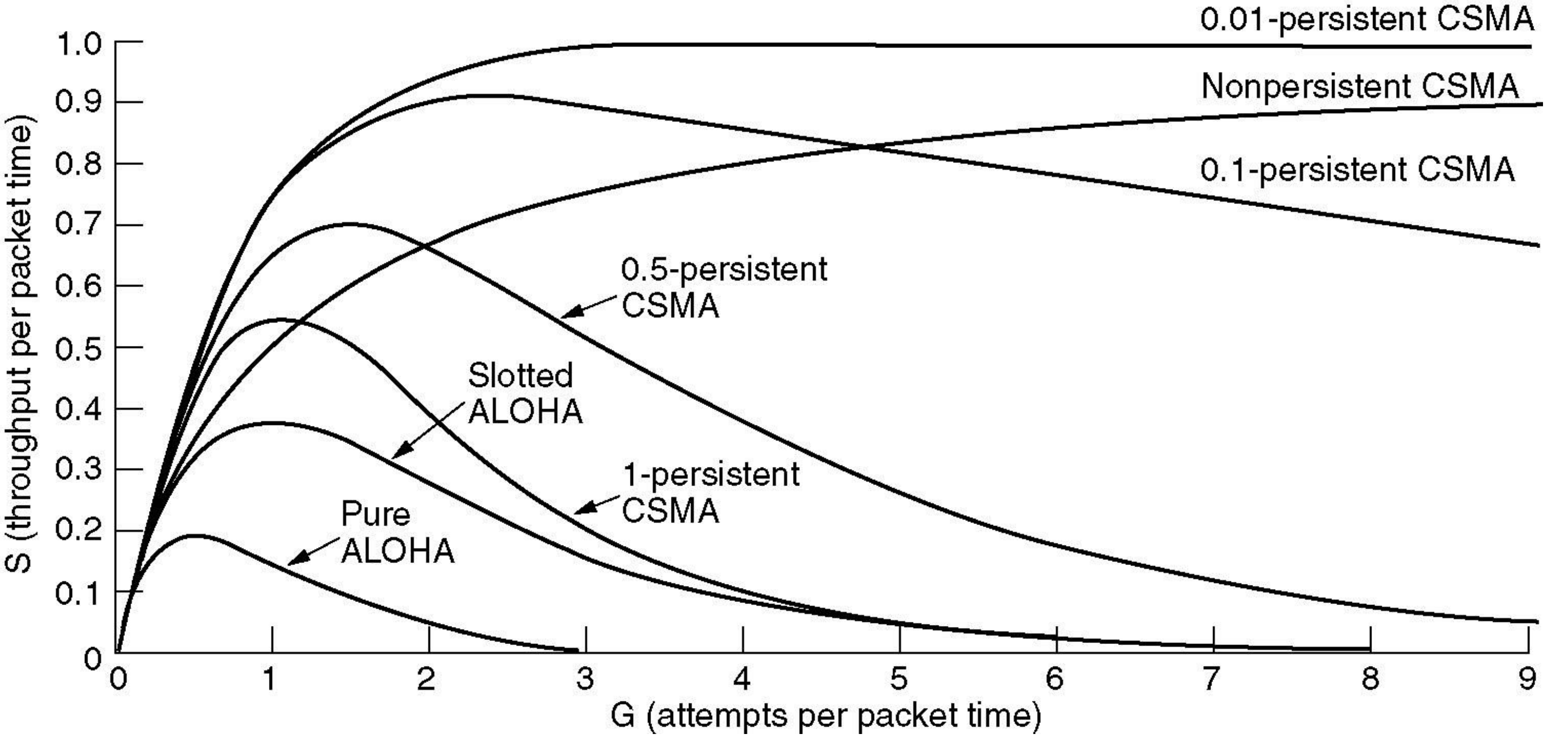
CSMA improves on ALOHA by sensing the channel!

- 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

Persistent and Nonpersistent CSMA



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

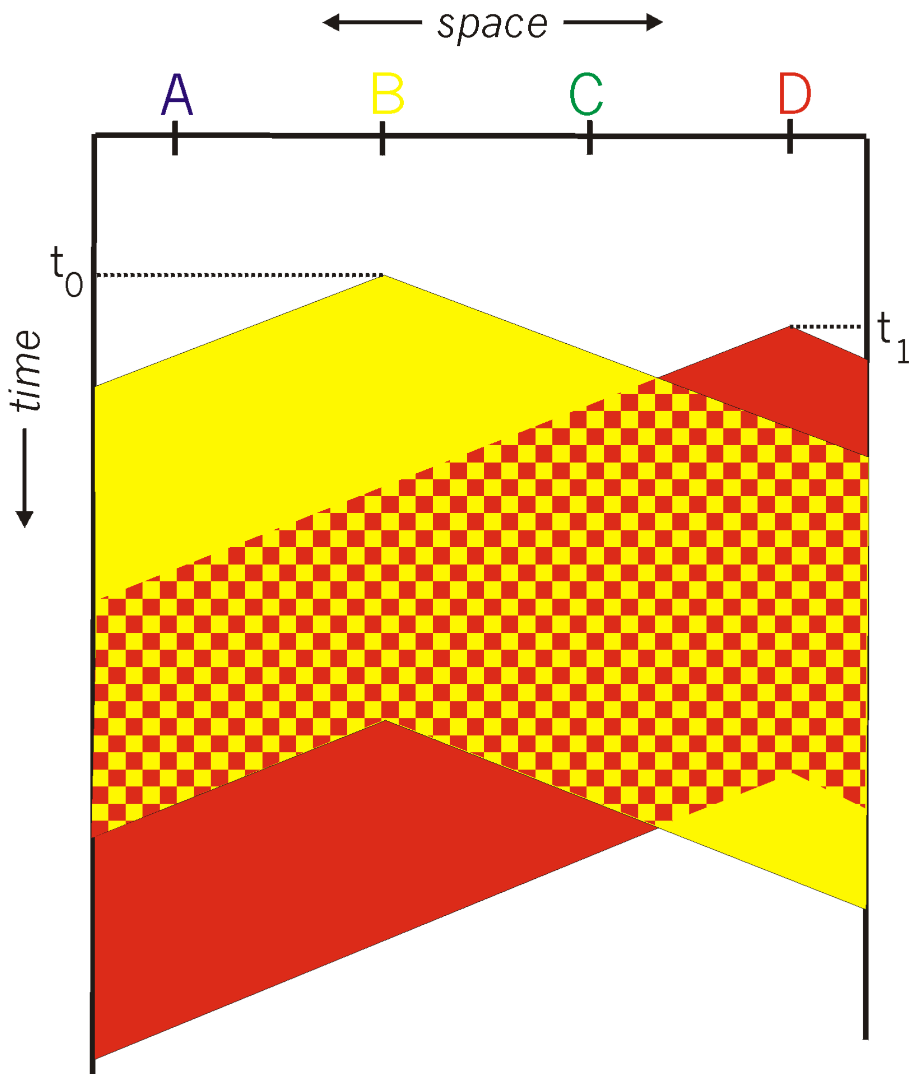
CSMA Collisions

Collisions *can* still occur:

propagation delay means two nodes may not hear each other's transmission

Collision:

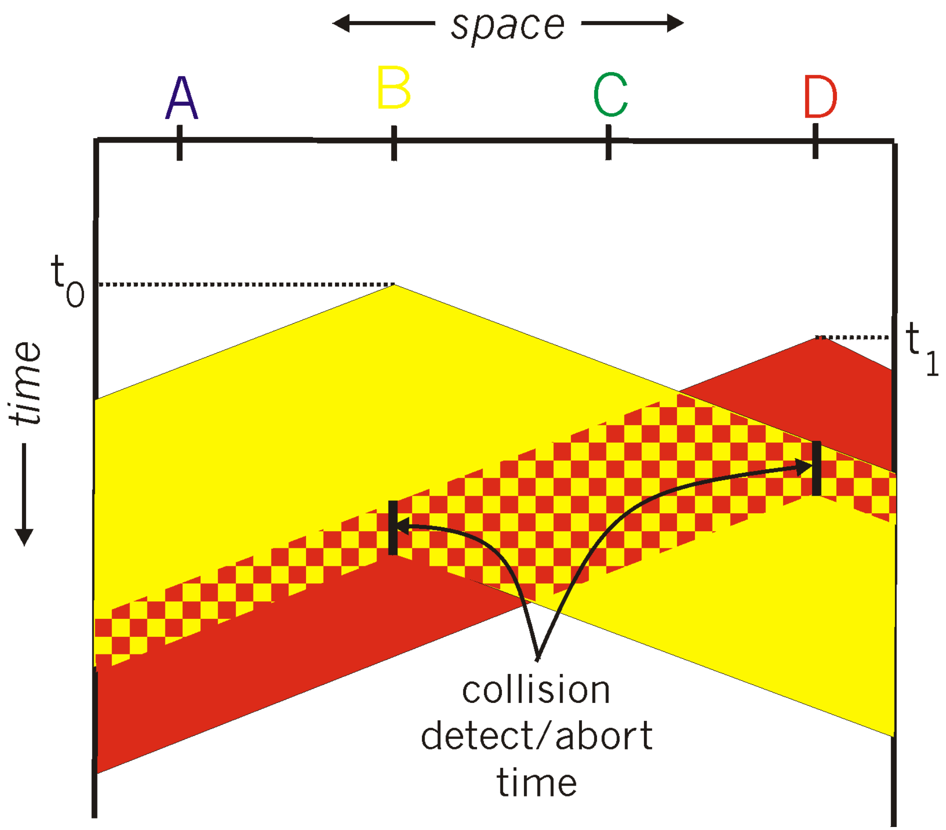
entire packet transmission time wasted



CSMA/CD (Collision Detection)

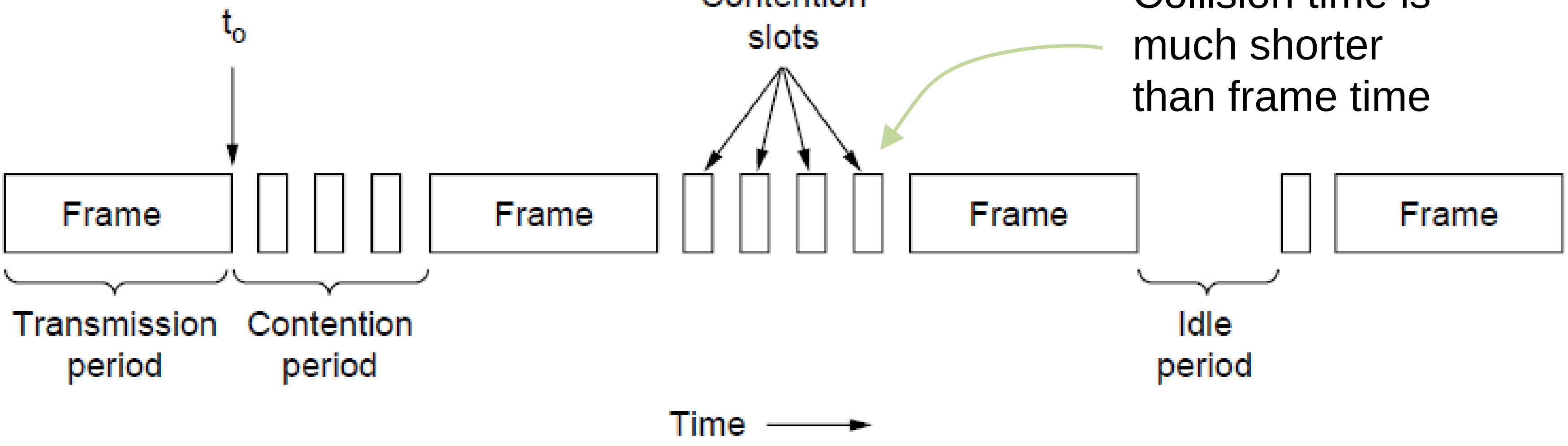
- CSMA/CD: carrier sensing, deferral as in CSMA
  - Collisions detected within short time
  - Colliding transmissions aborted, reducing wastage
- Collision detection
  - Easy in wired LANs: measure signal strengths, compare transmitted, received signals
  - Difficult in wireless LANs: receiver shut off while transmitting
- Human analogy: the polite conversationalist

CSMA/CD Collision Detection



CSMA (3) – Collision Detection

- CSMA/CD improvement is to detect/abort collisions
  - Reduced contention times improve



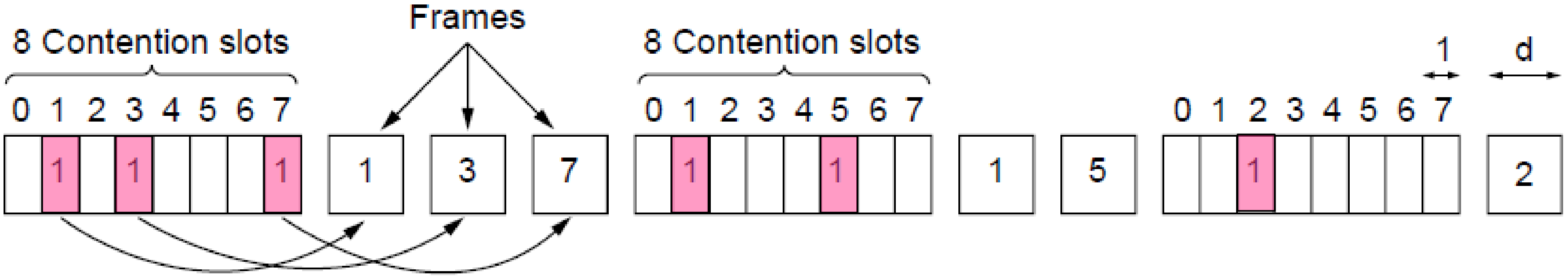
Collision time is much shorter than frame time

Collision-Free Protocols (1) – Bitmap

Collision-free protocols avoid collisions entirely

- Senders must know when it is their turn to send

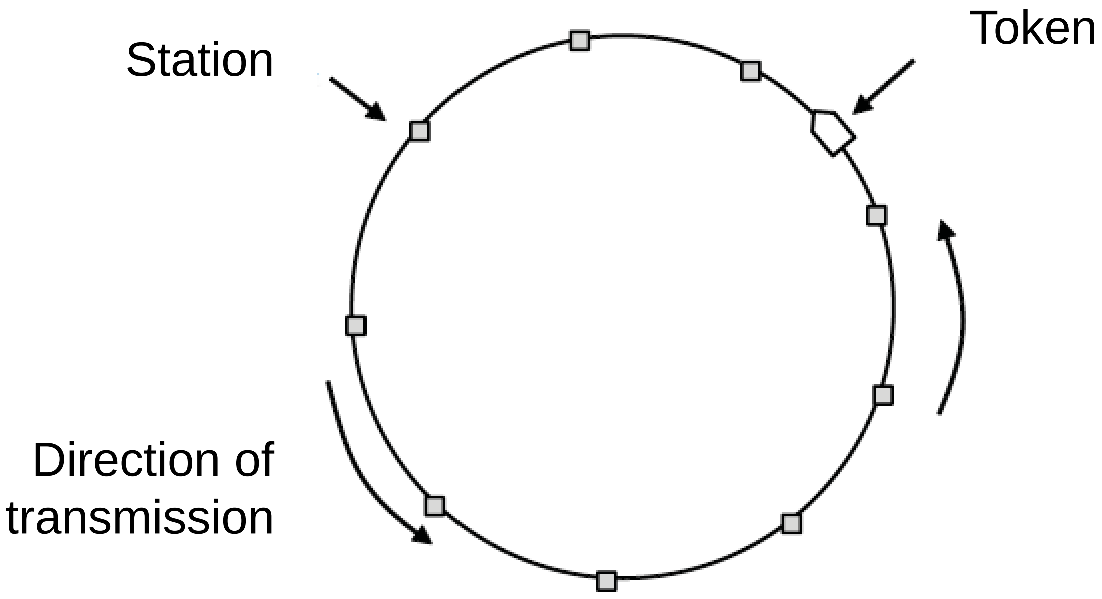
The basic bit-map protocol:



Collision-Free Protocols– Token Ring

Token sent round ring defines the sending order

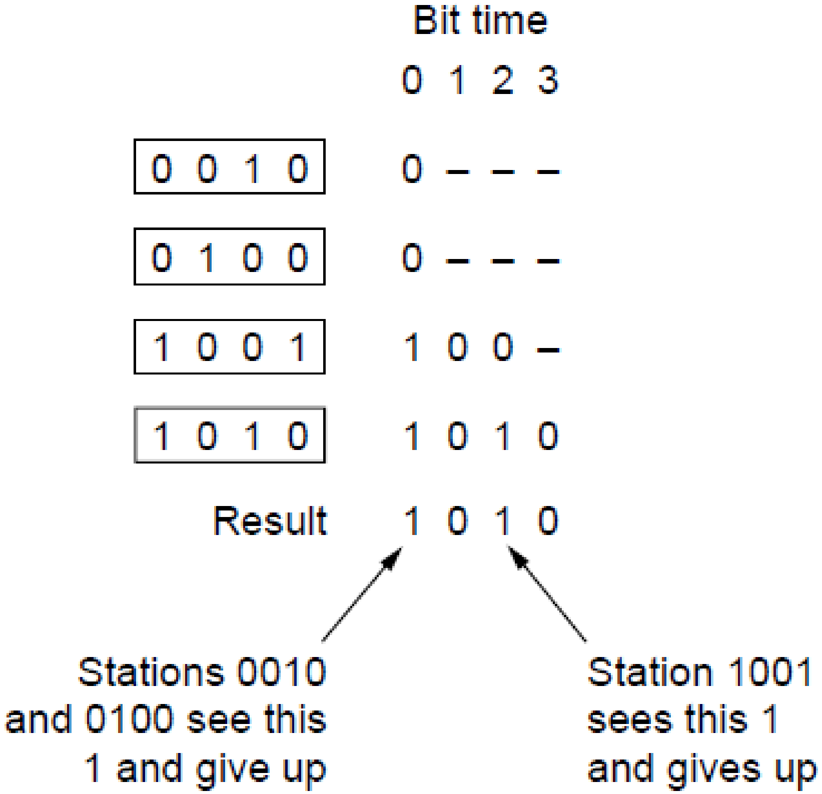
- Station with token may send a frame before passing
- Idea can be used without ring too, e.g., token bus



Collision-Free Protocols– 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



Bit time

	0	1	2	3
0 0 1 0	0	–	–	–
0 1 0 0	0	–	–	–
1 0 0 1	1	0	0	–
1 0 1 0	1	0	1	0
Result	1	0	1	0

Stations 0010 and 0100 see this 1 and give up

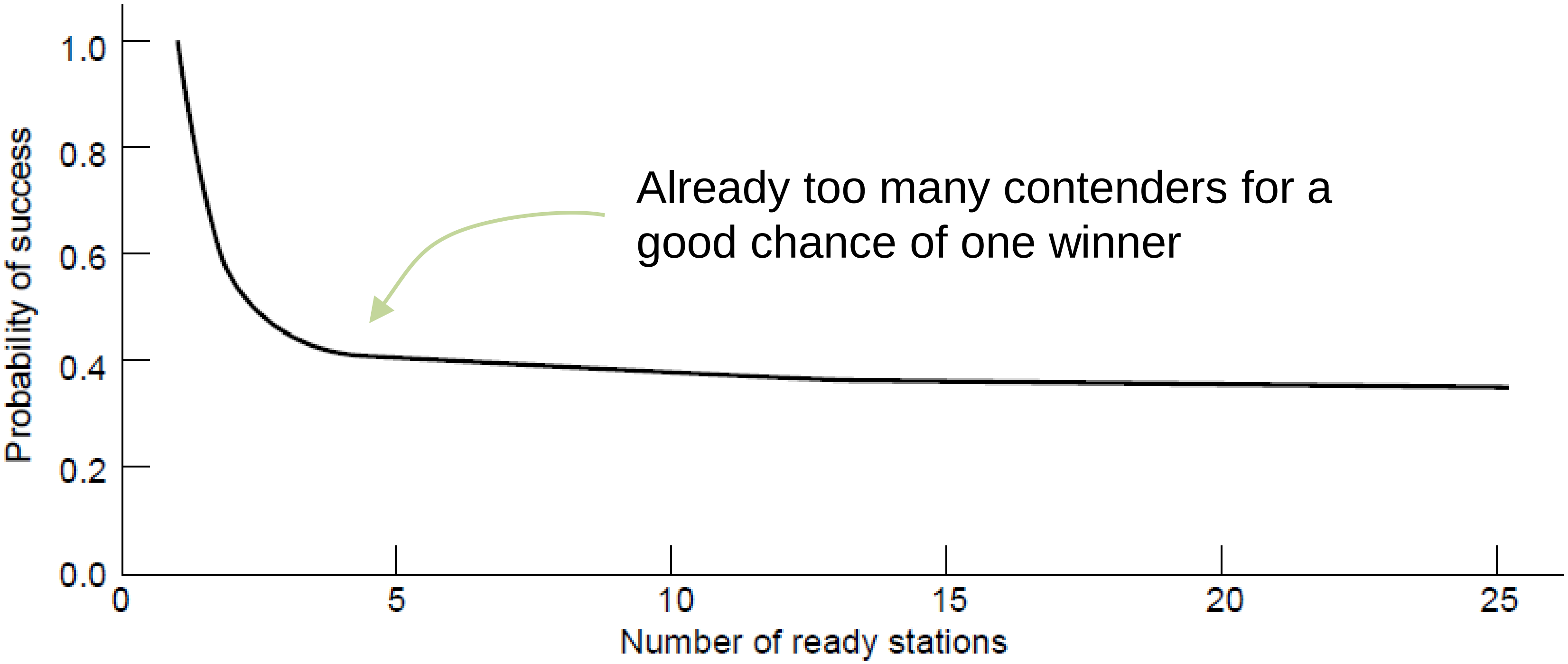
Station 1001 sees this 1 and gives up

Analysis of Contention

- k stations, always ready to transmit
- Assume constant retransmission probability p
- Probability, A that some station acquires channel during a given slot
- $A = kp(1-p)^{k-1}$
- Optimal value of p – differentiate w.r.t. p and equate to 0
  - $p = \frac{1}{k}$ then optimal $A = [\frac{k-1}{k}]^{k-1}$
  - As k → ∞ $p \rightarrow \frac{1}{e}$

Limited-Contention Protocols (1)

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

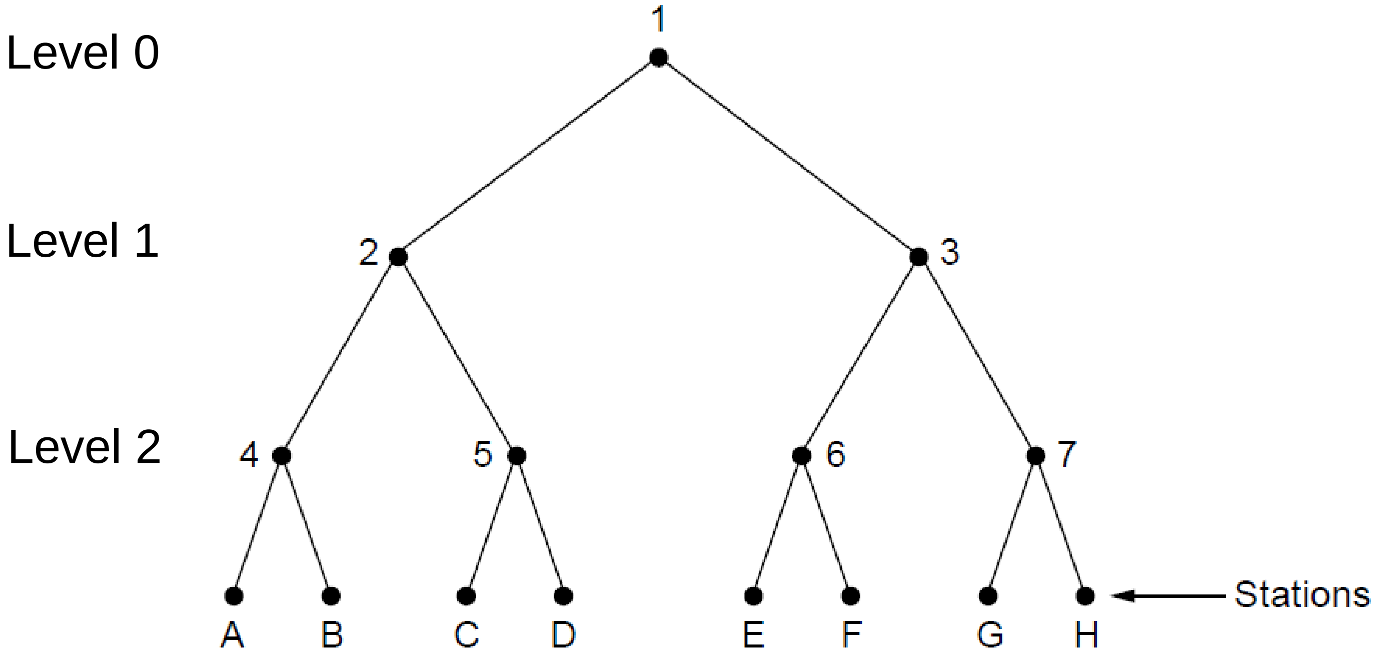


Already too many contenders for a good chance of one winner

Limited Contention
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

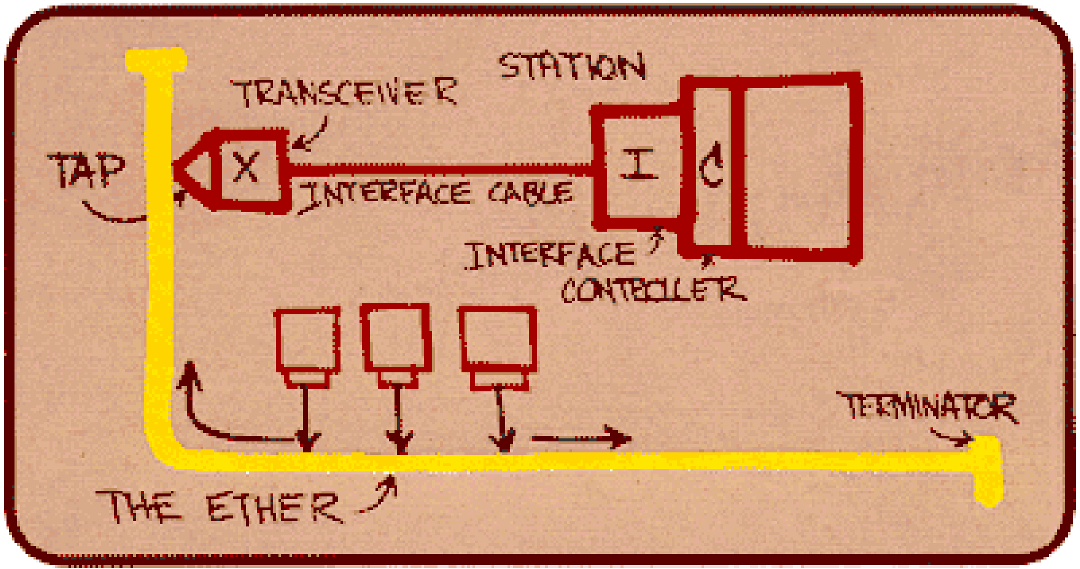


Ethernet

- Ethernet Cabling
- Manchester Encoding
- The Ethernet MAC Sublayer Protocol
- The Binary Exponential Backoff Algorithm
- Ethernet Performance
- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet
- IEEE 802.2: Logical Link Control
- Retrospective on Ethernet

Ethernet

- Dominant wired LAN technology:
- First widely used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10 Mbps – 10 Gbps

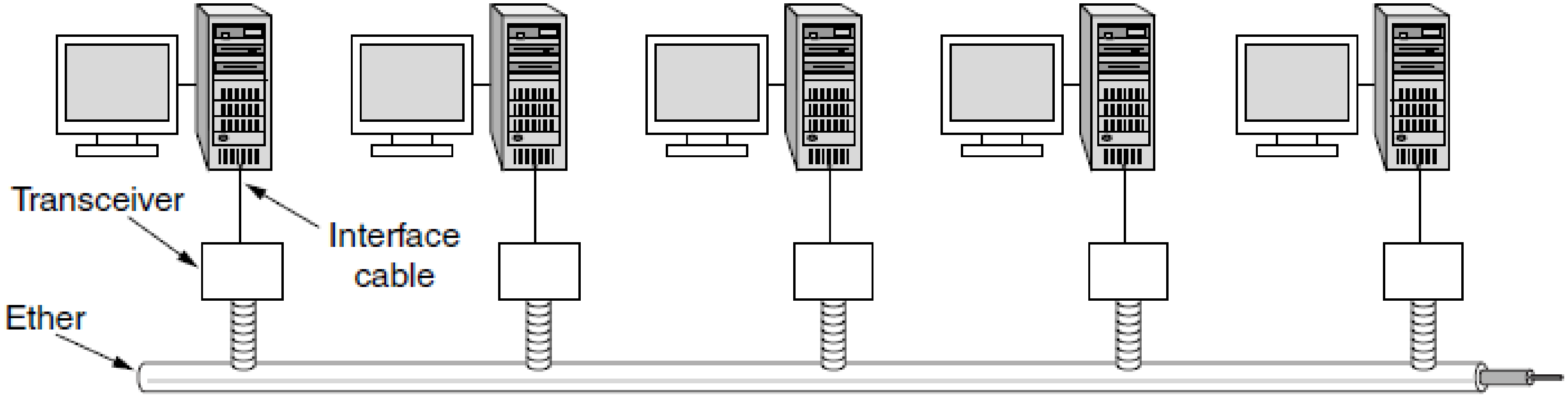


Metcalfe's Ethernet sketch

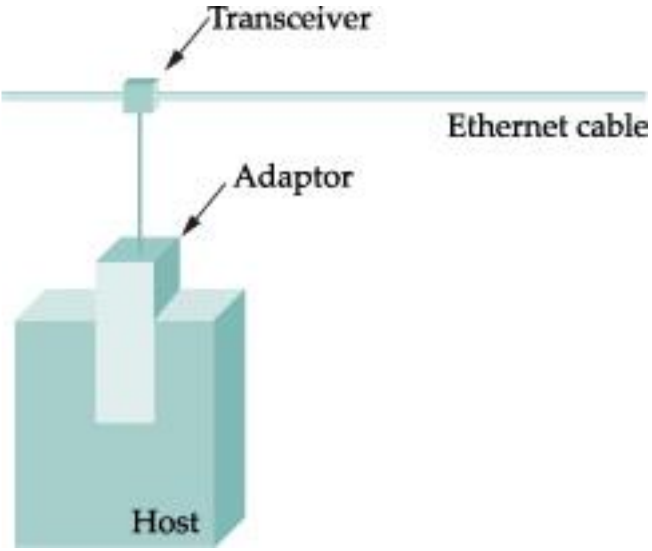
Classic Ethernet– Physical Layer

One shared coaxial cable to which all hosts attached

- Up to 10 Mbps, with Manchester encoding



Ethernet Transceiver and Adapter



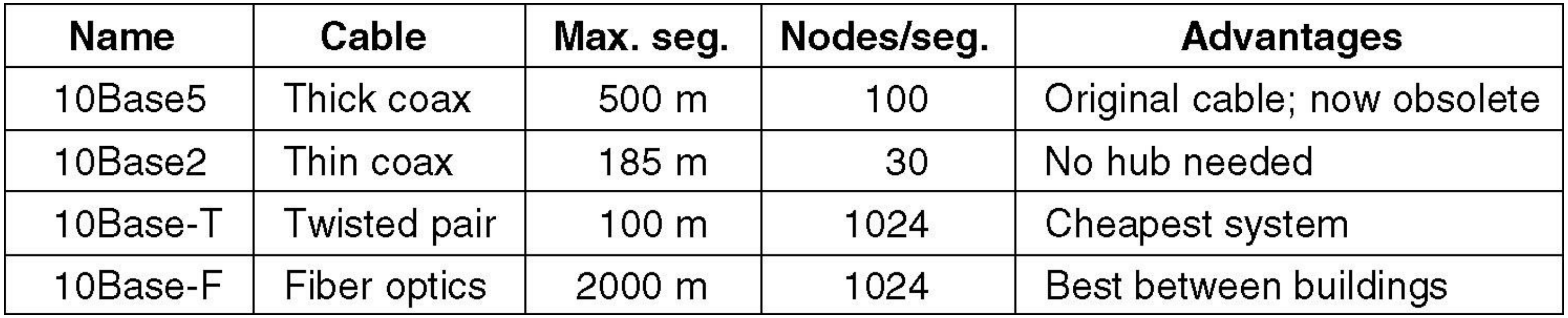
- Medium – 50 ohm cable
- Taps 2.5 m apart
- Transceiver – can send and receive
- Multiple segments can be joined by repeaters – no more than 4
- Max end-to-end distance – 2500 m

Ethernet Uses CSMA/CD

- Carrier sense: wait for link to be idle
  - Channel idle: start transmitting
  - Channel busy: wait until idle
- Collision detection: listen while transmitting
  - No collision: transmission is complete
  - Collision: abort transmission, and send jam signal
- Random access: exponential back-off
  - After collision, wait a random time before trying again
  - After m^{th} collision, choose K randomly from $\{0, …, 2^m-1\}$
  - … and wait for K*512 bit times before trying again

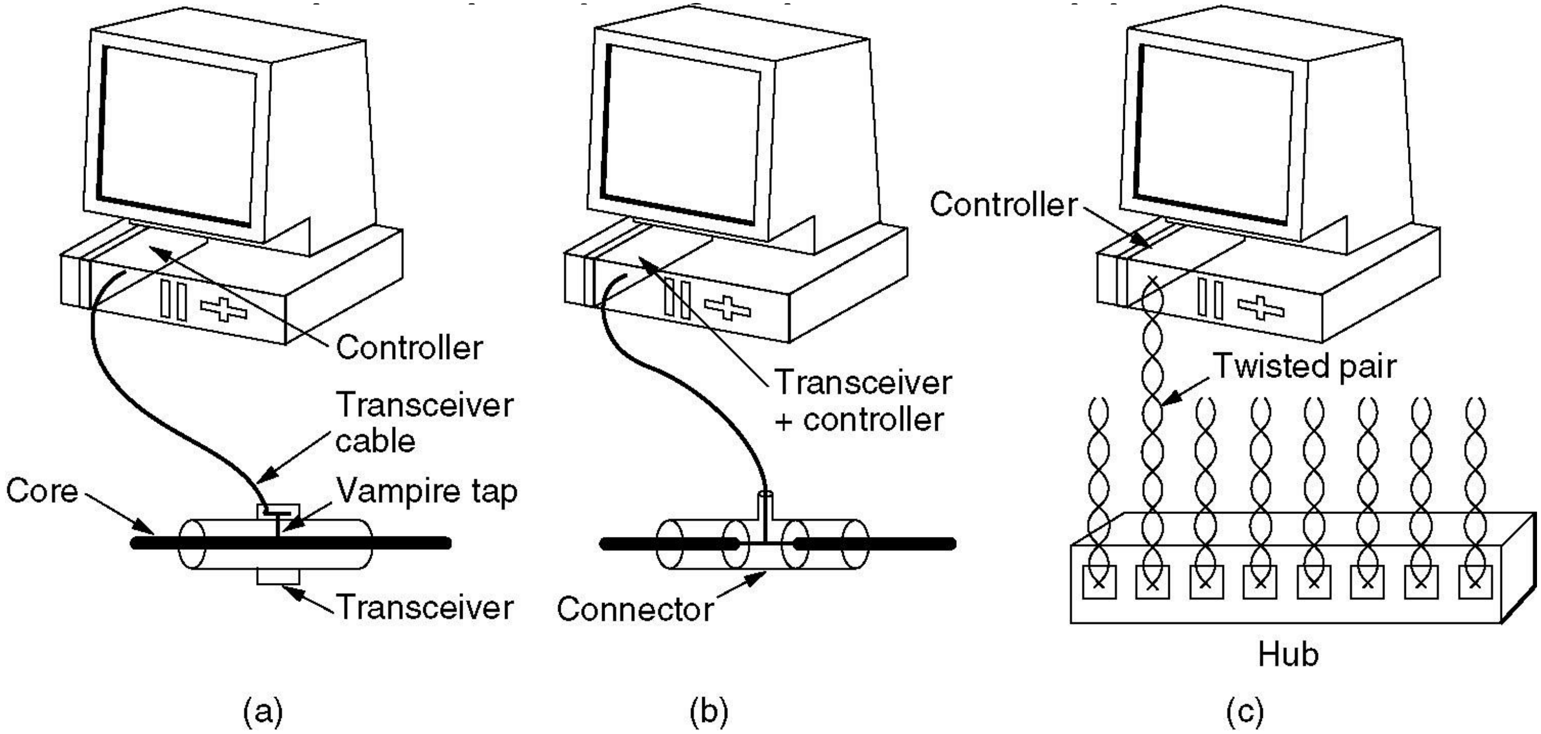
Ethernet Cabling

The most common kinds of Ethernet cabling.



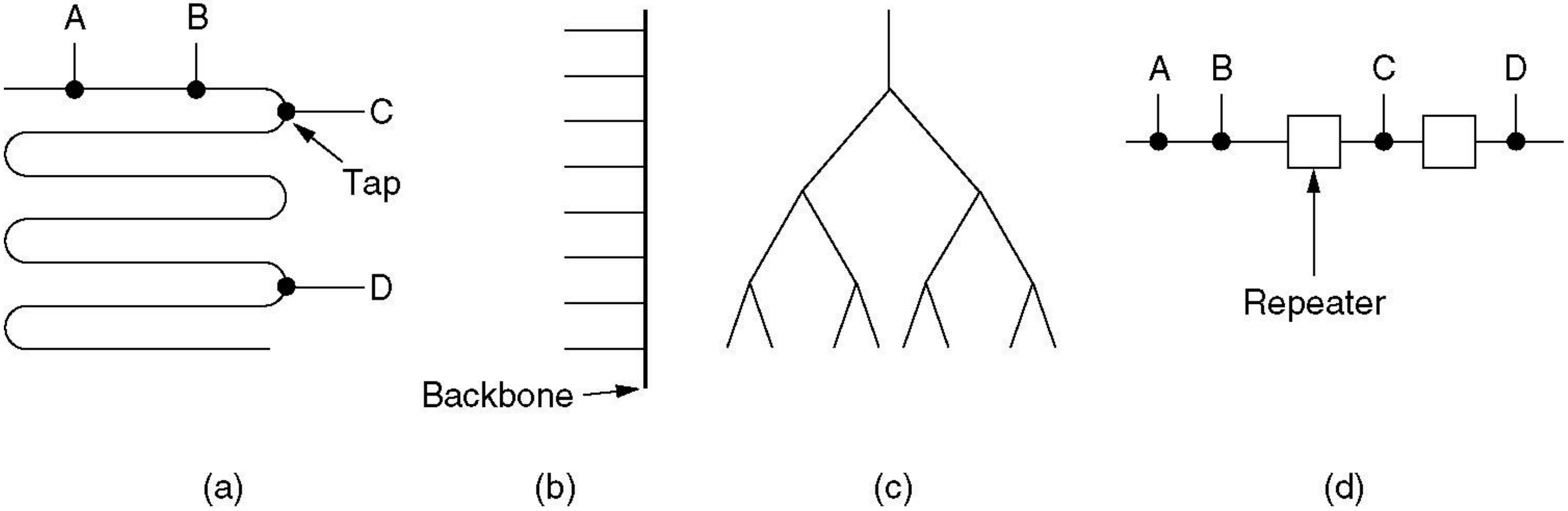
Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Ethernet Cabling (2)

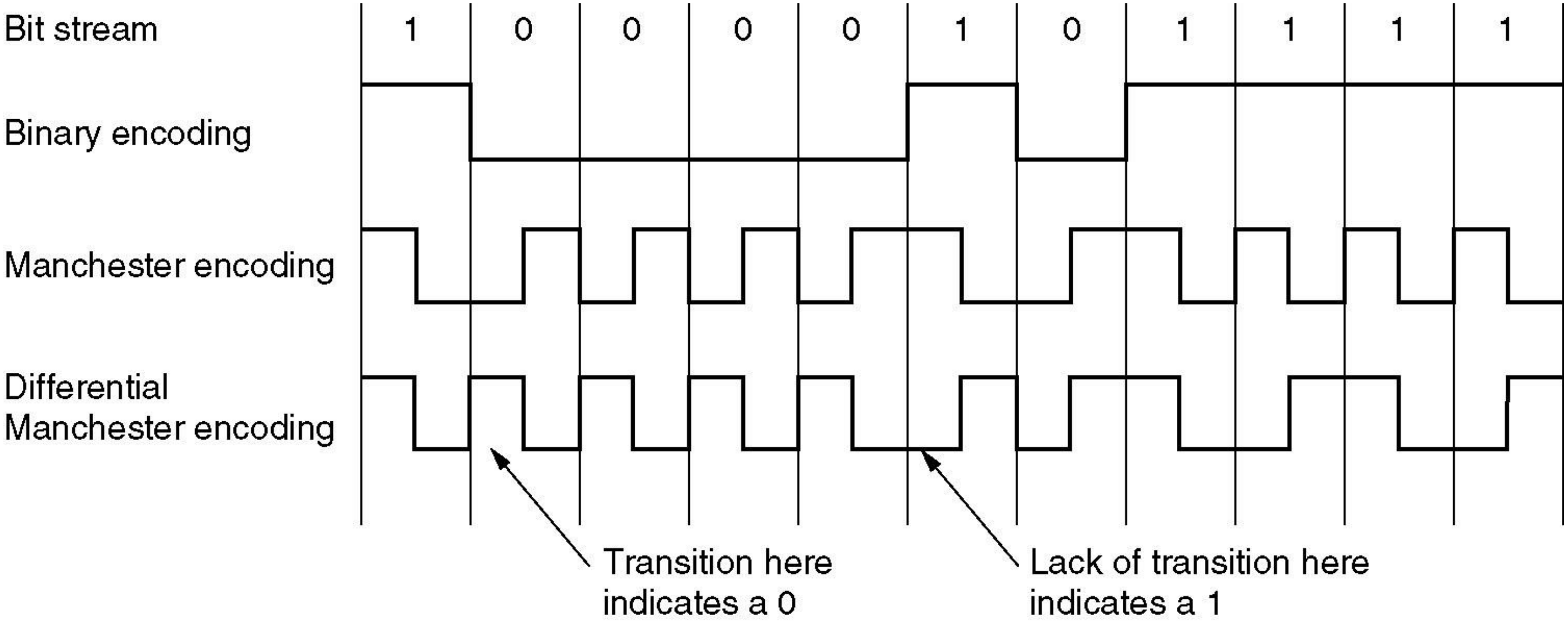


Ethernet Cabling (3)

Cable topologies. (a) Linear, (b) Spine, (c) Tree, (d)

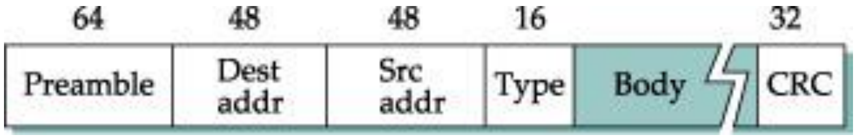


Ethernet Signalling


Bit stream
1
0
0
0
0
1
0
1
1
1
1
Binary encoding
Manchester encoding
Differential Manchester encoding
Transition here indicates a 0
Lack of transition here indicates a 1

(a) Binary encoding, (b) Manchester encoding, (c) Differential Manchester encoding.

