EECS, University of Ottawa

ELG5374 –Fall 2021
Computer Communication Network

Local Area Networks (LANs)

Note: some material in the slides has been taken from various other sources 1-1

1

Local Area Networks

- It expands over small geographic areas (within a building or close-by buildings)
- It is usually owned by the same organization
- The internal data rates are typically much greater than those of WANs
- Typically, they make use of broadcast approach than switching approach

1-2

2

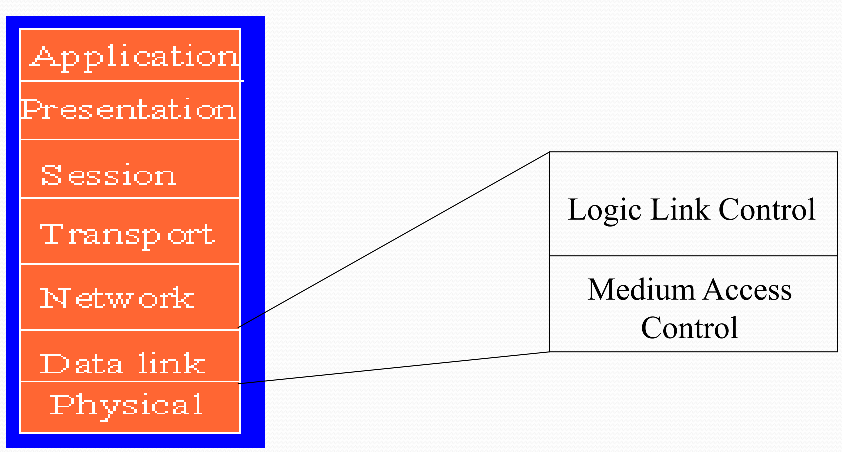
Examples of LANs

- Ethernet (10 Mbps)
- Fast Ethernet (100 Mbps)
- Gigabit Ethernet (1,000 Mbps)
- Token Ring
- ATM LANs
- IEEE 802.11 Wireless LAN
- HYPERLAN (European Wireless Standard)

1-3

3

Open System Interconnection (OSI) Reference Model



1-4

4

Functions Performed by Physical Layer

- Encoding/decoding of signals
- Preamble generation / removal (for synchronization)
- Bit Transmission / Reception

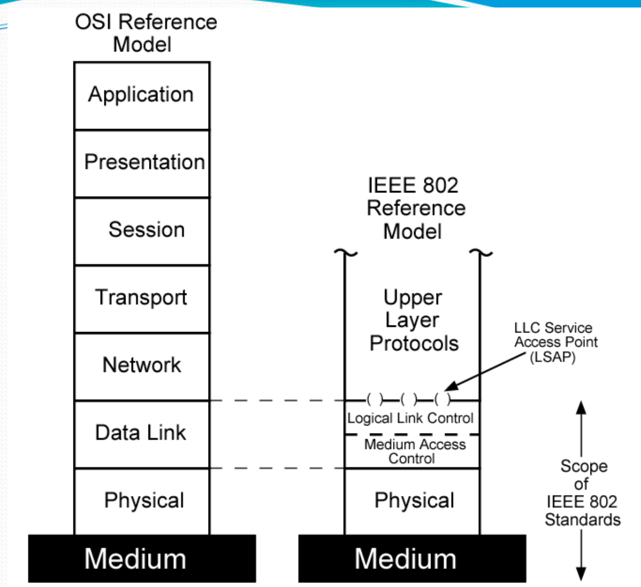
Functions Performed at Data Link Layer

LLC

- Provide an interface to higher layers
- Perform flow and error control

MAC

- Assemble data into frame with address and error-detection fields
- Assemble/de-assemble frame, perform address recognition and error detection
- Govern Access to the LAN transmission medium



1-7

7

MAC Frame Format

MAC Control	Destination MAC address	Source MAC address	LLC PDU	CRC

DSAP	SSAP	LLC Control	Variable

I/G	DSAP value	C/R	SSAP value

D/S-SAP: Destination/Source Access Point: 7-bit address, specifying the destination/source users of LLC; 1 bit of DSAP indicates Individual or Group address (I/G); 1 bit of SSAP indicates Command or Response

1-8

8

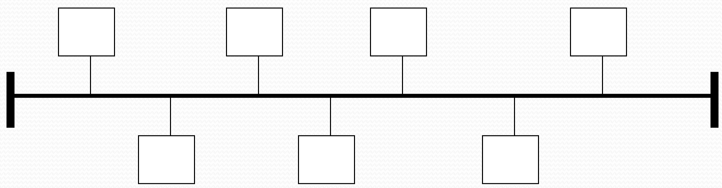
Topologies

- Tree
- Bus
  - Special case of tree
    - One trunk, no branches
- Ring
- Star

1-9

9

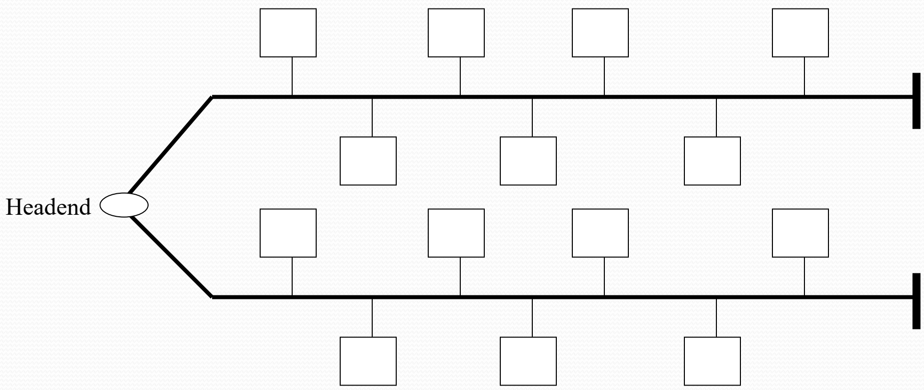
Bus Topology



1-10

10

Tree Topology



1-11

11

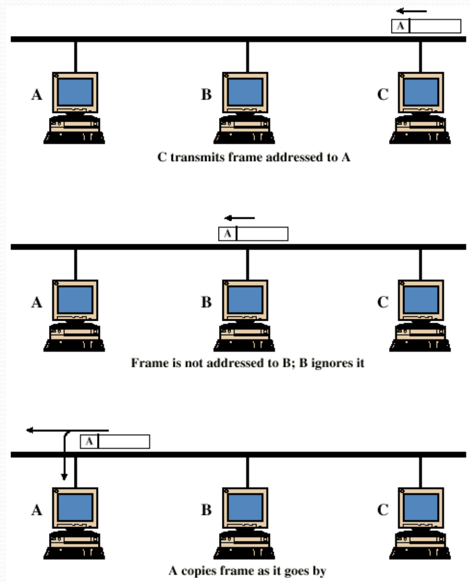
Bus and Tree

- Multipoint medium
- Signal propagates throughout medium
- Heard by all stations
  - Need to identify target station
    - Each station has unique address
- "Full duplex" connection between station and tap
  - Allows for transmission and reception
- Need to regulate transmission
  - To avoid collision and hogging Data in small blocks - frames
- Terminator absorbs frames at end of medium

1-12

12

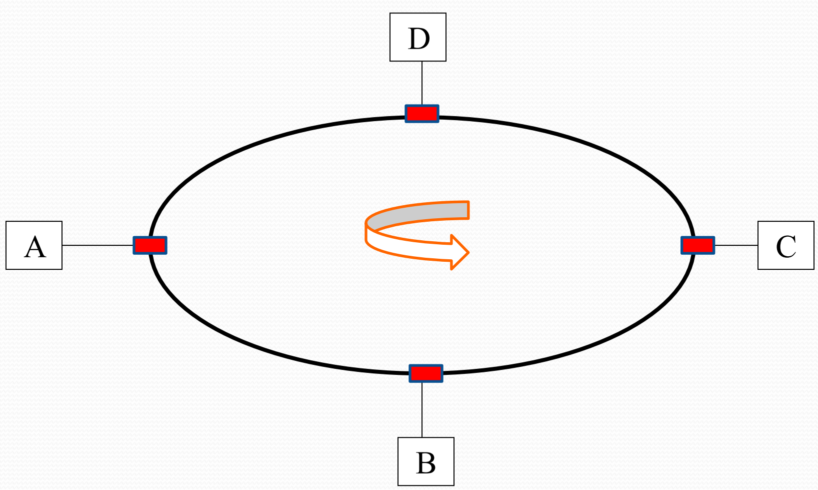
Frame Transmission - Bus LAN



1-13

13

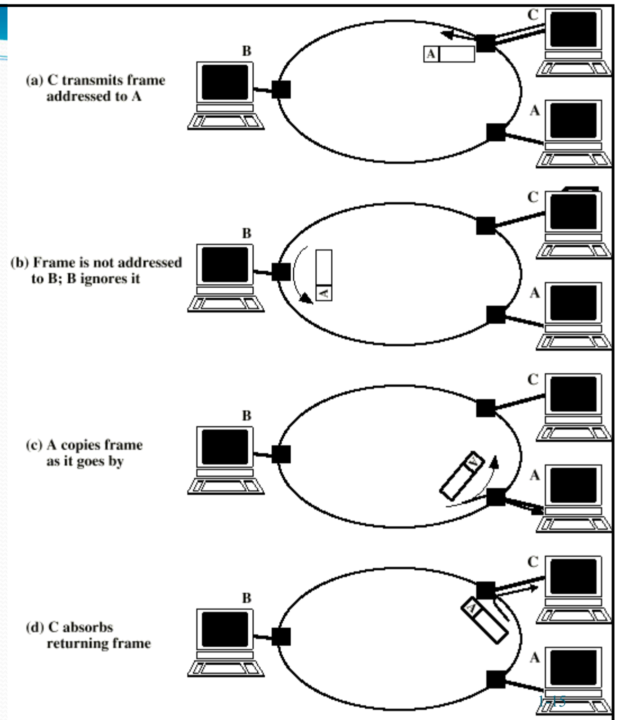
Token Ring



1-14

14

Frame Transmission Ring LAN



15

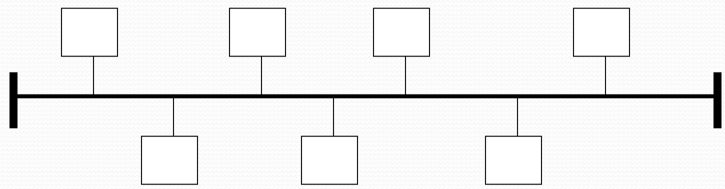
Ring Topology

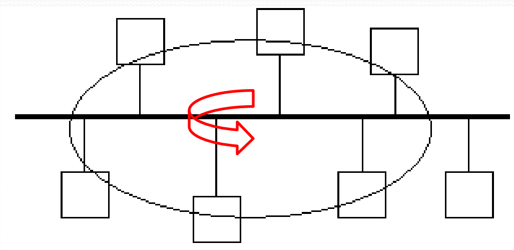
- Repeaters joined by point-to-point links in closed loop
  - Receive data on one link and retransmit on another
  - Links unidirectional
  - Stations attach to repeaters
- Data in frames
  - Circulate past all stations
  - Destination recognizes address and copies frame
  - Frame circulates back to source where it is removed
- Media access control determines when station can insert frame