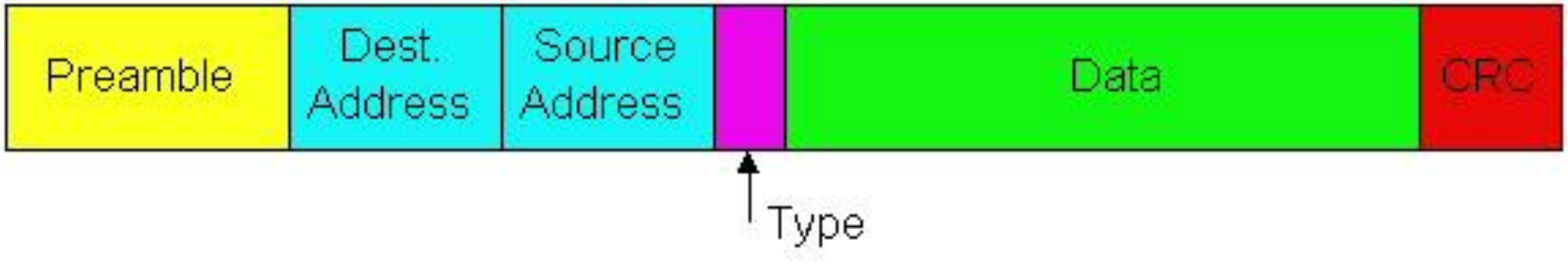
Ethernet Frame Format



- Preamble –
  - For synchronizing
  - Alternate 0 and 1
- Address – 48 bit MAC
- Type – Id for higher level protocol
- Length – up to 1500 bytes, with minimum of 46 bytes, of data
- 802.3 – Length for Type field.

Ethernet Frame Structure

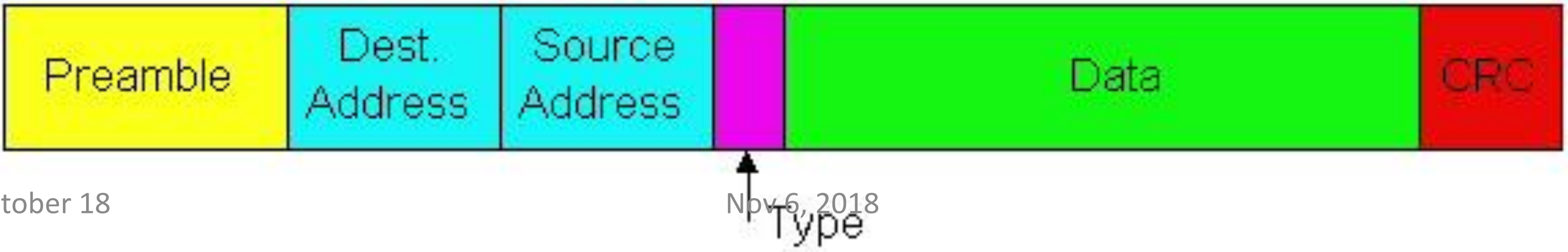
- Sending adapter encapsulates packet in frame



- Preamble: synchronization
  - Seven bytes with pattern 10101010, followed by one byte with pattern 10101011
  - Used to synchronize receiver, sender clock rates

Ethernet Frame Structure (Continued)

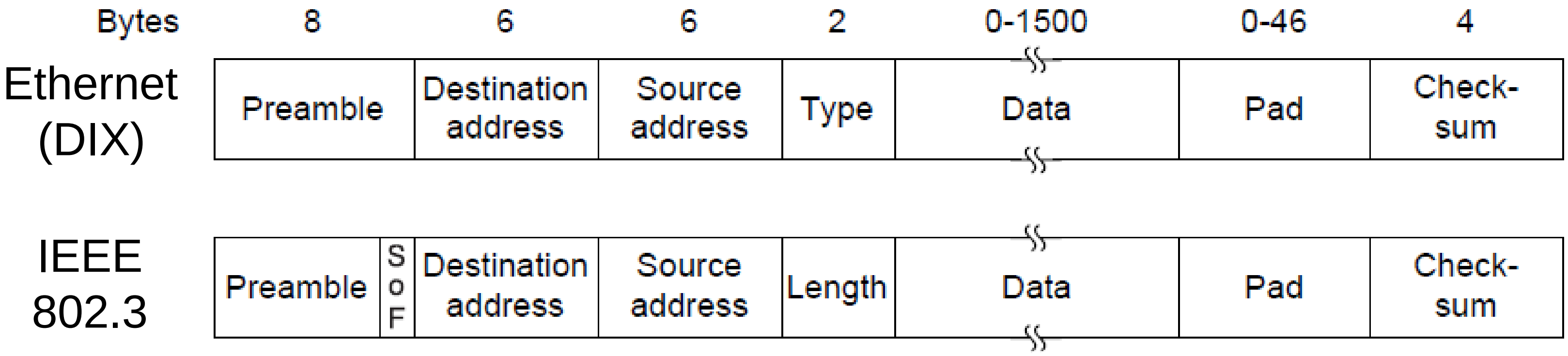
- Addresses: source and destination MAC addresses
  - Adaptor passes frame to network-level protocol
    - If destination address matches the adaptor
    - Or the destination address is the broadcast address
  - Otherwise, adapter discards frame
- Type: indicates the higher layer protocol
  - Usually IP
  - But also Novell IPX, AppleTalk, …
- CRC: cyclic redundancy check
  - Checked at receiver
  - If error is detected, the frame is simply dropped



Classic Ethernet (2) – MAC

MAC protocol is 1-persistent CSMA/CD

- Random Delay (backoff) after collision is computed with BEB (Binary Exponential Backoff)



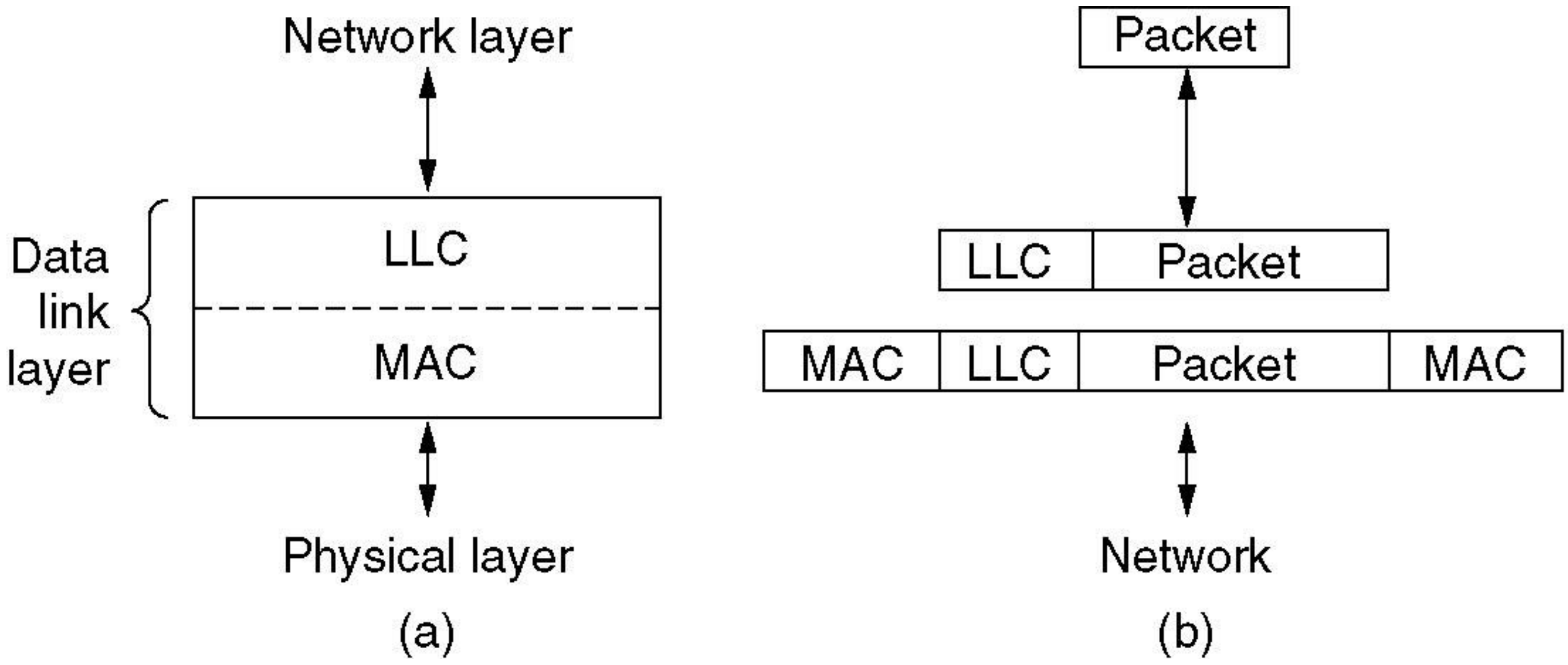
Bytes	8	6	6	2	0-1500	0-46	4
Ethernet (DIX)	Preamble	Destination address	Source address	Type	Data	Pad	Check-sum
IEEE 802.3	Preamble SoF	Destination address	Source address	Length	Data	Pad	Check-sum

Ethernet Transmitter Algorithm

- P-persistent
  - Transmit with prob p when line goes idle
- Ethernet uses 1-persistent algorithm
- On Collision-
  - 32 bit jamming sequence
  - Stops transmitting
  - Runt frame – 64 synch + 32 bit jamming sequence

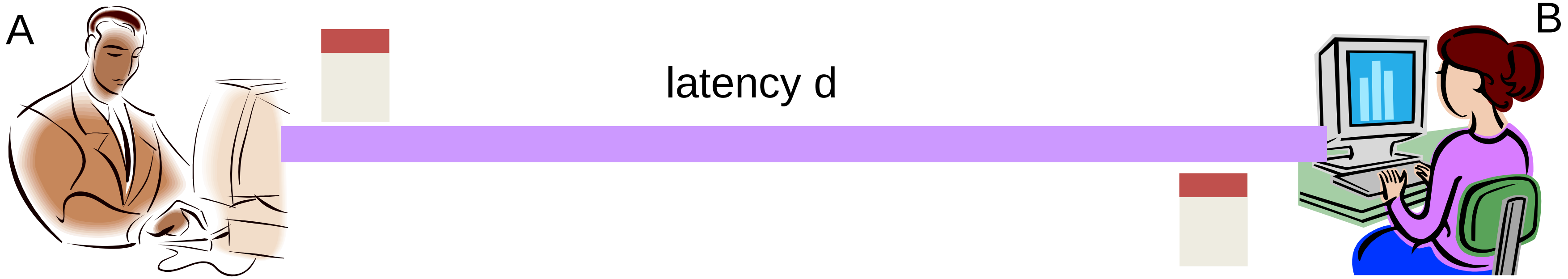
- Min frame size – 64 bytes – 46 + 14 + 4
- For 2500 m line with up to 4 repeaters max round trip delay – 51.2μs
- Exponential Backoff
  - In steps of 51.2μs
  - Wait k* rand (0,.. 2^{k}-1)

IEEE 802.2: Logical Link Control



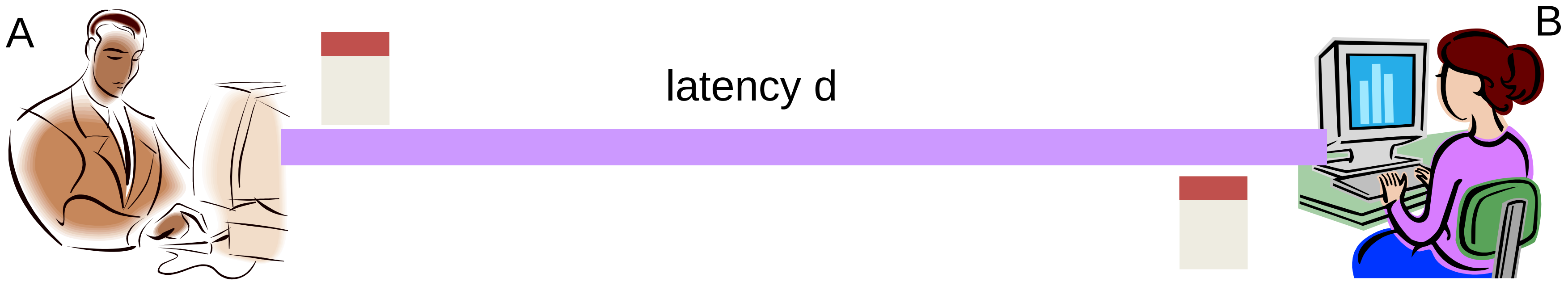
(a) Position of LLC. (b) Protocol formats.

Limitations on Ethernet Length



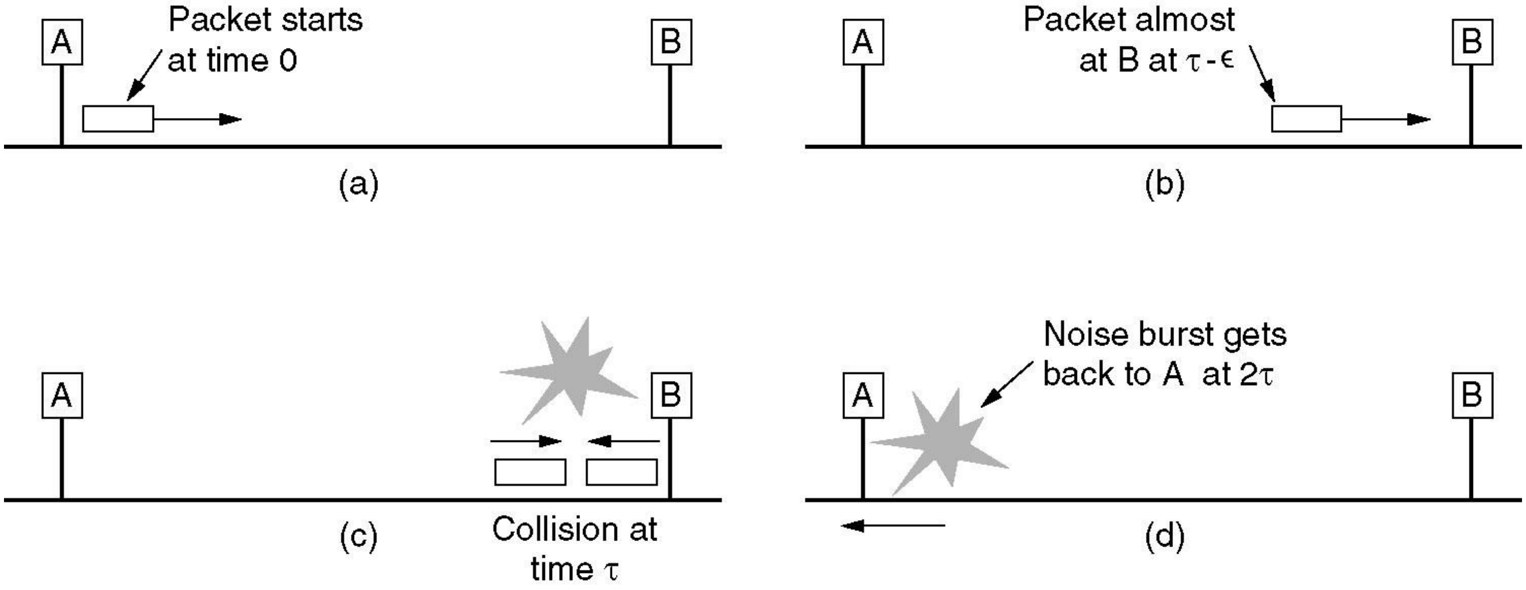
- Latency depends on physical length of link
  - Time to propagate a packet from one end to the other
- Suppose A sends a packet at time t
  - And B sees an idle line at a time just before t+d
  - … so B happily starts transmitting a packet
- B detects a collision, and sends jamming signal
  - But A doesn’t see collision till t+2d

Limitations on Ethernet Length



- A needs to wait for time 2d to detect collision
  - So, A should keep transmitting during this period
  - … and keep an eye out for a possible collision
- Imposes restrictions on Ethernet
  - Maximum length of the wire: 2500 meters
  - Minimum length of the packet: 512 bits (64 bytes)

Ethernet MAC Sublayer Protocol (2)



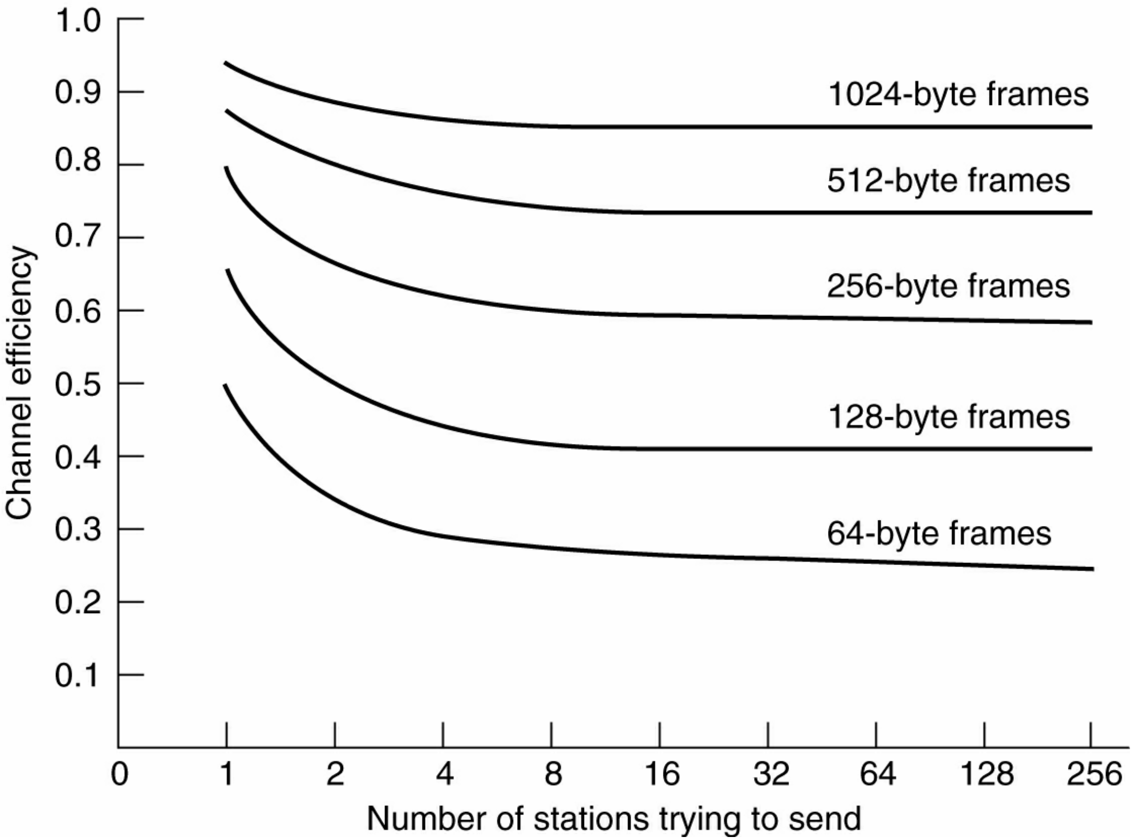
Collision detection can take as long as 2τ.

Ethernet Performance

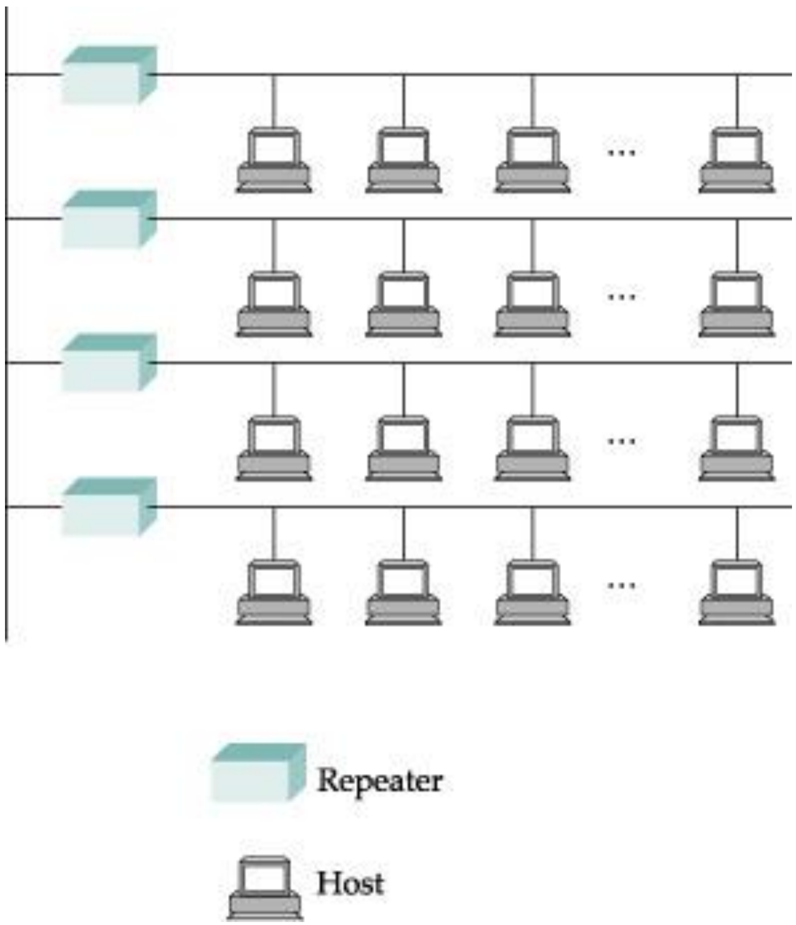
- k stations, always ready to transmit
- Assume constant retransmission probability p
- Probability, A that some station acquires channel during a given slot
- $A = \ kp(1-p)^{k-1}$
- Optimal value of p – differentiate w.r.t. p and equate to 0
  - $p = \frac{1}{k}$ then optimal $A = \ [\frac{k-1}{k}]^{k-1}$
  - As k → ∞ $p \ \rightarrow \ \frac{1}{e}$
- Probability that Contention Interval is exactly j slots is $A(1-A)^{j-1}$
- So, the mean number of slots per contention
  - $\sum_{j=0}^{\infty} jA(1-A)^{j-1} = \frac{1}{A}$
- Slot duration = 2τ
- Mean contention interval $w = \frac{2\tau}{A}$ …. Mean number of cont. slots = e
- If frame transmission time = P
- Channel efficiency $= \frac{P}{P+2\tau/A}$ = $\frac{1}{1+2BLe/cF}$
  - Where F=Frame length, B=network Bandwidth, L = cable length

Ethernet Performance

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



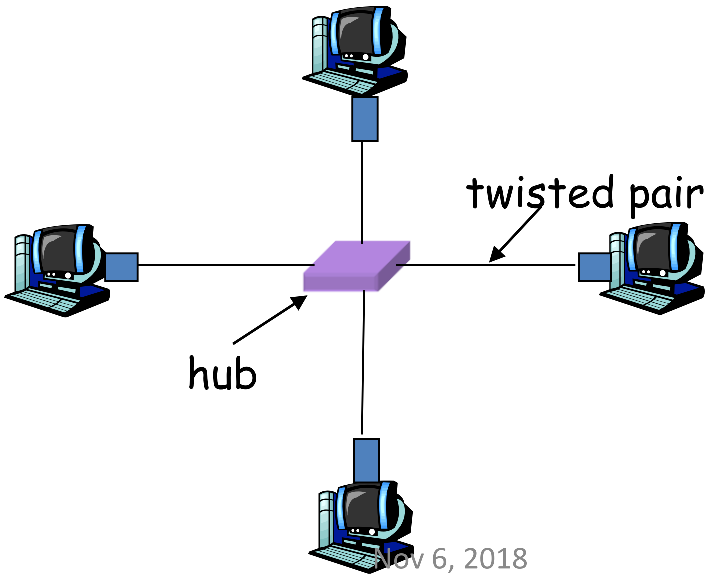
Ethernet Repeaters



- Up to 4 Repeaters
- Cables
  - 10Base 5
    - 10Mbps
    - Baseband
    - 500 Meters
  - 10Base2
  - 10BaseT
    - Twisted Pair 100 M
  - Category 5 (Cat 5)
    - 10 M and 100 M
    - Twisted Pair

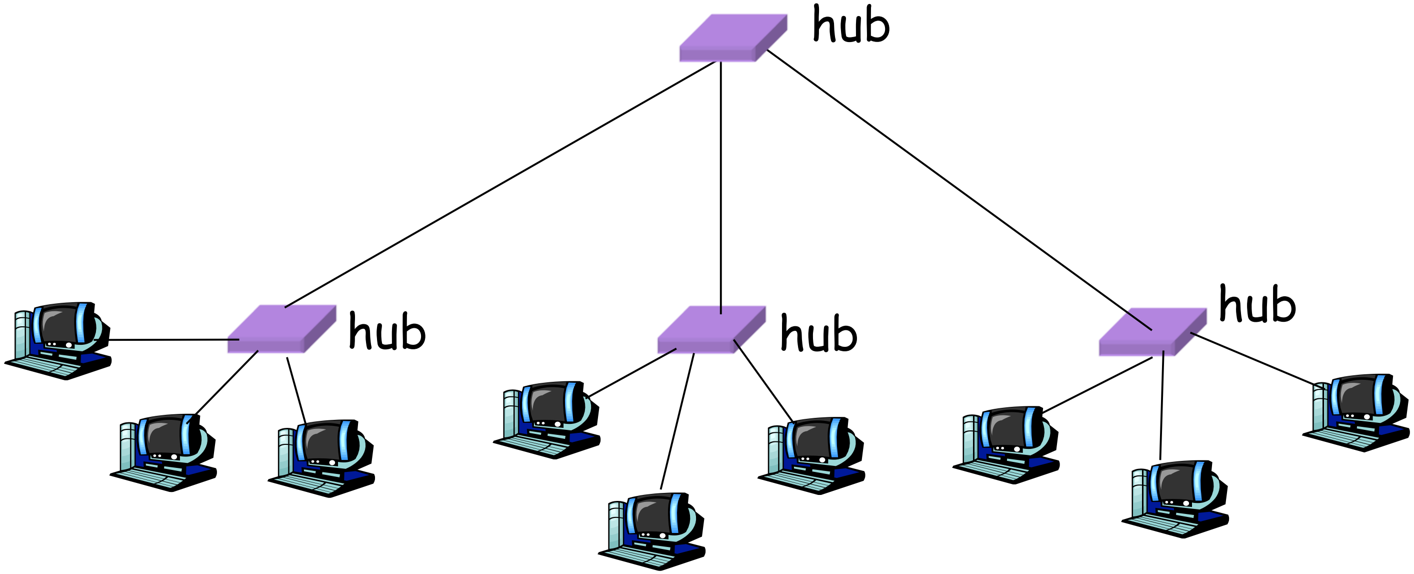
Hubs: Physical-Layer Repeaters

- Hubs are physical-layer repeaters
  - Bits coming from one link go out all other links
  - At the same rate, with no frame buffering
  - No CSMA/CD at hub: adapters detect collisions



Interconnecting with Hubs

- Backbone hub interconnects LAN segments
- All packets seen everywhere, forming one large collision domain
- Can’t interconnect Ethernets of different speeds

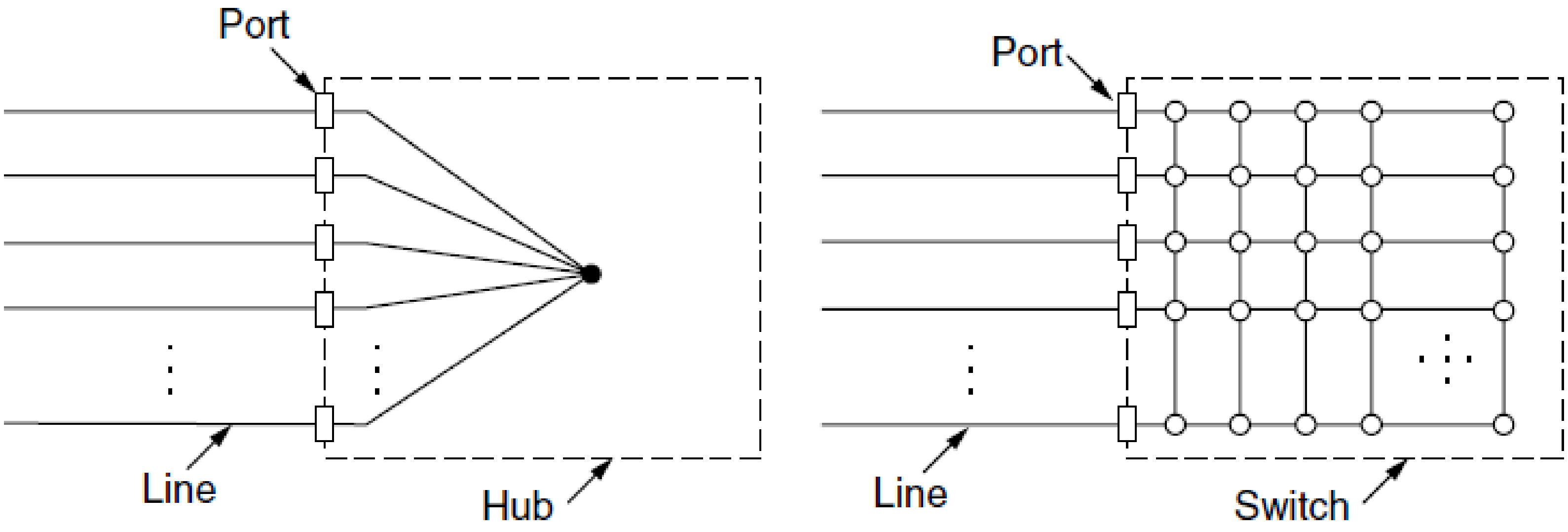


Switch

- Link layer device
  - Stores and forwards Ethernet frames
  - Examines frame header and selectively forwards frame based on MAC dest address
  - When frame is to be forwarded on segment, uses CSMA/CD to access segment
- Transparent
  - Hosts are unaware of presence of switches
- Plug-and-play, self-learning
  - Switches do not need to be configured

Switched/Fast Ethernet (1)

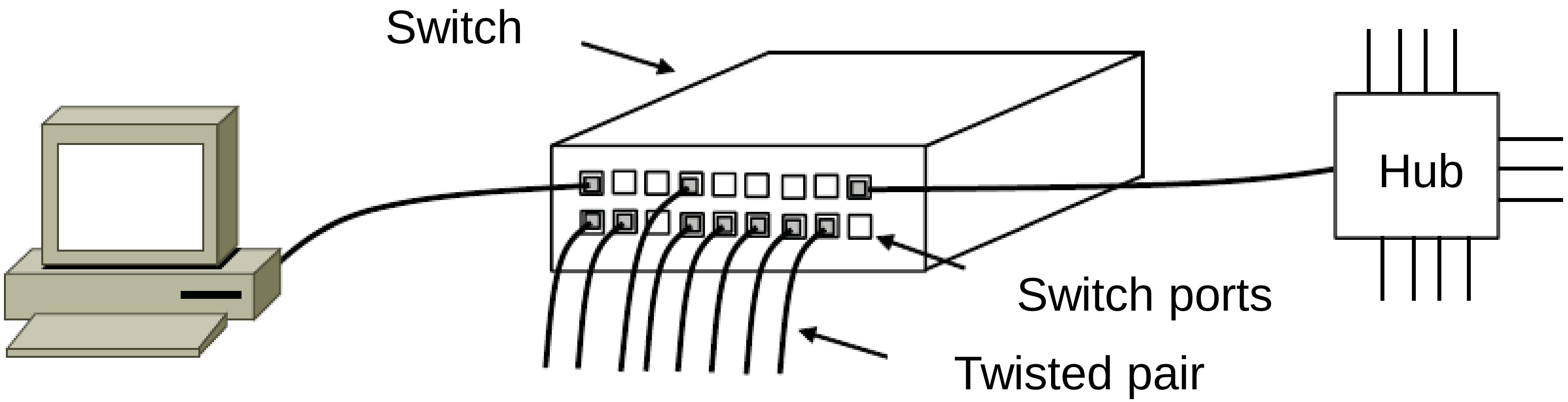
- Hubs wire all lines into a single CSMA/CD domain
- Switches isolate each port to a separate domain
  - Much greater throughput for multiple ports
  - No need for CSMA/CD with full-duplex lines



Switched/Fast Ethernet (2)

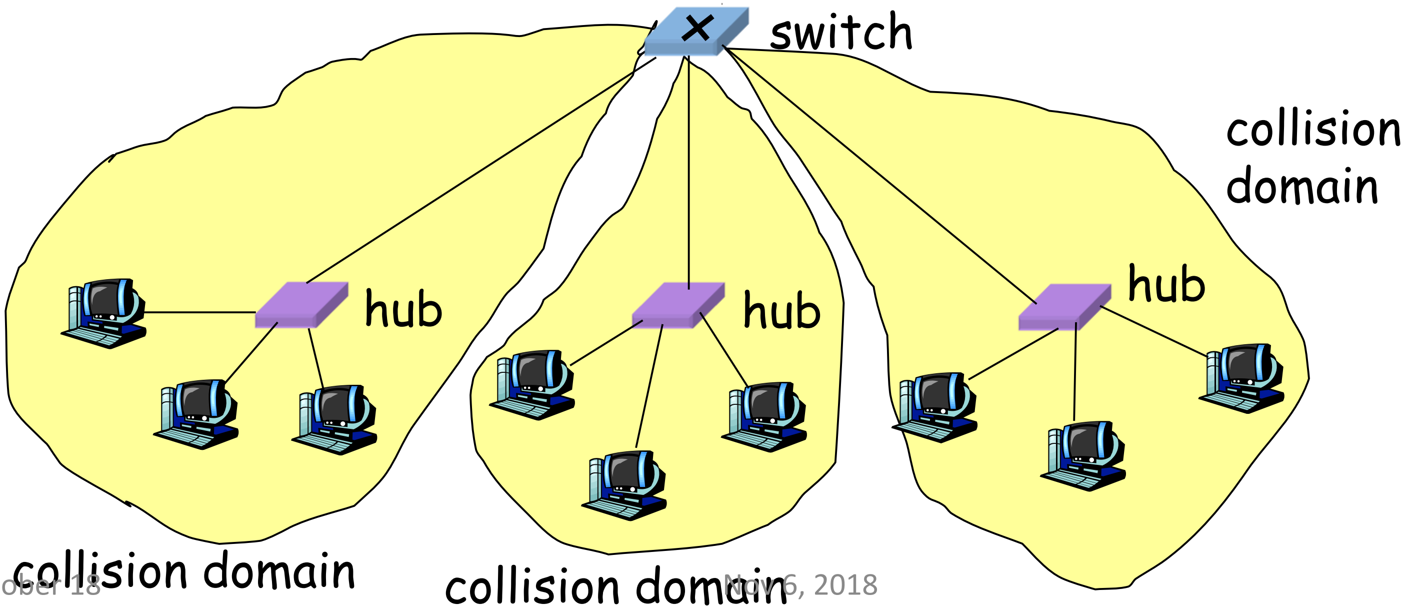
Switches can be wired to computers, hubs and switches

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



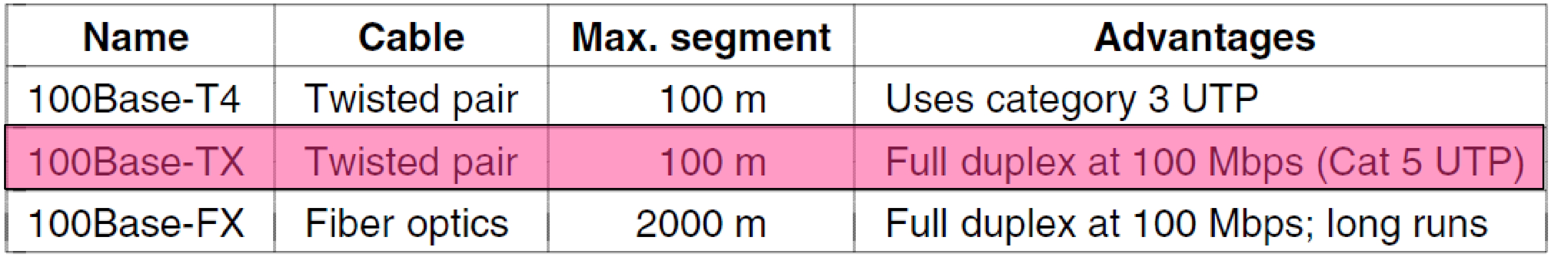
Switch: Traffic Isolation

- Switch breaks subnet into LAN segments
- Switch filters packets
  - Same-LAN-segment frames not usually forwarded onto other LAN segments
  - Segments become separate collision domains



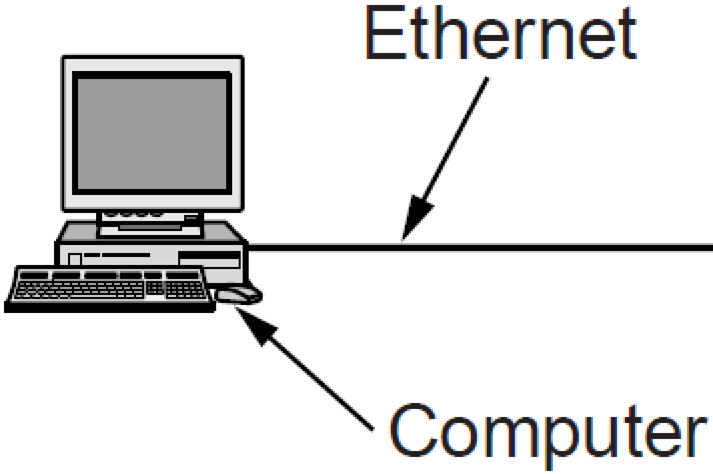
Switched/Fast Ethernet (3)

- 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

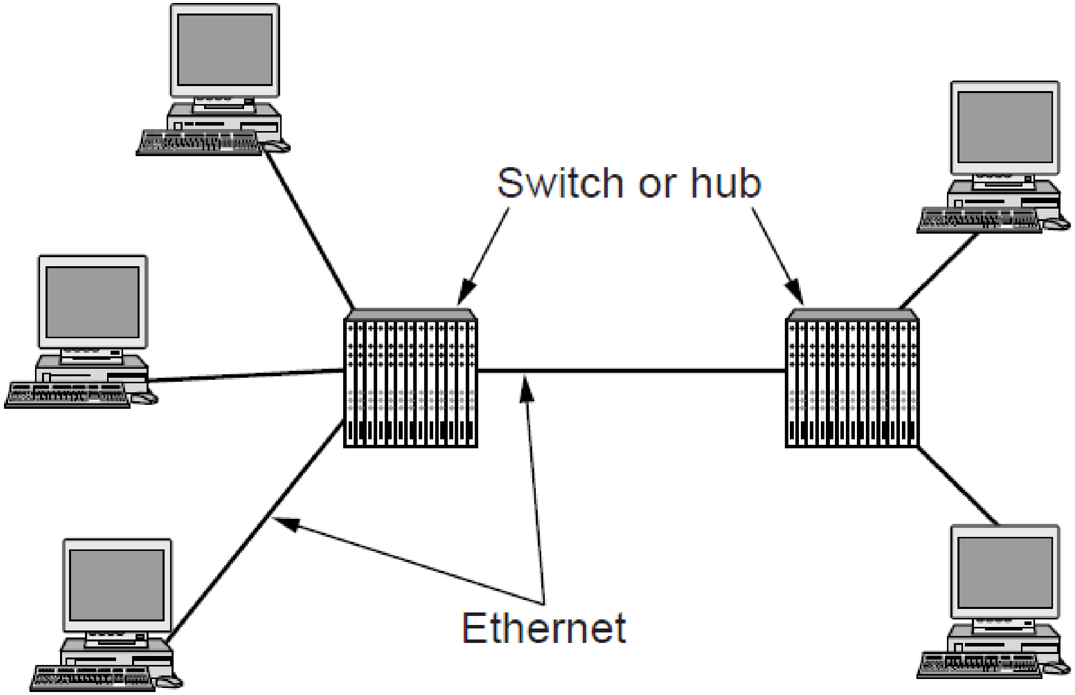
Gigabit Ethernet (1)



A two-station Ethernet

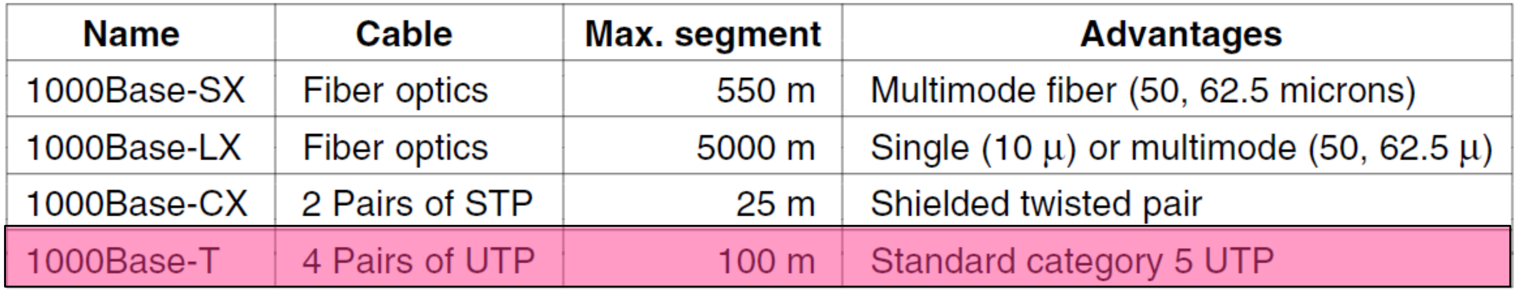
Gigabit / 10 Gigabit Ethernet (1)

Switched Gigabit Ethernet is now the garden variety



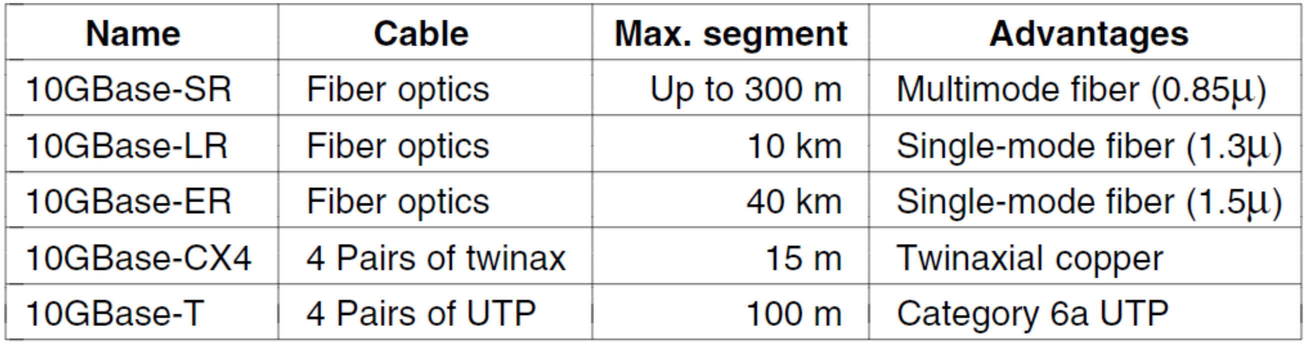
Gigabit / 10 Gigabit Ethernet (1)

- 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

Benefits of Ethernet

- Easy to administer and maintain
- Inexpensive
- Increasingly higher speed

- Moved from shared media to switches
  - Change everything except the frame format
  - A good general lesson for evolving the Internet

Unreliable, Connectionless Service

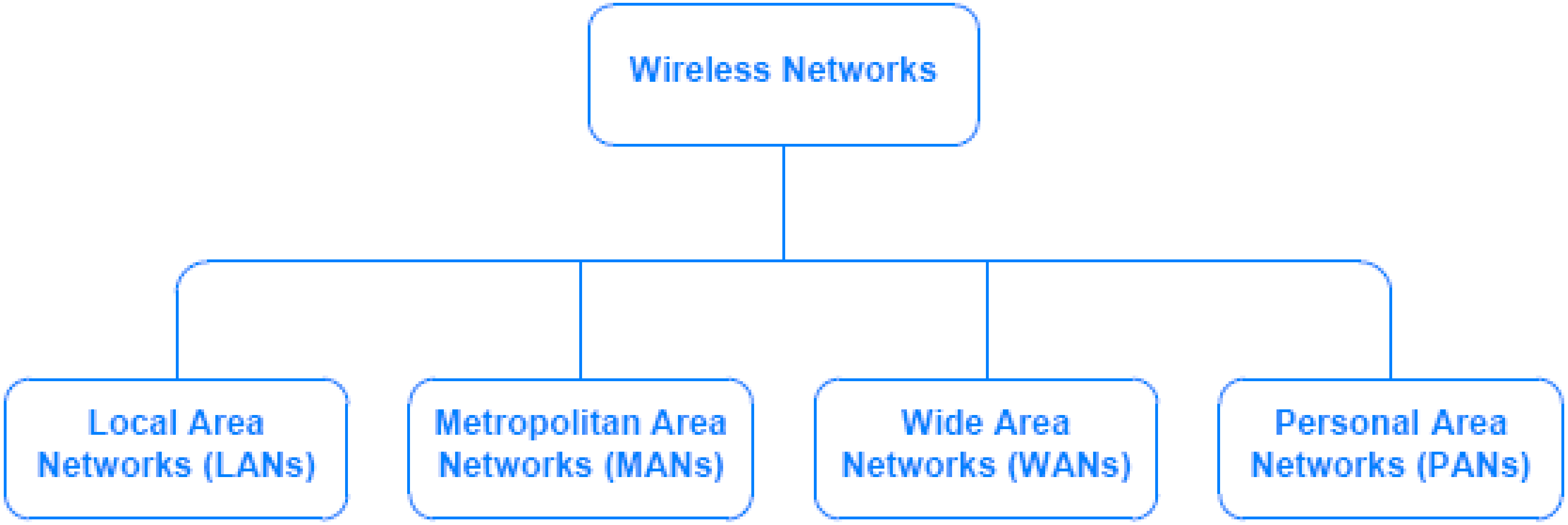
- Connectionless
  - No handshaking between sending and receiving adapter.
- Unreliable
  - Receiving adapter doesn’t send ACKs or NACKs
  - Packets passed to network layer can have gaps
  - Gaps will be filled if application is using TCP
  - Otherwise, the application will see the gaps

Wireless Networking Technologies

A Taxonomy of Wireless Networks

- Wireless communication applies across a wide range of network types and sizes
- Part of the motivation for variety
  - government regulations that make specific ranges of the electromagnetic spectrum available for communication
- A license is required to operate transmission equipment in some parts of the spectrum
  - and other parts of the spectrum are unlicensed
- Many wireless technologies have been created
  - and new variants appear continually
- Wireless technologies can be classified broadly according to network type

A Taxonomy of Wireless Networks



Wireless Networks

Local Area Networks (LANs)

Metropolitan Area Networks (MANs)

Wide Area Networks (WANs)

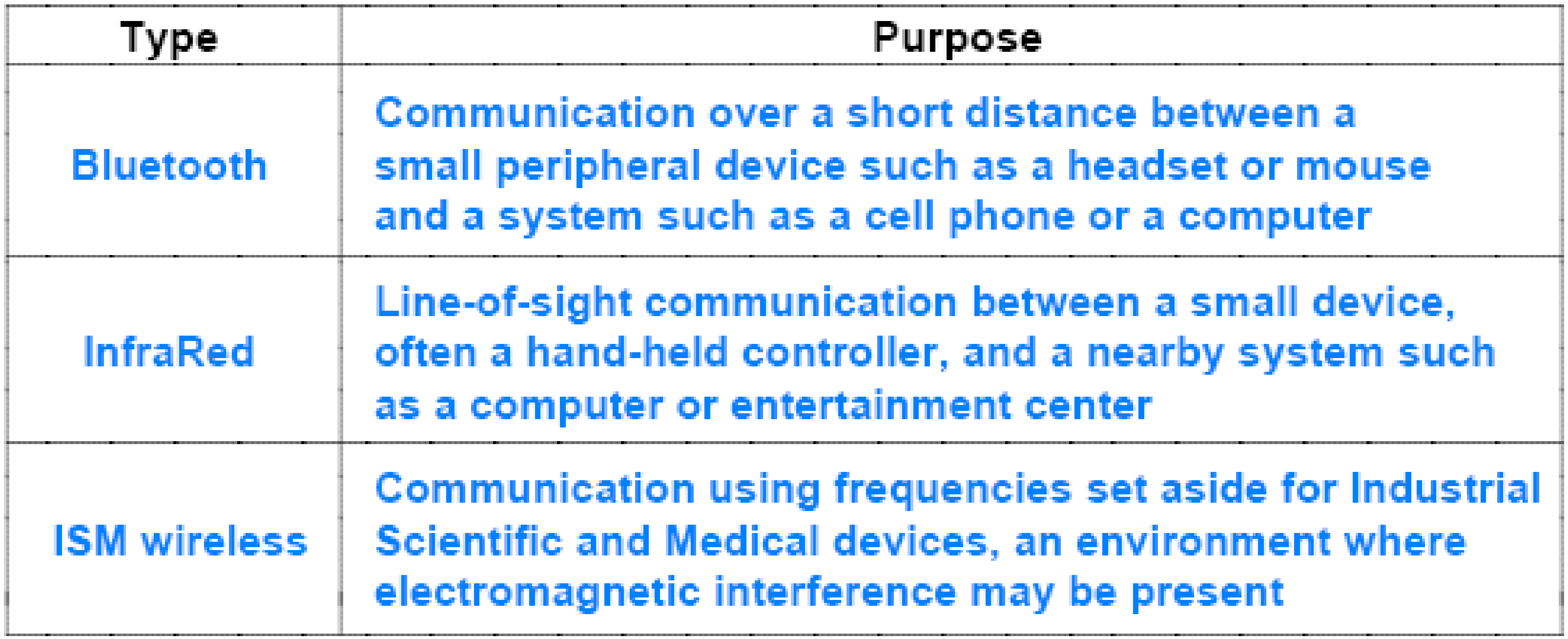
Personal Area Networks (PANs)

A taxonomy of wireless networking technologies.

Personal Area Networks (PANs)

- A PAN technology provides communication over a short distance
- It is intended for use with devices that are owned and operated by a single user. For example
  - between a wireless headset and a cell phone
  - between a computer and a nearby wireless mouse or keyboard
- PAN technologies can be grouped into three categories
- Later sections explain PAN communication in more detail
  - and list PAN standards

Personal Area Networks (PANs)

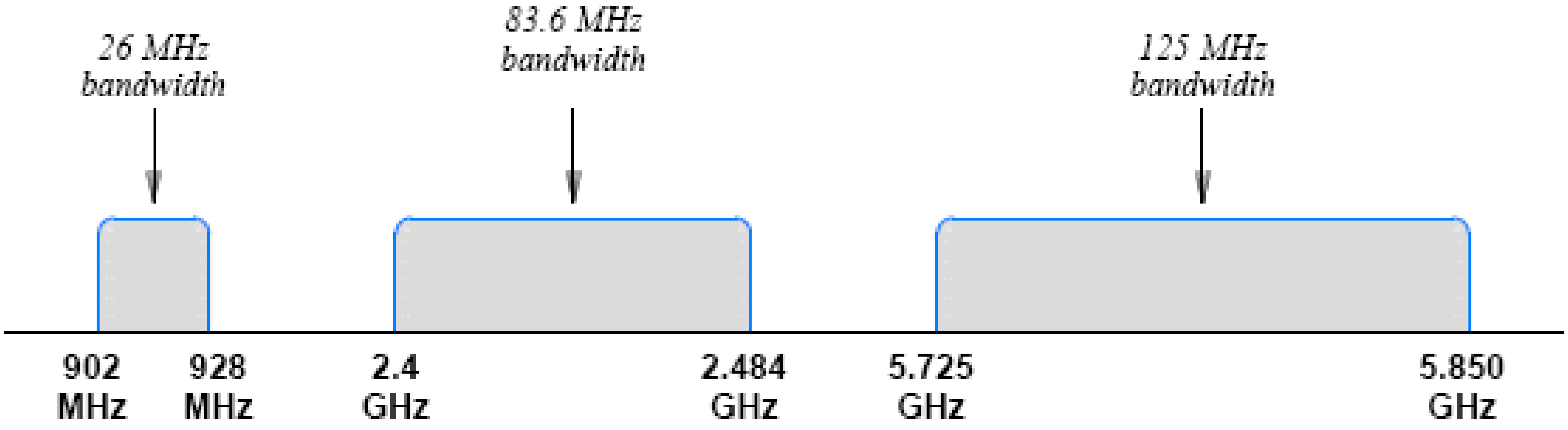


Type	Purpose
Bluetooth	Communication over a short distance between a small peripheral device such as a headset or mouse and a system such as a cell phone or a computer
InfraRed	Line-of-sight communication between a small device, often a hand-held controller, and a nearby system such as a computer or entertainment center
ISM wireless	Communication using frequencies set aside for Industrial Scientific and Medical devices, an environment where electromagnetic interference may be present

Three basic types of wireless Personal Area Network technologies.

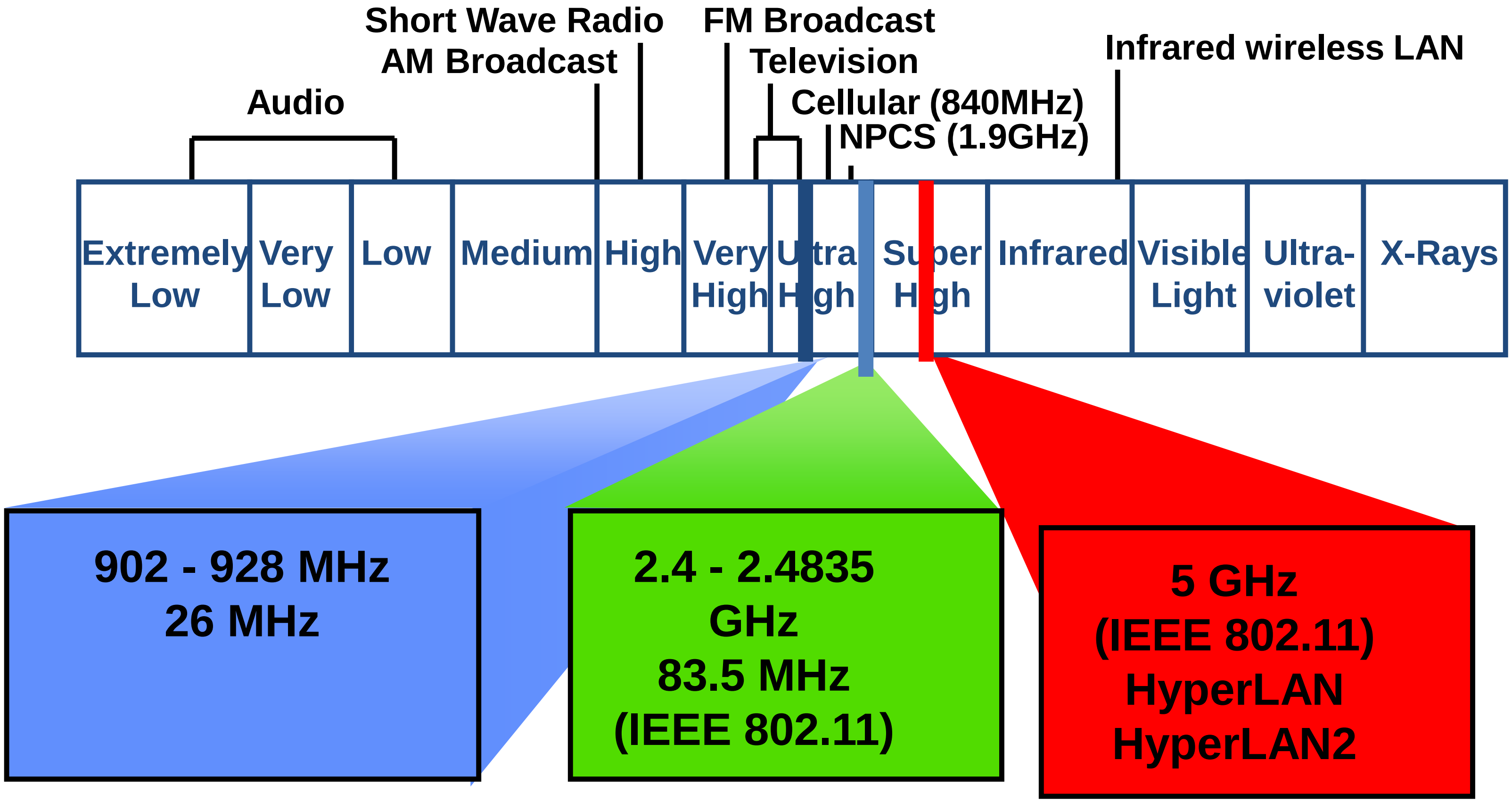
ISM Wireless Bands Used by LANs and PANs

- A region of electromagnetic spectrum is reserved for use by Industrial, Scientific, and Medical (ISM) groups
  - Known as ISM wireless
- The frequencies are not licensed to specific carriers
  - are broadly available for products, and are used for LANs and PANs



Frequency Bands- ISM

- Industrial, Scientific, and Medical (ISM) bands
- Unlicensed



902 - 928 MHz
26 MHz

2.4 - 2.4835 GHz
83.5 MHz
(IEEE 802.11)

5 GHz
(IEEE 802.11)
HyperLAN
HyperLAN2

Wireless LAN Technologies and Wi-Fi

- A variety of wireless LAN technologies exist that use
  - various frequencies
  - modulation techniques
  - and data rates
- IEEE provides most of the standards
  - which are categorized as IEEE 802.11
- A group of vendors who build wireless equipment formed the Wi-Fi Alliance
  - a non-profit organization that tests and certifies wireless equipment using the 802.11 standards
- Alliance has received extensive marketing, most consumers associate wireless LANs with the term Wi-Fi

802.11 Standards

- IEEE 802.11-1997: The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
- IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b: Enhancements to 802.11 to support 5.5 Mbit/s and 11 Mbit/s (1999)
- IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d: International (country-to-country) roaming extensions (2001)
- IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F: Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i: Enhanced security (2004)
- IEEE 802.11j: Extensions for Japan (2004)
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i, and j. (July 2007)
- IEEE 802.11k: Radio resource measurement enhancements (2008)
- IEEE 802.11n: Higher-throughput improvements using MIMO (multiple-input, multiple-output antennas) (September 2009)
- IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
- IEEE 802.11r: Fast BSS transition (FT) (2008)
- IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)

802.11 Standards

- IEEE 802.11u: Improvements related to HotSpots and 3rd-party authorization of clients, e.g., cellular network offload (February 2011)
- IEEE 802.11v: Wireless network management (February 2011)
- IEEE 802.11w: Protected Management Frames (September 2009)
- IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010)
- IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y, and z (March 2012)
- IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (June 2012)
- IEEE 802.11ac: Very High Throughput <6 GHz;[49] potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO;[50] (December 2013)
- IEEE 802.11ad: Very High Throughput 60 GHz (December 2012) — see WiGig
- IEEE 802.11ae: Prioritization of Management Frames (March 2012)
- IEEE 802.11af: TV Whitespace (February 2014)

In process

- IEEE 802.11mc: Roll-up of 802.11-2012 with the aa, ac, ad, ae & af amendments to be published as 802.11-2016 *(~ March 2016)*
- IEEE 802.11ah: Sub-1 GHz license exempt operation (e.g., sensor network, smart metering) *(~ March 2016)*
- IEEE 802.11ai: Fast Initial Link Setup *(~ September 2016)*
- IEEE 802.11aj: China Millimeter Wave *(~ June 2016)*
- IEEE 802.11ak: General Links *(~ May 2016)*
- IEEE 802.11aq: Pre-association Discovery *(~ July 2016)*
- IEEE 802.11ax: High Efficiency WLAN *(~ May 2018)*
- IEEE 802.11ay: Enhancements for Ultra High Throughput in and around the 60 GHz Band *(~ TBD)*
- IEEE 802.11az: Next Generation Positioning *(~ TBD)*

802.11 Standards

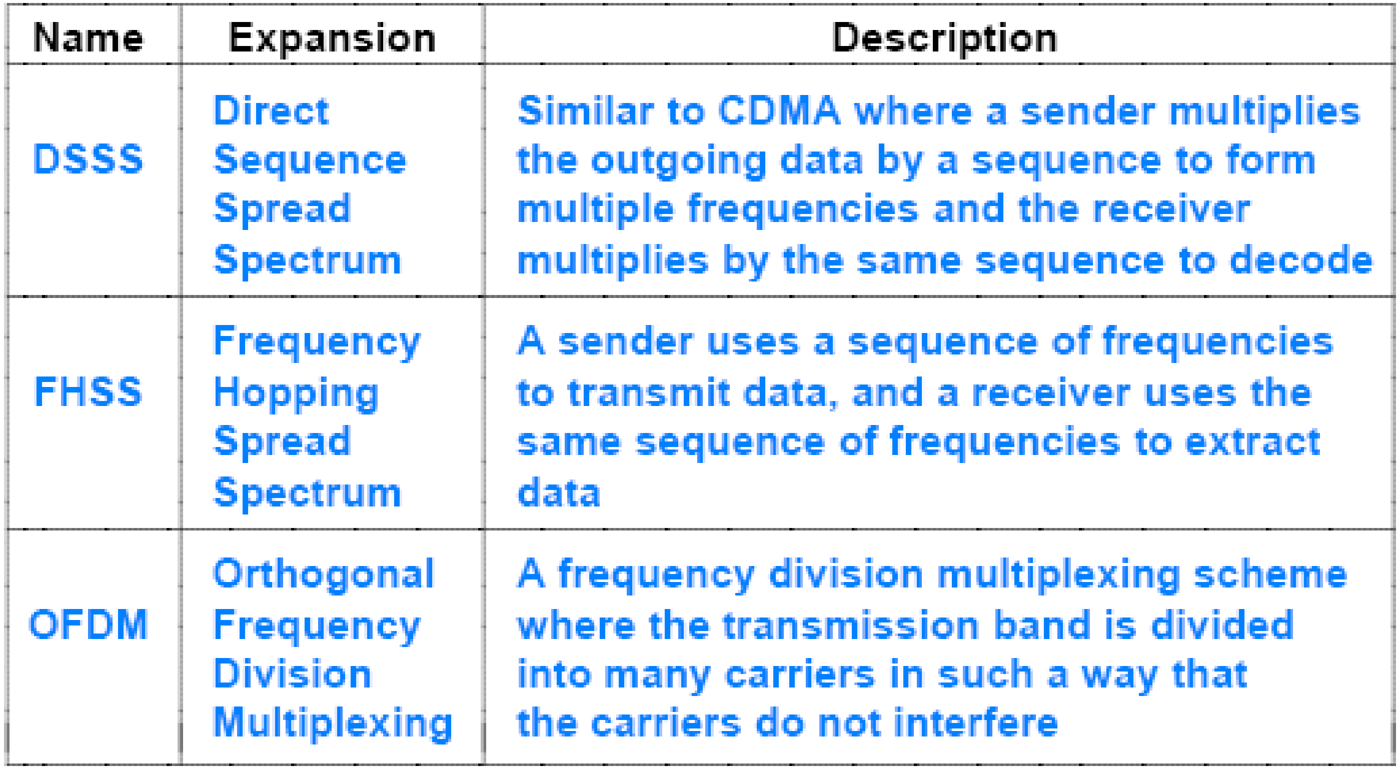
802.11 network PHY standards

802.11 protocol	Release date[6]	Fre-quency	Band-width	Data Rate	Allowable MIMO streams	Modulation	Approximate range			
							Indoor		Outdoor	
		(GHz)	(MHz)	MBPS				(ft)		(ft)
802.11-1997	Jun 1997	2.4	22	2	N/A	DSSS, FHSS		66		330
a	Sep 1999	5	20	54	N/A	OFDM		115		390
		3.7[A]						—		16,000
b	Sep 1999	2.4	22	11	N/A	DSSS		115		460
g	Jun 2003	2.4	20	54	N/A	OFDM		125		460
n	Oct 2009	2.4/5	20	72.2	4	MIMO-OFDM		230		820
			40	135				230		820
ac	Dec 2013	5	20	96.3	8			115		
			40	180				115		
			80	390				115		
			160	780				115		
ad	Dec 2012	60	2,160	6,912	N/A	OFDM, single carrier, low-power single carrier		200		300
ay	2017	60	8000	100,000	4	OFDM, single carrier,		200		3000

Spread Spectrum Techniques

- The term spread spectrum transmission uses multiple frequencies to send data
  - the sender spreads data across multiple frequencies
  - the receiver combines the information obtained from multiple frequencies to reproduce the original data
- Spread spectrum can be used to achieve one of the following two goals:
  - Increase overall performance
  - Make transmission more immune to noise
- The table summarizes the three key multiplexing techniques used in Wi-Fi wireless networks
  - Each technique has advantages
  - Thus, when a wireless technology is defined, the designers choose an appropriate multiplexing technique

Spread Spectrum Techniques



Name	Expansion	Description
DSSS	Direct Sequence Spread Spectrum	Similar to CDMA where a sender multiplies the outgoing data by a sequence to form multiple frequencies and the receiver multiplies by the same sequence to decode
FHSS	Frequency Hopping Spread Spectrum	A sender uses a sequence of frequencies to transmit data, and a receiver uses the same sequence of frequencies to extract data
OFDM	Orthogonal Frequency Division Multiplexing	A frequency division multiplexing scheme where the transmission band is divided into many carriers in such a way that the carriers do not interfere

The major multiplexing techniques used with Wi-Fi.

Other Wireless LAN Standards

- IEEE has created many wireless networking standards
  - that handle various types of communication
- Each standard specifies
  - the frequency range
  - the modulation
  - the multiplexing to be used
  - the data rate
- Figure on next slide lists the major standards that have been created or proposed, and gives a brief description of each
- In 2007, IEEE “rolled up” many of the existing 802.11 standards into a single document known as 802.11-2007
  - The document describes basics
  - It has an appendix for each variant

IEEE 802.11 Overview

- Adopted in 1997.

Defines;

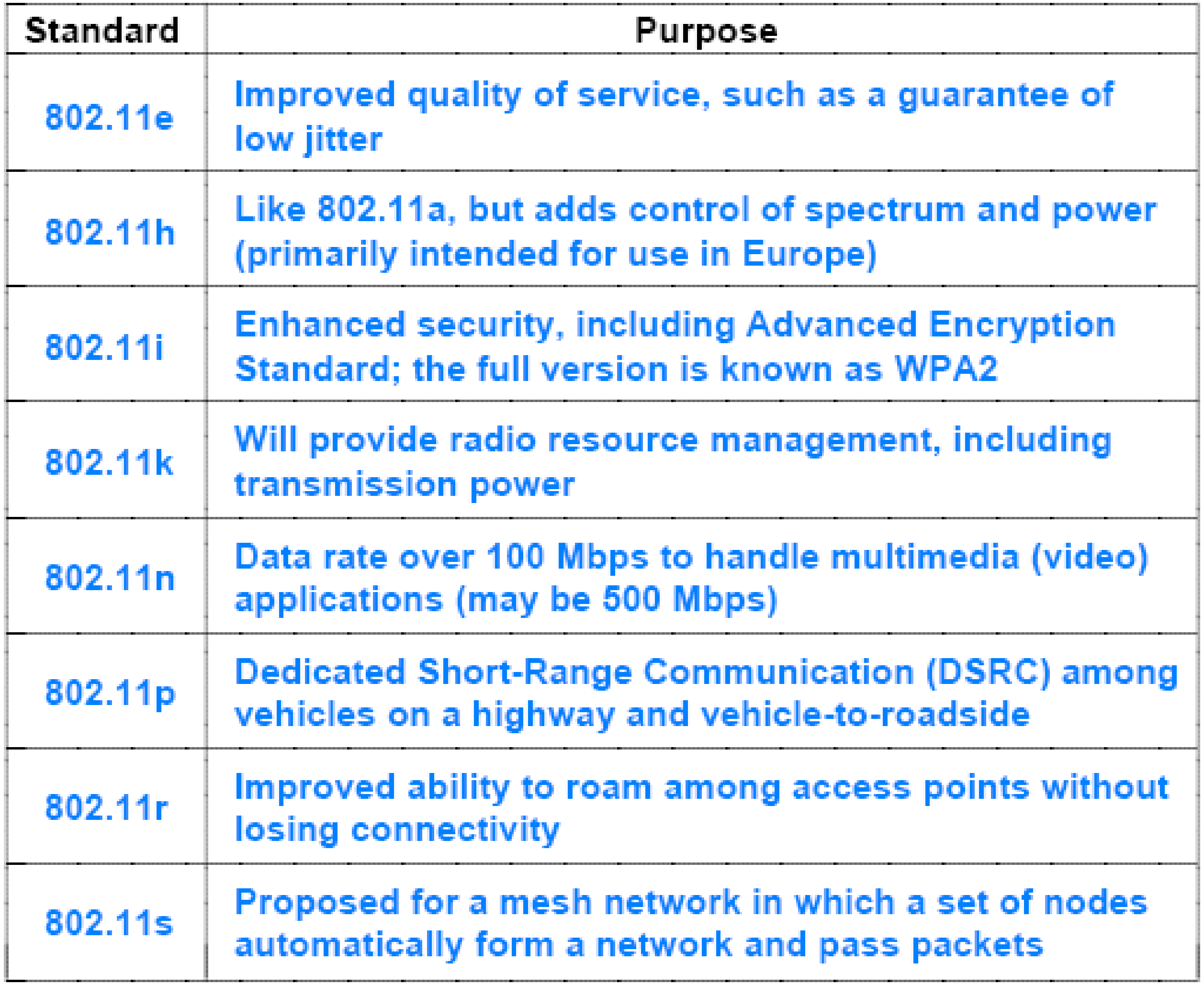
- MAC sublayer
- MAC management protocols and services
- Physical (PHY) layers
  - IR
  - FHSS
  - DSSS

Goals

- To deliver services in wired networks
- To achieve high throughput
- To achieve highly reliable data delivery
- To achieve continuous network connection.

Other Wireless LAN Standards

Major wireless standards and the purpose of each



Standard	Purpose
802.11e	Improved quality of service, such as a guarantee of low jitter
802.11h	Like 802.11a, but adds control of spectrum and power (primarily intended for use in Europe)
802.11i	Enhanced security, including Advanced Encryption Standard; the full version is known as WPA2
802.11k	Will provide radio resource management, including transmission power
802.11n	Data rate over 100 Mbps to handle multimedia (video) applications (may be 500 Mbps)
802.11p	Dedicated Short-Range Communication (DSRC) among vehicles on a highway and vehicle-to-roadside
802.11r	Improved ability to roam among access points without losing connectivity
802.11s	Proposed for a mesh network in which a set of nodes automatically form a network and pass packets

Wireless LAN Architecture

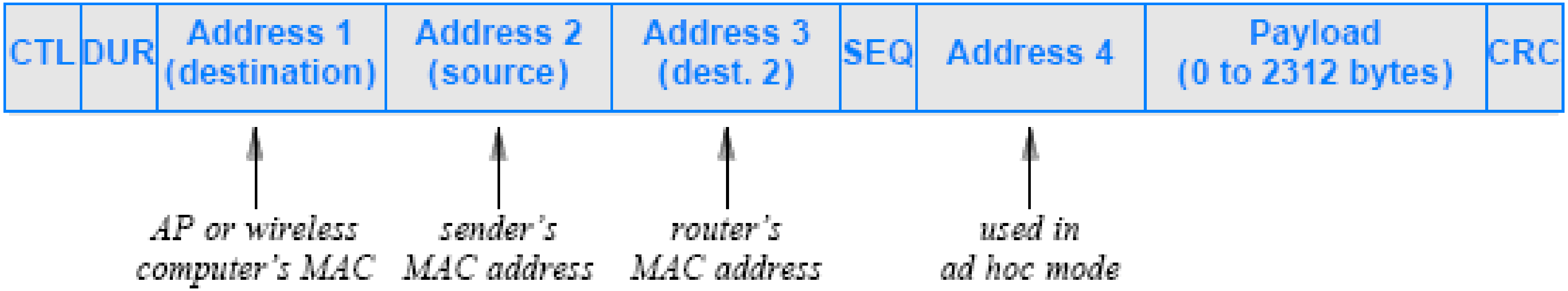
- The three building blocks of a wireless LAN are:
  - access points (AP)
    - which are informally called base stations
  - an interconnection mechanism
    - such as a switch or router used to connect access points
  - a set of wireless hosts
    - also called wireless nodes or wireless stations
- In principle, two types of wireless LANs are possible:
  - Ad hoc
    - wireless hosts communicate amongst themselves without a base station
  - Infrastructure based
    - a wireless host only communicates with an access point, and the access point relays all packets
- An organization might deploy AP throughout its buildings

The Physical Layer

  - PLCP: frame exchange between the MAC and PHY
  - PMD: uses signal carrier and spread spectrum modulation to transmit data frames over the media.
- Direct Sequence Spread Spectrum (DSSS) PHY
  - 2.4 GHz : RF : 1 – 2 Mbps
- The Frequency Hopping Spread Spectrum (FHSS) PHY
  - 110KHz deviation : RF : PMD controls channel hopping : 2 Mbps
- Infrared (IR) PHY
  - Indoor : IR : 1 and 2 Mbps
- The OFDM PHY – IEEE 802.11a
  - 5.0 GHz : 6-54 Mbps :
- High Rate DSSS PHY – IEEE 802.11b
  - 2.4 GHz : 5.5 Mbps – 11 Mbps :

Overlap, Association, and 802.11 Frame Format

- To handle overlap, 802.11 networks require a wireless host to associate with a single AP
  - That is, a wireless host sends frames to a particular AP
  - Then AP forwards the frames across the network
- Frame format
  - When used with an infrastructure architecture the frame carries the MAC address of an AP as well as the address of an Internet router



CTL	DUR	Address 1 (destination)	Address 2 (source)	Address 3 (dest. 2)	SEQ	Address 4	Payload (0 to 2312 bytes)	CRC

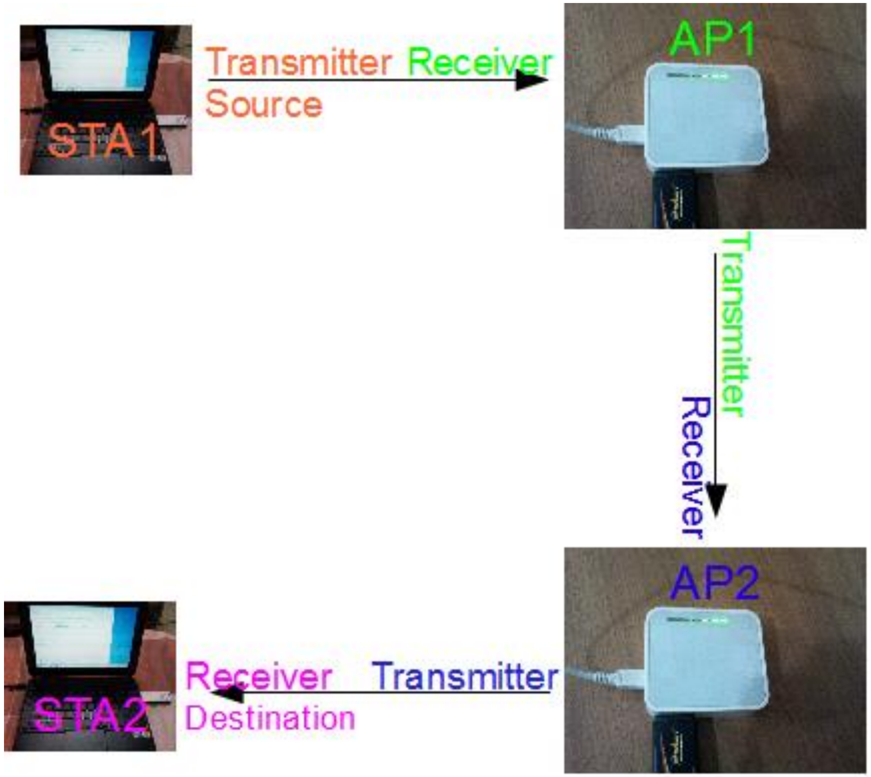
AP or wireless computer's MAC

sender's MAC address

router's MAC address

used in ad hoc mode

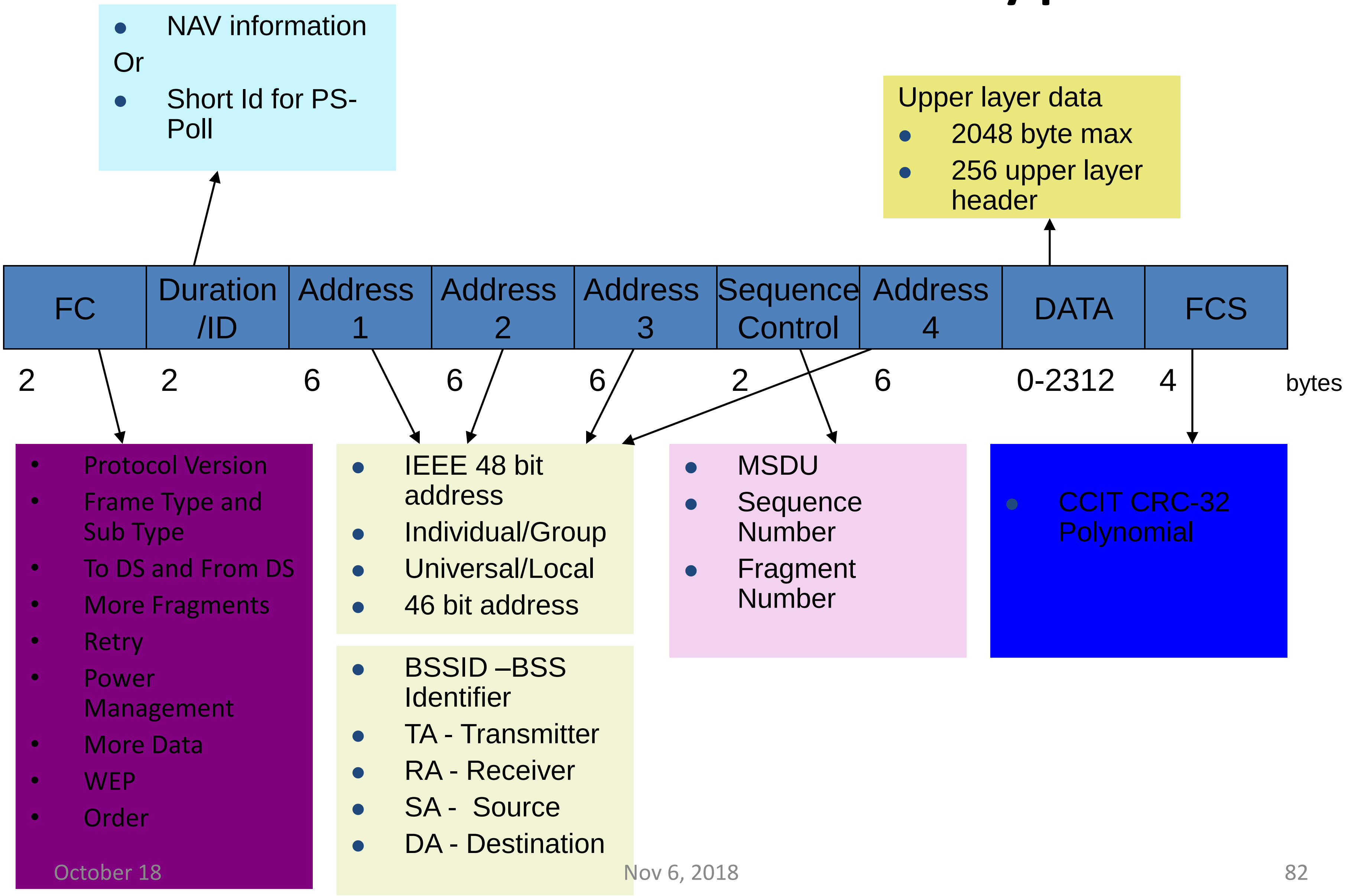
Mac Addresses



Overlap, Association, and 802.11 Frame Format

- Many details can complicate an infrastructure architecture
  - On one hand, if a pair of APs are too far apart
    - a dead zone will exist between them
    - a physical location with no wireless connectivity
  - On the other hand, if a pair of access points is too close together
    - an overlap will exist in which a wireless host can reach both access points
- Most wireless LANs connect to the Internet
  - Thus, the interconnect mechanism usually has an additional wired connection to an Internet router