1-16

16

Token Bus

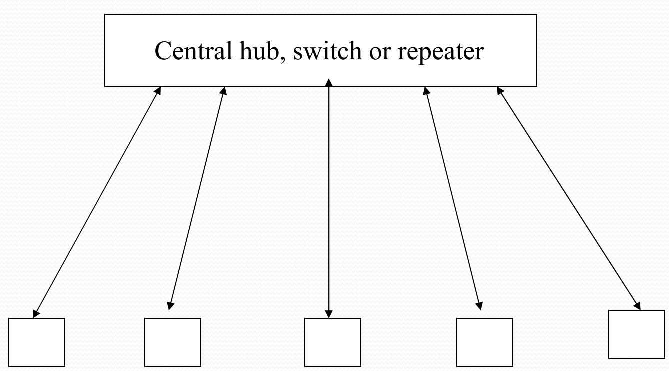




1-17

17

Star Topology



1-18

18

Star Topology

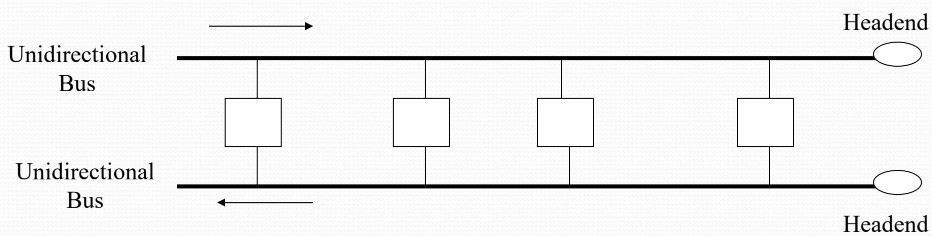
- Each station connected directly to central node
  - Usually via two point to point links
- Central node can broadcast
  - Physical star, logical bus
  - Only one station can transmit at a time
- Central node can act as frame switch

1-19

19

Distributed Queue Dual Bus (DQDB)

Used with Fiber Links



1-20

20

LAN/MAN MAC Standards

- CSMA/CD
- Token Bus
- Round Robin
- Token Ring
- DQDB
- CSMA/CA

1-21

21

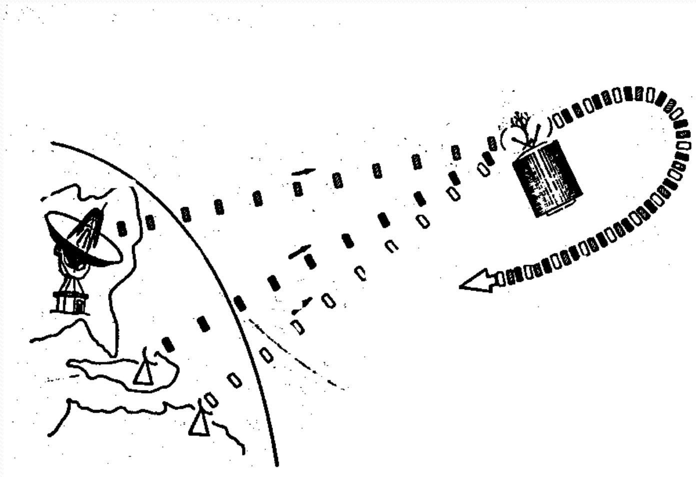
IEEE802.3 Medium Access Control

- Random Access
  - Stations access medium randomly
- Contention
  - Stations content for time on medium

1-22

22

Random Access Packet Radio-Satellite Communication Net



1-23

23

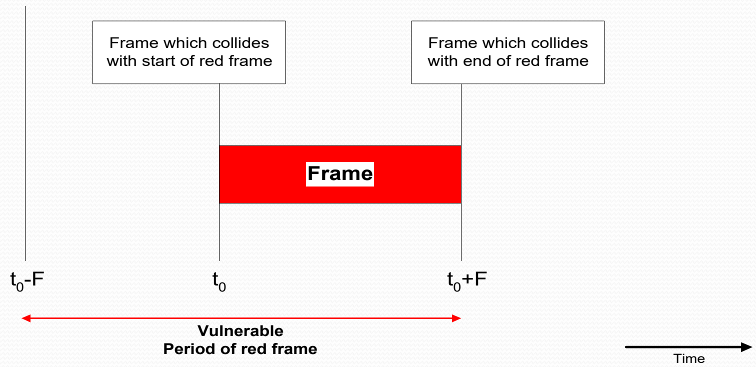
ALOHA

- Packet Radio
- When station has frame, it sends
- Station listens (for max round trip time) plus small increment
- If ACK, fine. If not, retransmit
- If no ACK after repeated transmissions, give up
- Frame check sequence (as in HDLC)
- If frame OK and address matches receiver, send ACK
- Frame may be damaged by noise or by another station transmitting at the same time (collision)
- Any overlap of frames causes collision
- Max utilization 18%

1-24

24

Collisions and Vulnerable Period

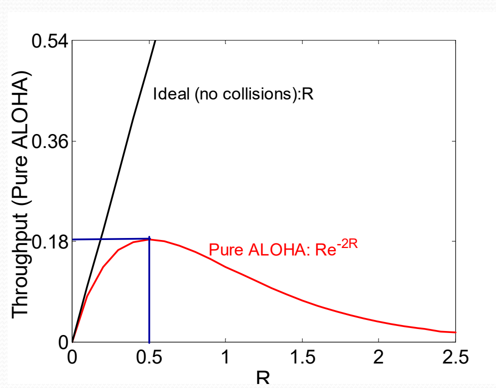


- A frame (red frame) will be in a collision if and only if another transmission begins in the vulnerable period of the frame
- Vulnerable period has the length of 2 frame times

1-25

25

Performance of ALOHA



- Maximum throughput approximately 18% of the capacity
- Can do better with improved control
- **However, ALOHA is still used for its simplicity**

1-26

26

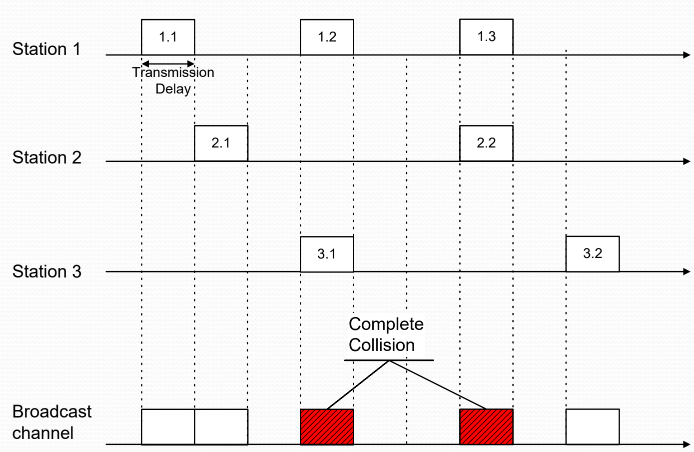
Slotted ALOHA

- Time in uniform slots equal to frame transmission time
- Need central clock (or other sync mechanism)
- Transmission begins at slot boundary
- Frames either miss or overlap totally
- Max utilization 37%

1-27

27

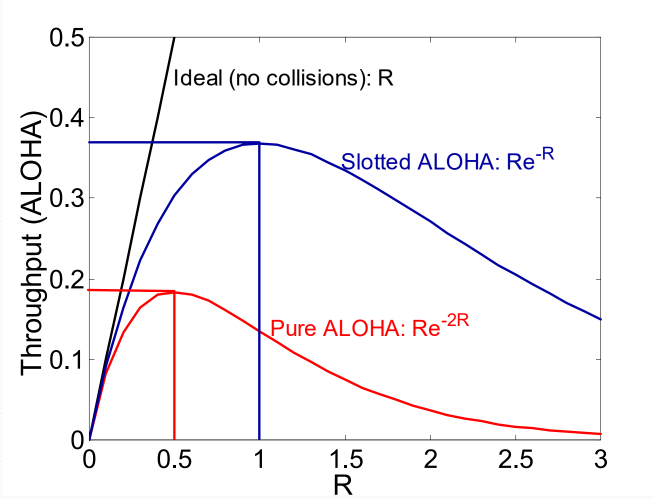
Collisions in S-ALOHA



1-28

28

Comparison of ALOHA and S-ALOHA



1-29

29

Carrier Sense Multiple Access (CSMA)

- Propagation time is much less than transmission time
- All stations know that a transmission has started almost immediately
- First listen for clear medium (carrier sense)
- If medium idle, transmit
- If two stations start at the same instant, collision
- Wait reasonable time (round trip plus ACK contention)
- No ACK then retransmit
- Max utilization depends on propagation time (medium length) and frame length
  - Longer frame and shorter propagation gives better utilization

1-30

30

If Busy?

- If medium is idle, transmit.
- If busy, listen for idle; then transmit immediately 1-persistent.
- If two or more stations are waiting, collision.
- Probability for collision higher when waiting in busy channel because during waiting time for transmission to complete, another or more stations might have produced frames for transmission.
- Use p-persistent: after channel idle, transmit with probity p (0<p<1). If you decide not to transmit wait for next "slot" and repeat process.