Frame Types



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

- NAV information

Or

- Short Id for PS-Poll

Upper layer data

- 2048 byte max
- 256 upper layer header

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

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

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

- MSDU
- Sequence Number
- Fragment Number

- CCIT CRC-32 Polynomial

Frame Subtypes

CONTROL

- RTS
- CTS
- ACK
- PS-Poll
- CF-End & CF-End ACK

DATA

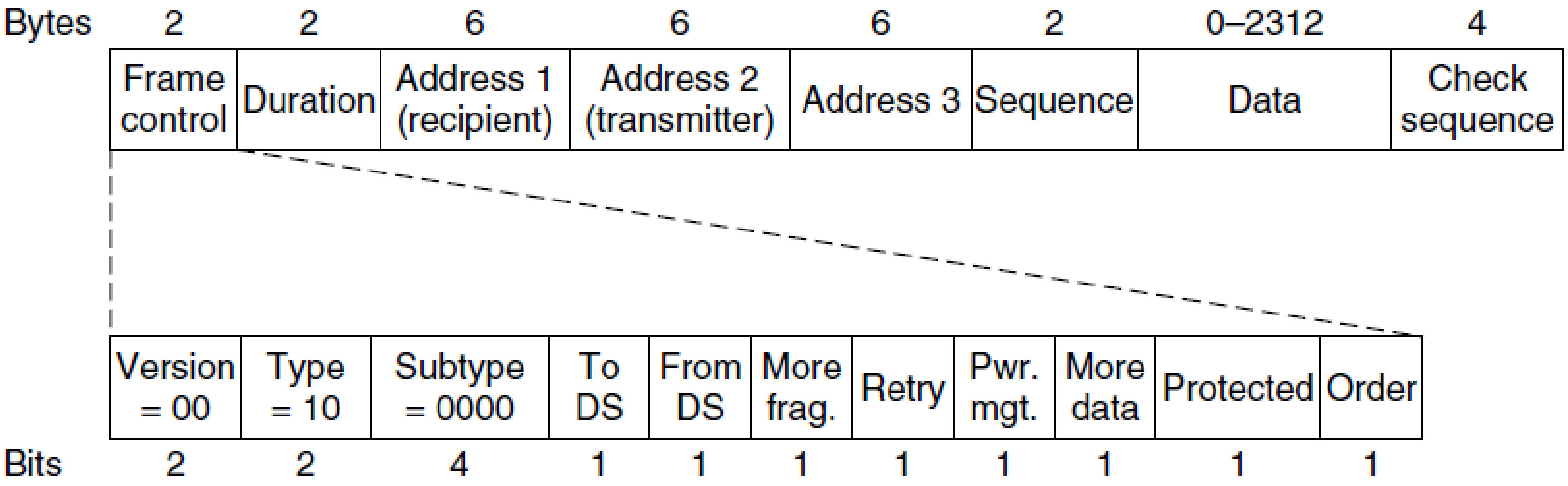
- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null Function
- CF-ACK (nodata)
- CF-Poll (nodata)
- CF-ACK+CF+Poll

MANAGEMENT

- Beacon
- Probe Request & Response
- Authentication
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation
- Announcement Traffic Indication Message (ATIM)

802.11 Frames

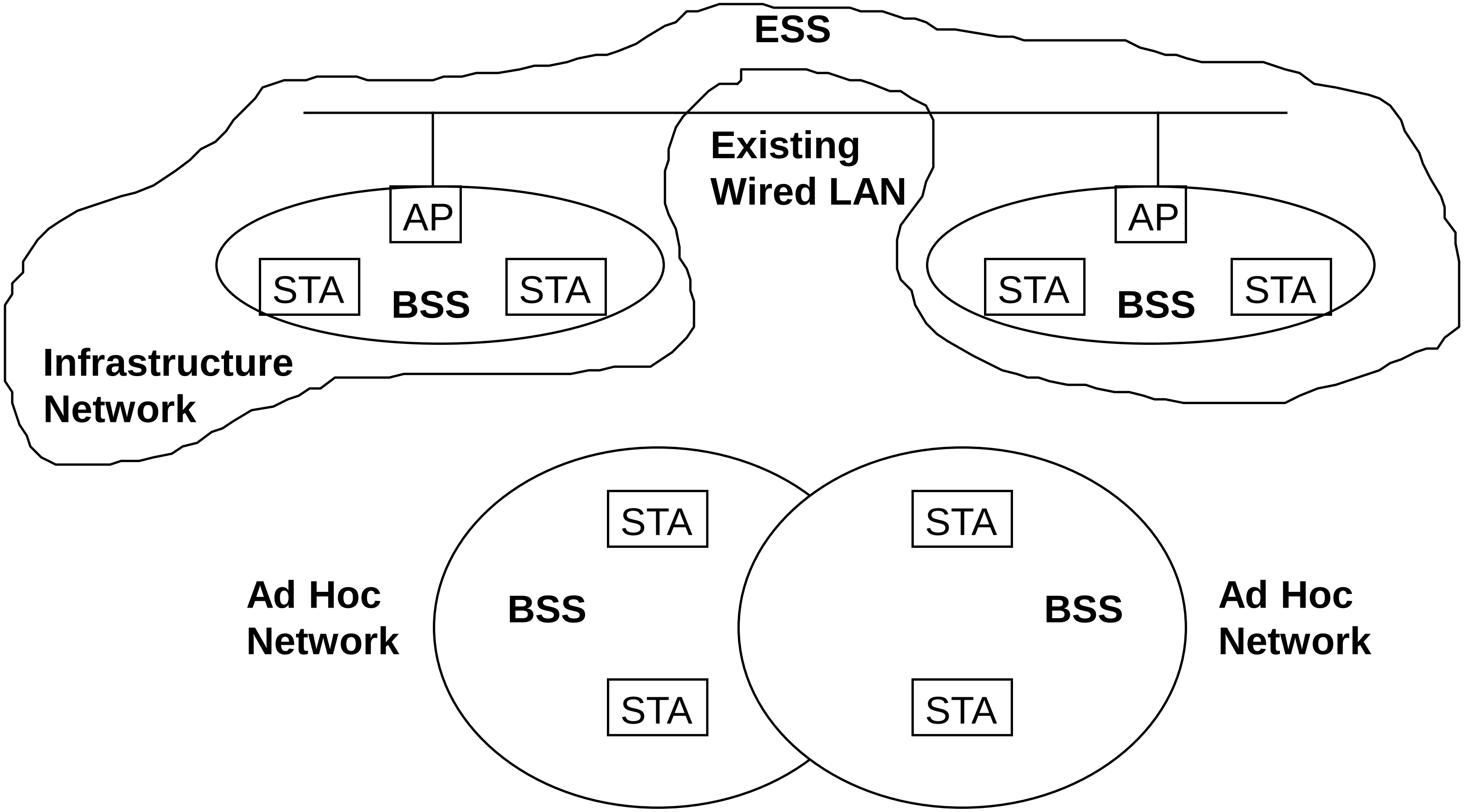
- Frames vary depending on their type (Frame control)
- Data frames have 3 addresses to pass via APs



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

Overview, 802.11 Architecture



Components

- Station
- BSS - Basic Service Set
  - IBSS : Infrastructure BSS : QBSS
- ESS - Extended Service Set
  - A set of infrastrucute BSSs.
  - Connection of APs
  - Tracking of mobility
- DS – Distribution System
  - AP communicates with another

Wireless LAN Architecture

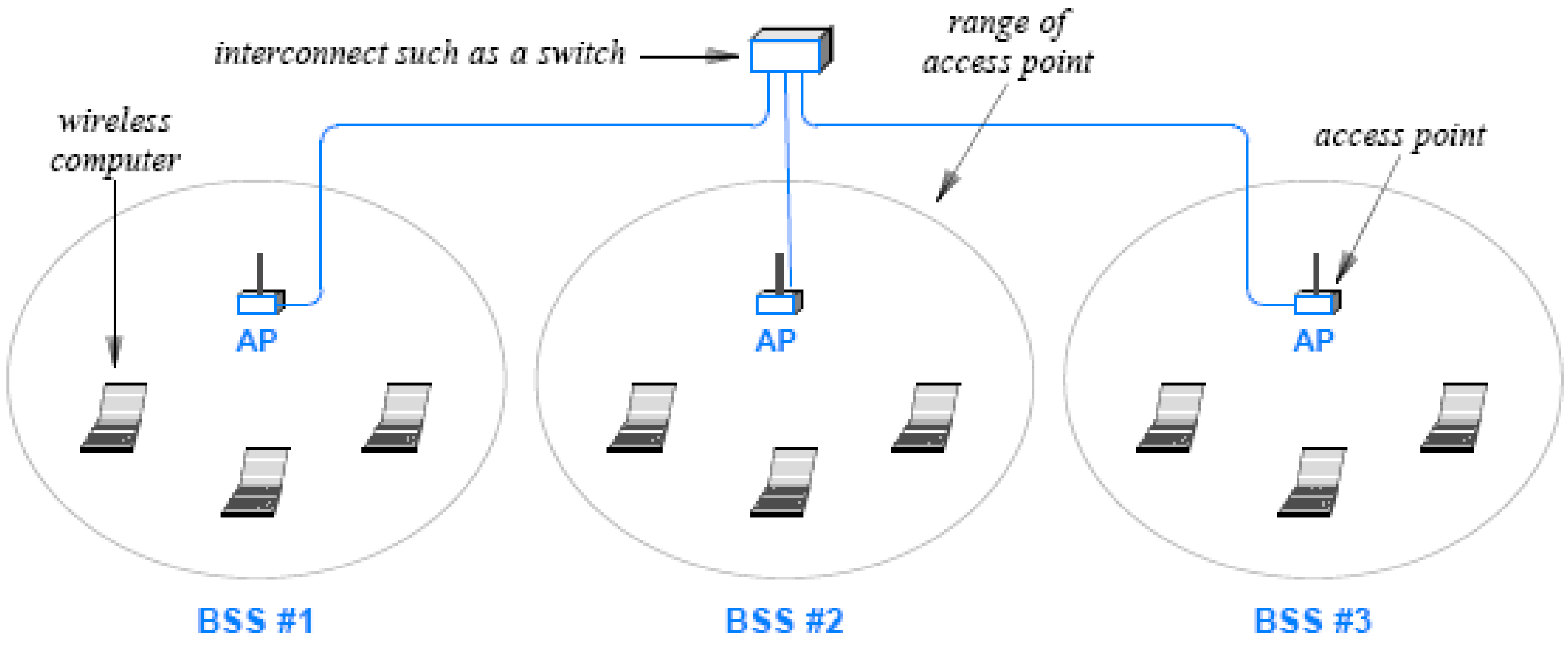


Illustration of an infrastructure architecture for a wireless LAN.

Note: The set of computers within range of a given access point is known as a *Basic Service Set* *(BSS)*

Overlap, Association, and 802.11 Frame Format

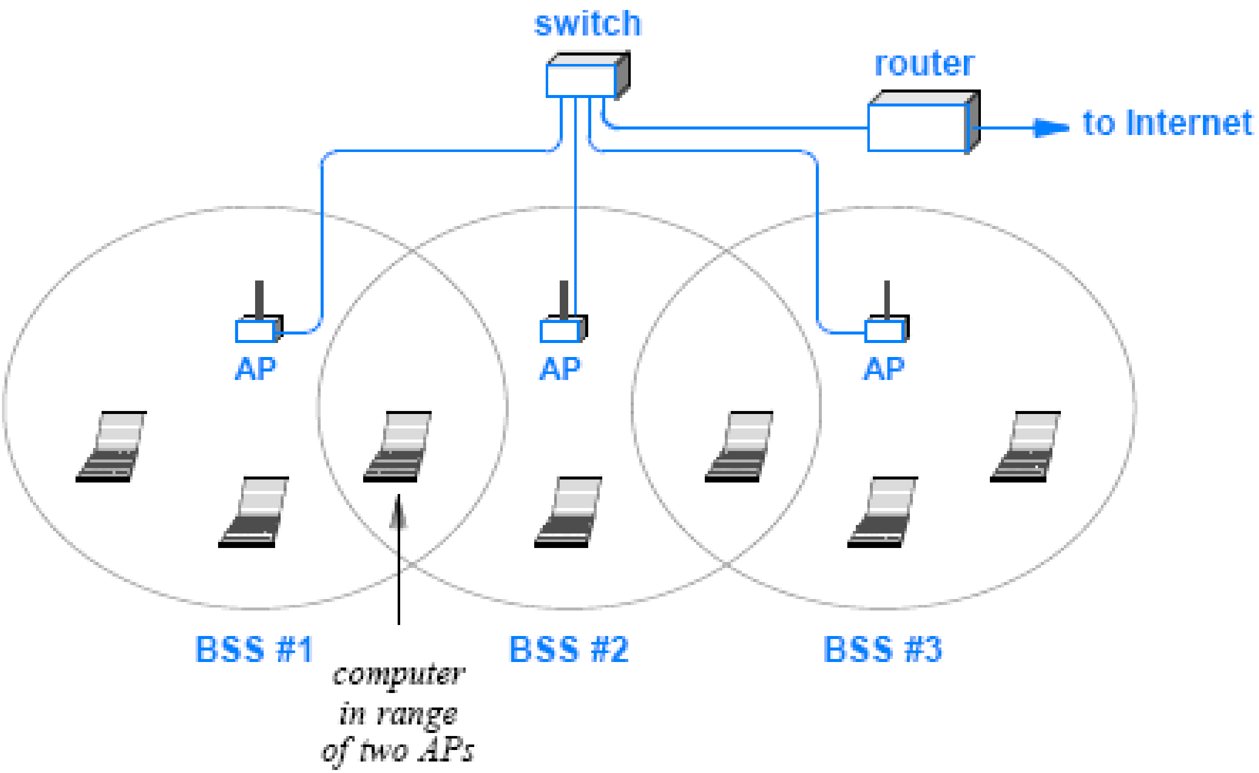
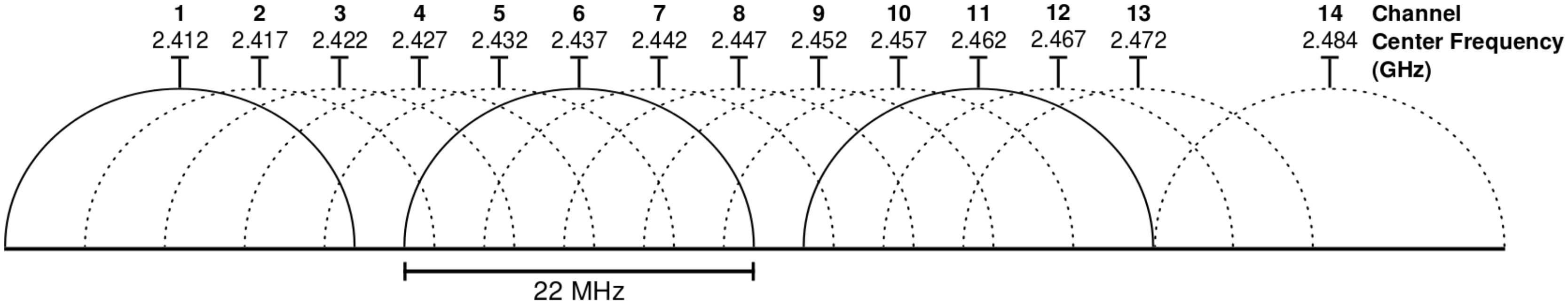
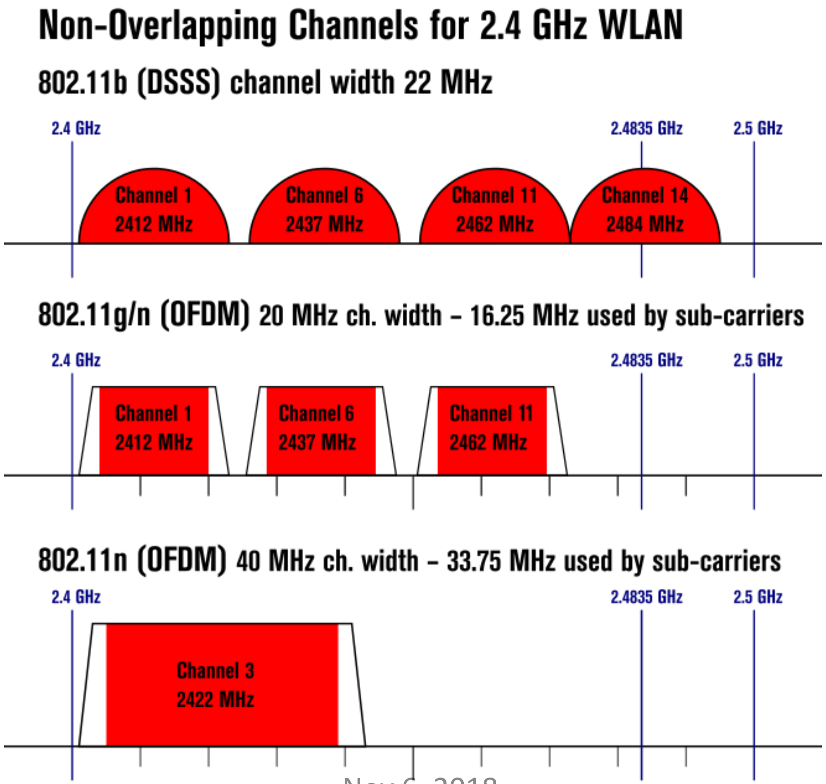


Illustration of an infrastructure with overlapping regions.

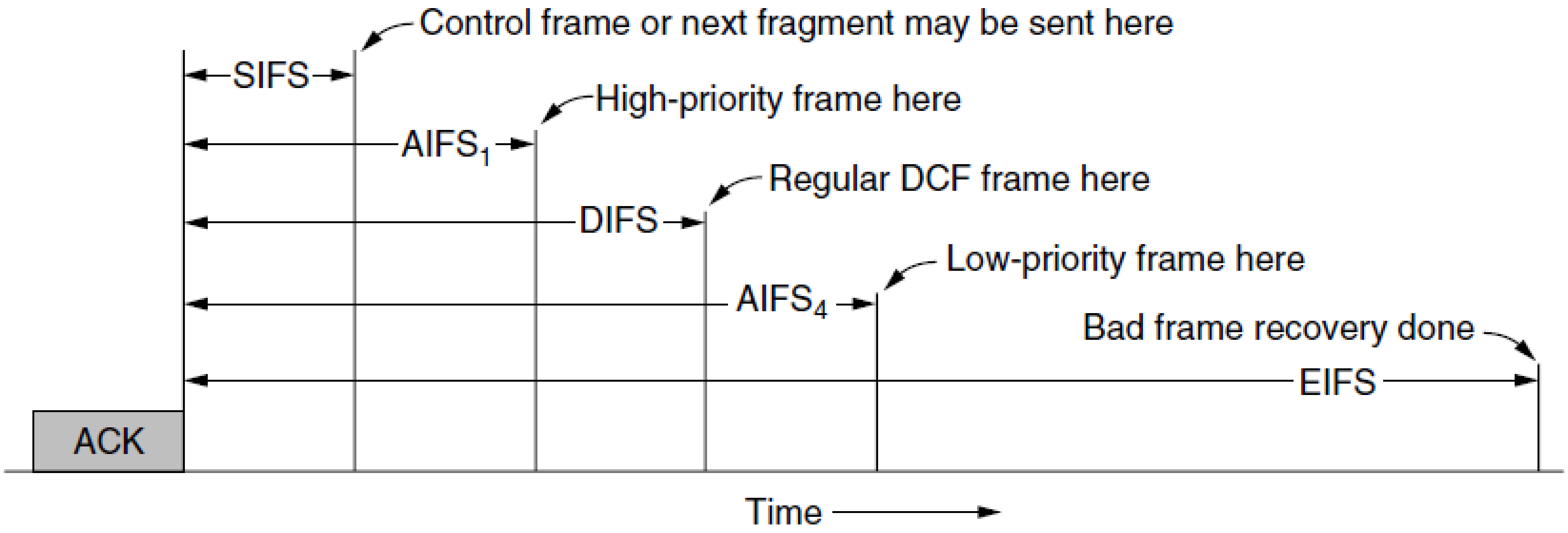
802.11 b Channels





802.11 MAC

- 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



SIFS Values

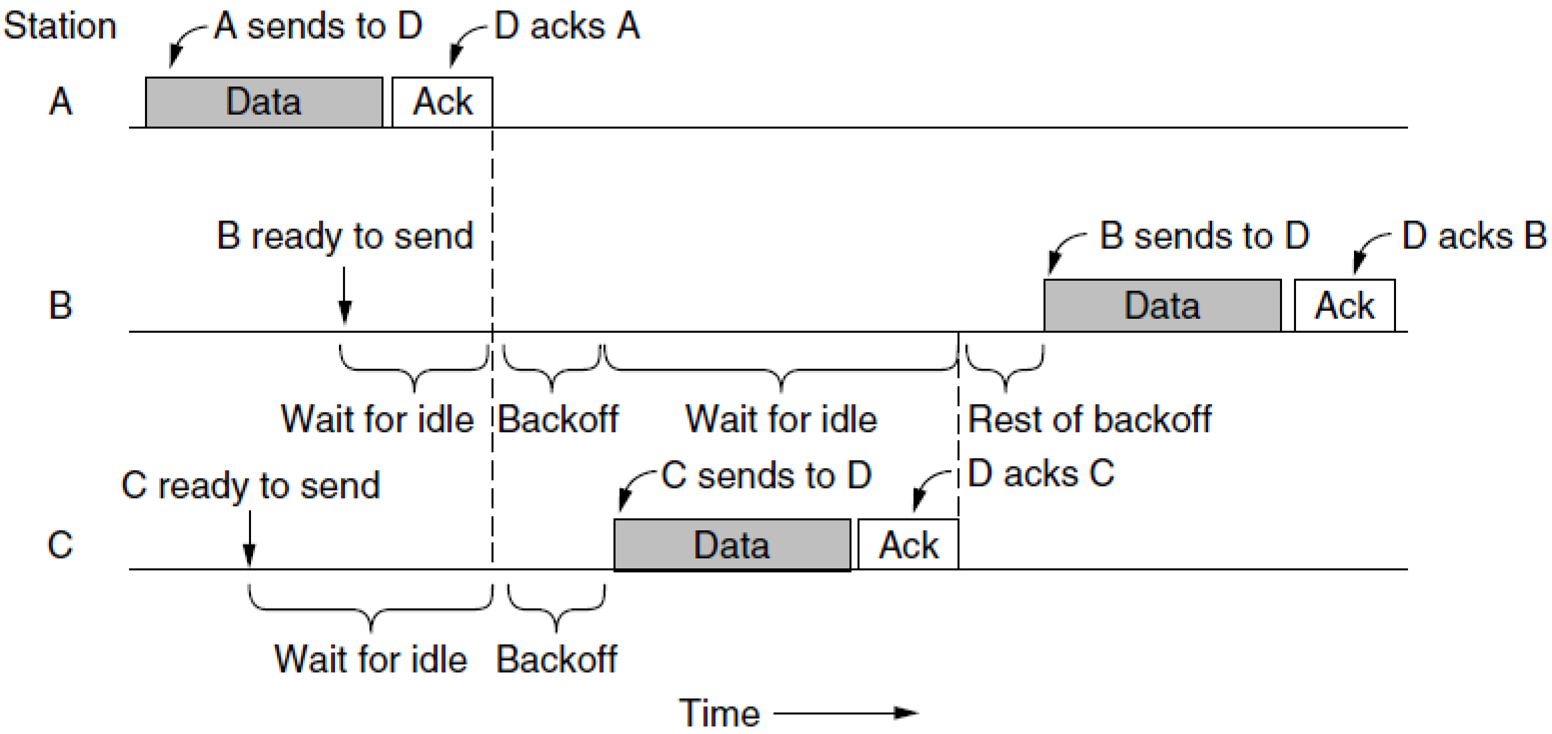
WLAN Physical layer	SIFS value
FHSS	28 µs
DSSS	10 µs
OFDM	6 µs
HR/DSSS	10 µs
ERP	10 µs

Times for DSSS

Time	In Microseconds
Slot	20
SIFS	10
AIFS	SIFS + AIFS#*Slot Time
DIFS	SIFS + 2 Slot Time
EIFS	AckFrame Time (at 1MB/s)+SIFS+DISF
Backoff Time	Random()X Slot Time

802.11 MAC (1)

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

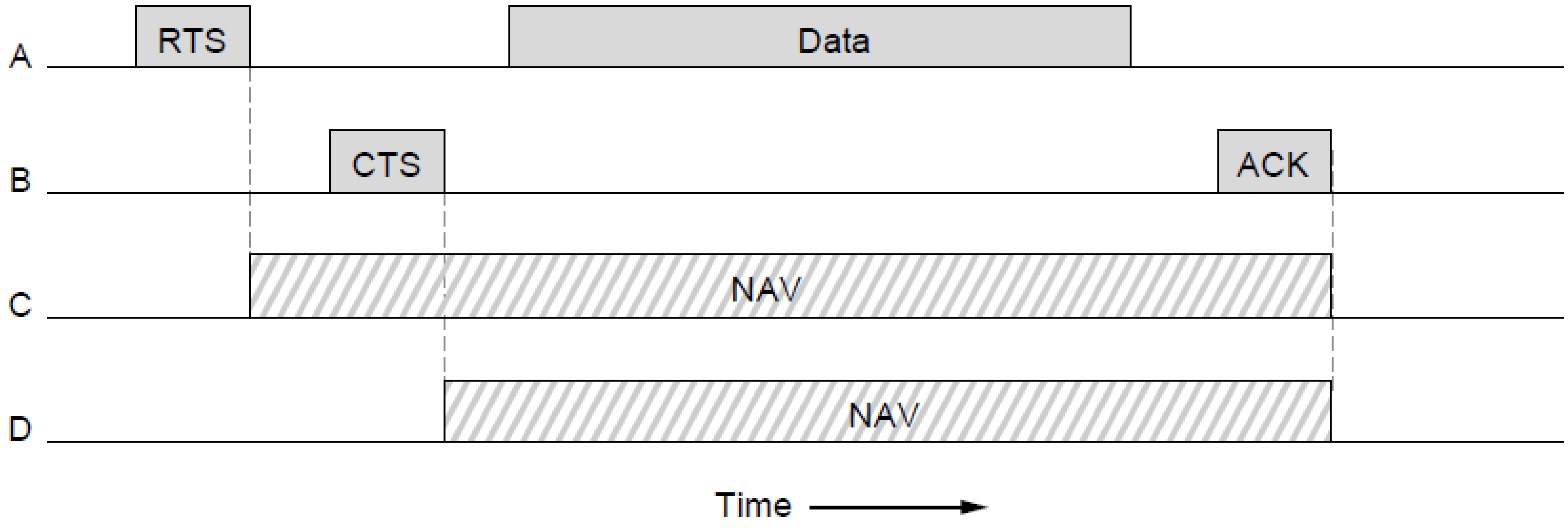


PCF Operation

- Poll – eliminates contention
- PC – Point Coordinator
  - Polling List
  - Over DCF
  - PIFS (less than DIFS ~ 30 μs)
- CFP – Contention Free Period
  - Alternate with DCF
- Periodic Beacon – contains length of CFP
- CF-Poll – Contention Free Poll
- NAV prevents during CFP
- CF-End – resets NAV

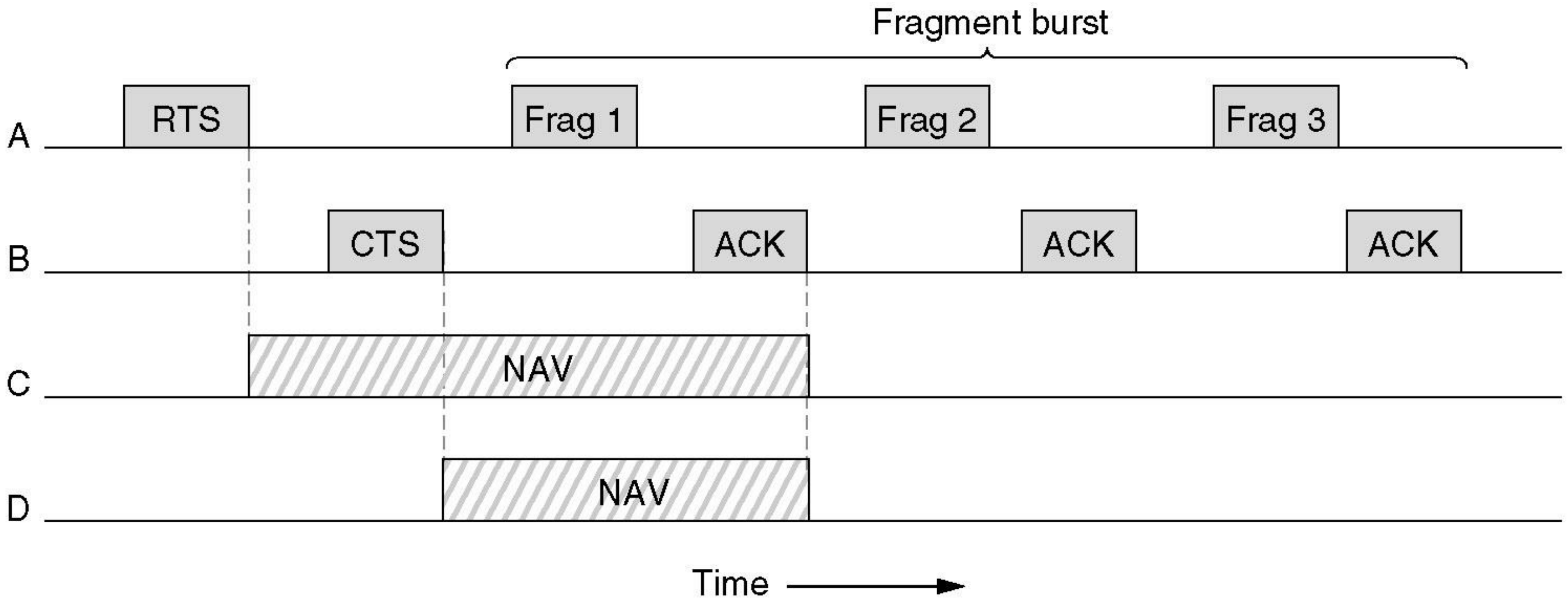
802.11 MAC (2)

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

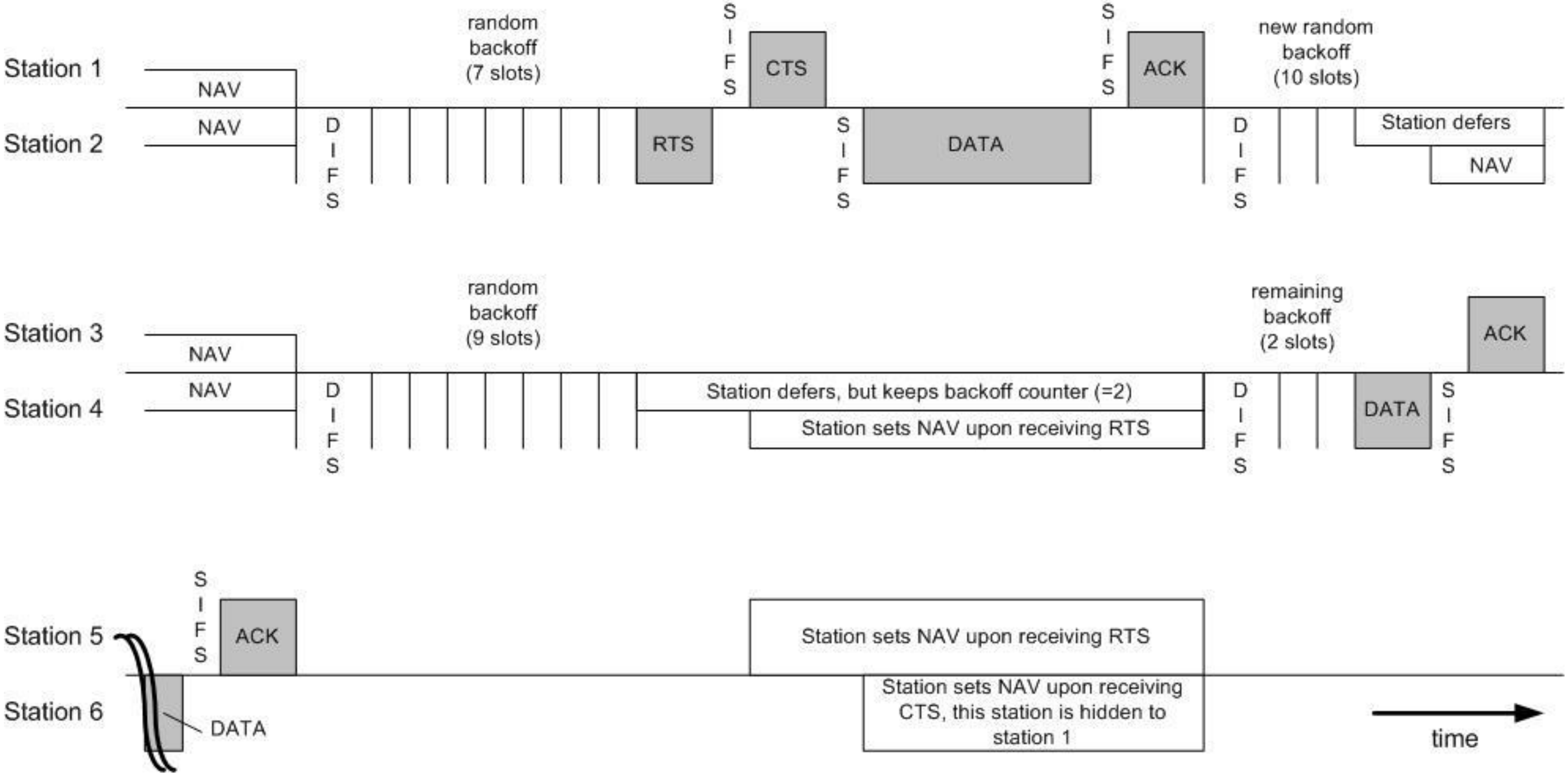


The 802.11 MAC Sublayer Protocol (3)

A fragment burst.



DCF Operation


Station 1
NAV
random backoff (7 slots)
SIFS
CTS
SIFS
ACK
new random backoff (10 slots)
Station 2
NAV
DIFS
RTS
SIFS
DATA
DIFS
Station defers
NAV
Station 3
NAV
random backoff (9 slots)
remaining backoff (2 slots)
ACK
Station 4
NAV
DIFS
Station defers, but keeps backoff counter (=2)
Station sets NAV upon receiving RTS
DIFS
DATA
SIFS
Station 5
SIFS
ACK
Station sets NAV upon receiving RTS
Station 6
DATA
Station sets NAV upon receiving CTS, this station is hidden to station 1
time

Services

- Station services:
  - authentication,
  - de-authentication,
  - privacy,
  - delivery of data
- Distribution Services *(A thin layer between MAC and LLC sublayer)*
  - association
  - disassociation
  - reassociation
  - distribution
  - Integration

A station maintain two variables:

- authentication state (=> 1)
- association state (<= 1)

Medium Access Control

Functionality;

- Reliable data delivery
- Fairly control access
- Protection of data

Deals;

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

MAC

- Retry Counters
  - Short retry counter
  - Long retry counter
  - Lifetime timer
- Basic Access Mechanism
  - CSMA/CA
  - Binary exponential back-off
  - NAV – Network Allocation Vector
- Timing Intervals: SIFS, Slot Time, PIFS, DIFS, EIFS
- DCF Operation
- PCF Operation

Other MAC Operations

- Fragmentation
  - Sequence control field
  - In burst
  - Medium is reserved
  - NAV is updated by ACK

- Privacy
  - WEP bit set when encrypted.
  - Only the frame body.
  - Medium is reserved
  - NAV is updated by ACK
  - Symmetric variable key

- WEP Details
  - Two mechanism
    - Default keys
    - Key mapping
  - WEP header and trailer
    - KEYID in header
    - ICV in trailer
  - *dot11UndecryptableCount*
    - *Indicates an attack.*
  - *dot11ICVErrorCount*
    - *Attack to determine a key is in progress.*

MAC Management

- Interference by users that have no concept of data communication. Ex: Microwave
- Interference by other WLANs
- Security of data
- Mobility
- Power Management

Authentication

- Authentication
  - Prove identity to another station.
  - Open system authentication
  - Shared key authentication
    - A sends
    - B responds with a text
    - A encrypt and send back
    - B decrypts and returns an authentication management frame.
  - May authenticate any number of station.

- Security Problem
  - A rogue AP
    - SSID of ESS
    - Announce its presence with beaconing
    - A active rogue reach higher layer data if unencrypted.

Association

- Association
  - Transparent mobility
  - After authentication
  - Association request to an AP
  - After established, forward data
  - To BSS, if DA is in the BSS.
  - To DS, if DA is outside the BSS.
  - To AP, if DA is in another BSS.
  - To "**portal**", if DC is outside the ESS.
  - **Portal** : transfer point : track mobility. (AP, bridge, or router) transfer 802.1h
  - New AP after reassociation, communicates with the old AP.

Address Filtering

- More than one WLAN
- Three Addresses
- Receiver examine the DA, BSSID

Privacy MAC Function

- WEP Mechanism

Power Management

- Independent BSS
  - Distributed
  - Data frame handshake
  - Wake up every beacon.
  - Awake a period of ATIM after each beacon.
  - Send ACK if receive ATIM frame & awake until the end of next ATIM.
  - Estimate the power saving station, and delay until the next ATIM.
  - Multicast frame : No ACK : optional

Overhead

- Sender
  - Announcement frame
  - Buffer
  - Power consumption in ATIM
- Receiver
  - Awake for every Beacon and ATIM

Power Management

- Infrastructure BSS
  - Centralized in the AP.
  - Greater power saving
  - Mobile Station sleeps for a number of beacon periods.
  - Awake for multicast indicated in DTIM in Beacon.
  - AP buffer, indicate in TIM
  - Mobile requests by PS-Poll

Synchronization

- Timer Synchronization in an Infrastructure BSS
  - Beacon contains TSF
  - Station updates its with the TSF in beacon.

- Timer Synchronization in an IBSS
  - Distributed. Starter of the BSS send TSF zero and increments.
  - Each Station sends a Beacon
  - Station updates if the TSF is bigger.
  - Small number of stations: the fastest timer value
  - Large number of stations: slower timer value due to collision.

- Synchronization with Frequency Hopping PHY Layers
  - Changes in a frequency hopping PHY layer occurs periodically (the dwell period).
  - Change to new channel when the TSF timer value, modulo the dwell period, is zero

Scanning & Joining

- Scanning
  - Passive Scanning : only listens for Beacon and get info of the BSS. Power is saved.
  - Active Scanning: transmit and elicit response from APs. If IBSS, last station that transmitted beacon responds. Time is saved.
- Joining a BSS
  - Syncronization in TSF and frequency : Adopt PHY parameters : The BSSID : WEP : Beacon Period : DTIM

Combining Management Tools

- Combine Power Saving Periods with Scanning
  - Instead of entering power saving mode, perform active scanning.
  - Gather information about its environments.
- Preauthentication
  - Scans and initiate an authentication
  - Reduces the time

Coordination Among Access Points

- To what extent do APs need to coordinate?
- Many early AP designs were complex
- The access points coordinated to provide seamless mobility similar to the cellular phone system
  - That is, the APs communicated amongst themselves to insure smooth handoff as a wireless computer moved from the region to another
  - Some designs measured signal strength and attempted to move a wireless node to a new AP
    - when the signal received at the new AP exceeded the signal strength at the existing AP

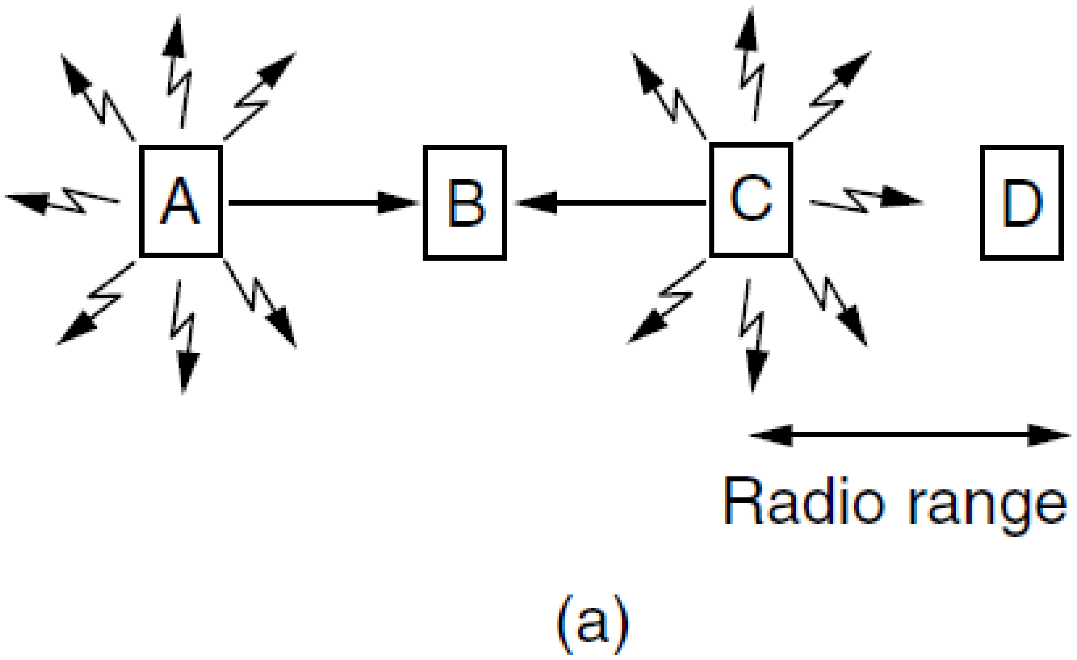
Coordination Among Access Points

- Some vendors began to offer lower cost, less complex APs that do not coordinate
- The vendors argue that signal strength does not provide a valid measure of mobility
  - a mobile computer can handle changing from one AP to another
  - and that the wired infrastructure connecting APs has sufficient capacity to allow more centralized coordination
- A less complex AP design is appropriate in situations where an installation consists of a single AP

Contention and Contention-Free Access

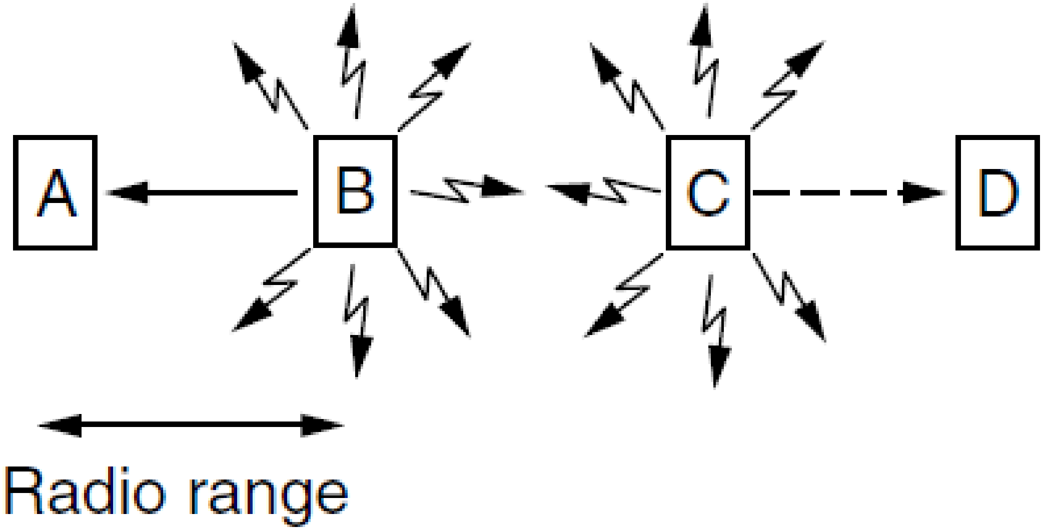
- The original 802.11 standard defined two general approaches for channel access
  - Point Coordinated Function (PCF) for contention-free service
    - an AP controls stations in the Basic Service Set (BSS) to insure that transmissions do not interfere with one another
    - For example, an AP can assign each station a separate frequency
    - In practice, PCF is never used
  - Distributed Coordinated Function (DCF) for contention-based service
    - arranges for each station in a BSS to run a random access protocol
- Wireless networks can experience a hidden station problem
  - where two stations can communicate but a third station can only receive the signal from one of them
- 802.11 networks use CSMA/CA
  - which requires a pair to exchange Ready To Send (RTS) and Clear To Send (CTS) messages before transmitting a packet

Hidden Terminal



A wireless LAN. (a) A and C are hidden terminals when transmitting to B.

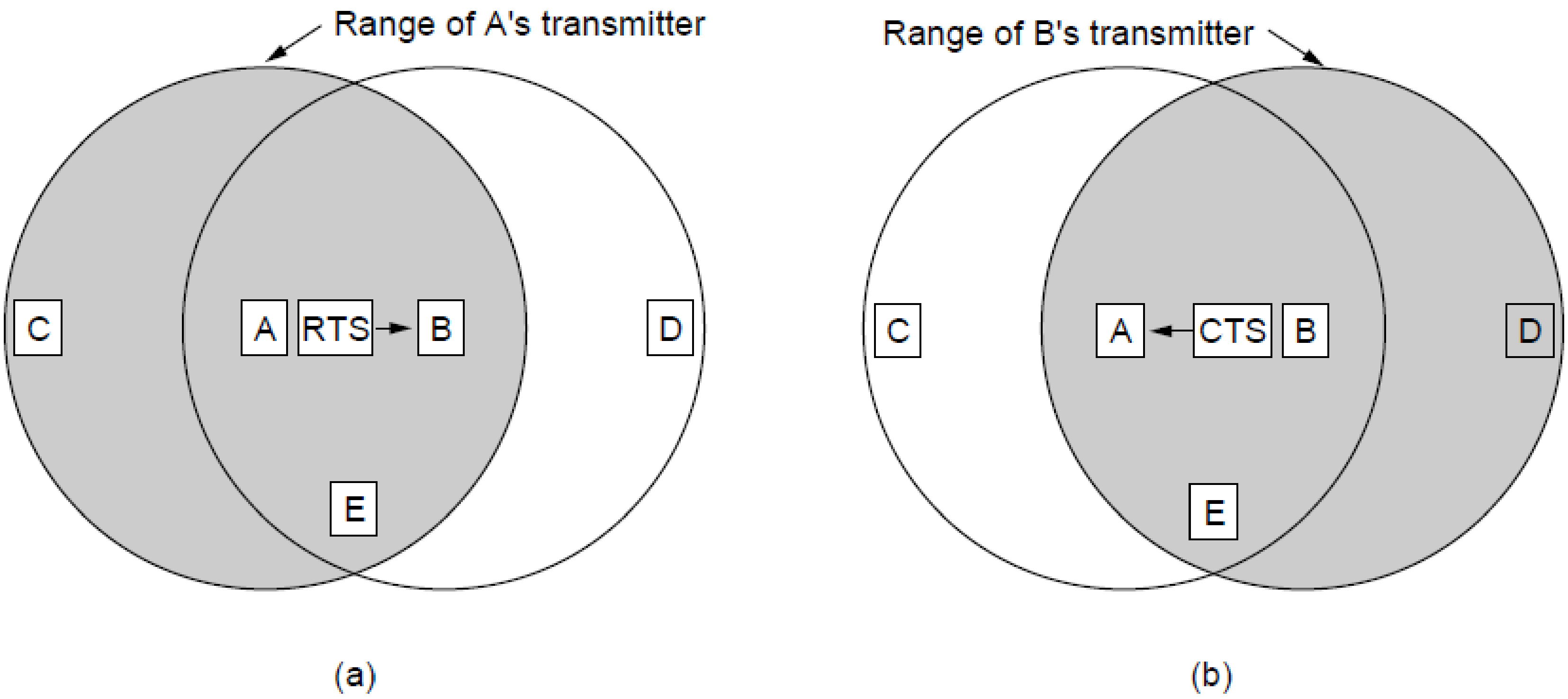
Exposed Terminal



(b)

A wireless LAN. (b) B and C are exposed terminals when transmitting to A and D.

RTS/CTS



The MACA protocol. (a) *A sending an RTS to B. (b) B responding* with a CTS to *A.*

Contention and Contention-Free Access

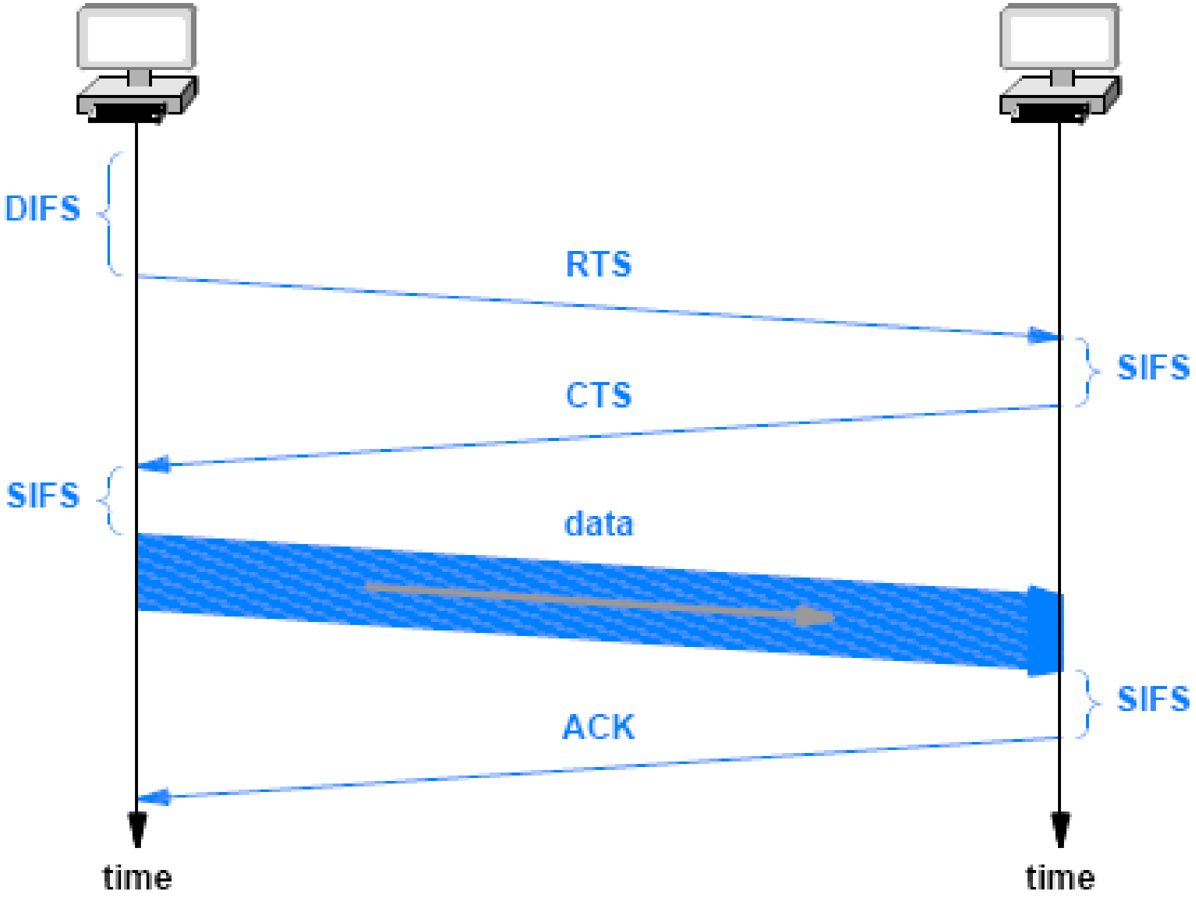
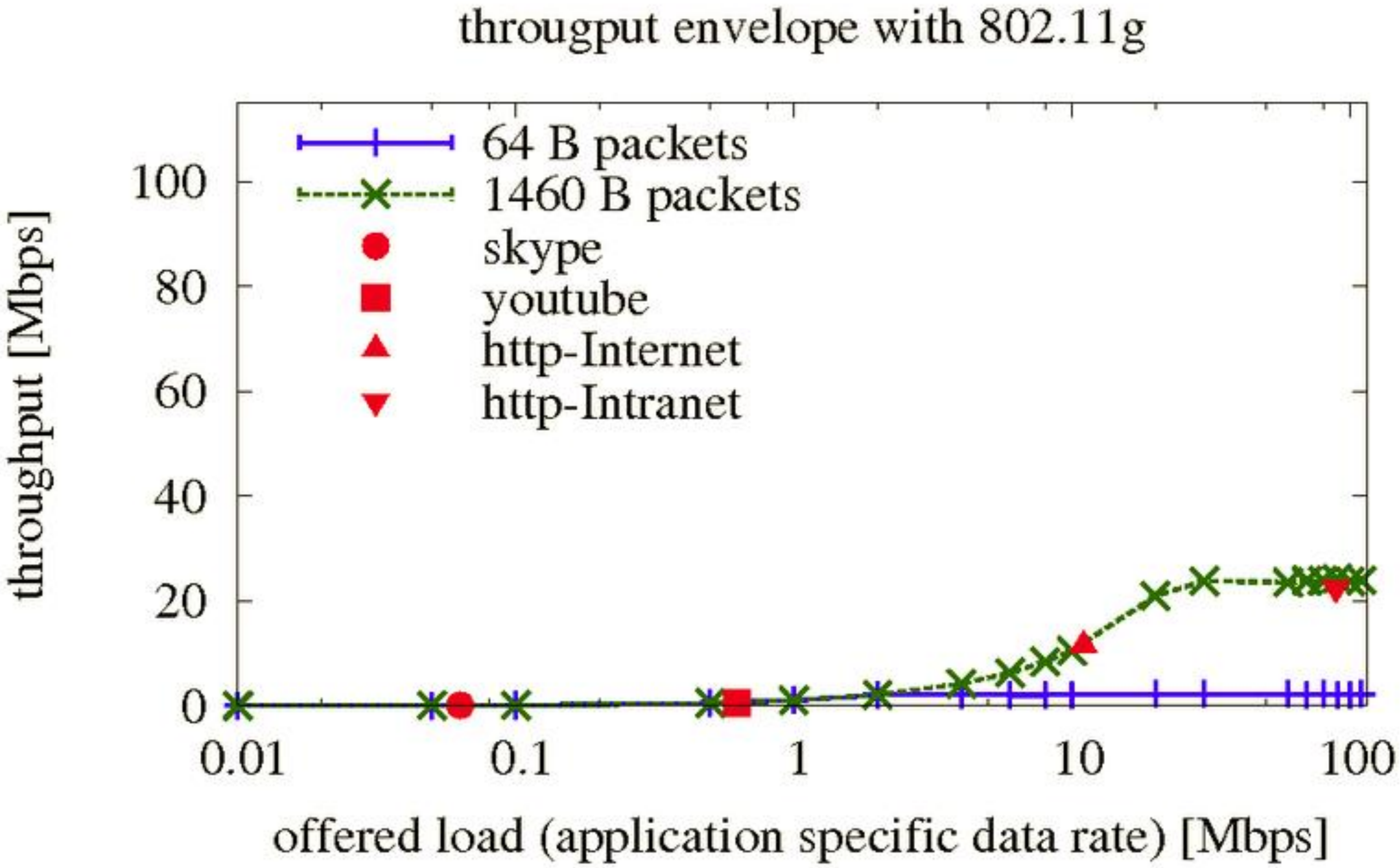


Illustration of CSMA/CA with SIFS and DIFS timing.

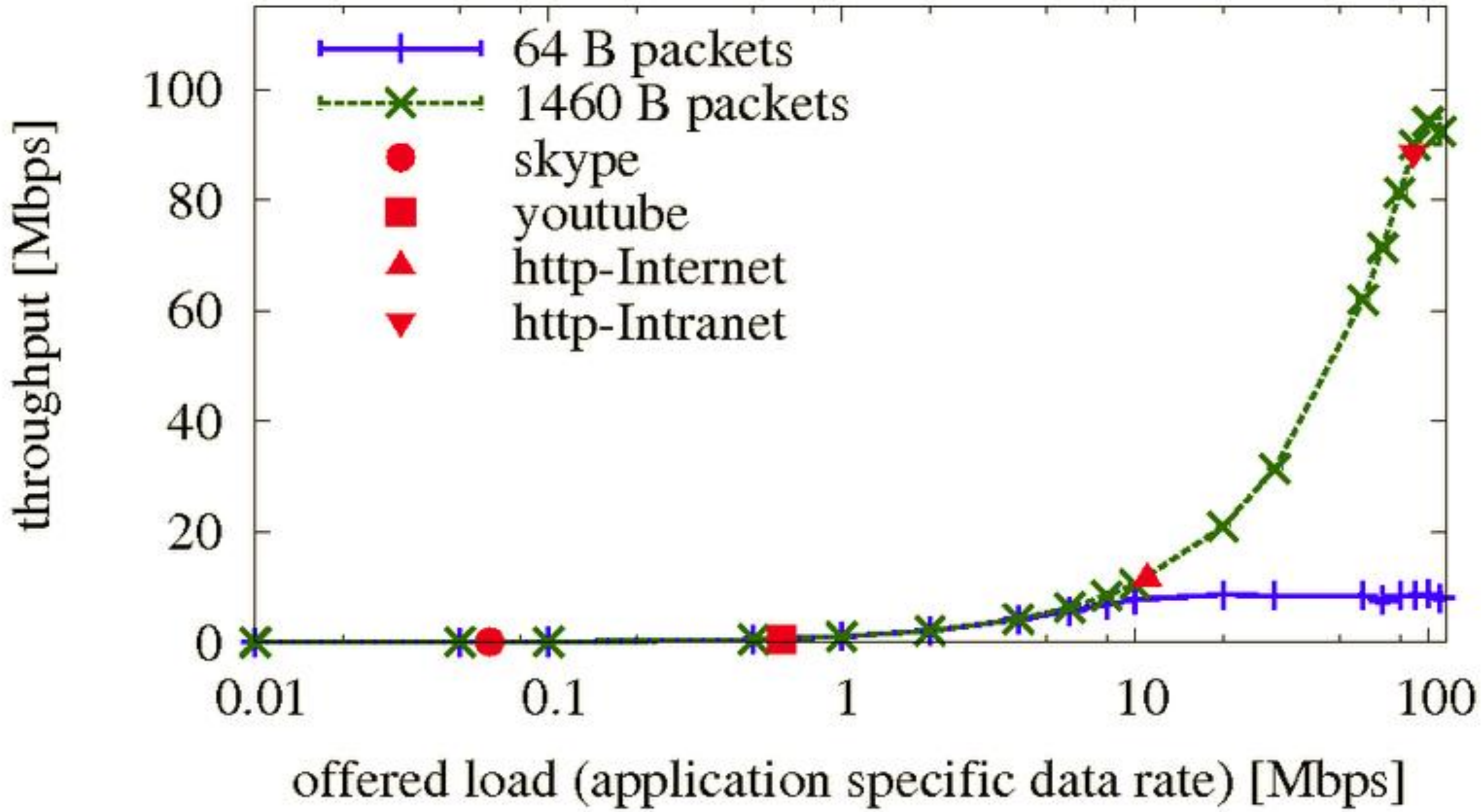
Contention and Contention-Free Access

- Physical separation among stations and electrical noise makes it difficult to distinguish between
  - weak signals, interference, and collisions
- Wi-Fi networks do not employ collision detection
  - That is, the hardware does not attempt to sense interference during a transmission
  - Instead, a sender waits for an acknowledgement (ACK) message
  - If no ACK arrives, the sender assumes the transmission was lost
    - and employs a backoff strategy similar to the strategy in wired Ethernet
- In practice, 802.11 networks that have few users and do not experience electrical interference seldom need retransmission
  - However, other 802.11 networks experience frequent packet loss and depend on retransmission



througput envelope with 802.11g

througput envelope with 802.11n (40MHz Channelwidth)



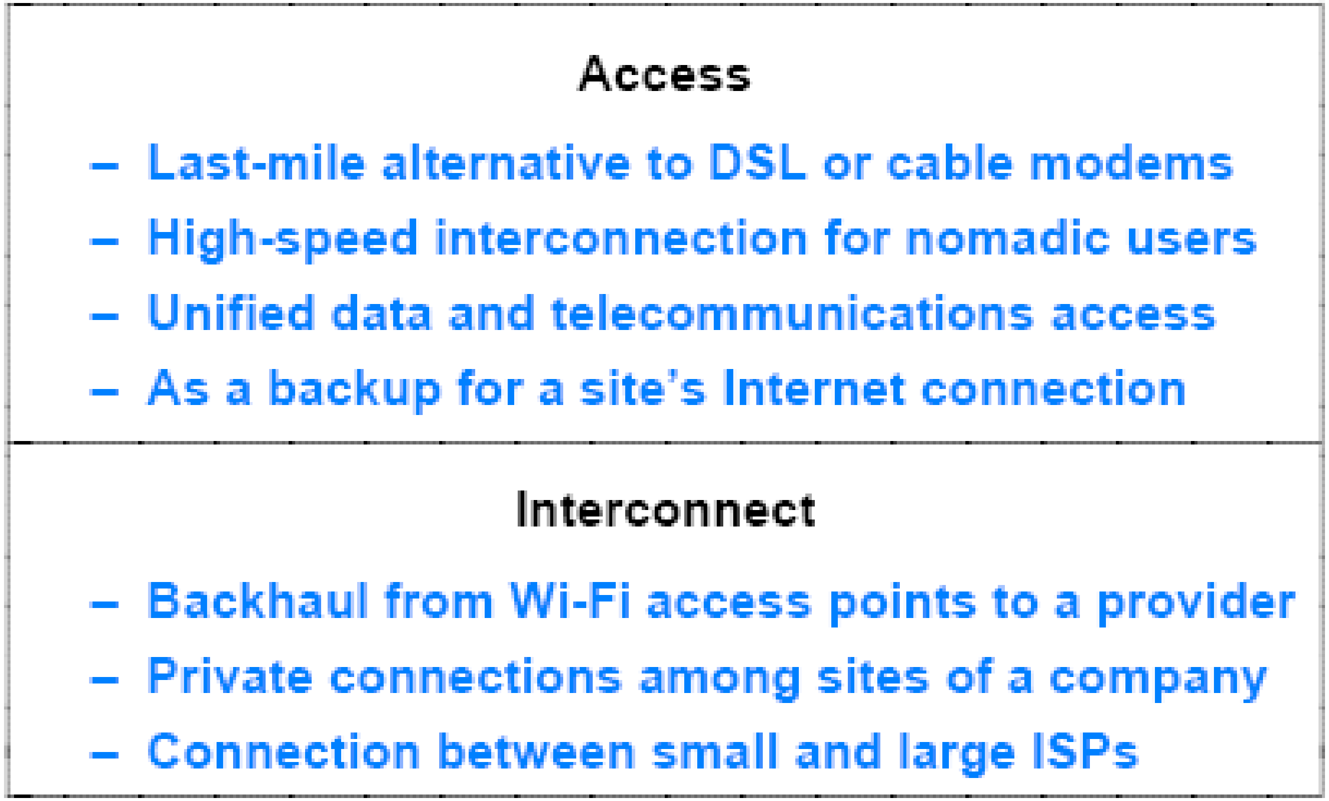
Wireless MAN Technology and WiMax

- Standardized by IEEE under the category 802.16
- A group of companies coined the term (WiMax)
  - which is interpreted to mean World-wide Interoperability for Microwave Access
  - and they formed WiMAX Forum to promote use of the technology
- Two main versions of WiMAX are being developed that differ in their overall approach:
- Fixed WiMAX
  - refers to systems built using IEEE 802.16-2004, which is informally called 802.16d
  - the technology does not provide for handoff among access points
  - designed to provide connections between a service provider and a fixed location
    - such as a residence or office building, rather than between a provider and a cell phone
- Mobile WiMAX

Wireless MAN Technology and WiMax

- Mobile WiMAX
  - built according to standard 802.16e-2005, known also as 802.16e
  - the technology offers handoff among APs
    - which means a mobile WiMAX system can be used with portable devices such as laptop computers or cell phones
- WiMAX offers broadband communication that can be used in a variety of ways:
  - WiMAX can be used as an Internet access technology
  - WiMAX can provide a general-purpose interconnection among physical sites
    - especially in a city
  - To be used as backhaul connection between a service provider's central network facility and remote locations
    - such as cell towers

Wireless MAN Technology and WiMax



Access

- Last-mile alternative to DSL or cable modems
- High-speed interconnection for nomadic users
- Unified data and telecommunications access
- As a backup for a site's Internet connection

Interconnect

- Backhaul from Wi-Fi access points to a provider
- Private connections among sites of a company
- Connection between small and large ISPs

Potential uses of WiMAX technology.

Wireless MAN Technology and WiMax

- Deployments of WiMAX used for backhaul will have the highest data rates
- It will use frequencies that require a clear Line-Of-Sight (LOS) between two entities
  - LOS stations are typically mounted on towers or on tops of buildings
- Deployments used for Internet access may use fixed or mobile WiMAX
  - such deployments usually use frequencies that do not require LOS
  - thus, they are classified as Non-Line-Of-Sight (NLOS)

Wireless MAN Technology and WiMax

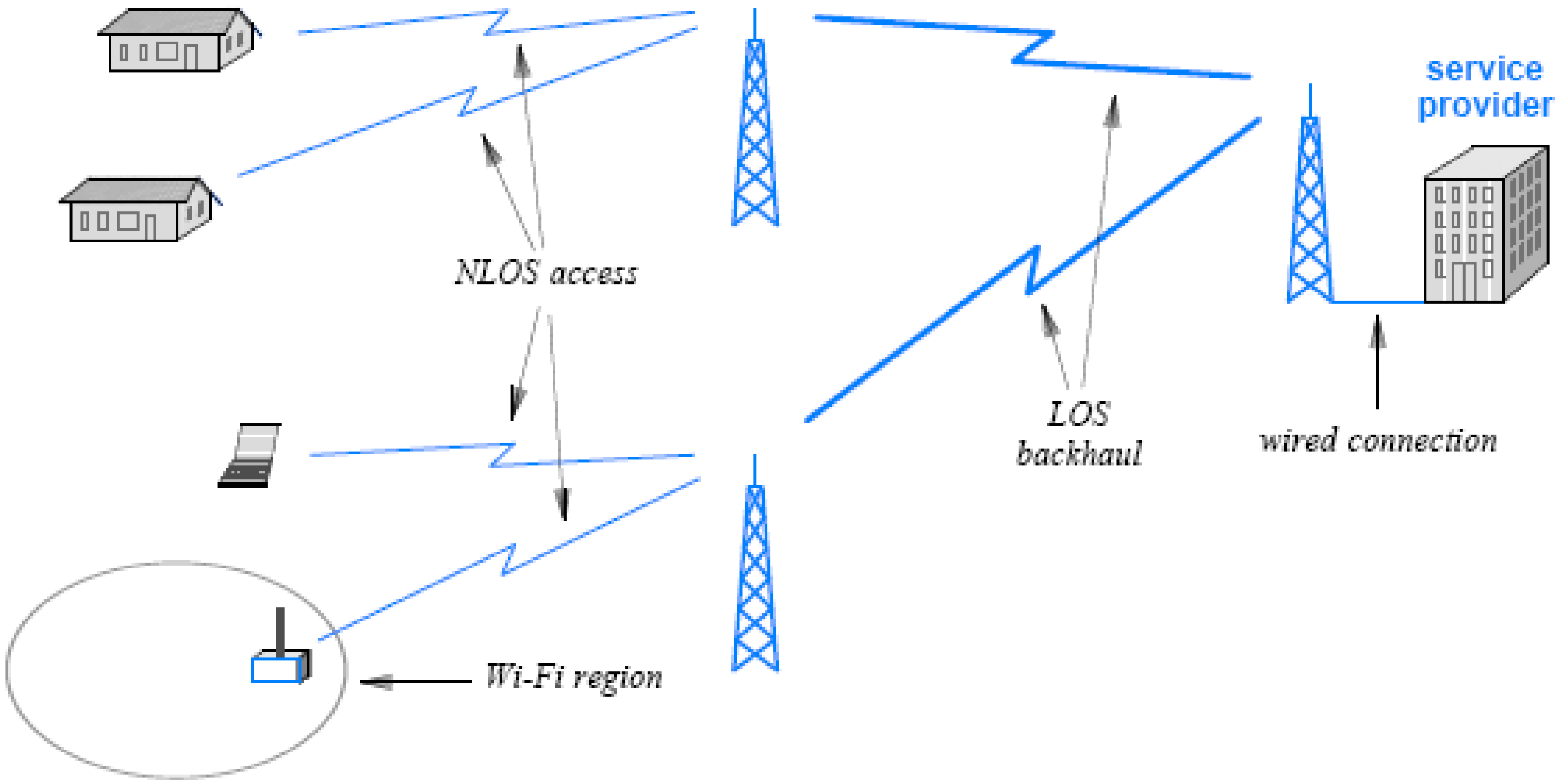
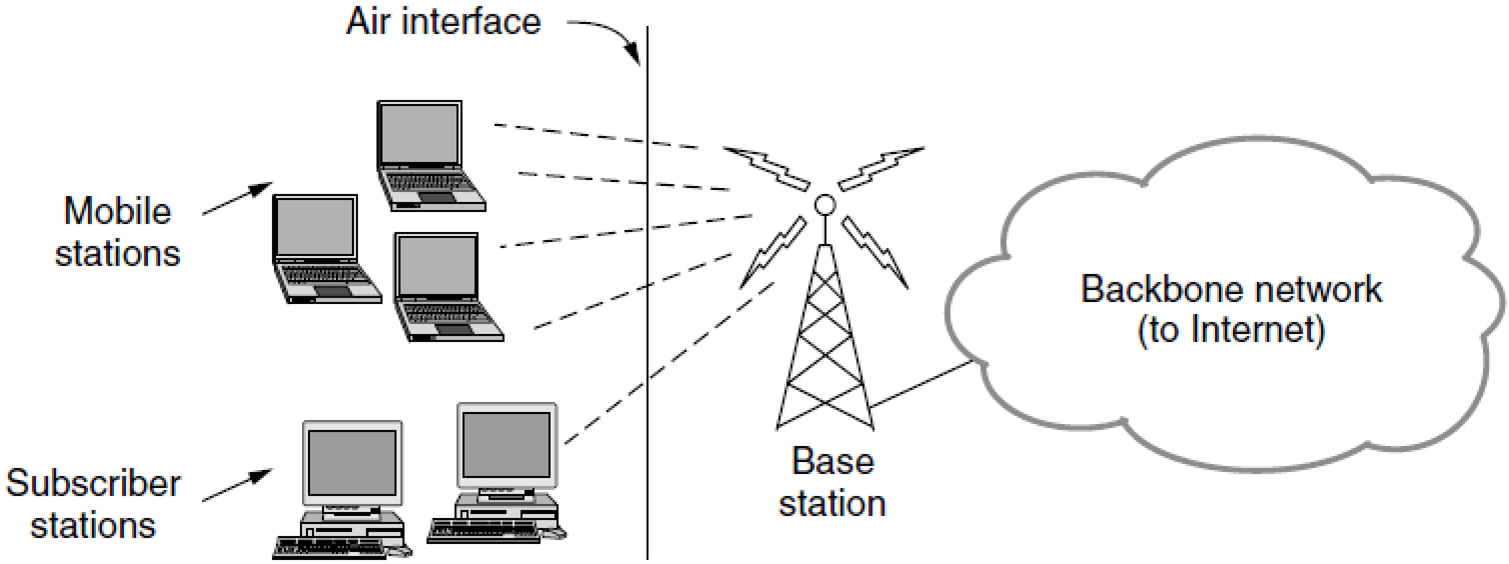


Illustration of WiMAX used for access and backhaul.

Wireless MAN Technology and WiMax

- The key features of WiMAX can be summarized as follows:
  - Uses licensed spectrum (i.e., offered by carriers)
  - Each cell can cover a radius of 3 to 10 Km
  - Uses scalable orthogonal FDM
  - Guarantees quality of services (for voice or video)
  - Can transport 70 Mbps in each direction at short distances
  - Provides 10 Mbps over a long distance (10 Km)

Comparison of 802.16 with 802.11 and 3G

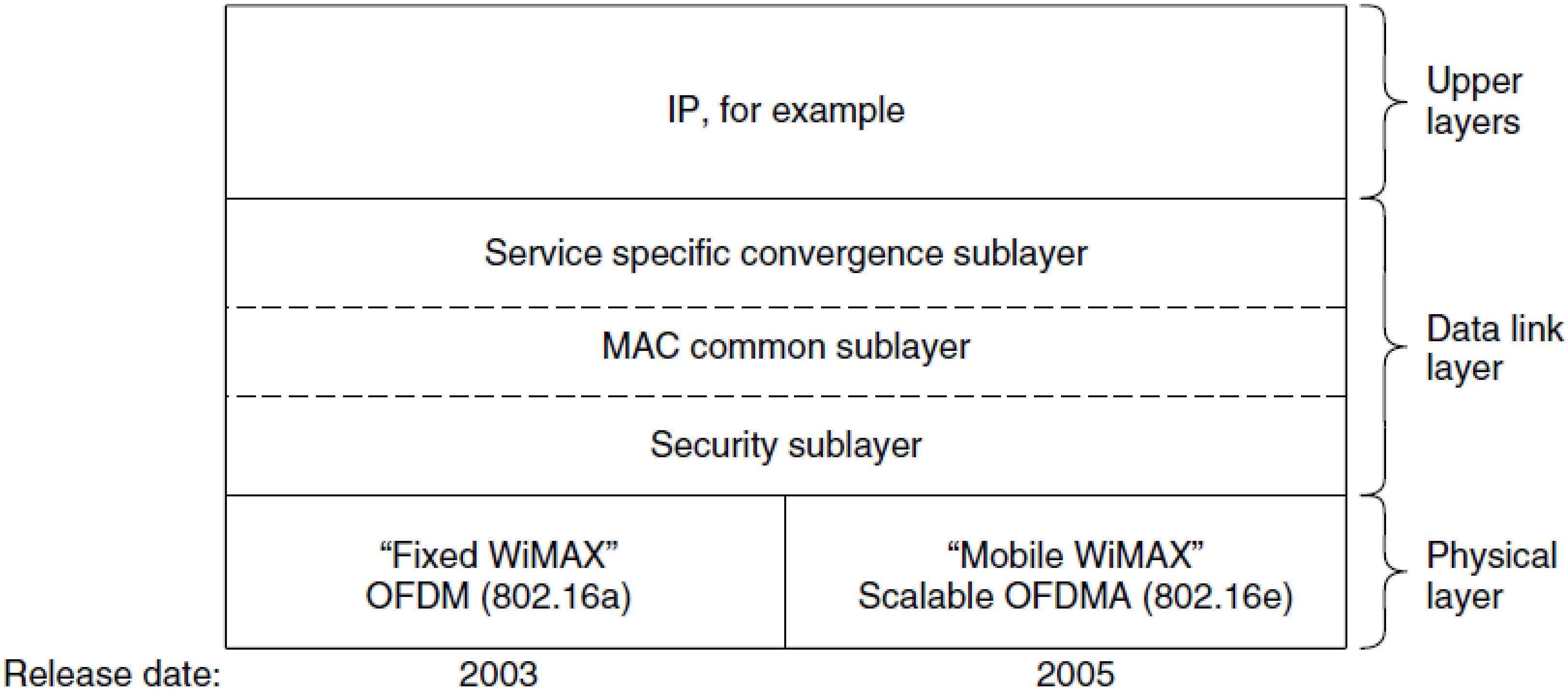


The 802.16 architecture

802.16 Architecture/Protocol Stack (2)

MAC is connection-oriented; IP is connectionless

- Convergence sublayer maps between the two



IP, for example

Service specific convergence sublayer

MAC common sublayer

Security sublayer

"Fixed WiMAX"
OFDM (802.16a)

"Mobile WiMAX"
Scalable OFDMA (802.16e)

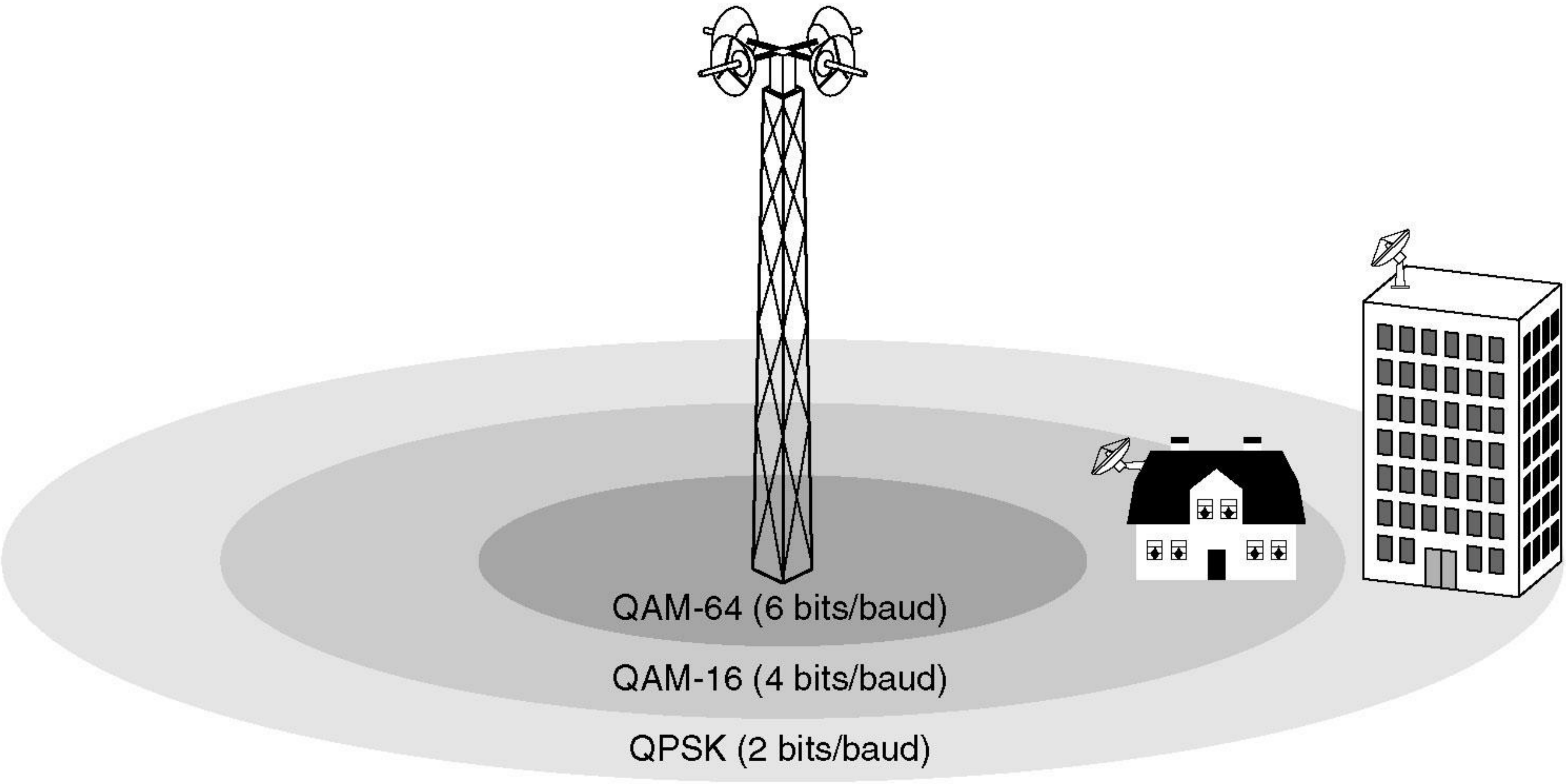
Upper layers

Data link layer

Physical layer

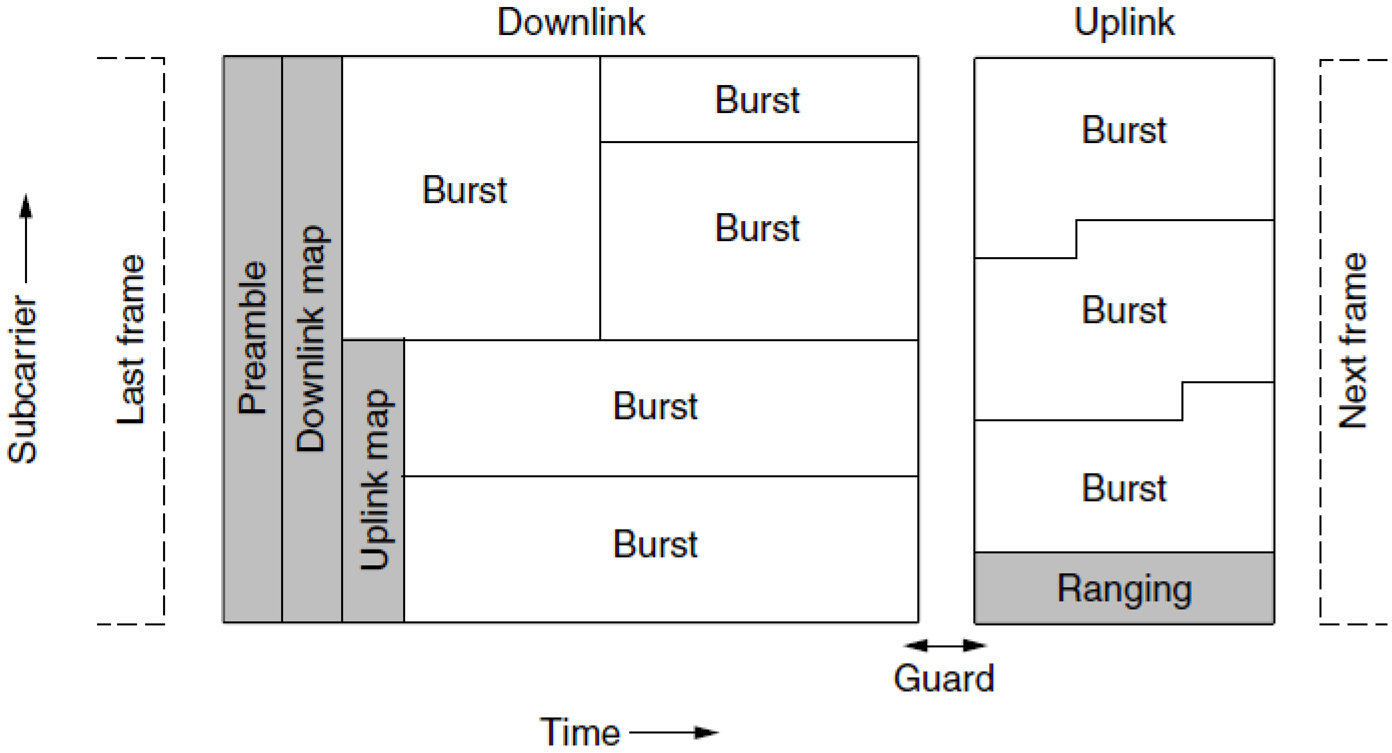
Release date: 2003 2005

The 802.16 Physical Layer



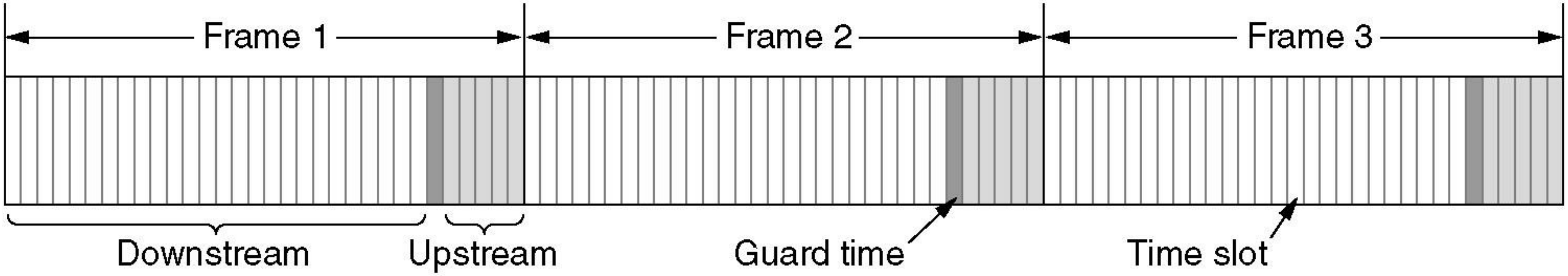
The 802.16 transmission environment.