1-31

31

Carrier Sensing Multiple Access / Collision Detection (CSMA/CD)

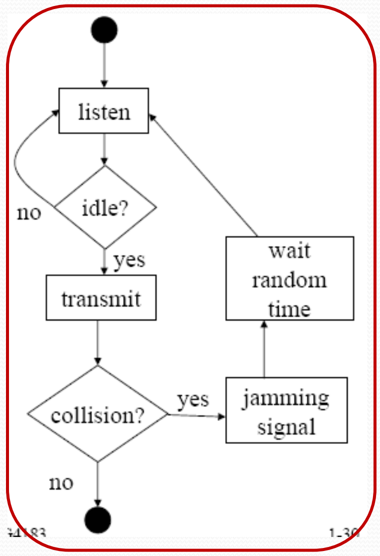
- Used in Ethernet
- Usually applied with Bus and Tree topologies

1-32

32

Carrier Sensing Multiple Access / Collision Detection (CSMA/CD)

- IEEE 802.3 standard
- Useful when propagation time much shorter to frame's duration
- Used in Ethernet (the most widely used type of LAN)
- Usually applied with Bus and Tree topologies



1-33

33

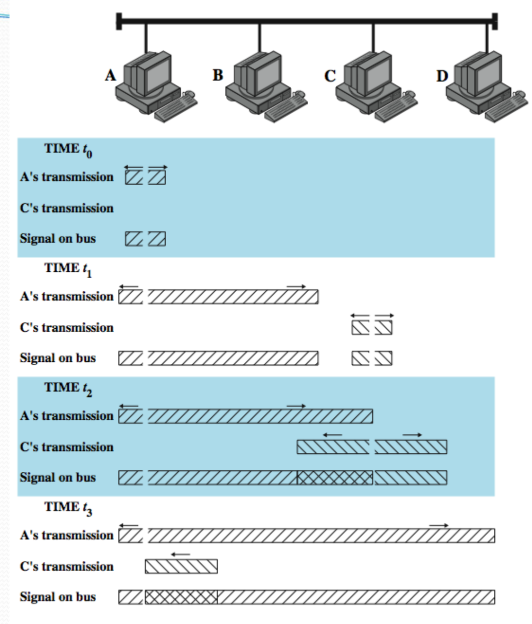
CSMA with Collision Detection (CSMA/CD)

- With CSMA, collision occupies medium for duration of transmission
- Stations listen while transmitting
- If medium idle, transmit
- If busy, listen for idle, then transmit
- If collision detected, jam then cease transmission
- After jam, wait random time then start again
  - Binary exponential back off

1-34

34

CSMA/CD Operation



1-35

35

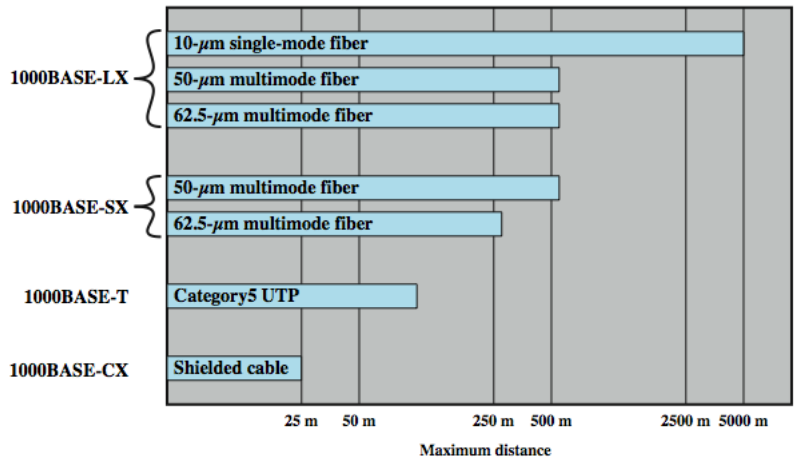
Collision Detection

- On baseband bus, collision produces significantly higher signal strength than a single signal does
- Collision detected if cable signal noticeably stronger than single station signal
- Signal attenuation increases with distance
- There are distance limits, e.g. 500m (10Base5) or 200m (10Base2), 100 meters (10Base-T)

1-36

36

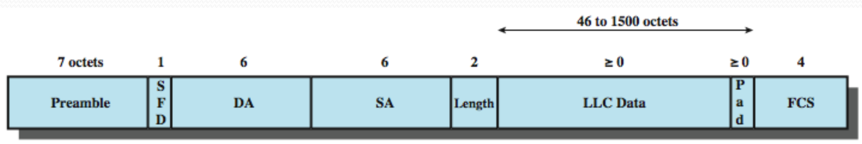
Gigabit Ethernet – Physical



1-37

37

IEEE 802.3 Frame Format



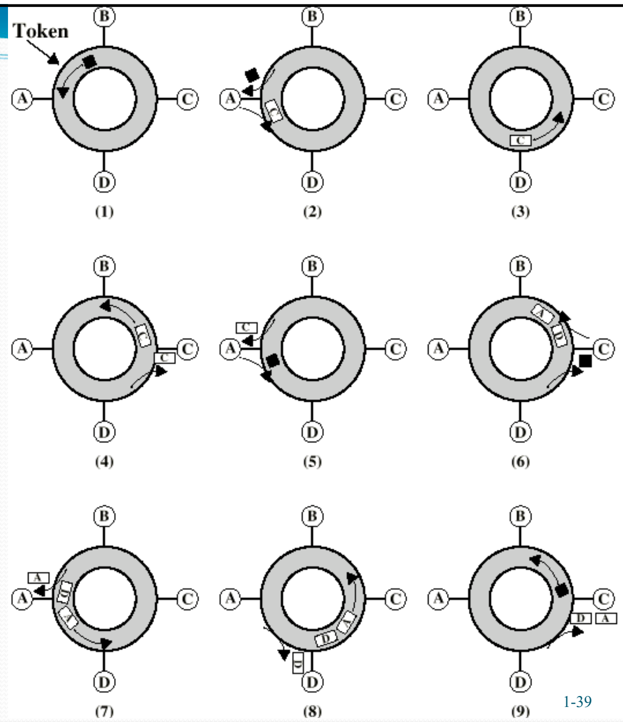
SFD = Start of frame delimiter
DA = Destination address
SA = Source address
FCS = Frame check sequence

1-38

38

Token Ring Operation

A→ C



1-39

39

Token Ring (802.5)

- MAC protocol
  - Small frame (token) circulates when idle
  - Station waits for token
  - Changes one bit in token to make it SOF for data frame
  - Append rest of data frame
  - Frame makes round trip and is absorbed by transmitting station
  - Station then inserts new token when transmission has finished and leading edge of returning frame arrives
  - Under light loads, some inefficiency
  - Under heavy loads, round robin

1-40

40

FDDI:
Fiber Distributed Data Interface

- 100Mbps
- LAN and MAN applications
- Based on Token Ring

1-41

41

FDDI MAC Protocol

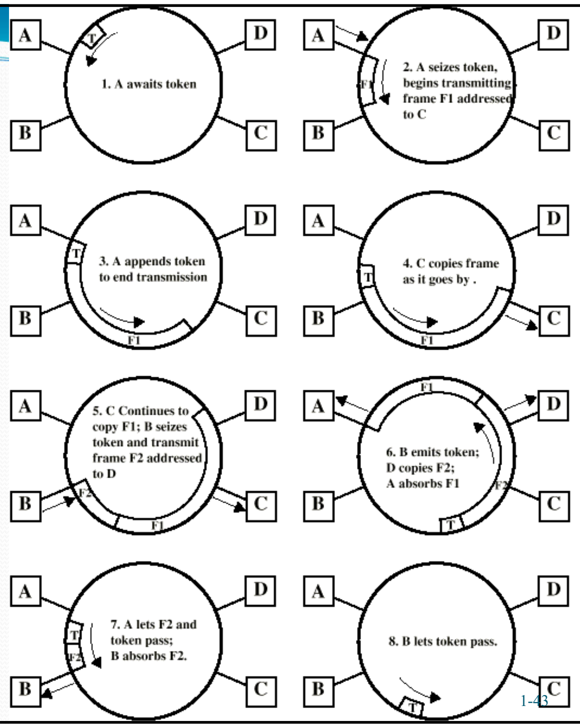
As for 802.5 except:

- Station seizes token by aborting (failing to repeat) token transmission
- Once token captured, one or more data frames transmitted
- New token released as soon as transmission finished (early token release in 802.5)

1-42

42

FDDI Operation



Wireless LANs & PANs

- Physical layer can use:
  - Infrared (IR)
  - Code Division Multiple Access (CDMA)
  - Frequency Hopping Spread Spectrum (FH/SS)
  - Orthogonal Frequency Multiplexing (OFM)
  - Multiple Input Multiple Output (MIMO)
- Standards:
  - IEEE 802.11
  - HIPERLAN
  - Bluetooth
  - Home RF
- Several important differences with wired environment

Wireless LAN Standards

- European standard : ETSI- HIPERLAN
  - + 5.15- 5.30, 17.1 -17.2 GHz transmission band
  - + Data rates up to 23.529 Mbps
  - + FEC for error correction
- American Standard : IEEE 802.11 WLAN
  - + 2.4 ISM/5 GHz UNII Bands (first generation products used 900 MHz)
  - + data rates up to 2 Mbps (today we have 1.7Gbps products)
  - + Stop and Wait ARQ

1-45

45

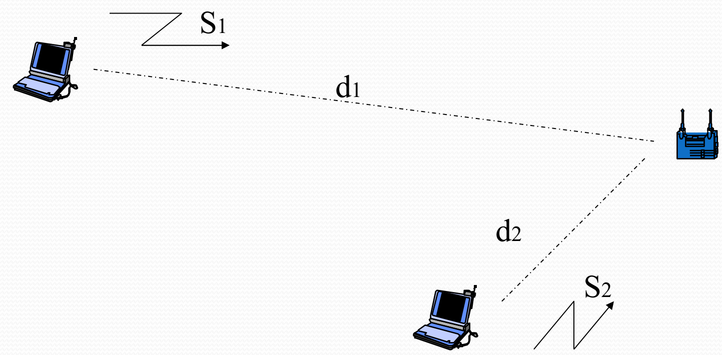
Wireless LAN Design Challenges

- Reliability, noise, fading, interference.
- Hidden Terminal issue.
- Fairness of access (capture effect).
- Handoff and roaming.
- The ability of having carrier sense.
- Battery power consumption.

1-46

46

Capture Effect



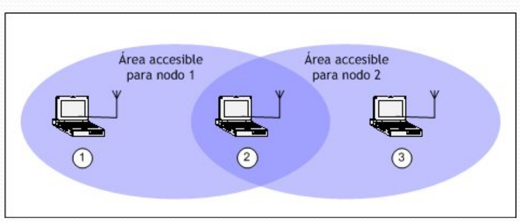
$d_1 >> d_2 \rightarrow \{(S_1)^2/(S_2)^2\} << 1$

1-47

47

The hidden node problem

This problem comes from the fact that not every station can hear everybody else's transmissions. For instance, in the figure node 2 can hear both stations 1 and 3, but these two stations cannot hear each other.

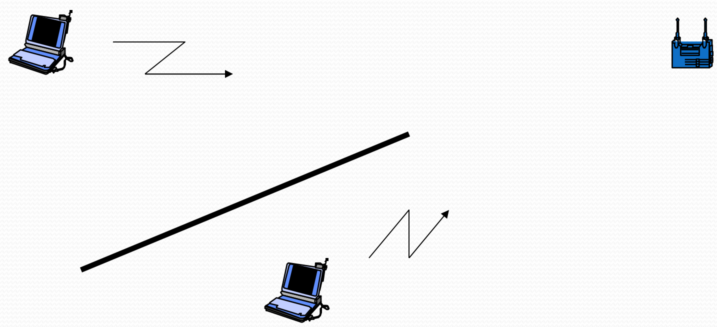


Node 1 and 3 are hidden from each other

1-48

48

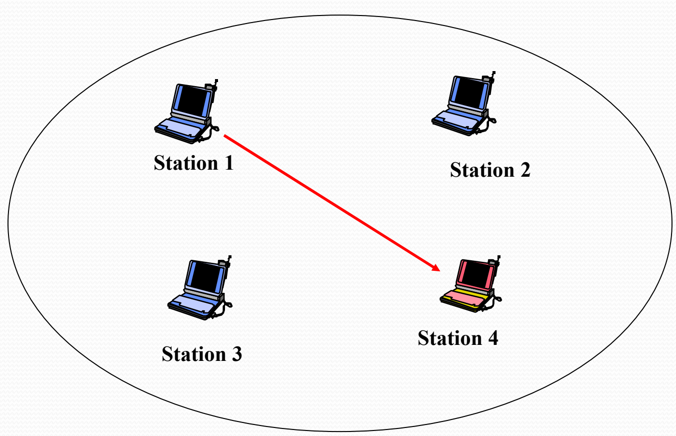
Hidden Terminal



1-49

49

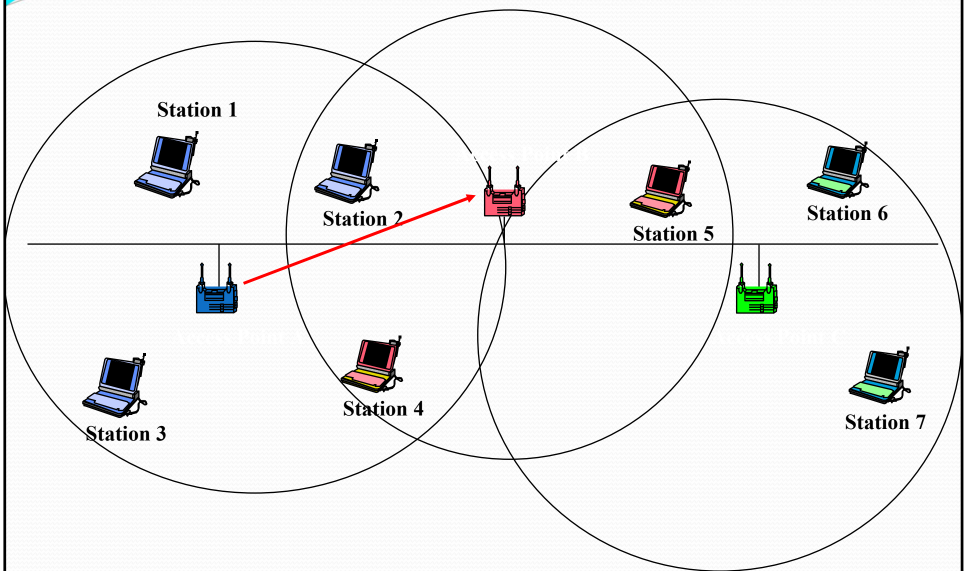
Ad Hoc Wireless LAN



1-50

50

Infrastructure Wireless LAN



1-51

51

IEEE 802.11

1-52

52

What is IEEE 802.11?

- IEEE standard addressing the 2.4 & 5 GHz WLAN market
- Spec is steered by the IEEE committee
  - Specifies "over the air" interface between a wireless client & a base station (or access point) or wireless clients
  - Conceived in 1990, final draft approved in June 1997
  - Like the IEEE 802.3 Ethernet & 802.5 Token Ring Standards.
  - Wide range: 152 m indoors/457 m outdoors for 802.11b

1-53

53

Modern WiFi Systems

Frequency	Theoretical	Speed Real-World Speed
2.4 **GHz** (802.11g)	54 Mbps	10 -29 Mbps
2.4 **GHz** (802.11n)	300 Mpbs	150 Mbps
5 **GHz** (802.11a)	6-54 Mbps	3 - 32 Mbps
5 **GHz** (802.11ac)	433 Mbps-1.7 Gbps	210 Mbps - 1 G

1-54

54

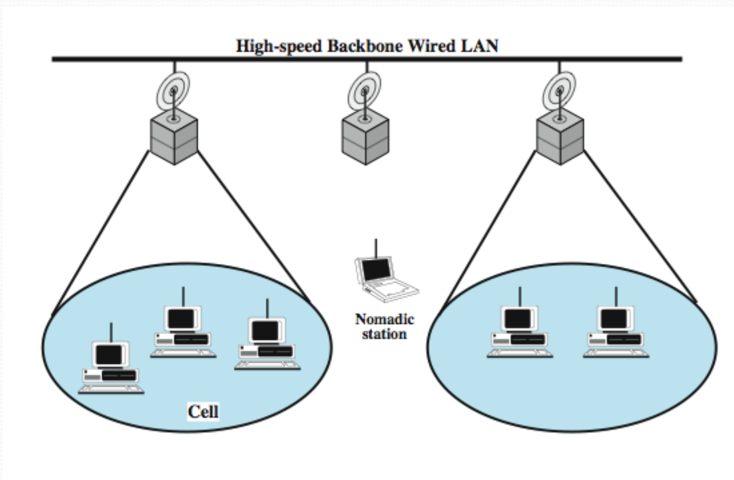
IEEE 802.11 WLAN Standard Requirements

- Provide reliable, efficient wireless data networking
- Define MAC & PHY layer specifications
- Provide a single MAC layer to work with multiple PHYs
- Be robust against interference
- Provide mechanism to handle hidden nodes
- Support peer-to-peer & infrastructure configurations
- Support time sensitive applications

1-55

55

Infrastructure Wireless LAN

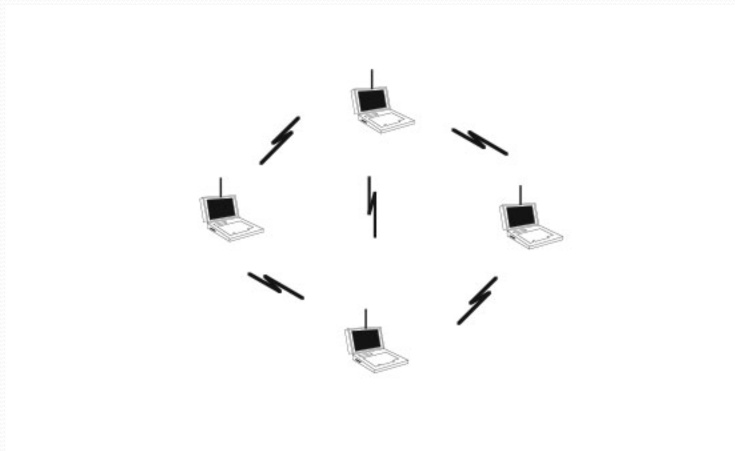


1-56

56

Ad Hoc Networking

- peer-to-peer network

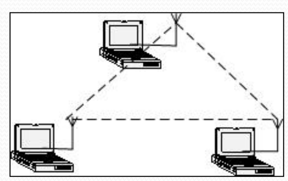


1-57

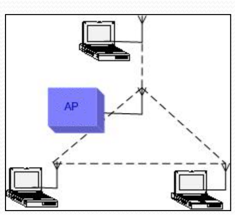
57

Architectures summary

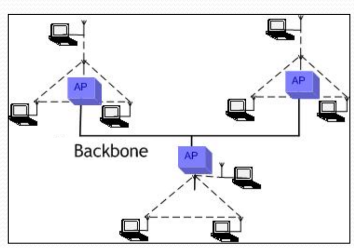
- There are different topologies for an IEEE 802.11 WLAN
- A basic service set (BSS) is a set of terminals that communicate locally, either directly or through multiple hops, but no wired segments



Independent BSS
(Ad-hoc, MANETs)



Infrastructure BSS

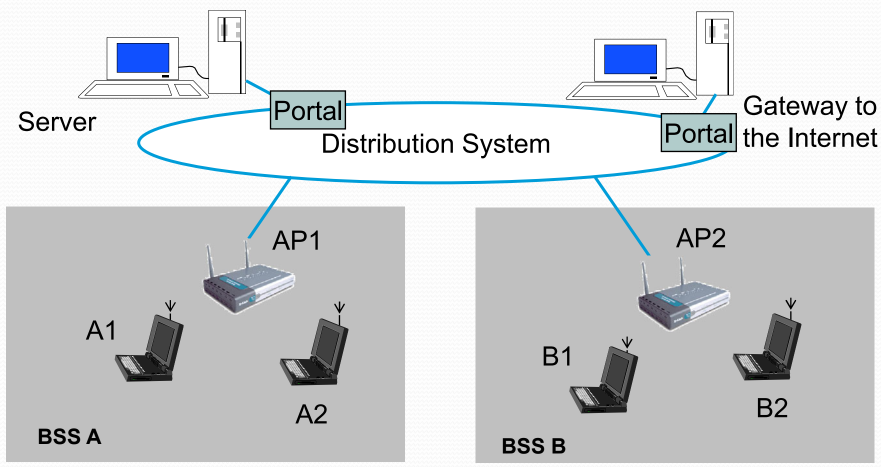


Extended SS

1-58

58

Extended Service Set



Access Points provide access to Internet

1-59

59

WLAN definitions

- *Basic Service Set (BSS)* is defined as a group of stations that coordinate their access to the medium under a given instance of the medium access control
- The geographical area covered by the BSS is known as the *basic service area (BSA)*
- An ad hoc network consists of a single BSS
- Infrastructure BSSs, on the other hand, can be interconnected by a *distribution system (DS)* to form an *extended service set (ESS)*
- Access points (APs) usually have more than one interface, one to connect wirelessly to the mobile nodes and one to connect to a wired network

1-60

60

Establishing Connectivity: Scanning

- When a station is activated it listens for a device with which it can associate (scanning).
- Scanning can be either passive or active.

1-61

61

Establishing Connectivity: Scanning

- Passive scanning
  - Nodes listen for **beacon** frames transmitted by AP (infrastructure mode) or peer stations (ad hoc).
  - Station attempts to join network (authentication and association steps) on reception of beacon frame containing SSID (Service Set ID) of network it wants to join.
  - Passive scanning is a continuous process as stations can associate or disassociate with APs as signal strength varies.

1-62

62

Establishing Connectivity: Scanning

- Active scanning
  - Instead of waiting for a beacon, a **probe request** is sent by a station wishing to join a network.
  - APs hearing the request issue a **probe response.**
  - The station can choose one of the APs that responded based on the received power level, or other network characteristics.
  - Authentication and association steps are then completed.

1-63

63

Authentication

- WLAN authentication occurs at layer 2 (authenticates device, not user)
  - Station sends authentication request frame to AP
  - AP sends authentication response frame (accept or reject)
  - AP may be configured to delegate authentication to an authentication server which does more thorough checking

1-64

64

Association

- Association, which is performed after authentication, is the state that permits a station to use the AP's services to transfer data.

1-65

65

IEEE 802.11 Draft Standard Description

- Mandatory support for asynchronous data transfer is specified
  - Asynchronous data transfer refers to traffic that is insensitive to time delay
- Optional support for distributed time-bounded services (DTBS)
  - Time-bounded traffic is bounded by specific time delays in order to achieve an acceptable QoS, e.g. packetized voice and video
- Support for 2 fundamentally different MAC schemes to transport asynchronous & time-bounded services
  - **Distributed Coordination Function (DCF)**
  - **Point Coordination Function (PCF)**

1-66

66

MAC & PHY Layer Operation

- MAC layer operates together with the PHY layer by sampling the energy over the medium transmitting data.
- PHY layer uses a clear channel assessment (CCA) algorithm to determine if the channel is clear.
  - This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal.
  - If the received signal strength is below a specified threshold the channel is declared clear and the MAC layer is given the clear channel status for data transmission.
  - If the RF energy is above the threshold, data transmissions are deferred in accordance with the protocol rules.