802.16 Physical Layer



The 802.16 Physical Layer (2)

Frames and time slots for time division duplexing.



802.16 MAC

Connection-oriented with base station in control

- Clients request the bandwidth they need

Different kinds of service can be requested:

- Constant bit rate, e.g., uncompressed voice
- Real-time variable bit rate, e.g., video, Web
- Non-real-time variable bit rate, e.g., file download
- Best-effort for everything else

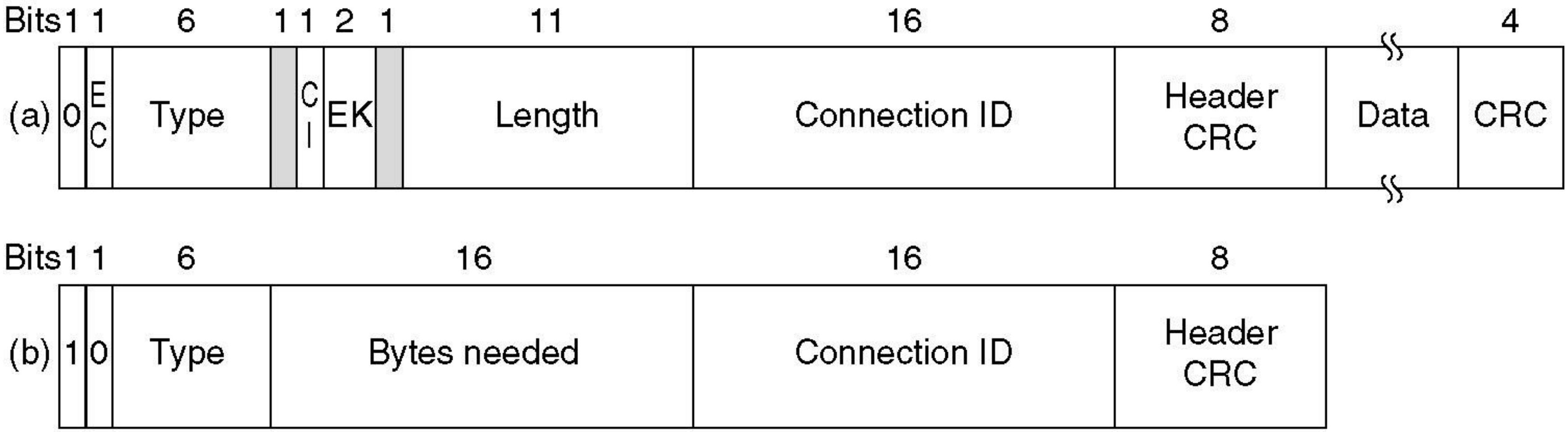
802.16 MAC Sublayer Protocol

Classes of service

1. Constant bit rate service.
2. Real-time variable bit rate service.
3. Non-real-time variable bit rate service.
4. Best-effort service.

The 802.16 Frame Structure

(a) A generic frame. (b) A bandwidth request frame.

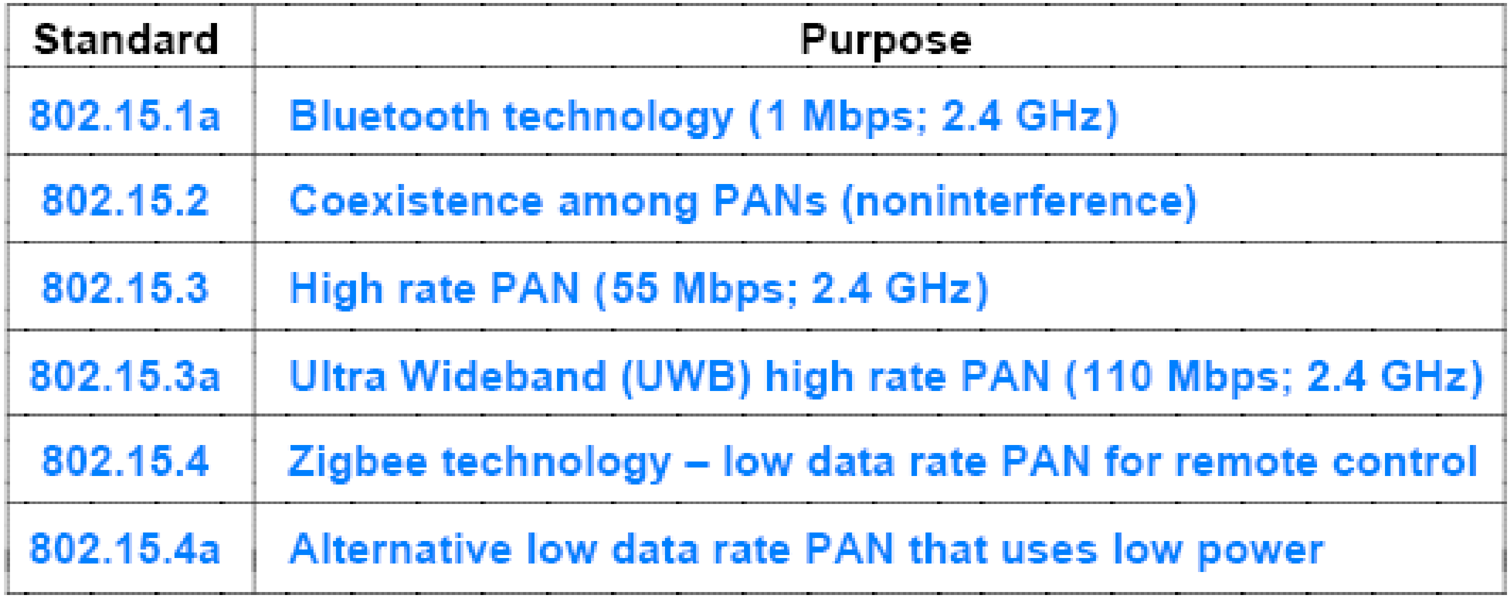


Bits	1	1	6	1	1	2	1	11	16	8		4
(a)	0	EC	Type	▨	CI	EK	▨	Length	Connection ID	Header CRC	Data	CRC

Bits	1	1	6	16	16	8
(b)	1	0	Type	Bytes needed	Connection ID	Header CRC

PAN Technologies and Standards

- IEEE has assigned the number 802.15 to PAN standards
- Several task groups and industry consortia have been formed for each of the key PAN technologies



Standard	Purpose
802.15.1a	Bluetooth technology (1 Mbps; 2.4 GHz)
802.15.2	Coexistence among PANs (noninterference)
802.15.3	High rate PAN (55 Mbps; 2.4 GHz)
802.15.3a	Ultra Wideband (UWB) high rate PAN (110 Mbps; 2.4 GHz)
802.15.4	Zigbee technology – low data rate PAN for remote control
802.15.4a	Alternative low data rate PAN that uses low power

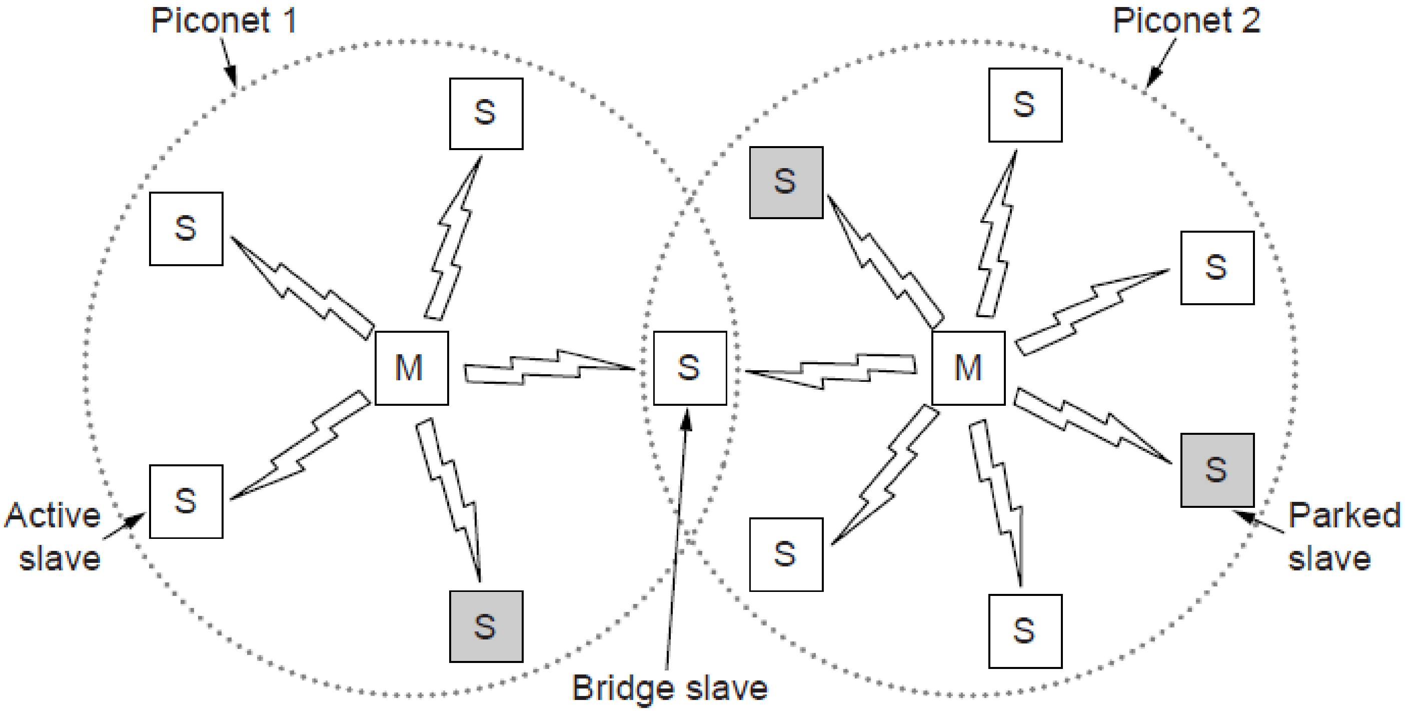
PAN Technologies and Standards

- Bluetooth
  - The IEEE 802.15.1a standard evolved after vendors created Bluetooth technology as a short-distance wireless connection technology
- The characteristics of Bluetooth technology are:
  - Wireless replacement for cables (e.g., headphones or mouse)
  - Uses 2.4 GHz frequency band
  - Short distance (up to 5 meters, with variations that extend the range to 10 or 50 meters)
  - Device is master or slave
  - Master grants permission to slave
  - Data rate is up to 721 Kbps

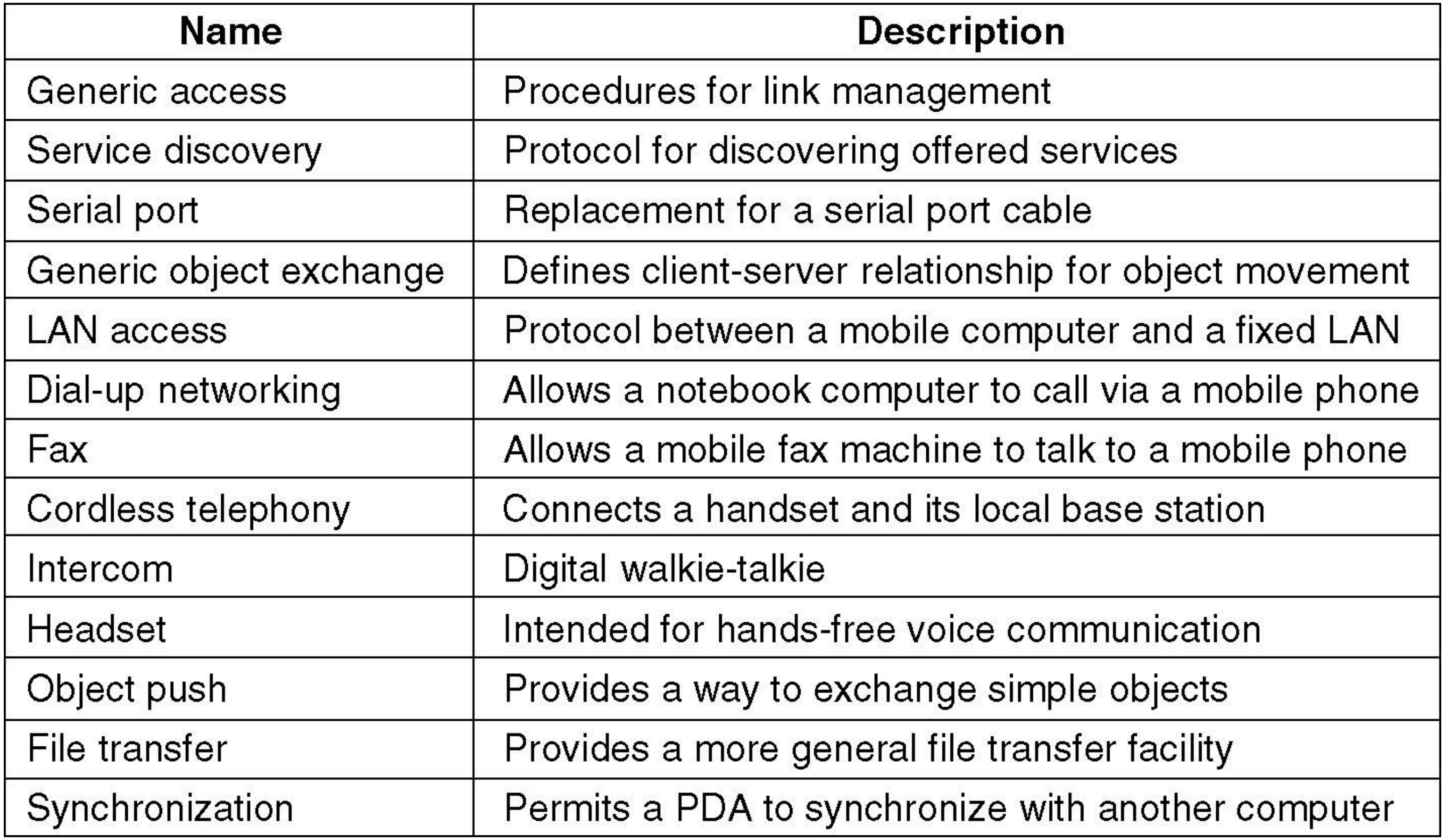
Bluetooth Architecture

Piconet master is connected to slave wireless devices

- Slaves may be asleep (parked) to save power



Bluetooth Applications

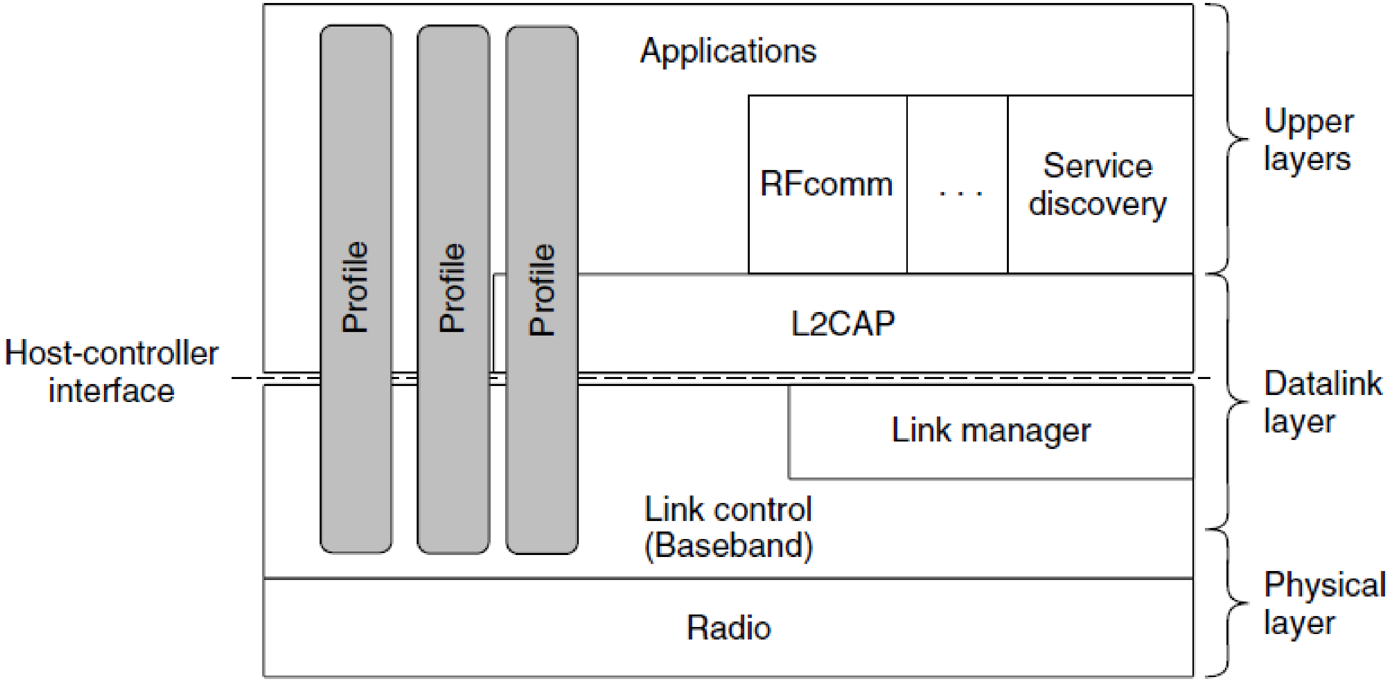


Name	Description
Generic access	Procedures for link management
Service discovery	Protocol for discovering offered services
Serial port	Replacement for a serial port cable
Generic object exchange	Defines client-server relationship for object movement
LAN access	Protocol between a mobile computer and a fixed LAN
Dial-up networking	Allows a notebook computer to call via a mobile phone
Fax	Allows a mobile fax machine to talk to a mobile phone
Cordless telephony	Connects a handset and its local base station
Intercom	Digital walkie-talkie
Headset	Intended for hands-free voice communication
Object push	Provides a way to exchange simple objects
File transfer	Provides a more general file transfer facility
Synchronization	Permits a PDA to synchronize with another computer

Bluetooth Applications / Protocol Stack

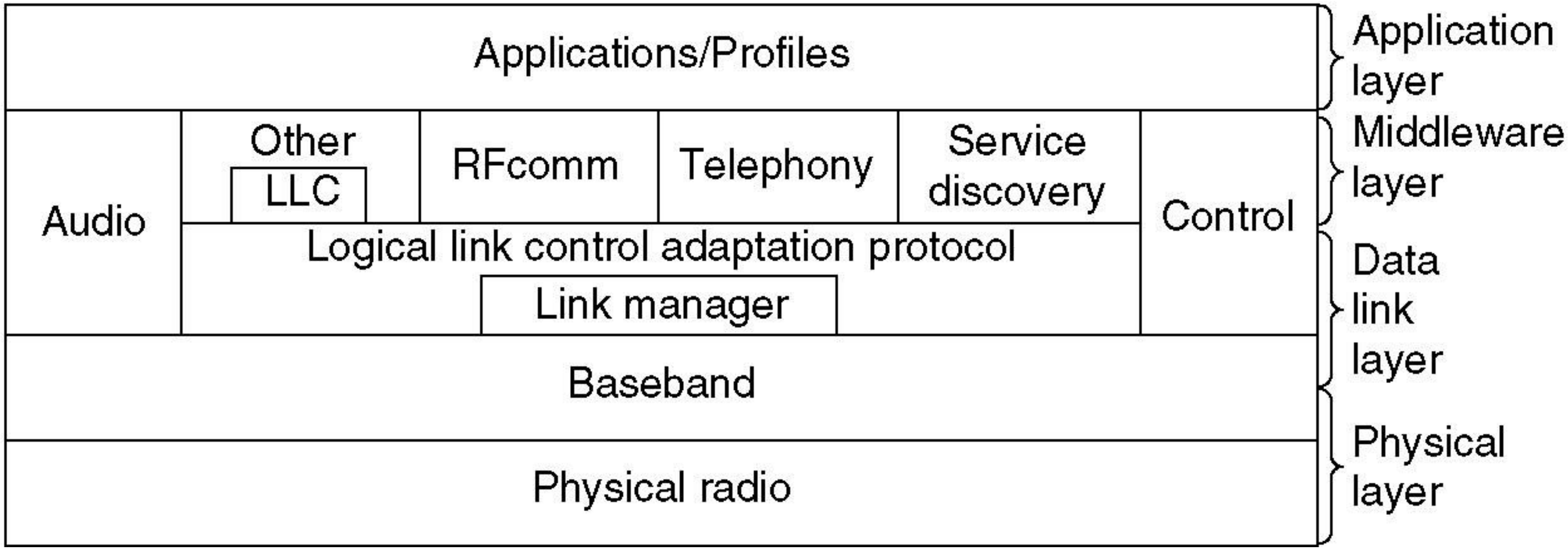
Profiles give the set of protocols for a given application

- 25 profiles, including headset, intercom, streaming audio, remote control, personal area network, …



The Bluetooth Protocol Stack

The 802.15 version of the Bluetooth protocol architecture.



Applications/Profiles

Audio

Other

LLC

RFcomm

Telephony

Service discovery

Control

Logical link control adaptation protocol

Link manager

Baseband

Physical radio

Application layer

Middleware layer

Data link layer

Physical layer

Bluetooth Radio / Link Layers

Radio layer

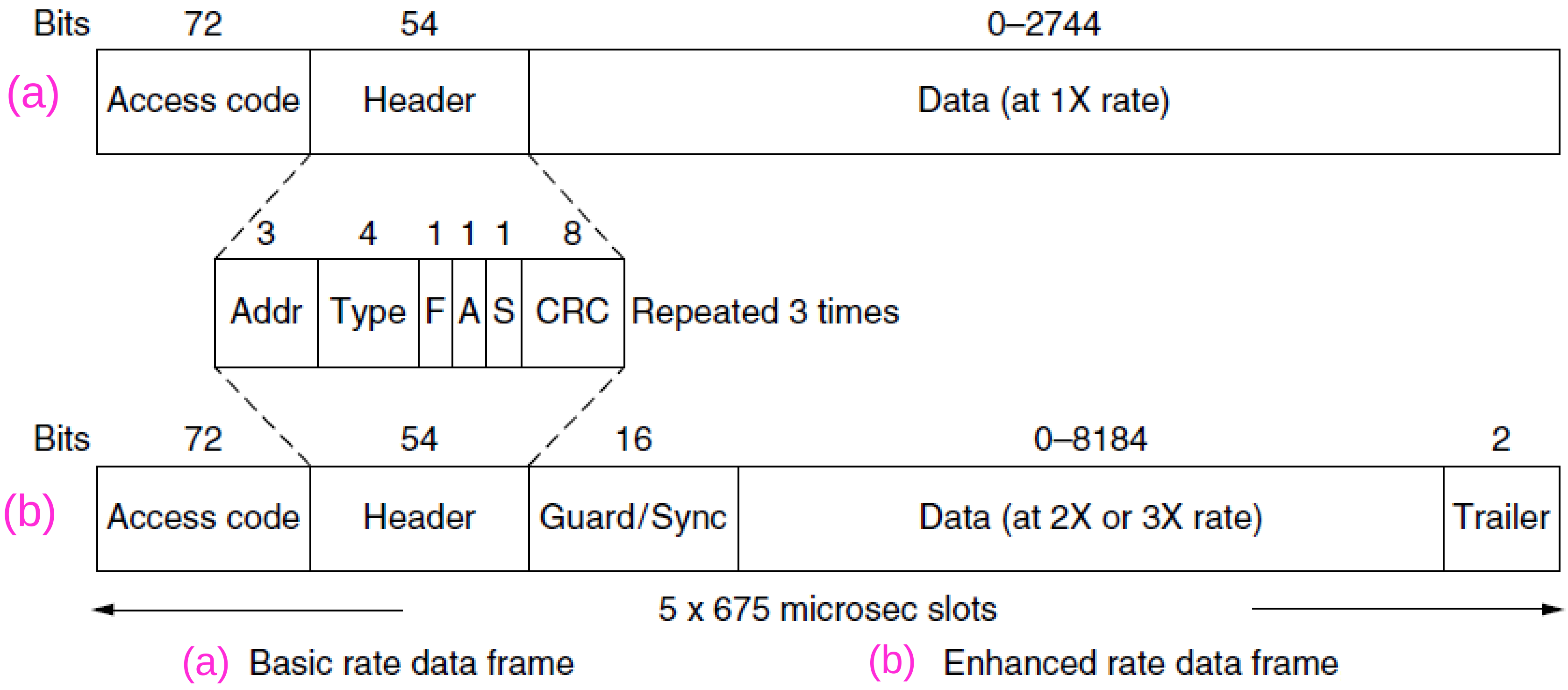
- Uses adaptive frequency hopping in 2.4 GHz band

Link layer

- TDM with timeslots for master and slaves
- Synchronous CO for periodic slots in each direction
- Asynchronous CL for packet-switched data
- Links undergo pairing (user confirms passkey/PIN) to authorize them before use

Bluetooth Frames

Time is slotted; enhanced data rates send faster but for the same time; addresses are only 3 bits for 8 devices



(a) Basic rate data frame (b) Enhanced rate data frame

PAN Technologies and Standards

- Ultra Wideband (UWB)
  - The idea behind UWB communication is that spreading data across many frequencies
    - requires less power to reach the same distance
- The key characteristics of UWB are:
  - Uses wide spectrum of frequencies
  - Consumes very low power
  - Short distance (2 to 10 meters)
  - Signal permeates obstacles such as walls
  - Data rate of 110 at 10 meters, and up to 500 Mbps at 2 meters
  - IEEE unable to resolve disputes and form a single standard

PAN Technologies and Standards

- Zigbee
  - The Zigbee standard (802.15.4) arose from a desire to standardize wireless remote control technology
    - especially for industrial equipment
  - Because remote control units only send short command
    - high data rates are not required
- The chief characteristics of Zigbee are:
  - Wireless standard for remote control, not data
  - Target is industry as well as home automation
  - Three frequency bands used (868 MHz, 915 MHz, and 2.4 GHz)
  - Data rate of 20, 40, or 250 Kbps, depending on frequency band
  - Low power consumption
  - Three levels of security being defined

Other Short-Distance Communication Technologies

- Two other wireless technologies provide communication over short distances, but they are not listed under PANs
  - InfraRED technologies provide control and low-speed data communications
  - RFID technologies are used with sensors

Other Short-Distance Communication Technologies

- InfraRED
  - InfraRED technology is often used in remote controls
    - and may be used as a cable replacement (e.g., for a wireless mouse)
  - The Infrared Data Association (IrDA) has produced a set of standards that are widely accepted
- The chief characteristics of the IrDA technology are:
  - Family of standards for various speeds and purposes
  - Practical systems have range of one to several meters
  - Directional transmission with a cone covering 30
  - Data rates between 2.4 Kbps (control) and 16 Mbps (data)
  - Generally low power consumption with very-low power versions
  - Signal may reflect from surfaces
    - but cannot penetrate solid objects

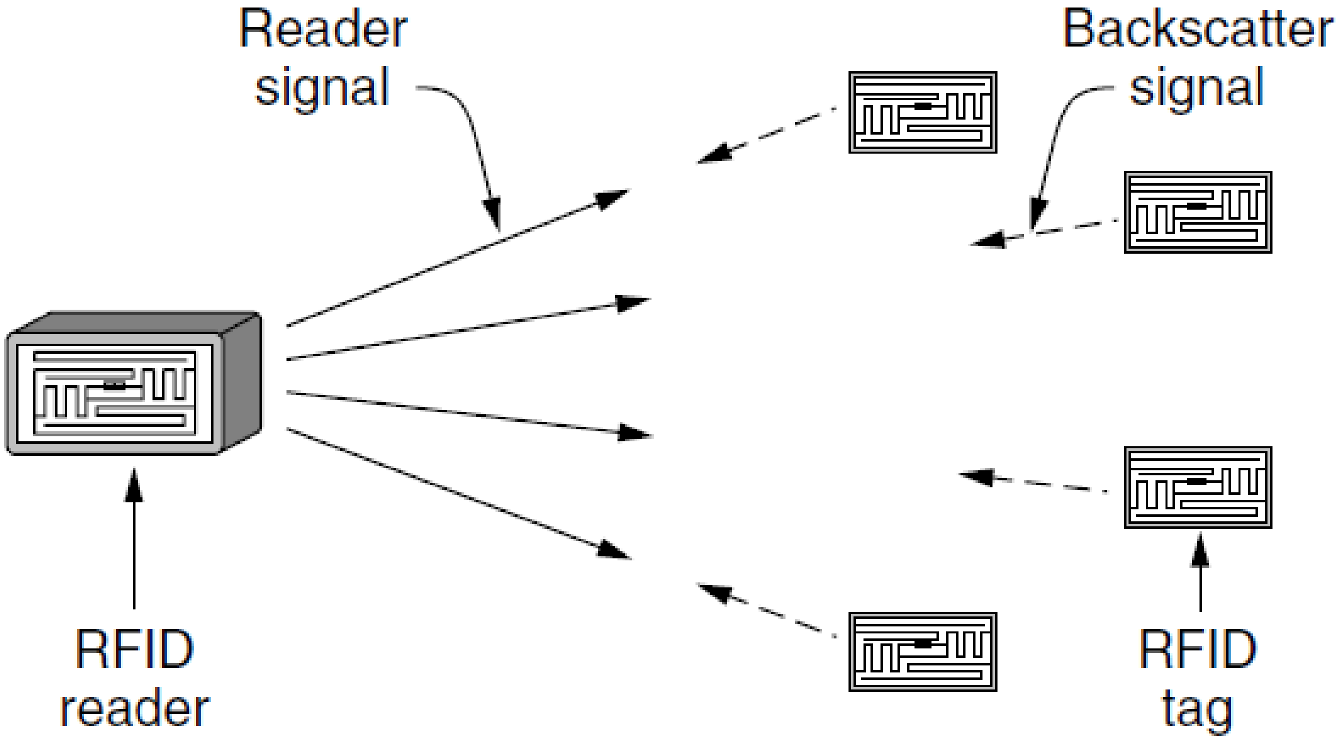
Other Short-Distance Communication Technologies

- Radio Frequency Identification (RFID)
  - RFID technology uses an interesting form of wireless communication to create a mechanism
  - A small tag contains identification information
    - that a receiver can “pull” from the tag
- Some features of RFID:
  - Over 140 RFID standards exist for a variety of applications
  - Passive RFIDs draw power from the signal sent by the reader
  - Active RFIDs contain a battery
    - which may last up to 10 years
  - Limited distance
    - although active RFIDs extend farther than passive
  - Can use frequencies from less than 100 MHz to 868-954 MHz
  - Used for
    - inventory control, sensors, passports, and other applications

RFID

- EPC Gen 2 architecture
- EPC Gen 2 physical layer
- EPC Gen 2 tag identification layer
- Tag identification message formats

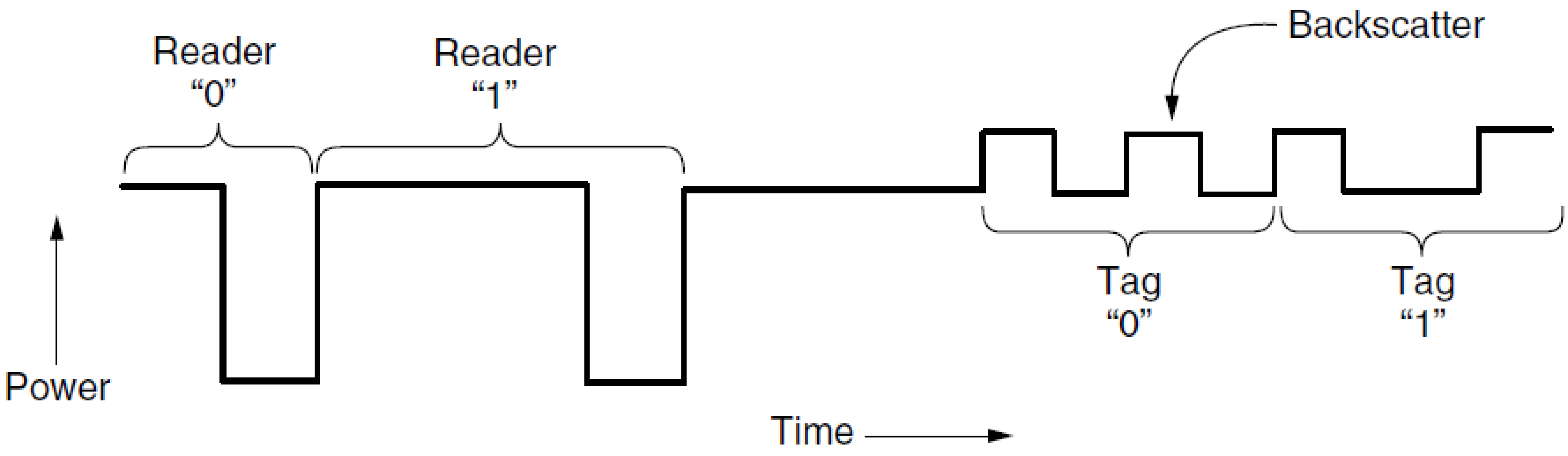
EPC Gen 2 Architecture



RFID architecture.