1-67

67

The MAC Sub-layer

- Mac specification for 802.11 has similarities to 802.3 (which is the Ethernet wired line standard)
- CSMA/CA protocol used for 802.11
  - Uses carrier-sense, multiple access, collision avoidance
  - Avoids collisions instead of detecting a collision like the algorithm in IEEE 802.3 (CSMA/CD)
  - Collision avoidance is used because it is difficult to detect collisions in an RF transmission network

1-68

68

Network Allocation Vector

- The NAV is a countdown timer maintained by each STA
  - A STA is not permitted to attempt accessing the medium until its NAV has reached zero
- NAV acts as a virtual carrier sense mechanism
  - When a STA checks for an idle medium, both the physical and virtual carrier sense mechanisms must show the medium to be clear

1-69

69

Physical and virtual sensing

- Physical sensing
  - Performed by the physical layer and indicated to the MAC sub-layer
- Virtual sensing
  - Most frames carry a field indicating the duration of the atomic frame exchange that they precede; it is interpreted as a channel reservation
  - The time that the channel has been reserved is known as network allocation vector (NAV)
  - If the NAV is greater than zero, the virtual sensing indicates that the channel is busy
  - All stations must read the header of all received frames, either addressed for them or not, to update their NAV
- The medium is considered free only when both, the physical and the virtual sensing, indicate so

1-70

70

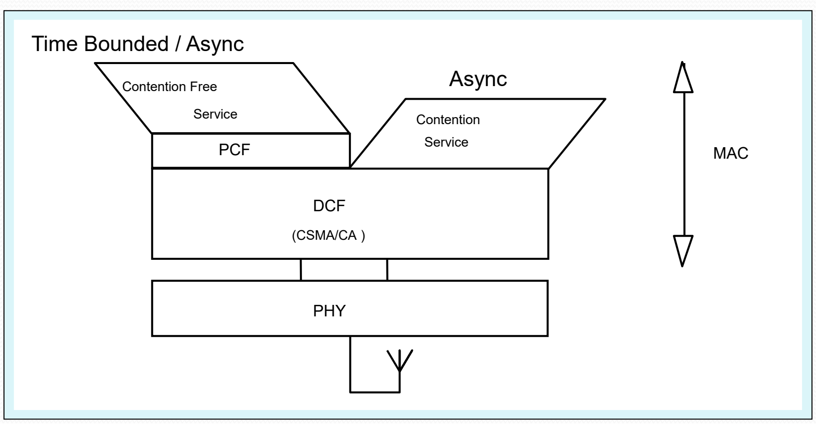
CSMA/CA: Interframe spaces

- Time, the stations have to wait after completion of a packet transmission
- Used to reduce collision probability between multiple stations accessing a medium (time when medium becomes free after a busy period)
- Used to provide some form of priority / service differentiation
  - Short Inter-frame Space (SIFS)
  - PCF Inter-frame Space (PIFS)
  - DCF Inter-frame Space (DIFS)
  - Extended Inter-frame Space (EIFS)

1-71

71

Optional Point Coordination Function

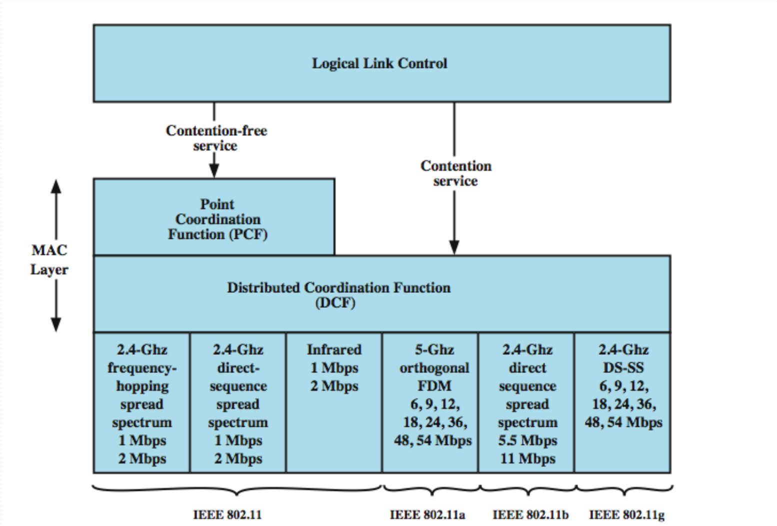


- Async Data, Voice, Video or mixed implementations
- Coexistence between Contention and Contention free

72

72

Media Access Control



1-73

73

Distributed Coordination Function (DCF)

1-74

74

CSMA/CA: Interframe spaces

- Time, the stations have to wait after completion of a packet transmission
- Used to reduce collision probability between multiple stations accessing a medium (time when medium becomes free after a busy period)
- Used to provide some form of priority / service differentiation
  - Short Inter-frame Space (SIFS)
  - PCF Inter-frame Space (PIFS)
  - DCF Inter-frame Space (DIFS)
  - Extended Inter-frame Space (EIFS)

1-75

75

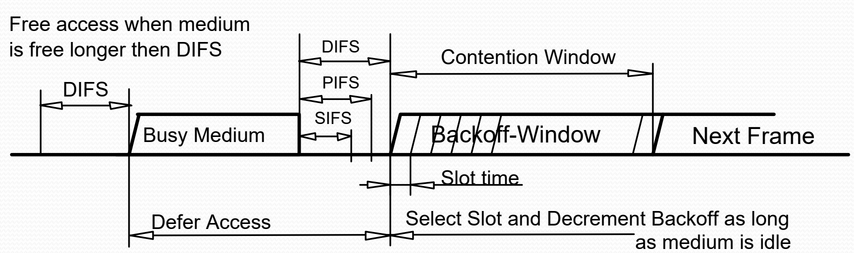
Network Allocation Vector

- The NAV is a countdown timer maintained by each STA
  - A STA is not permitted to attempt accessing the medium until its NAV has reached zero
- NAV acts as a virtual carrier sense mechanism
  - When a STA checks for an idle medium, both the physical and virtual carrier sense mechanisms must show the medium to be clear

1-76

76

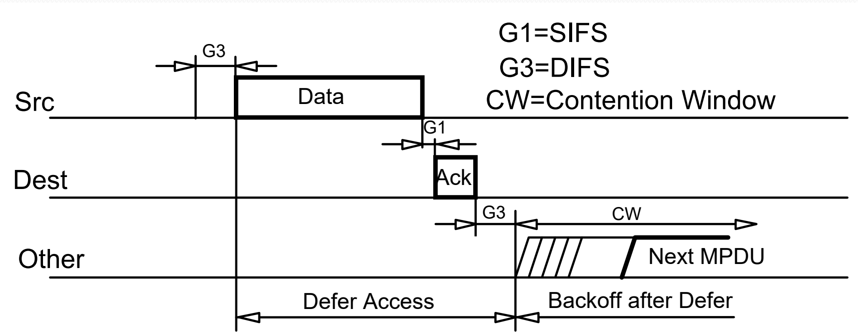
CSMA/CA



1-77

77

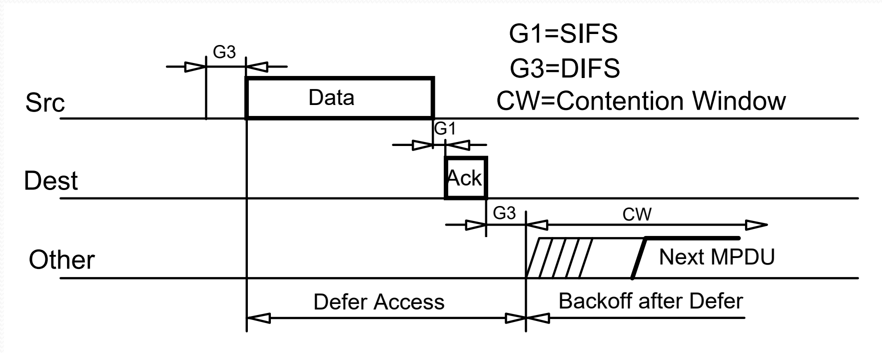
CSMA/CA + ACK



1-78

78

CSMA/CA + ACK

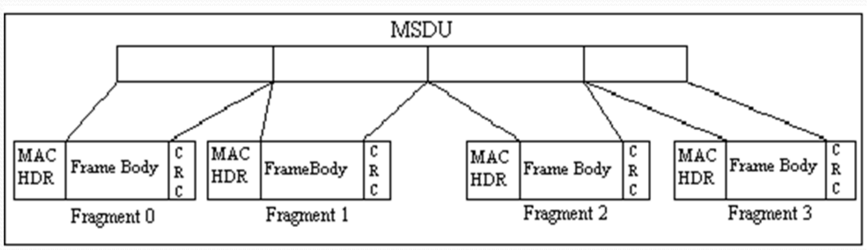


Think: what is the impact of collision in CSMA/CA compared to CSMA/CD?

1-79

79

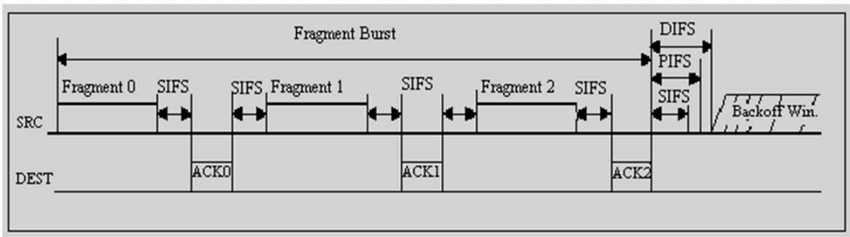
Fragmentation (1)



1-80

80

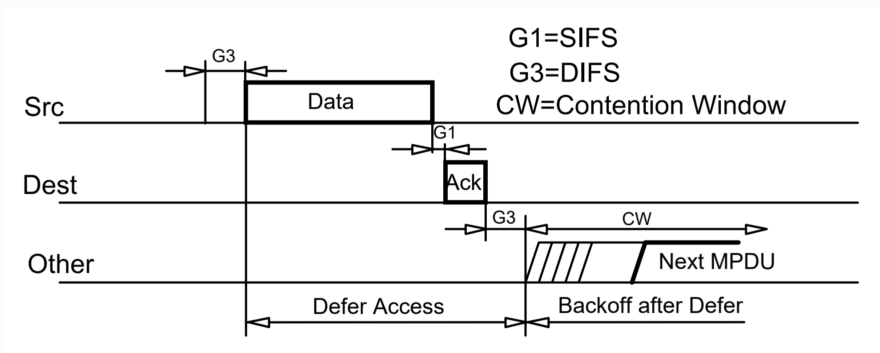
Fragmentation (2)



1-81

81

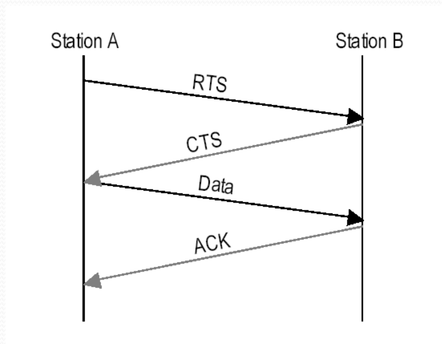
CSMA/CA + ACK



1-82

82

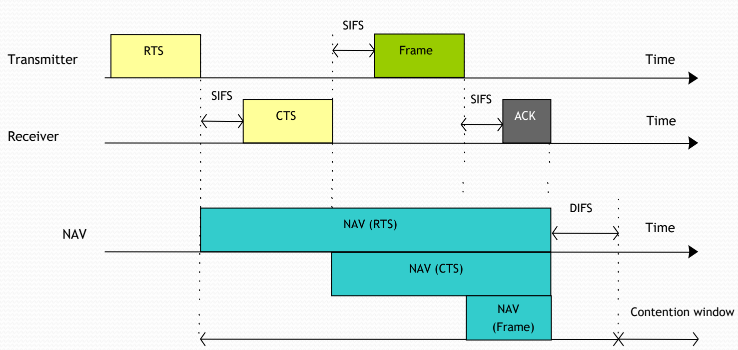
RTS/CTS/ACK Protocol



83

RTS/CTS Process Functioning

- Example:



84

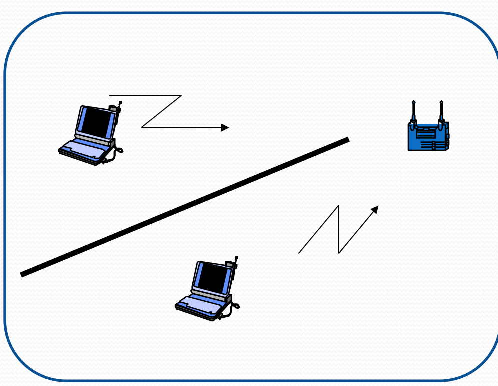
RTS/CTS Process

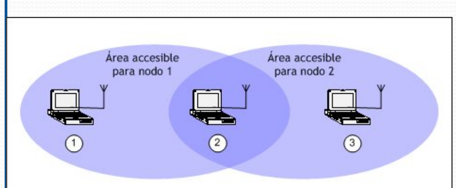
- Transmitting station sends an RTS message, specifying length of data and destination station
- The receiving station issues a CTS frame which echoes the sender address and the NAV
- If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over
- After the data frame is received, an ACK frame is sent back verifying a successful data transmission

1-85

85

RTS/CTS improves performance in the presence of hidden terminals

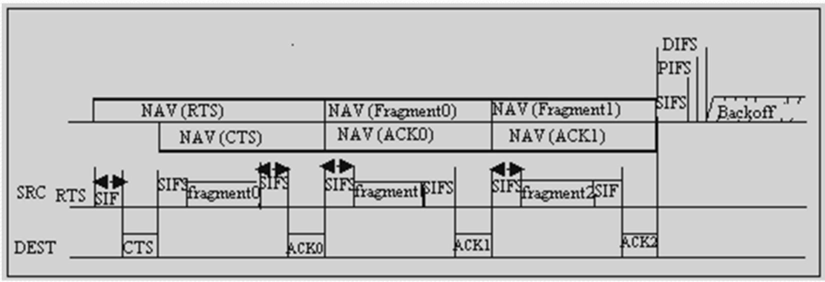




1-86

86

Fragmentation using RTS/CTS



1-87

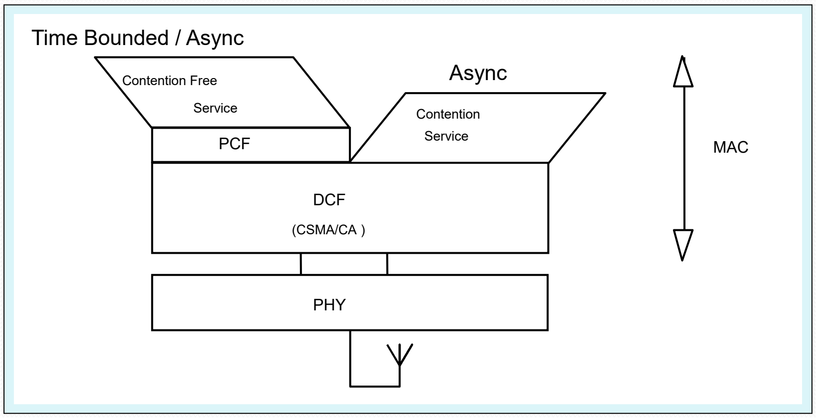
87

Point Coordination Function (PCF)

1-88

88

Optional Point Coordination Function

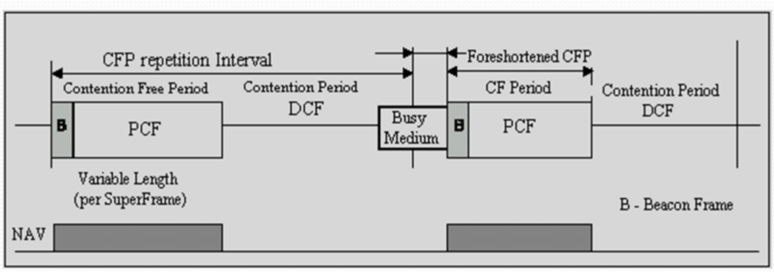


- Async Data, Voice, Video or mixed implementations
- Coexistence between Contention and Contention free

89

89

PCF

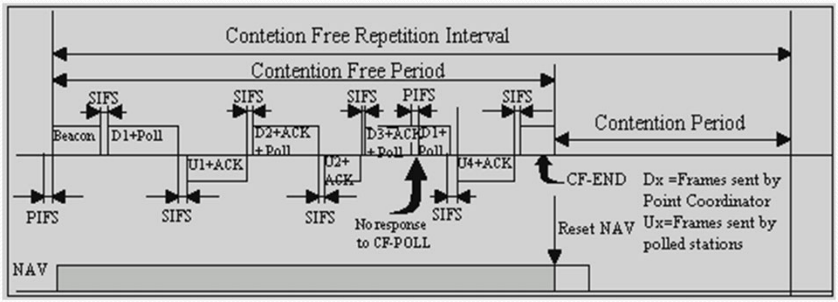


SIFS < PIFS < DIFS

1-90

90

PCF Operation



1-91

91

PCF Limitations

- PCF doesn't support multiple overlapping PCFs.
- More complexity & bandwidth consumption& cost.
- PCF means longer delay with less variance.
- Not suitable for non-periodic time bounded data.
- Provides only two levels of QoS.

1-92

92

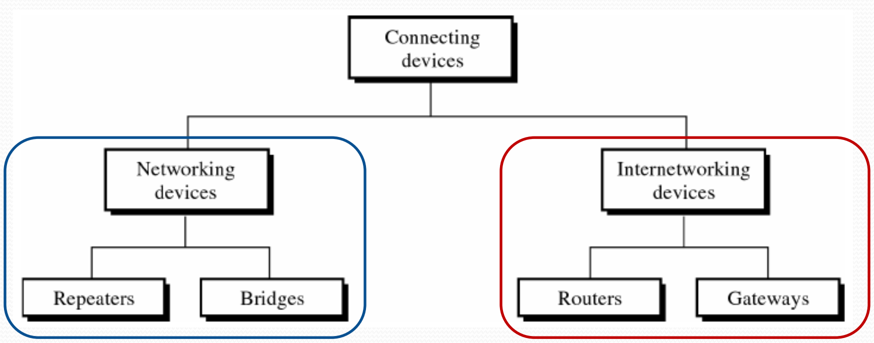
IEEE 802.11e standard (QoS MAC)

- The MAC protocol of the original IEEE 802.11 standard cannot satisfy quality-of-service (QoS) requirements of multimedia applications
- Study group E was created to define an extension to the existing MAC protocol to make it QoS capable
- The protocol IEEE 802.11e became a standard in late 2005
- This new standard includes features for establishing priorities among stations, for connection admission negotiation, for resource reservation, for the direct communication among mobile stations without going through the AP, for new ways to handle ACKs, etc.
- A new and unique coordination function is defined, known as *Hybrid Coordination Function* (HCF), which combines and improves the characteristics of DCF and PCF.

1-93

93

Connecting Networks



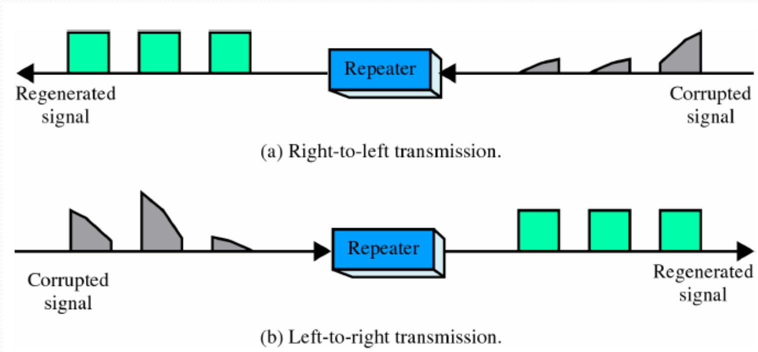
Networks of same technology

Networks of different technologies

1-94

94

Function of Repeater

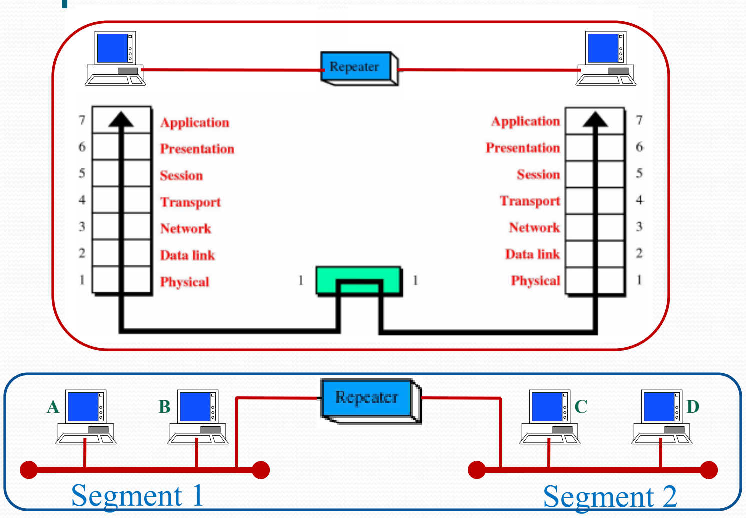


Repeaters operate at Physical layer (Layer 1)