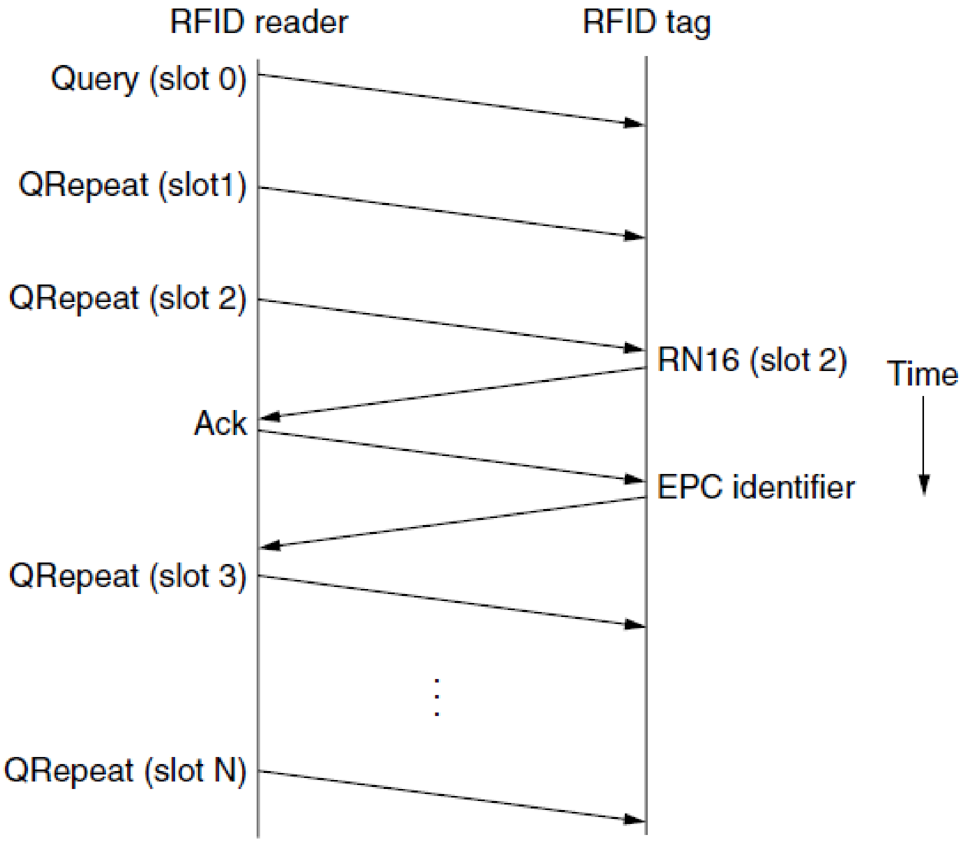
Gen 2 Physical Layer

- Reader uses duration of on period to send 0/1
- Tag backscatters reader signal in pulses to send 0/1



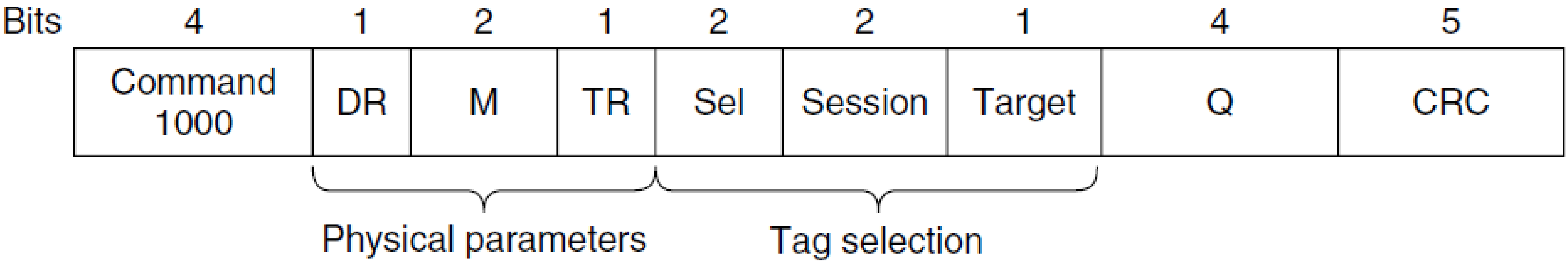
Gen 2 Tag Identification Layer

- Reader sends query and sets slot structure
- Tags reply (RN16) in a random slot; may collide
- Reader asks one tag for its identifier (ACK)
- Process continues until no tags are left



Gen 2 Frames

- Reader frames vary depending on type (Command)
  - Query shown below, has parameters and error detection
- Tag responses are simply data
  - Reader sets timing and knows the expected format



Bits	4	1	2	1	2	2	1	4	5
	Command 1000	DR	M	TR	Sel	Session	Target	Q	CRC

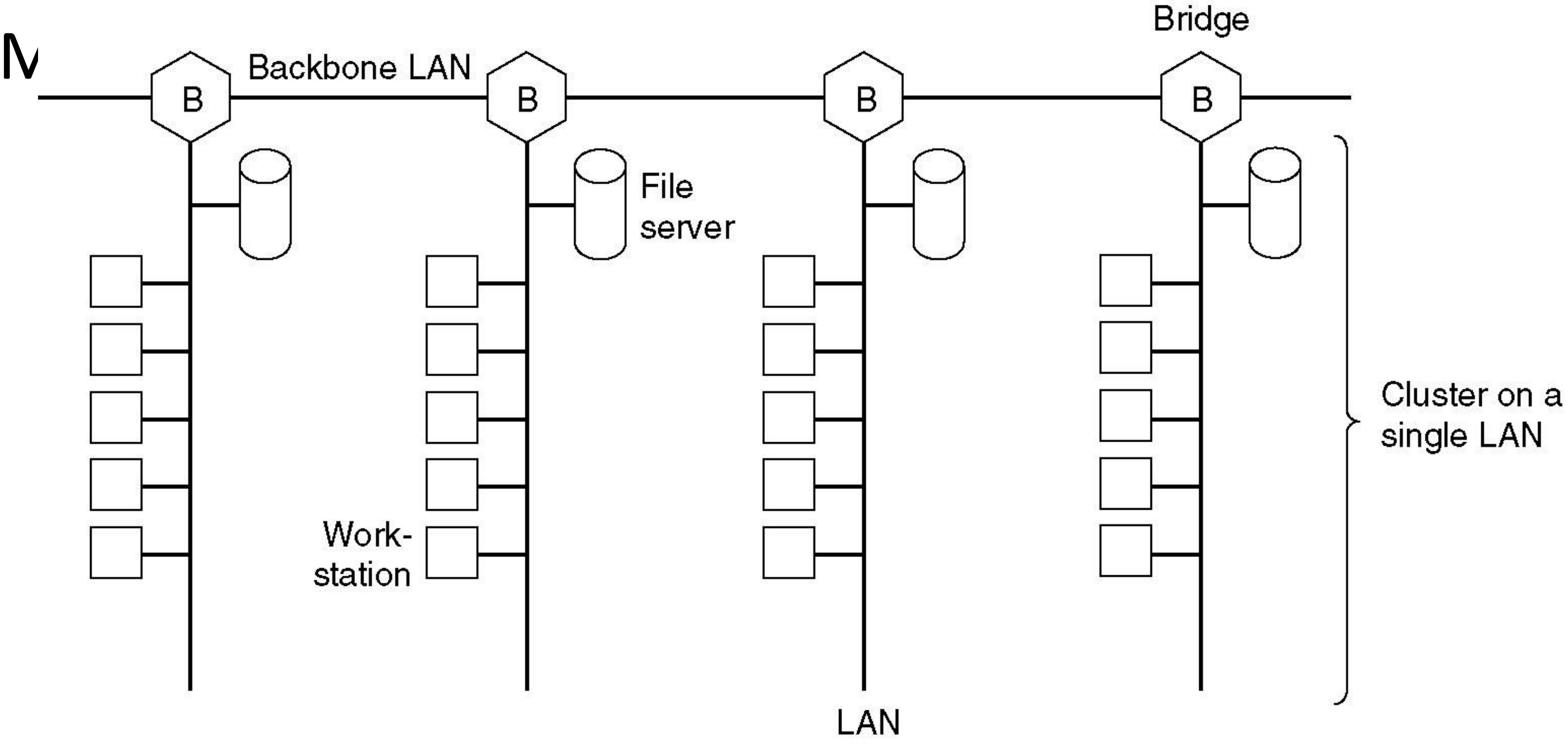
Query message

Data Link Layer Switching

- Bridges from 802.x to 802.y
- Local Internetworking
- Spanning Tree Bridges
- Remote Bridges
- Repeaters, Hubs, Bridges, Switches, Routers, Gateways
- Virtual LANs

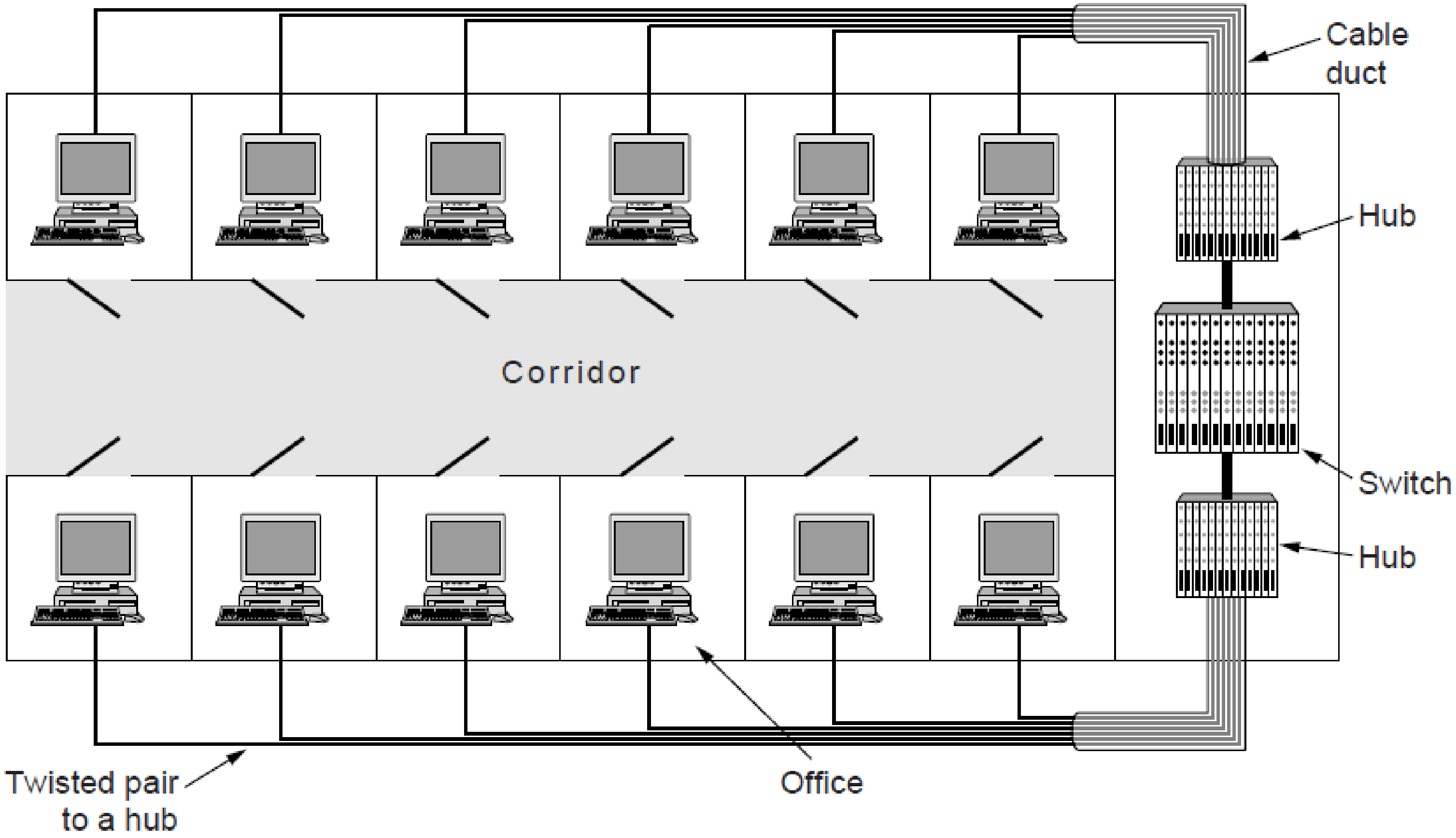
Data Link Layer Switching

M



Uses of Bridges

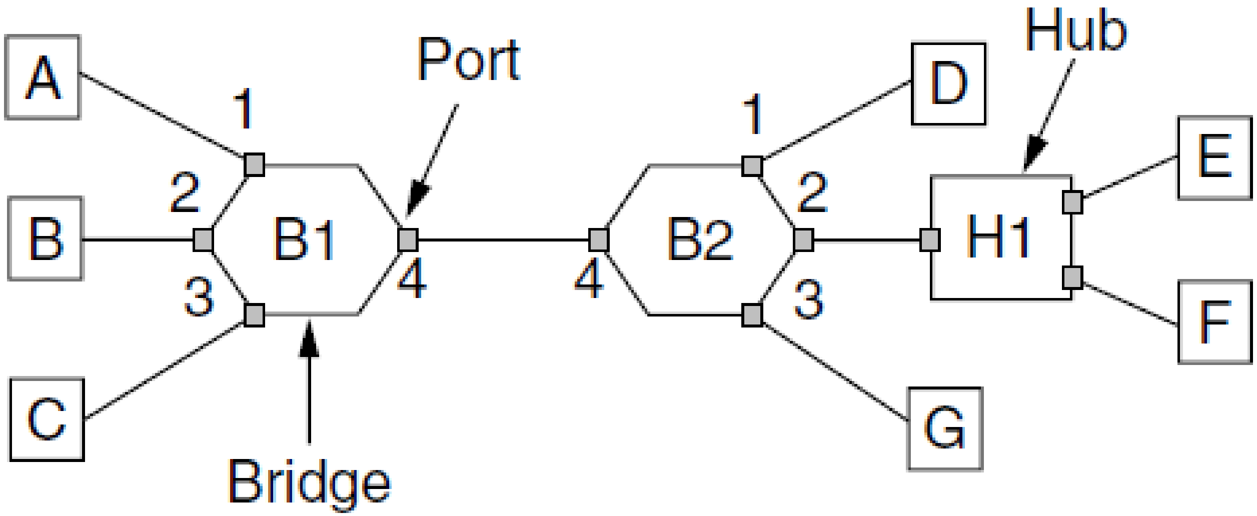
- Common setup is a building with centralized wiring
  - Bridges (switches) are placed in or near wiring closets



Learning Bridges

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

- Computers, bridges, and hubs connect to its ports



Learning Bridges

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

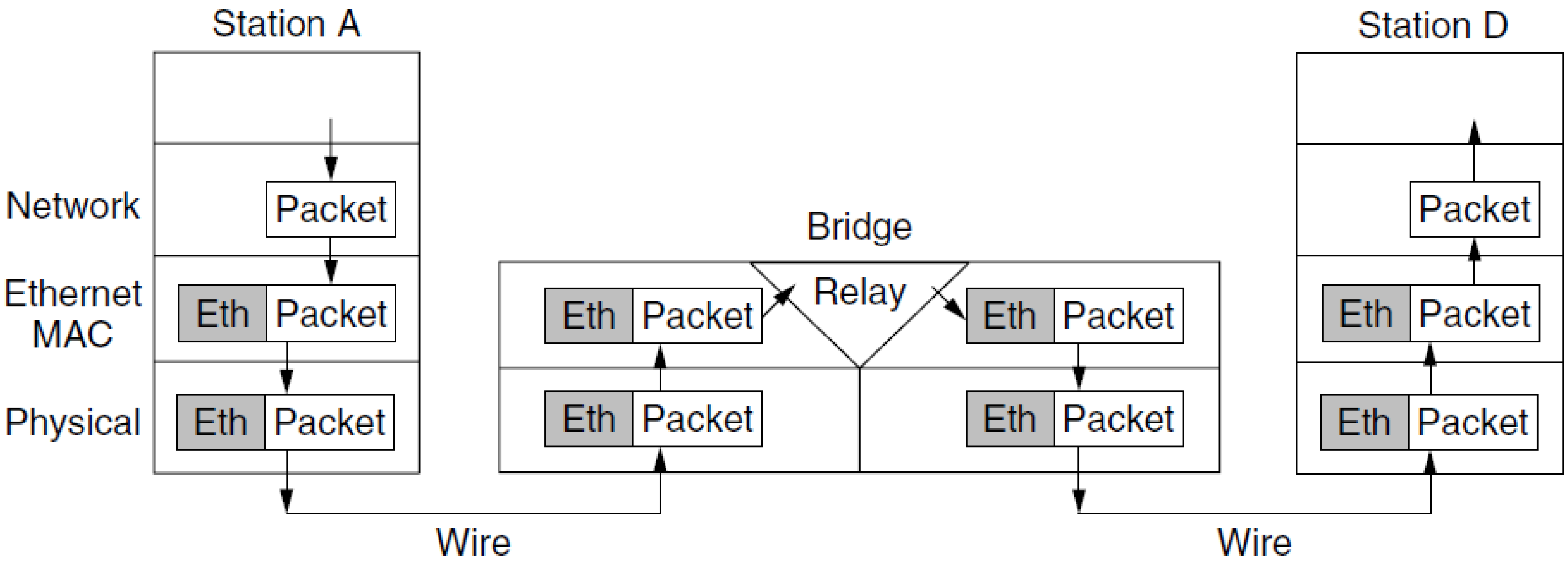
Needs no configuration

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

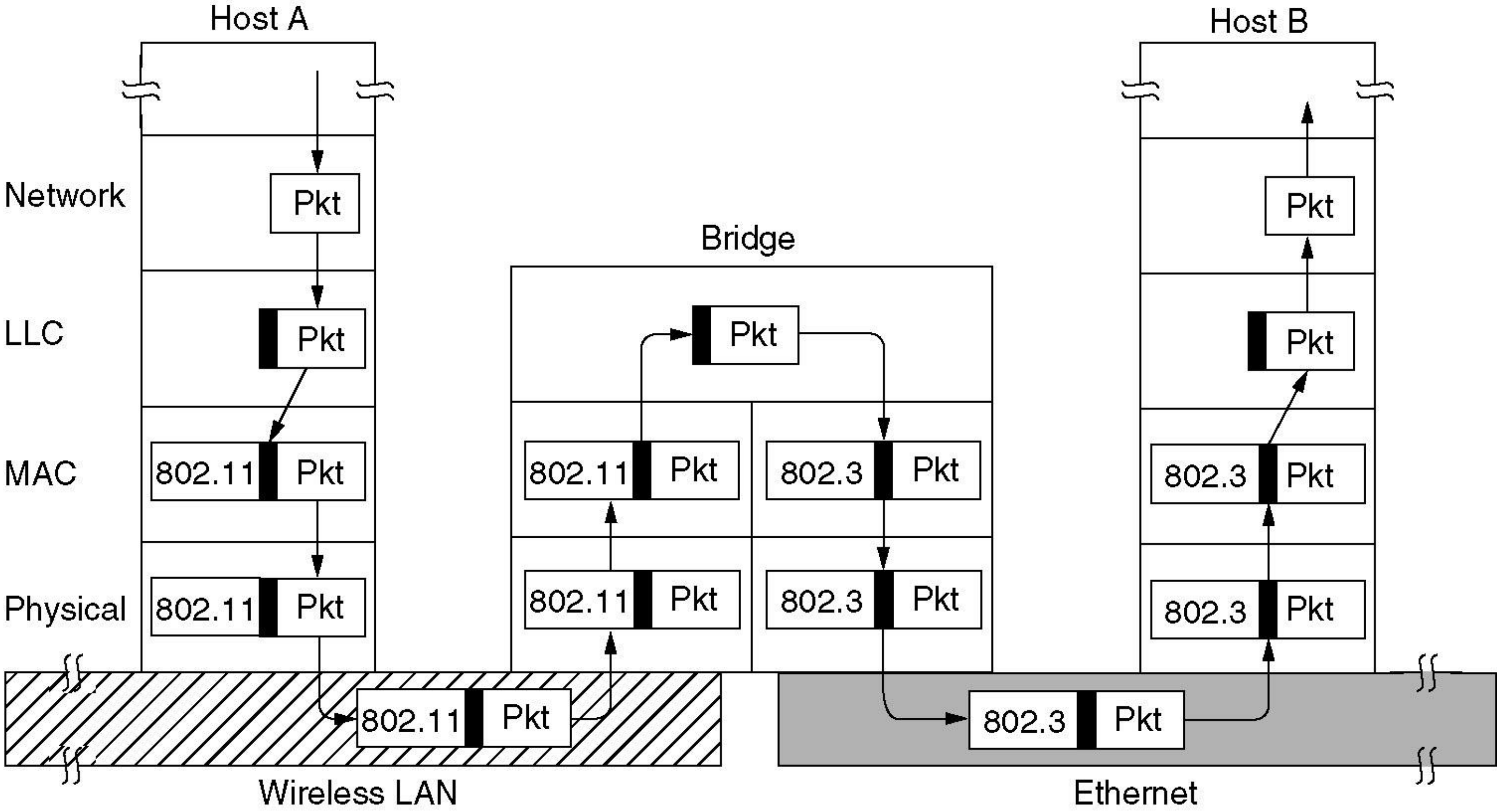
Learning Bridges

Bridges extend the Link layer:

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

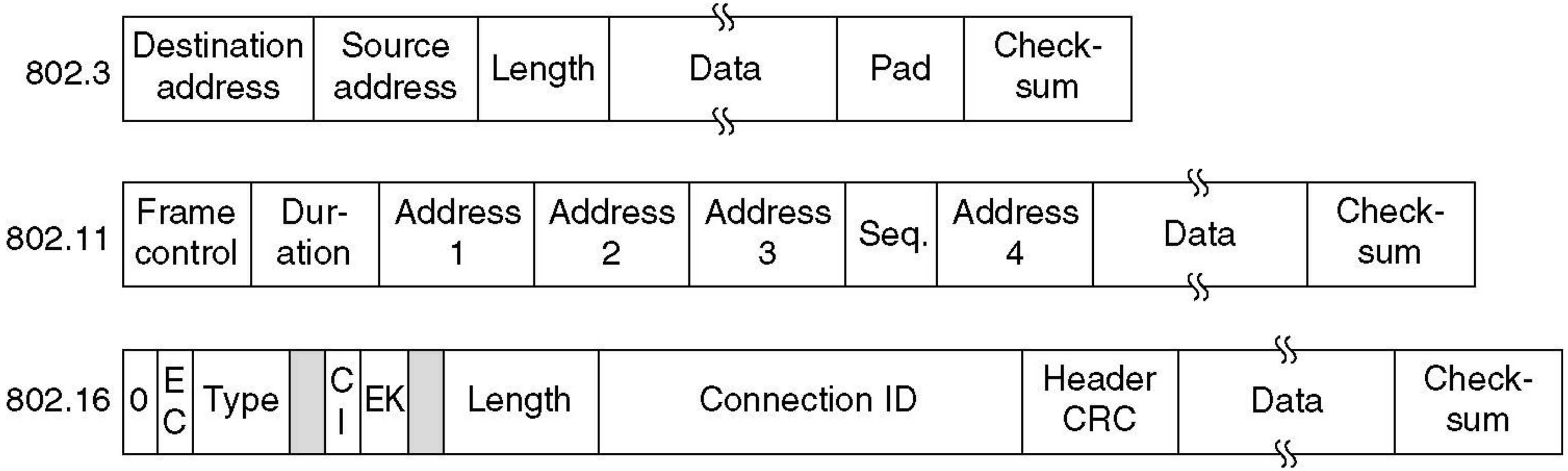


Bridges from 802.x to 802.y



Bridges from 802.x to 802.y (2)

The IEEE 802 frame formats. The drawing is not to scale.



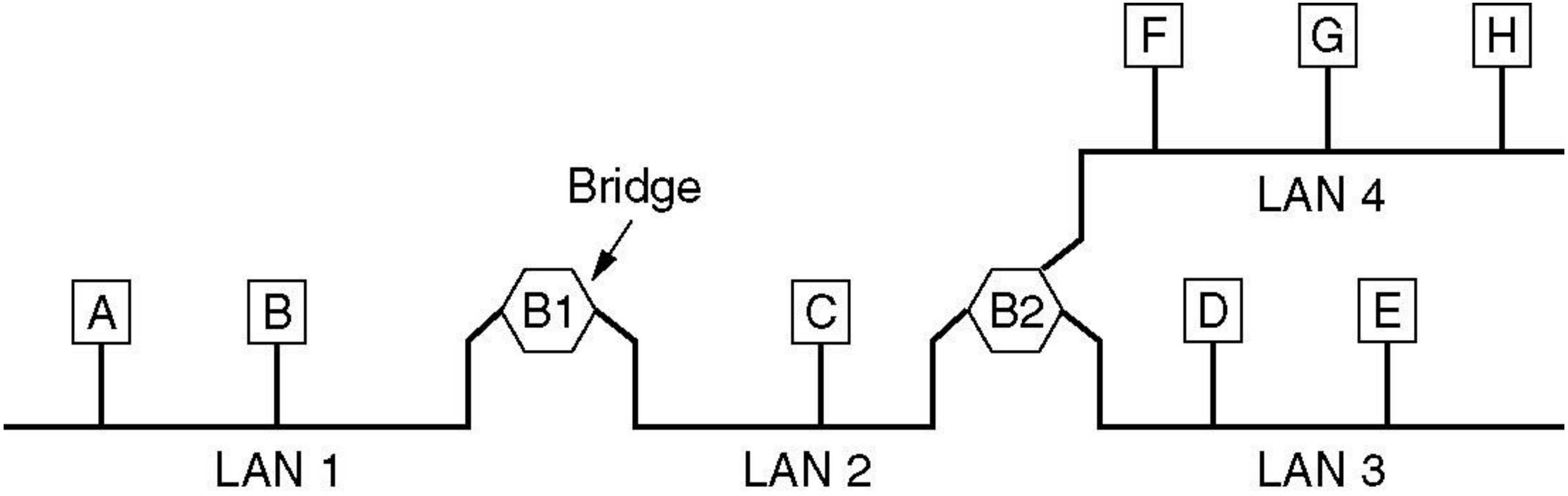
802.3: Destination address | Source address | Length | Data | Pad | Checksum

802.11: Frame control | Duration | Address 1 | Address 2 | Address 3 | Seq. | Address 4 | Data | Checksum

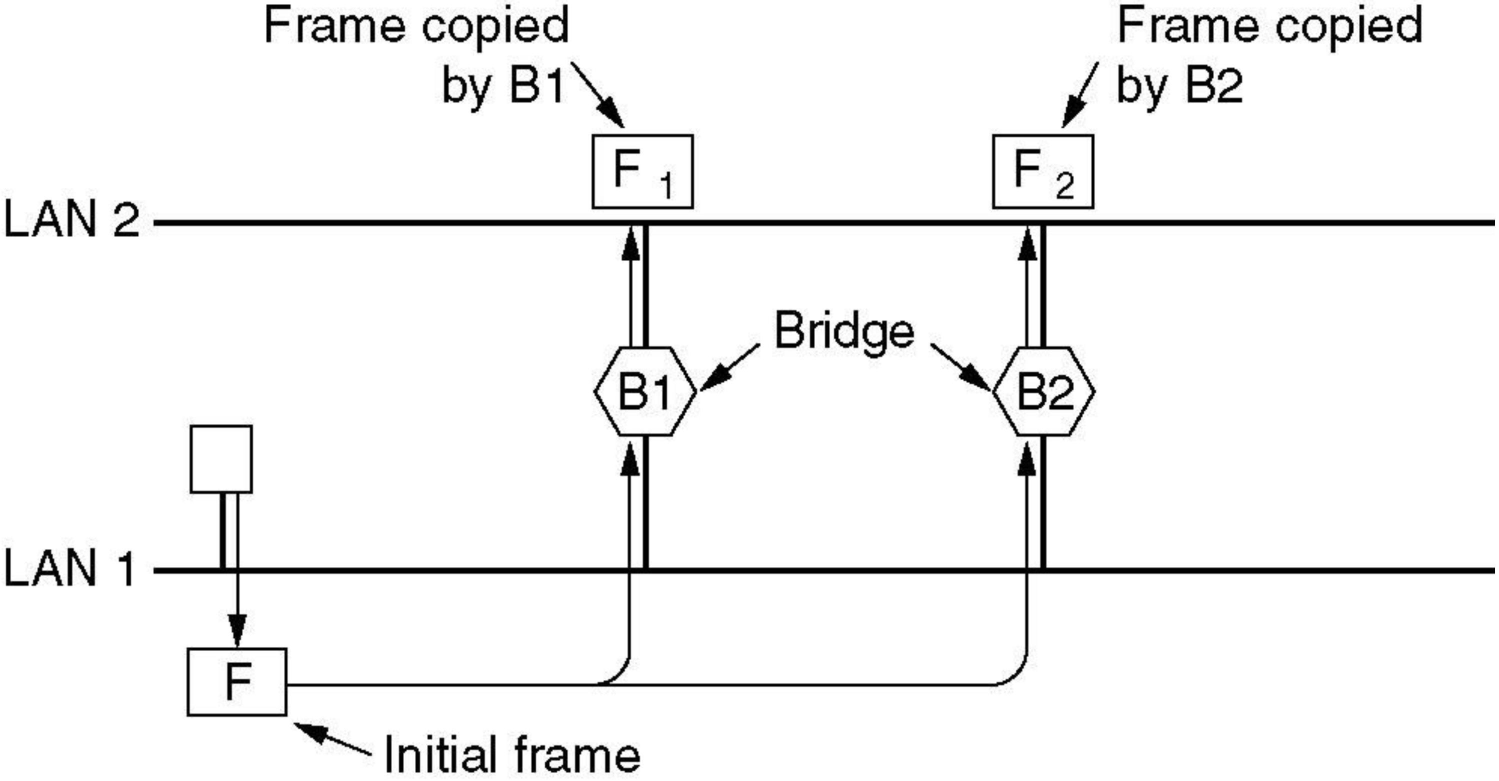
802.16: 0 | EC | Type | | CI | EK | | Length | Connection ID | Header CRC | Data | Checksum

Local Internetworking

A configuration with four LANs and two bridges.



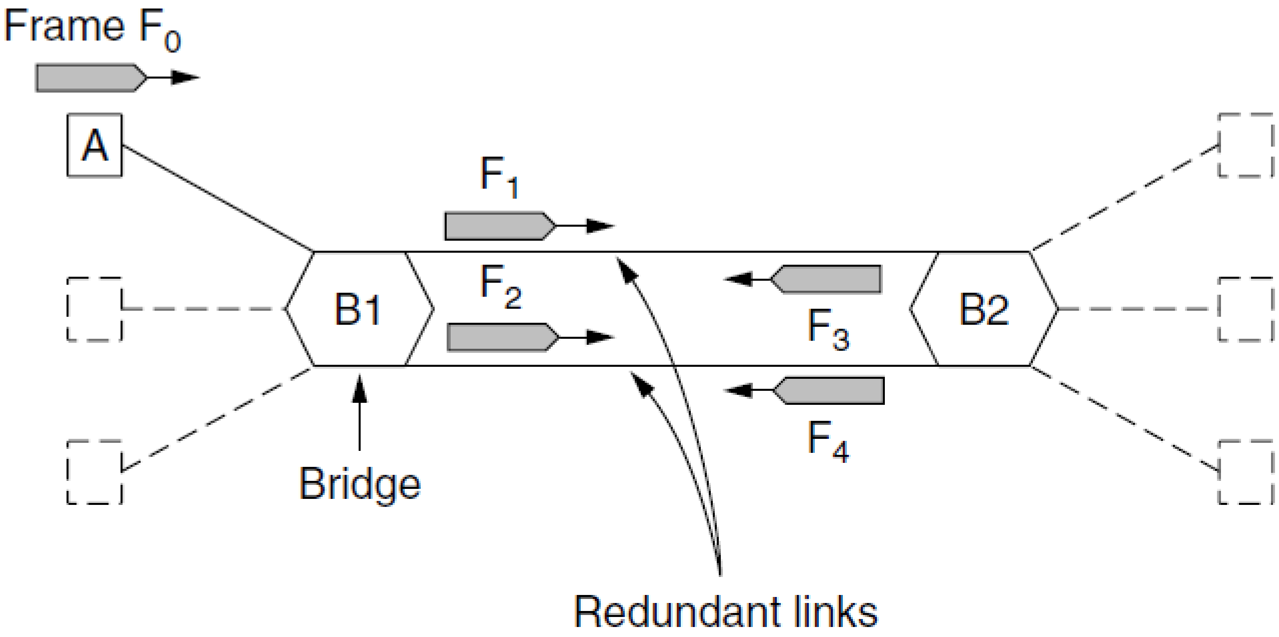
Spanning Tree Bridges



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

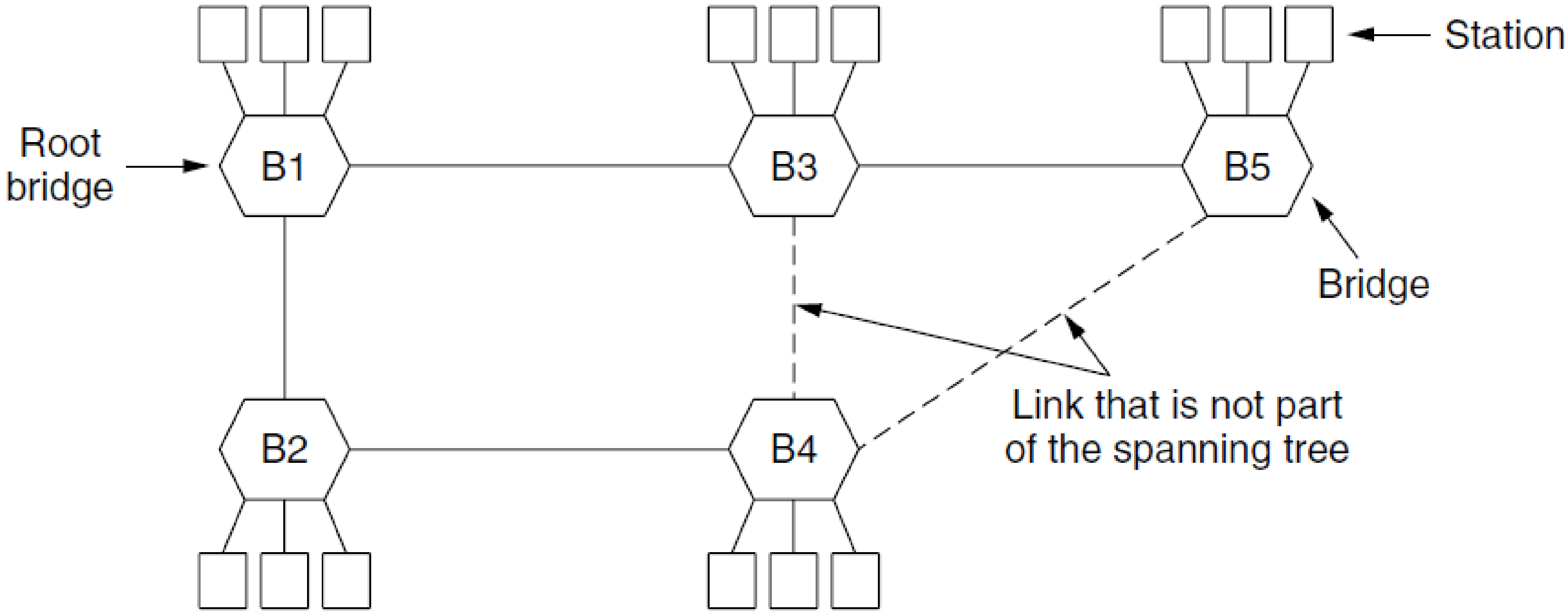
I think that I shall never see
A graph more lovely than a tree.
A tree whose crucial property
Is loop-free connectivity.
A tree which must be sure to span.
So packets can reach every LAN.
First the Root must be selected
By ID it is elected.
Least cost paths from Root are traced
In the tree these paths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

– Radia Perlman, 1985.

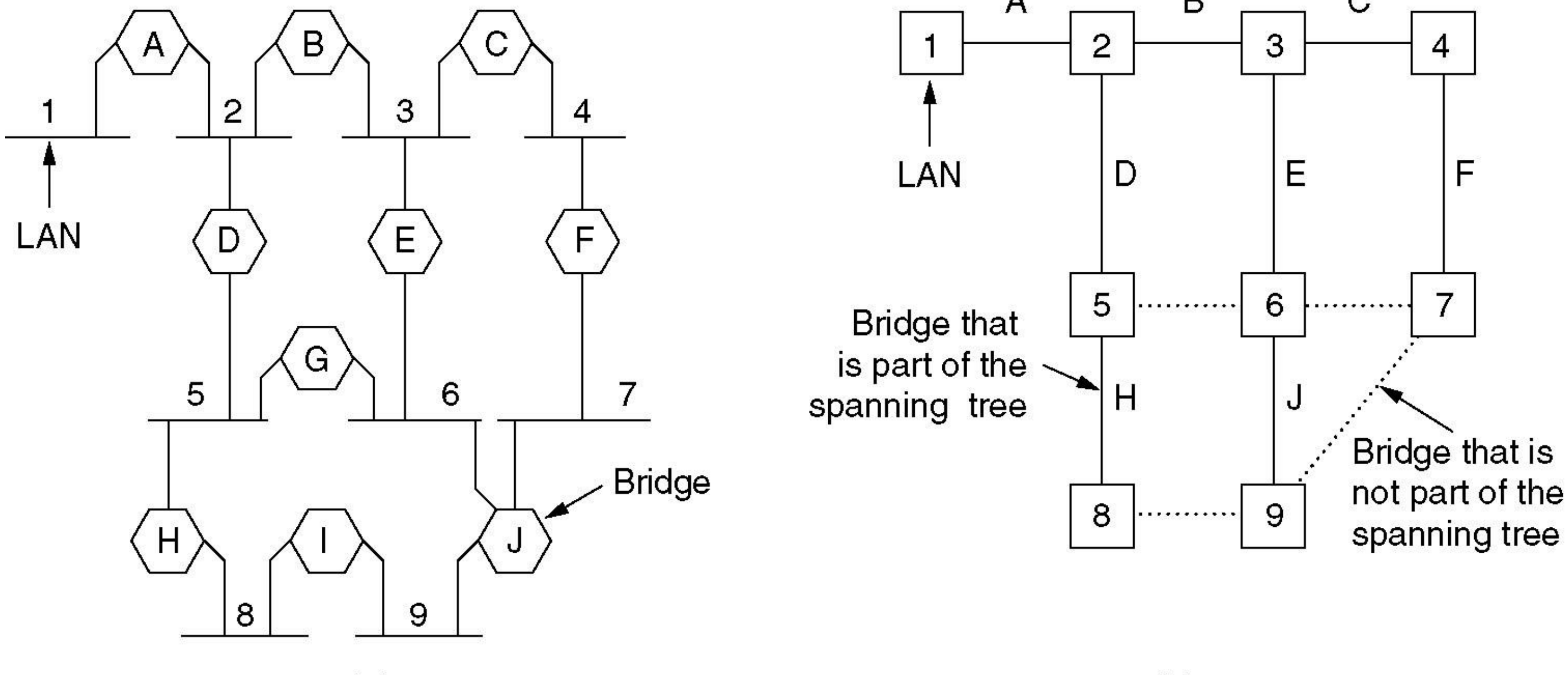
Spanning Tree (3) – Example

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)



Spanning Tree Bridges (2)

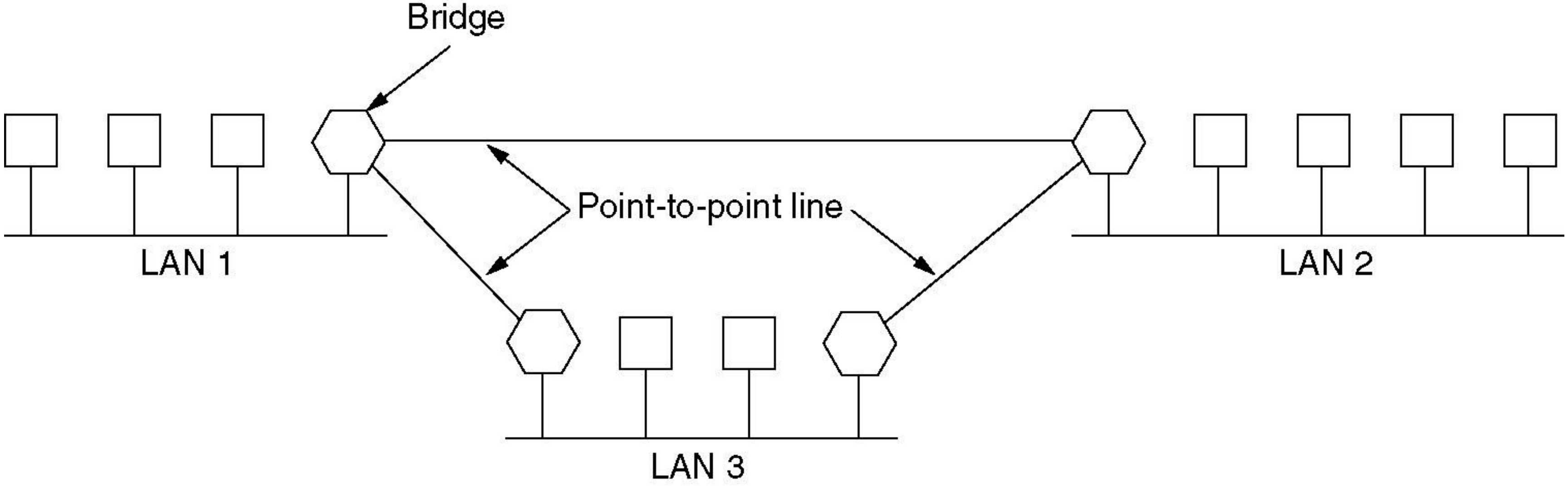

A
B
C
1
2
3
4
LAN
D
E
F
G
5
6
7
Bridge
H
I
J
8
9
A
B
C
1
2
3
4
LAN
D
E
F
5
6
7
Bridge that is part of the spanning tree
H
J
Bridge that is not part of the spanning tree
8
9

(a) (b)

(a) Interconnected LANs. (b) A spanning tree covering the LANs. The dotted lines are not part of the spanning tree.

Remote Bridges

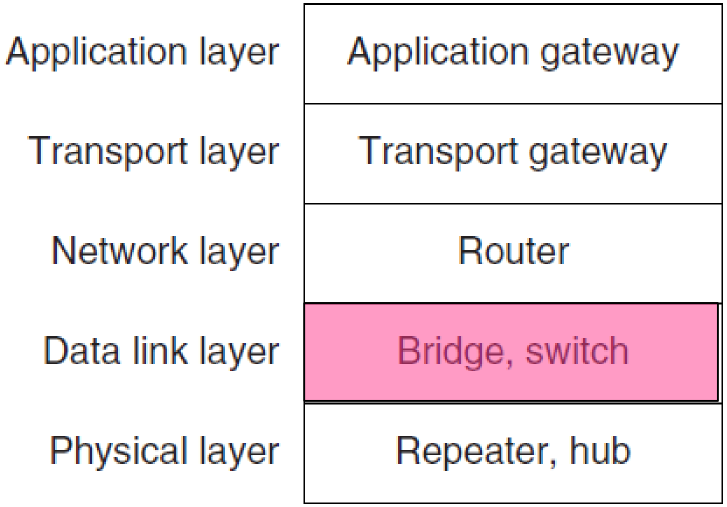
Remote bridges can be used to interconnect distant



Repeaters, Hubs, Bridges, Switches, Routers, and Gateways

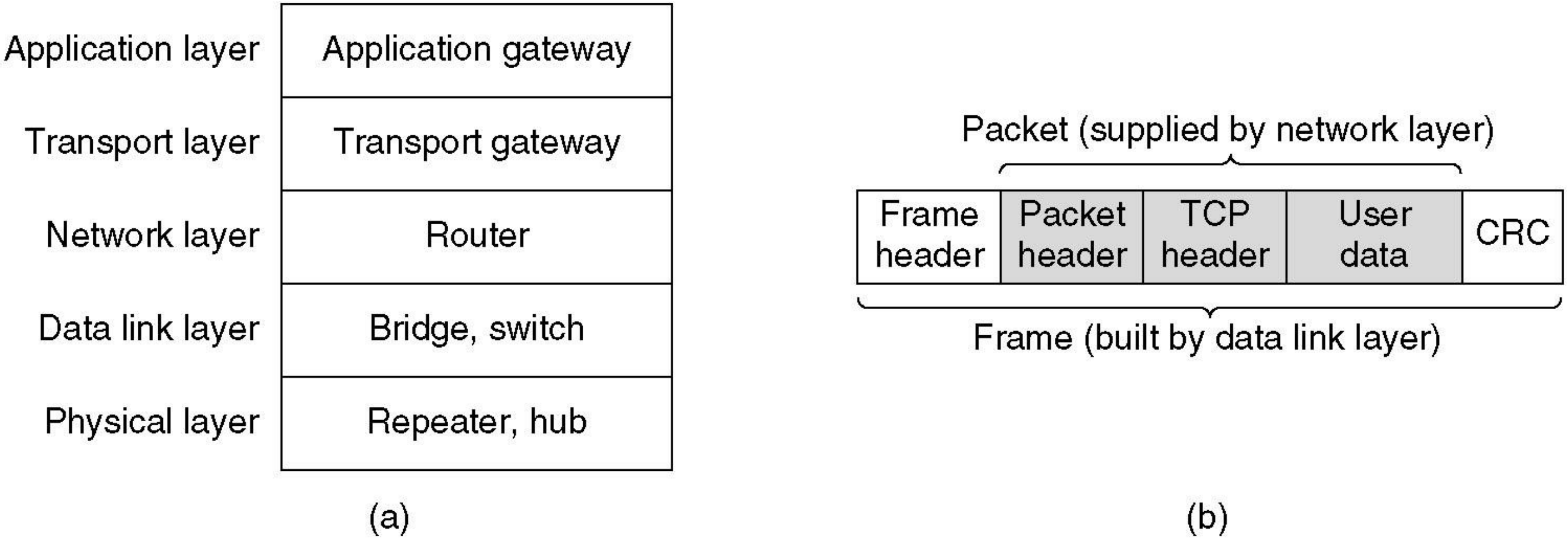
Devices are named according to the layer they process

- 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

Repeaters, Hubs, Bridges, Switches, Routers and Gateways



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

(a)

Packet (supplied by network layer)
Frame header
Packet header
TCP header
User data
CRC
Frame (built by data link layer)

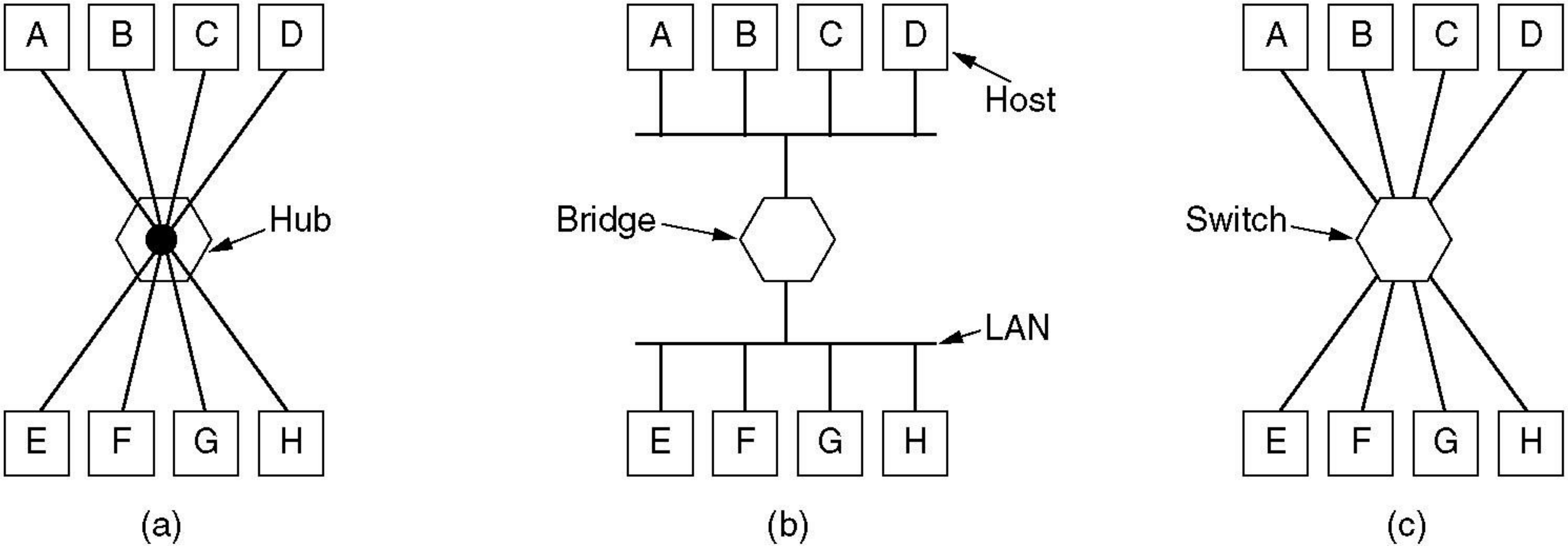
(b)

(a) Which device is in which layer.

(b) Frames, packets, and headers.

Repeaters, Hubs, Bridges, Switches, Routers and Gateways (2)

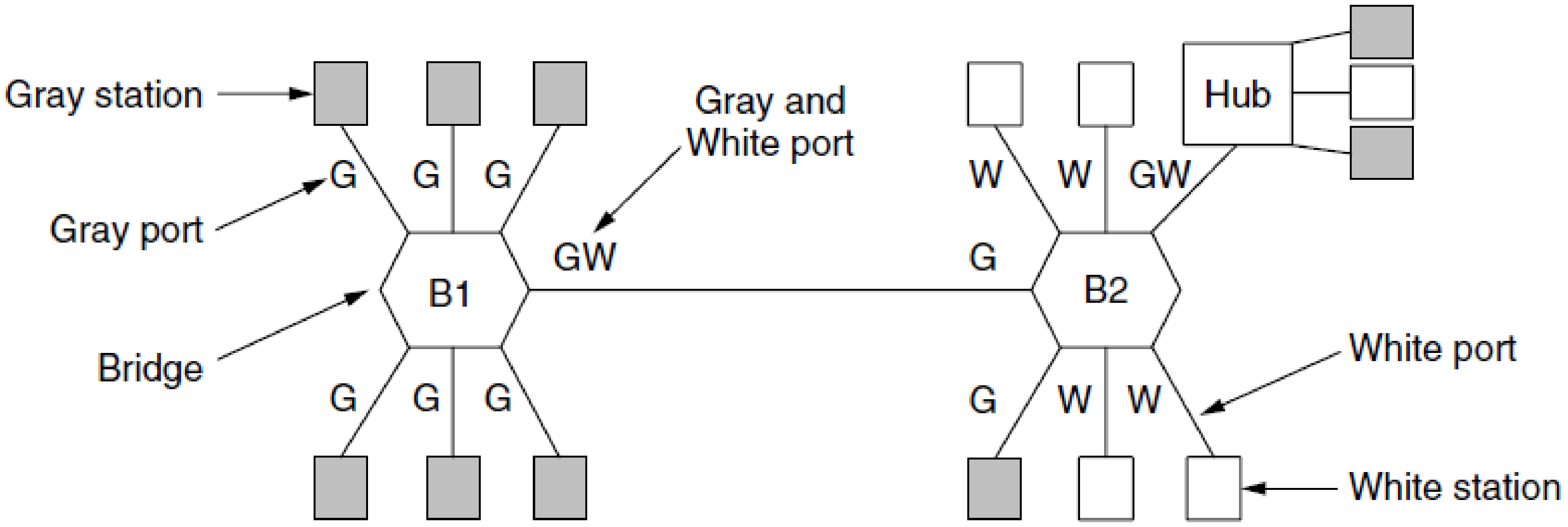
(a) A hub. (b) A bridge. (c) a switch.



Virtual LANs

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

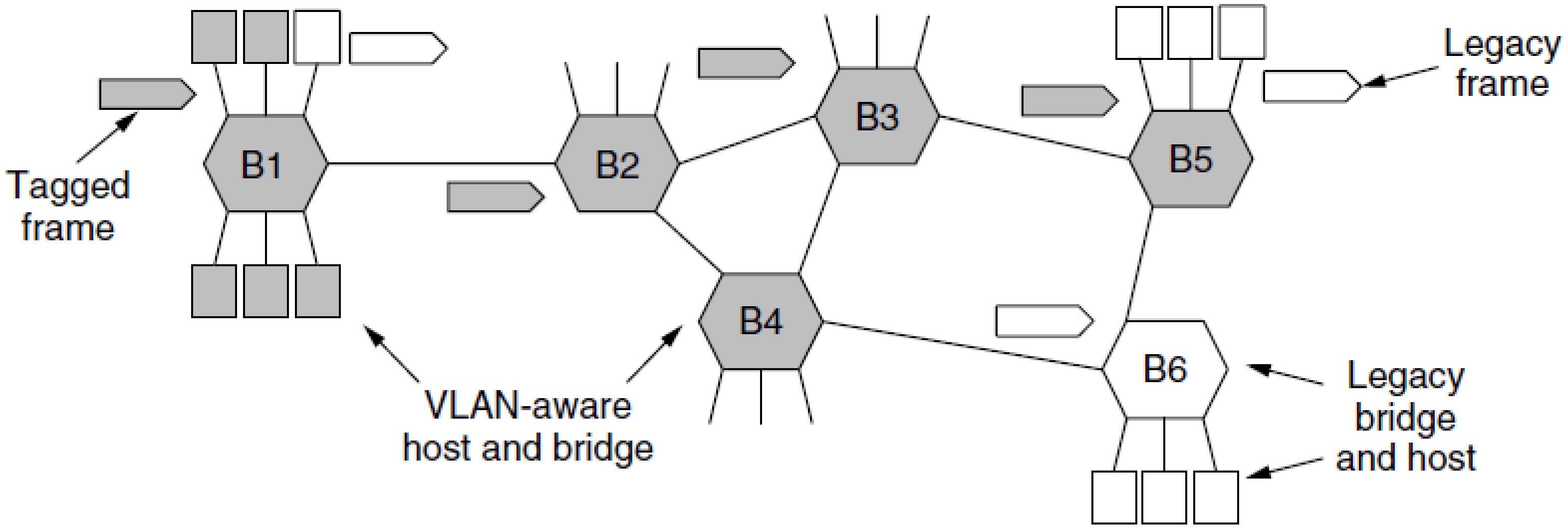
- Ports are “colored” according to their VLAN



Virtual LANs– IEEE 802.1Q

Bridges need to be aware of VLANs to support them

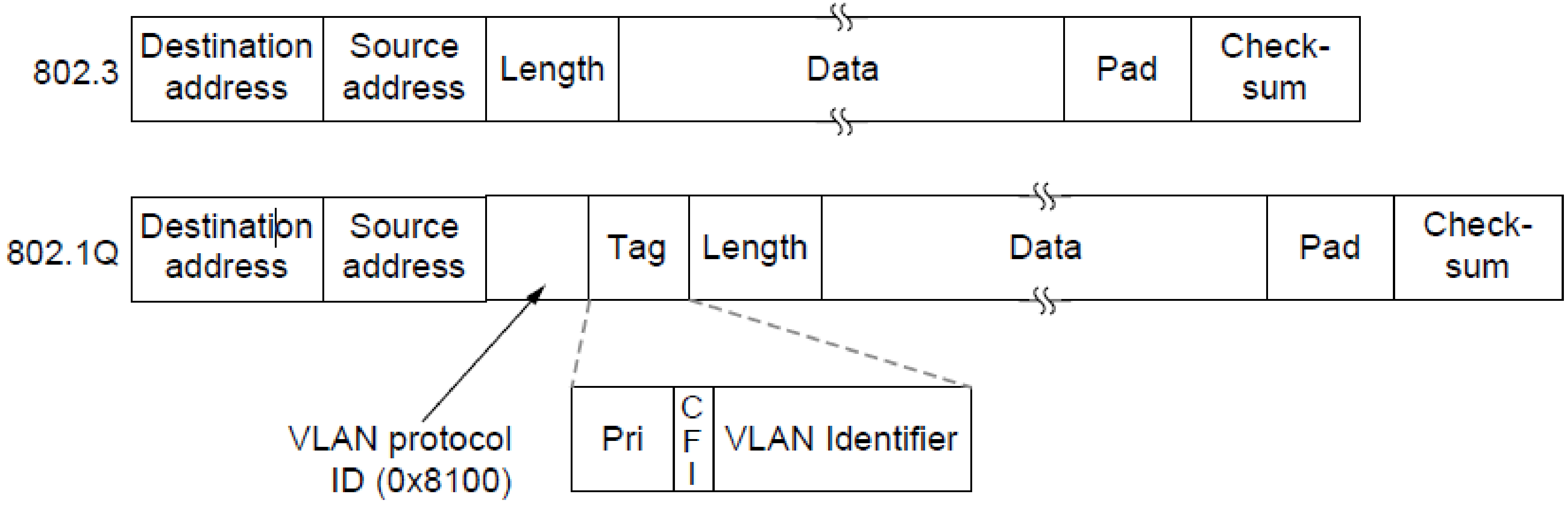
- In 802.1Q, frames are tagged with their “color”



Virtual LANs (3) – IEEE 802.1Q

802.1Q frames carry a color tag (VLAN identifier)

- Length/Type value is 0x8100 for VLAN protocol

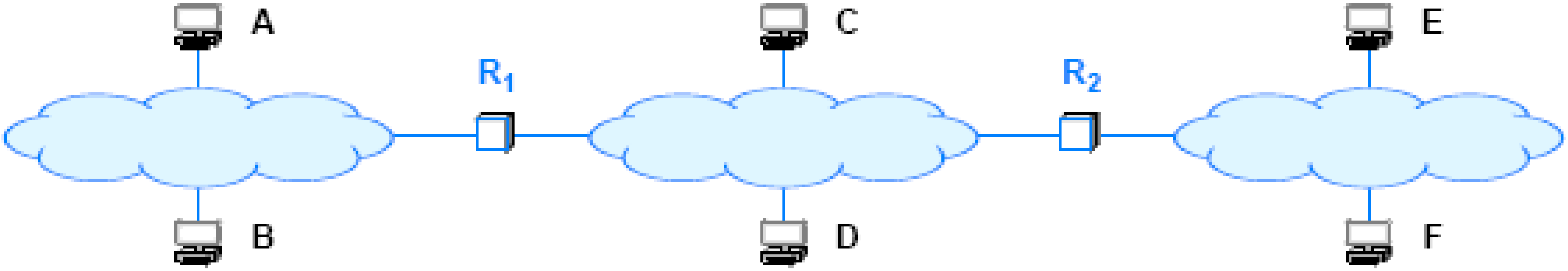


Address Resolution

- A crucial step of the forwarding process requires a translation:
  - forwarding uses IP addresses
  - a frame transmitted must contain the MAC address of the next hop
  - IP must translate the next-hop IP address to a MAC address
- The principle is:
  - IP addresses are abstractions
    - provided by protocol software
  - Network does not know how to locate a computer from its IP address
    - the next-hop address must be translated to an equivalent MAC address
- Translation from a computer's IP address to an equivalent hardware address is known as address resolution
  - And an IP address is said to be resolved to the correct MAC address
- Address resolution is local to a network

Address Resolution

- One computer can resolve the address of another computer only if both computers attach to the same physical network
  - A computer never resolves the address of a computer on a remote network
  - Address resolution is always restricted to a single network.
- For example, consider the simple internet



An example internet of three networks and computers connected to each.

The Address Resolution Protocol (ARP)

- What algorithm does software use to translate?
  - The answer depends on the protocol and hardware addressing
    - here we are only concerned with the resolution of IP
- Most hardware has adopted the 48-bit Ethernet Address
- In Ethernet: Address Resolution Protocol (ARP)
- Consider
  - Suppose B needs to resolve the IP address of C
  - B broadcasts a request that says:

"I'm looking for the MAC address of a computer that has IP address C"

  - The broadcast only travels across one network
  - An ARP request message reaches all computers on a network
  - When C receives a copy of the request along other hosts
    - Only C sends a directed reply back to B that says:

"I'm the computer with IP address C, and my MAC address is M"

The Address Resolution Protocol (ARP)

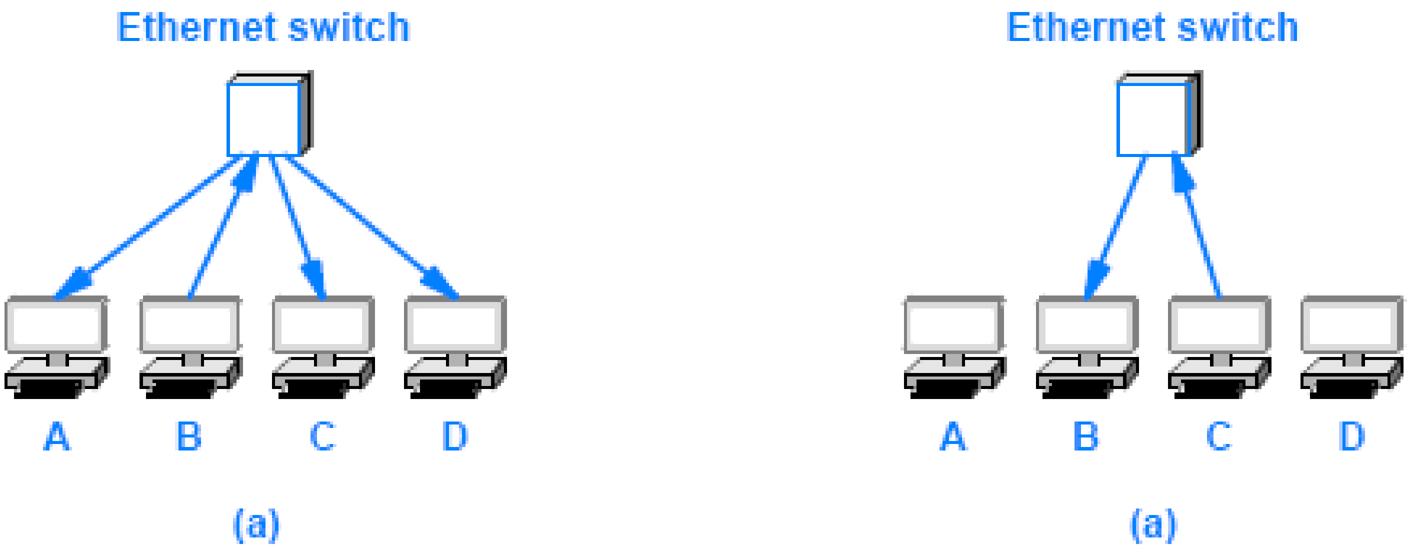


Illustration of the ARP message exchange when computer *B* resolves the address of computer *C*.

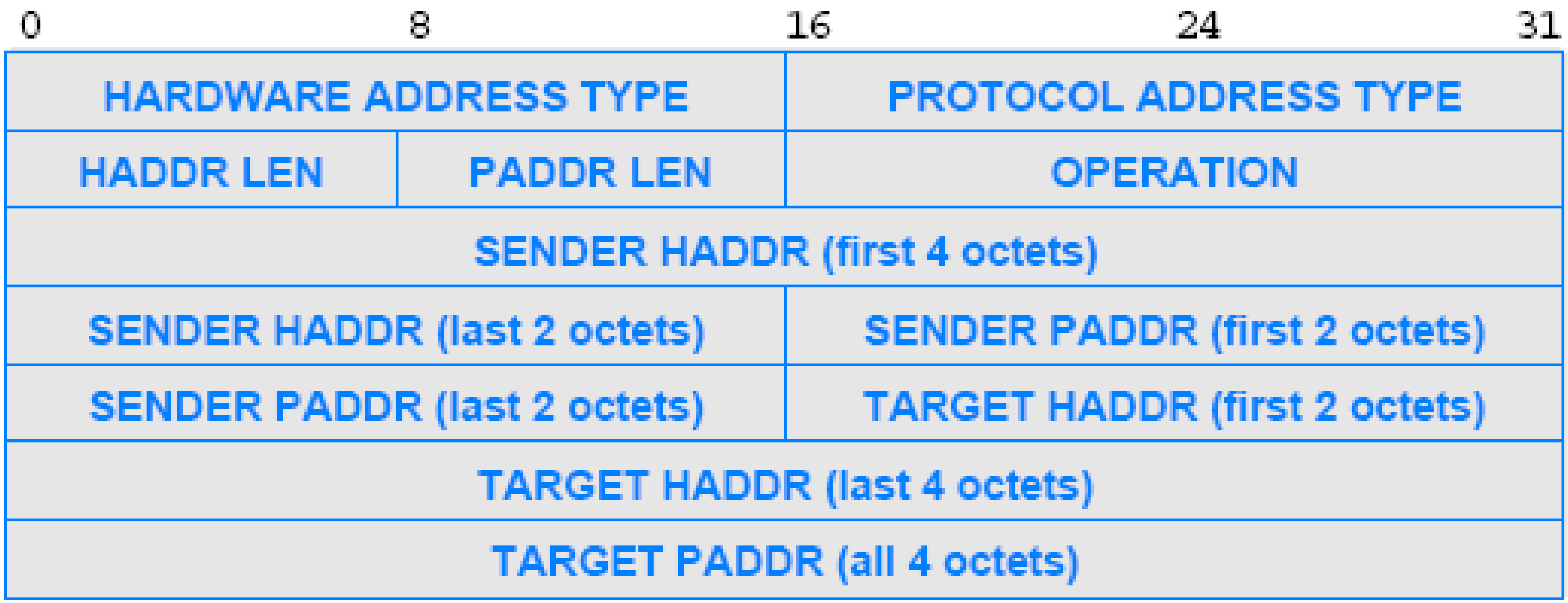
ARP Message Format

- Rather than restricting ARP to IP and Ethernet
  - The standard describes a general form for ARP messages
  - It specifies how the format is adapted for each type of protocol
- Choosing a fixed size for a hardware address is not suitable
  - New network technologies might be invented that have addresses larger than the size chosen
  - The designers included a fixed-size field at the beginning of an ARP message to specify the size of the hardware addresses being used
- For example, when ARP is used with an Ethernet
  - the hardware address length is set to 6 octets
    - because an Ethernet address is 48 bits long

ARP Message Format

- To increase the generality of ARP
  - the designers also included an address length field
- ARP protocol can be used to bind an arbitrary high-level address to an arbitrary hardware address
- In practice, the generality of ARP is seldom used
  - most implementations of ARP are used to bind IP addresses to Ethernet addresses
- Figure illustrates the format of an ARP message
  - when the protocol is used with an IP version 4 address (4 octets) and Ethernet hardware address (6 octets)
  - each line of the figure corresponds to 32 bits of an ARP message

ARP Message Format



<table>
<tr><th>0</th><th>8</th><th>16</th><th>24 31</th></tr>
<tr><td colspan="2">HARDWARE ADDRESS TYPE</td><td colspan="2">PROTOCOL ADDRESS TYPE</td></tr>
<tr><td>HADDR LEN</td><td>PADDR LEN</td><td colspan="2">OPERATION</td></tr>
<tr><td colspan="4">SENDER HADDR (first 4 octets)</td></tr>
<tr><td colspan="2">SENDER HADDR (last 2 octets)</td><td colspan="2">SENDER PADDR (first 2 octets)</td></tr>
<tr><td colspan="2">SENDER PADDR (last 2 octets)</td><td colspan="2">TARGET HADDR (first 2 octets)</td></tr>
<tr><td colspan="4">TARGET HADDR (last 4 octets)</td></tr>
<tr><td colspan="4">TARGET PADDR (all 4 octets)</td></tr>
</table>

The format for an ARP message when binding an IPv4 address to an Ethernet address.

ARP Message Format

- HARDWARE ADDRESS TYPE
  - 16-bit field that specifies the type of hardware address being used
  - the value is 1 for Ethernet
- PROTOCOL ADDRESS TYPE
  - 16-bit field that specifies the type of protocol address being used
  - the value is 0x0800 for IPv4
- HADDR LEN
  - 8-bit integer that specifies the size of a hardware address in bytes
- PADDR LEN
  - 8-bit integer that specifies the size of a protocol address in bytes
- OPERATION
  - 16-bit field that specifies whether the message
    - request (the field contains 1) or
    - response (the field contains 2)

ARP Message Format

- SENDER HADDR
  - HADDR LEN bytes for the sender's hardware address
- SENDER PADDR
  - PADDR LEN bytes for the sender's protocol address
- TARGET HADDR
  - HADDR LEN bytes for the target's hardware address
- TARGET PADDR
  - PADDR LEN bytes for the target's protocol address

ARP Message Format

- An ARP message contains fields for two address bindings
  - one binding to the sender
  - other to the intended recipient, ARP calls it target
- When a request is sent
  - the sender does not know the target's hardware address (that is the *information being requested*)
    - therefore, field TARGET HADDR in an ARP request can be filled with zeroes (0s) because the contents are not used
- In a response
  - the target binding refers to the initial computer that sent the request
  - Thus, the target address pair in a response serves no purpose
    - the inclusion of the target fields has survived from an early version of the protocol

ARP Encapsulation

- When it travels across a physical network
  - an ARP message is encapsulated in a hardware frame
- An ARP message is treated as data being transported
  - the network does not parse the ARP message or interpret fields

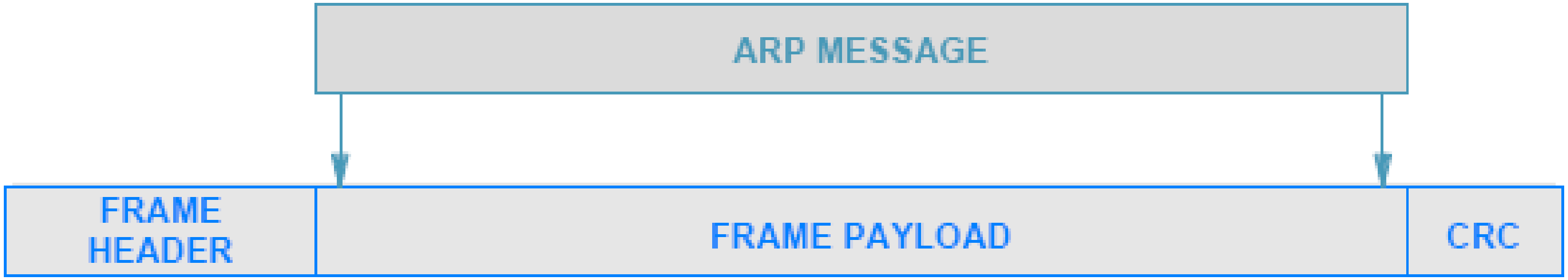


Illustration of ARP encapsulation in an Ethernet frame.

ARP Encapsulation

- The type field in the frame header specifies that the frame contains an ARP message
- A sender must assign the appropriate value to the type field
  - before transmitting the frame
- And a receiver must examine the type field
  - in each incoming frame
- Ethernet uses type field 0x806 to denote an ARP message
- The same value is used for both ARP requests/ responses
  - Frame type does not distinguish between types of ARP messages
  - A receiver must examine the OPERATION field in the message
    - to determine whether an incoming message is a request or a response

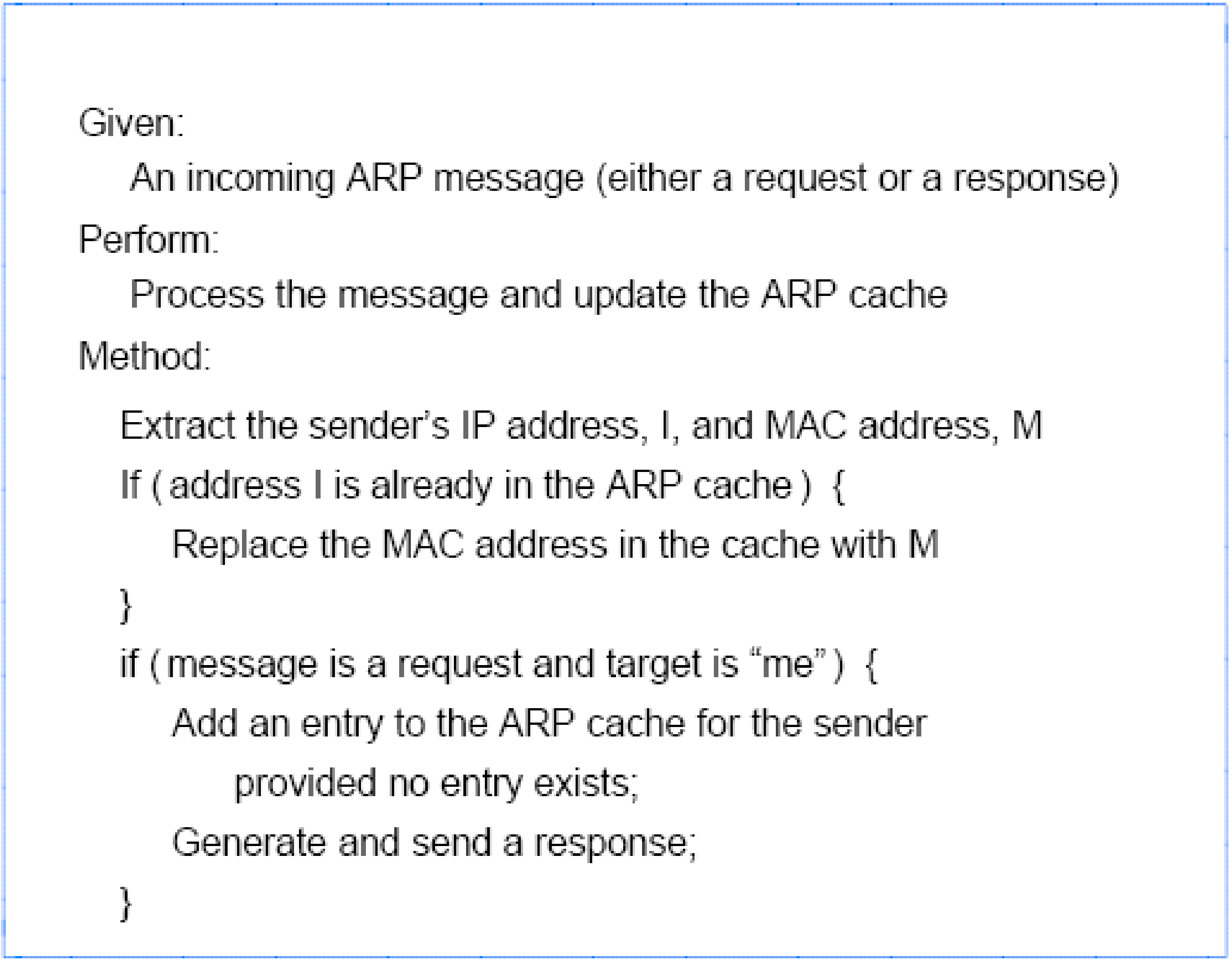
ARP Caching and Message Processing

- Sending an ARP request for each datagram is inefficient
  - Three (3) frames traverse the network for each datagram (an ARP request, ARP response, and the data datagram itself)
- Most communications involve a sequence of packets
  - a sender is likely to repeat the exchange many times
- To reduce network traffic
  - ARP software extracts and saves the information from a response
    - so it can be used for subsequent packets
  - The software does not keep the information indefinitely
    - Instead, ARP maintains a small table of bindings in memory
- ARP manages the table as a cache
  - an entry is replaced when a response arrives
  - the oldest entry is removed whenever the table runs out of space or after an entry has not been updated for a long period of time
  - ARP starts by searching the cache when it needs to bind an address

ARP Caching and Message Processing

- If the binding is present in the cache
  - ARP uses the binding without transmitting a request
- If the binding is not present in the cache
  - ARP broadcasts a request
  - waits for a response
  - updates the cache
  - and then proceeds to use the binding
- The cache is only updated when an ARP message arrives (either a request or a response)

ARP Caching and Message Processing



```
Given:
    An incoming ARP message (either a request or a response)
Perform:
    Process the message and update the ARP cache
Method:
   Extract the sender's IP address, I, and MAC address, M
   If ( address I is already in the ARP cache )  {
       Replace the MAC address in the cache with M
   }
   if ( message is a request and target is "me" )  {
       Add an entry to the ARP cache for the sender
            provided no entry exists;
       Generate and send a response;
   }
```

The steps ARP takes when processing an incoming message.

ARP Caching and Message Processing

- For optimization, it is necessary to know two facts:
  - Most computer communication involves two-way traffic
    - if a message from A to B, probability is high that a reply will be from B back to A
  - Each address binding requires memory
    - a computer cannot store an arbitrary number of address bindings
- The first fact explains why extracting the sender's address binding optimizes ARP performance

The Conceptual Address Boundary

- ARP provides an important conceptual boundary between MAC addresses and IP addresses:
  - ARP hides the details of hardware addressing
  - It allows higher layers of software to use IP addresses
- There is an important conceptual boundary imposed between the network interface layer and all higher layers
- illustrates the addressing boundary

The Conceptual Address Boundary

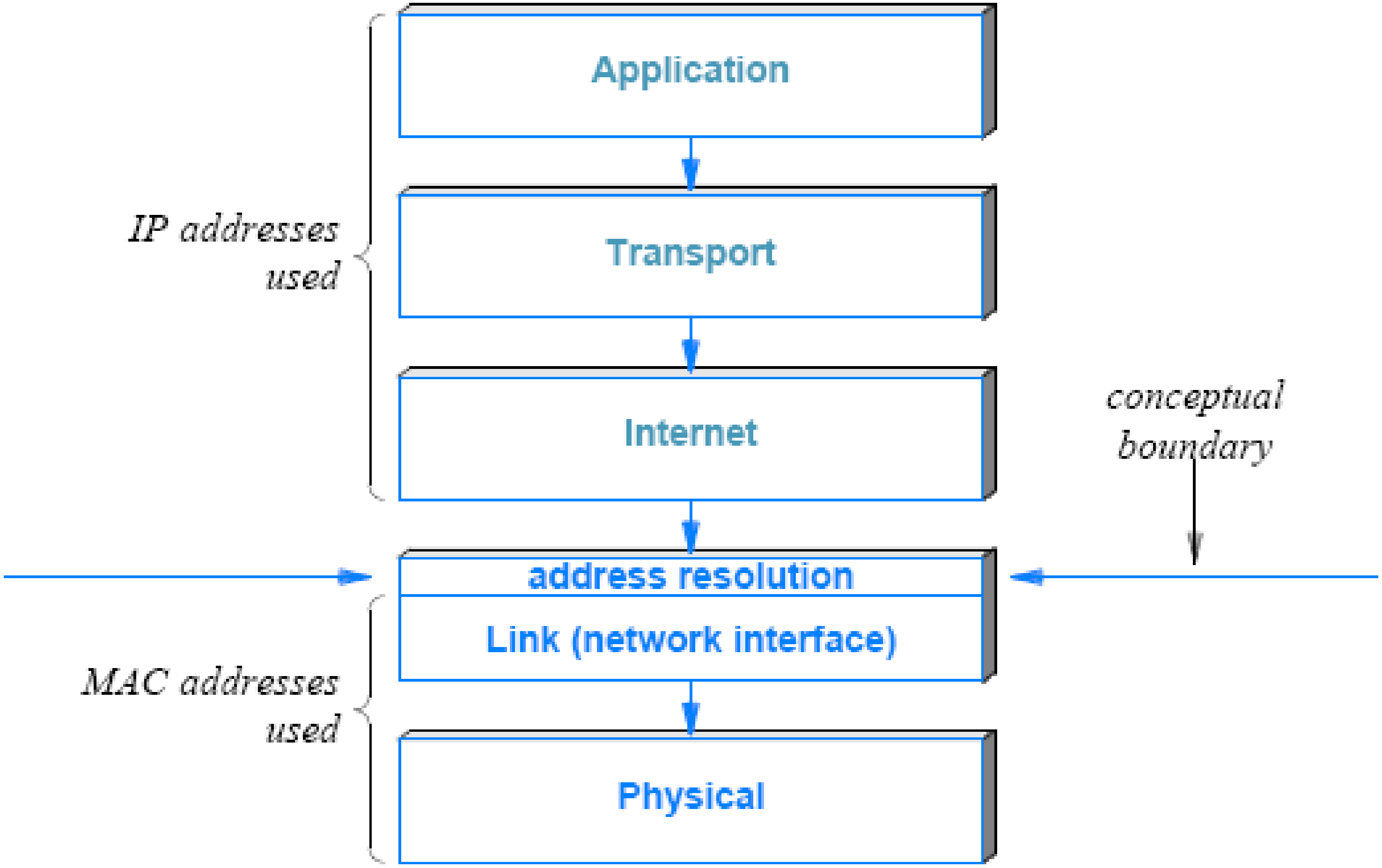
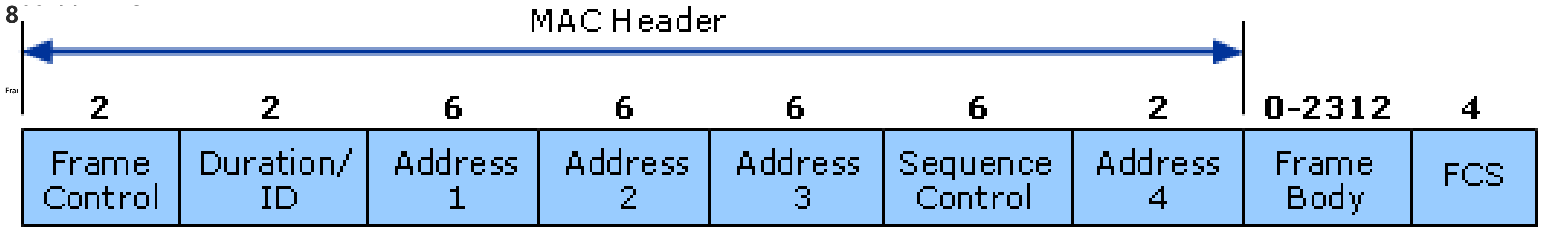
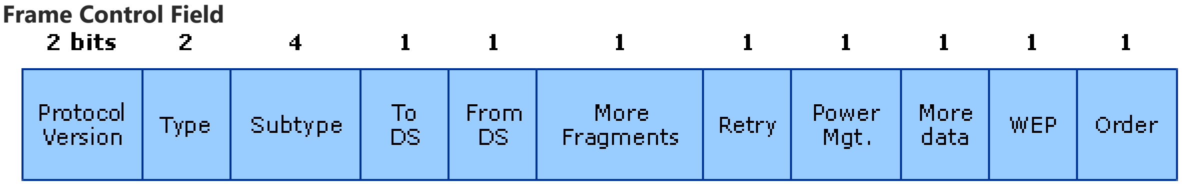


Illustration of the boundary between the use of IP addresses and MAC addresses.



2	2	6	6	6	6	2	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS



Frame Control Field

2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

•**Protocol Version** provides the current version of the 802.11 protocol used. Receiving STAs use this value to determine if the version of the protocol of the received frame is supported.

•**Type and Subtype** determines the function of the frame. There are three different frame type fields: control, data, and management. There are multiple subtype fields for each frame type . Each subtype determines the specific function to perform for its associated frame type.

To DS and From DS indicates whether the frame is going to or exiting from the DS (distributed system), and is only used in data type frames of STAs associated with an AP.

More Fragments indicates whether more fragments of the frame, either data or management type, are to follow.

Retry indicates whether or not the frame, for either data or management frame types, is being retransmitted.

Power Management indicates whether the sending STA is in active mode or power-save mode.

More Data indicates to a STA in power-save mode that the AP has more frames to send. It is also used for APs to indicate that additional broadcast/multicast frames are to follow.

WEP indicates whether or not encryption and authentication are used in the frame. It can be set for all data frames and management frames, which have the subtype set to authentication.

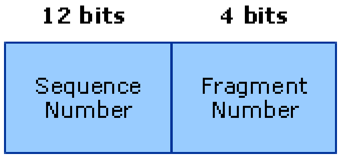
Order indicates that all received data frames must be processed in order.

Address Fields

- **BSS Identifier (BSSID).** BSSID uniquely identifies each BSS. When the frame is from an STA in an infrastructure BSS, the BSSID is the MAC address of the AP. When the frame is from a STA in an IBSS, the BSSID is the randomly generated, locally administered MAC address of the STA that initiated the IBSS.
- **Destination Address (DA).** DA indicates the MAC address of the final destination to receive the frame.
- **Source Address (SA).** SA indicates the MAC address of the original source that initially created and transmitted the frame.
- **Receiver Address (RA).** RA indicates the MAC address of the next immediate STA on the wireless medium to receive the frame.
- **Transmitter Address (TA).** TA indicates the MAC address of the STA that transmitted the frame onto the wireless medium.

Sequence Control

- The Sequence Control field contains two subfields, the Fragment Number field and the Sequence Number field, as shown in the following figure.



- **Sequence Number** indicates the sequence number of each frame. The sequence number is the same for each frame sent for a fragmented frame; otherwise, the number is incremented by one until reaching 4095, when it then begins at zero again.

- **Fragment Number** indicates the number of each frame sent of a fragmented frame. The initial value is set to 0 and then incremented by one for each subsequent frame sent of the fragmented frame.