1-95

95

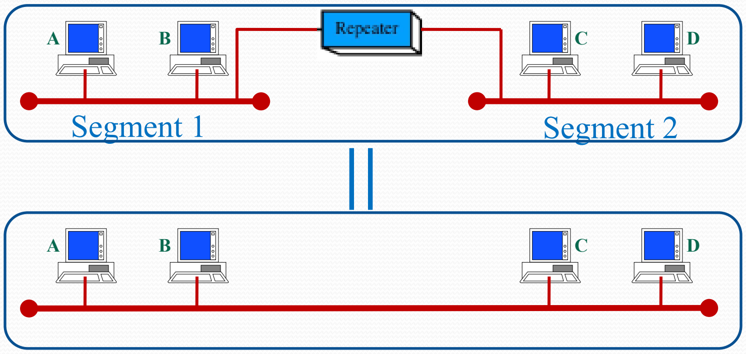
Repeater -- Hub



1-96

96

Repeater--Hub extends "segment"

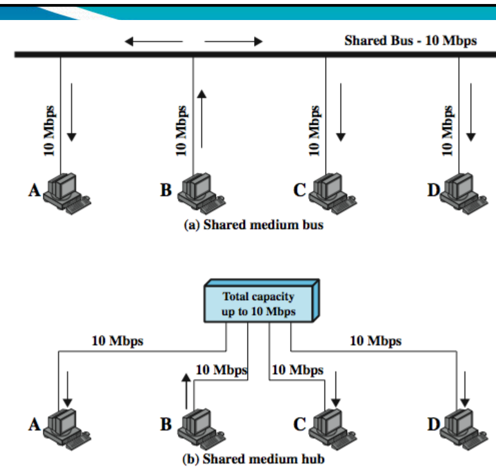


Simple and cheap
Transmissions of "A", "B" interfere with "C", "D" and vice versa.
Repeater DOES NOT isolate segments from each other
Repeaters connect segments of identical physical and data link layer technologies
(e.g. segment 1 is fast ethernet → segment 2 should be fast ethernet)

1-97

97

Shared Medium Bus and Hub



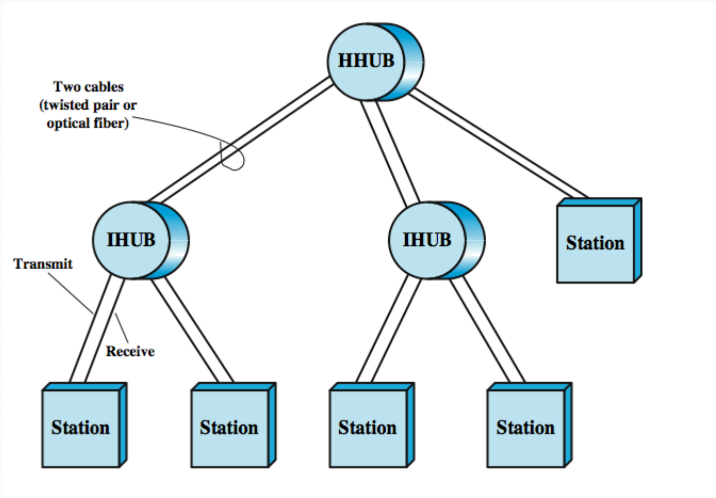
(a) Shared medium bus

(b) Shared medium hub

1-98

98

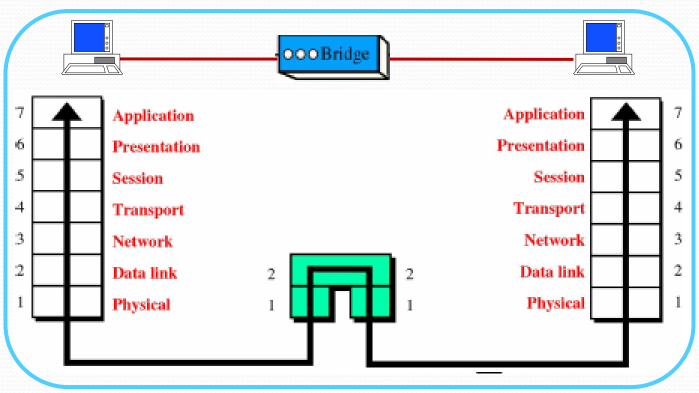
Two Level Hub Topology



1-99

99

Bridge



Bridges operate at Data Link layer (Layer 2)
They physically separate the PHY layers of different segments
They connect networks of same layer 2 technology

1-100

100

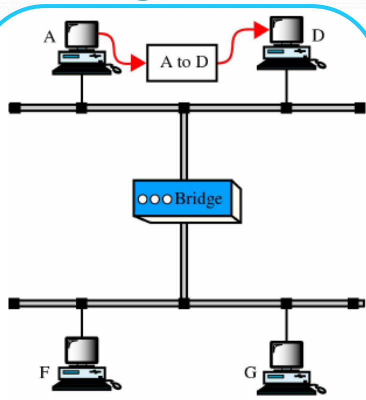
Interconnecting LANs - Hubs

- active central element of star layout
- each station is connected to hub by two UTP lines
- hub acts as a repeater
- limited to about 100 m by UTP properties
- optical fiber may be used out to 500m
- physically star, logically bus
- transmission from a station seen by all others
- if two stations transmit at the same time have a collision

1-101

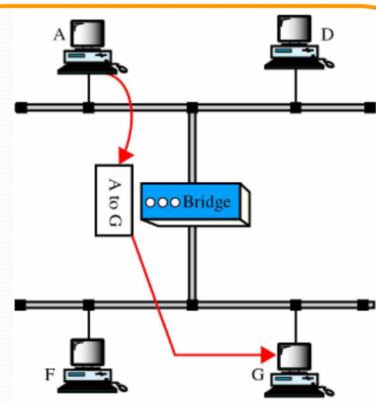
101

Bridges: example



a. A packet from A to D

Packets from A → D and D → A do not interfere with those of F and D



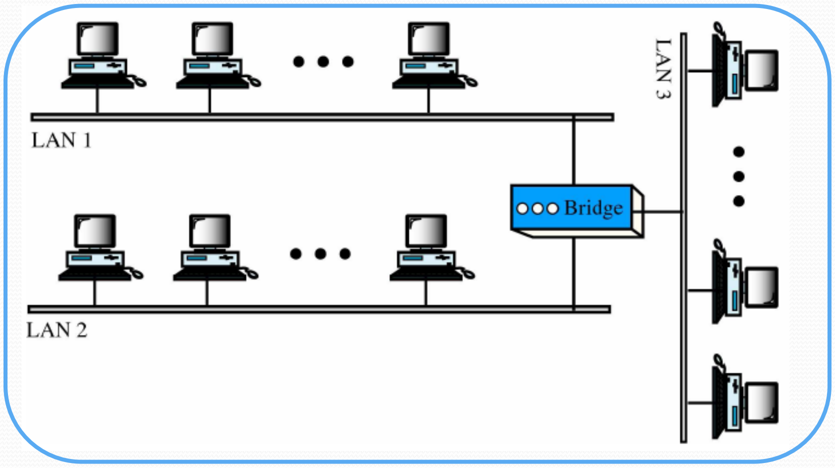
b. A packet from A to G

Packets destined to a node located in a different signal interfere with segments of the source (node A) and destination (node G)

1-102

102

Multiport Bridge

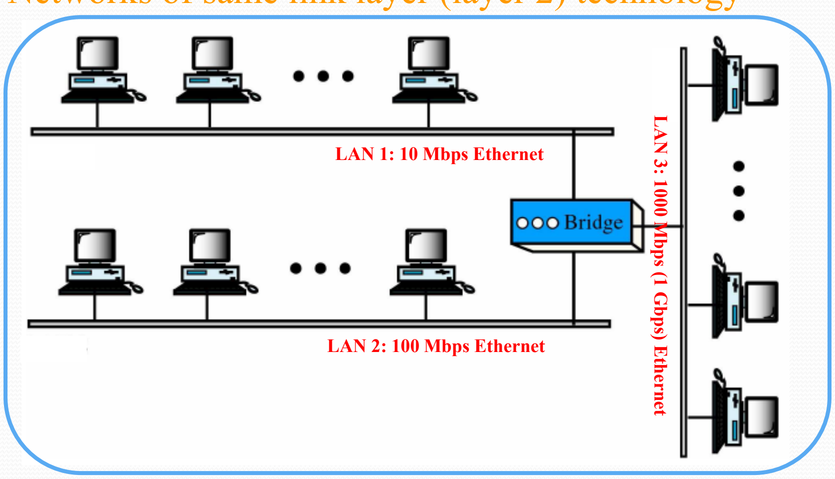


1-103

103

Bridge connects…

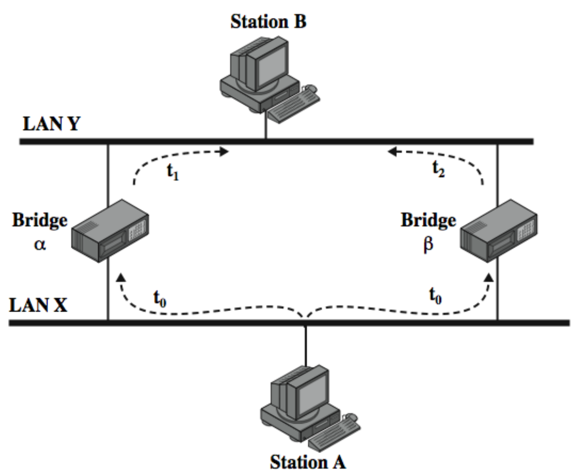
Networks of same link layer (layer 2) technology



1-104

104

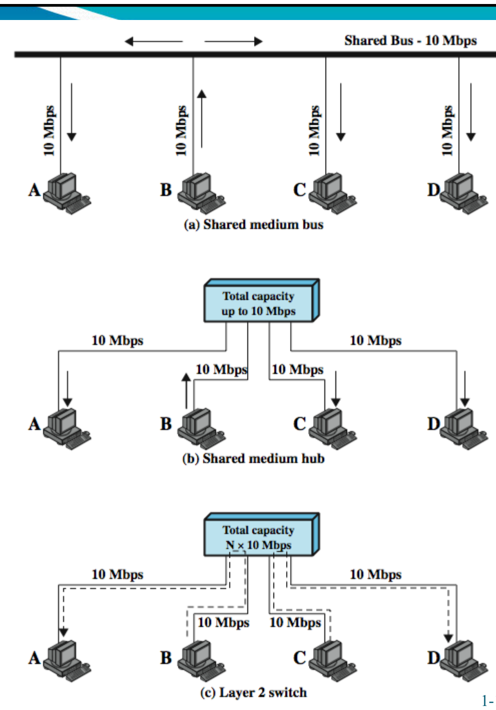
Loop of Bridges



1-105

105

Switches



1-106

106

Layer 2 Switch Benefits

- no change to attached devices to convert bus LAN or hub LAN to switched LAN
  - e.g. Ethernet LANs use Ethernet MAC protocol
- have dedicated capacity equal to original LAN
  - assuming switch has sufficient capacity to keep up with all devices
- scales easily
  - additional devices attached to switch by increasing capacity of layer 2

1-107

107

Layer 2 Switch vs Bridge

- Layer 2 switch can be viewed as full-duplex hub
- incorporates logic to function as multiport bridge
- differences between switches & bridges:
  - bridge frame handling done in software
  - switch performs frame forwarding in hardware
  - bridge analyzes and forwards one frame at a time
  - switch can handle multiple frames at a time
  - bridge uses store-and-forward operation
  - switch can have cut-through operation
- hence bridge have suffered commercially

1-108

108

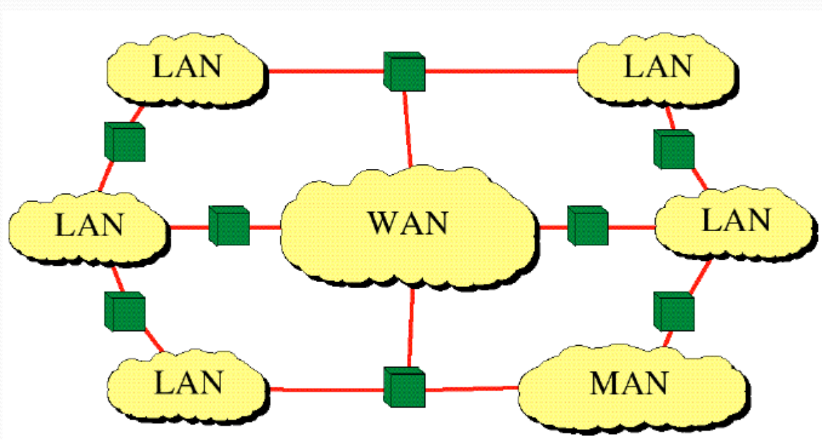
Layer 2 Switch Problems

- broadcast overload
  - users share common MAC broadcast address
  - broadcast frames are delivered to all devices connected by layer 2 switches and/or bridges
  - broadcast frames can create big overhead
  - broadcast storm from malfunctioning devices
- lack of multiple links
  - limits performance & reliability

1-109

109

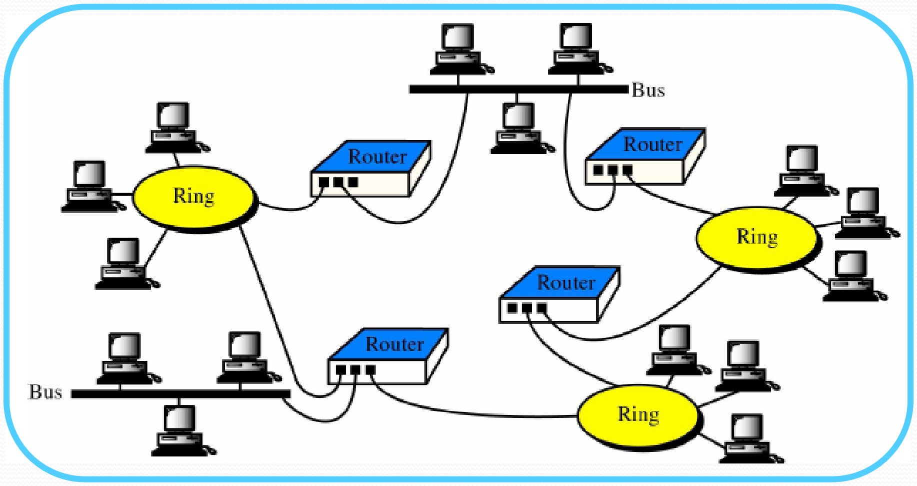
Internetwork (Internet)



1-110

110

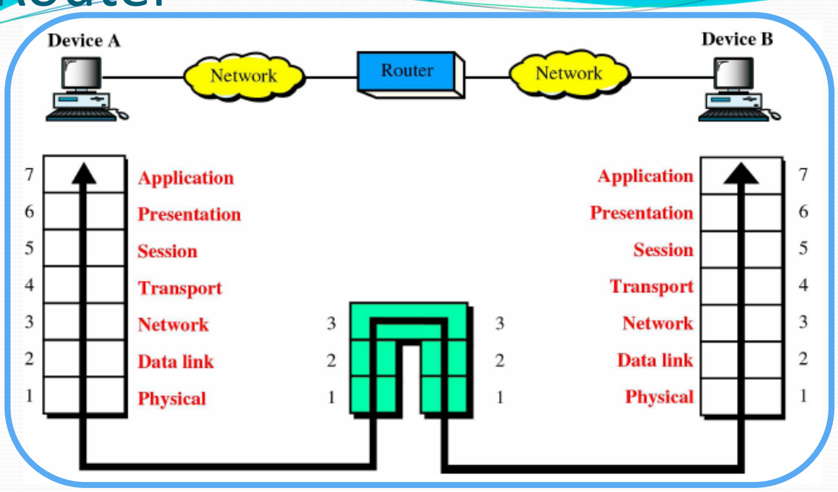
Example of internetworking



1-111

111

Router



Router operates as network layer (layer 3)
Can connect networks of dissimilar technologies

1-112

112

Router Advantages & Problems

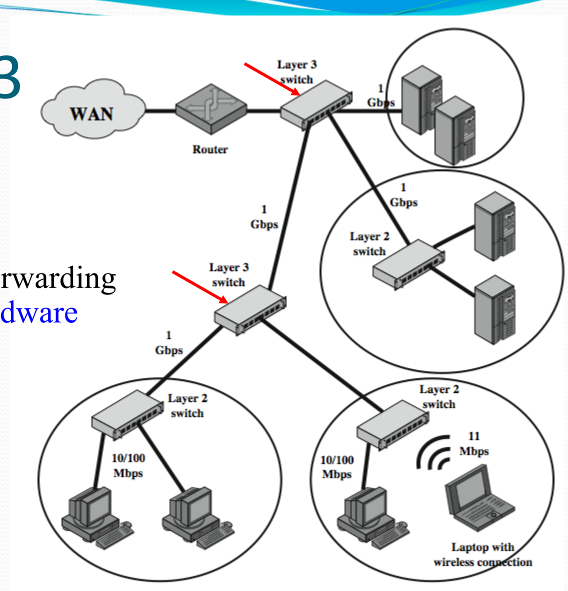
- Typically use subnetworks connected by routers
  - limits broadcasts to single subnet
  - supports multiple paths between subnets
- Routers do all IP-level processing in software
  - high-speed LANs and high-performance layer 2 switches pump millions of packets per second
  - software-based router only able to handle well under a million packets per second

1-113

113

Use of Layer 3 Switches

- Layer 3 switches
  - implement packet-forwarding logic of router in hardware
- Two categories
  - packet by packet
  - flow based



1-114

114

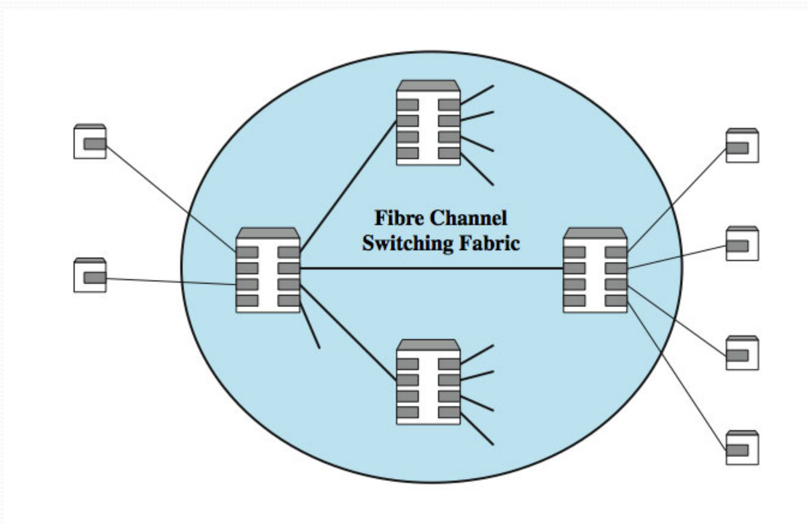
Packet by Packet or Flow Based

- Packet by packet
  - operates like a traditional router
  - order of magnitude increase in performance compared to software-based router
- Flow-based switch
  - enhances performance by identifying flows of IP packets with same source and destination
  - by observing ongoing traffic or using a special flow label in packet header (IPv6)
  - a predefined route is used for identified flows

1-115

115

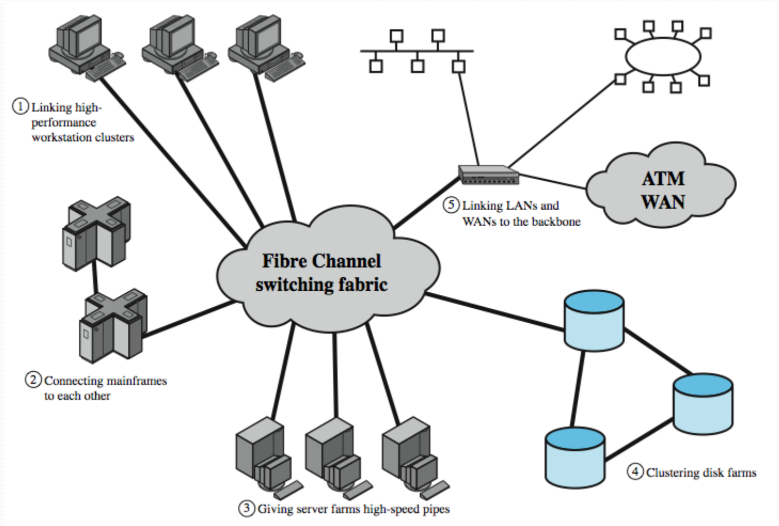
Fibre Channel Network



1-116

116

Fibre Channel Applications



1-117

117

Fibre Channel - Background

- I/O channel
  - direct point to point or multipoint comms link
  - hardware based, high speed, very short distances
- network connection
  - based on interconnected access points
  - software based protocol with flow control, error detection & recovery
  - for end systems connections

1-118

118

Fibre Channel

- combines best of both technologies
- channel oriented
  - data type qualifiers for routing frame payload
  - link level constructs associated with I/O ops
  - protocol interface specifications to support existing I/O architectures
- network oriented
  - full multiplexing between multiple destinations
  - peer to peer connectivity
  - internetworking to other connection technologies

1-119

119

Fibre Channel Requirements

- full duplex links with two fibers per link
- 100 Mbps to 800 Mbps on single line
- support distances up to 10 km
- small connectors
- high-capacity utilization, distance insensitivity
- greater connectivity than existing multidrop channels
- broad availability
- multiple cost/performance levels
- carry multiple existing interface command sets for existing channel and network protocols

1-120

120

Fibre Channel Fabric

- most general supported topology is fabric or switched topology
  - arbitrary topology with at least one switch to interconnect number of end systems
  - may also consist of switched network
- routing transparent to nodes
  - when data transmitted into fabric, edge switch uses destination port address to determine location
  - either deliver frame to node attached to same switch or transfers frame to adjacent switch

1-121

121

END

1-122

122