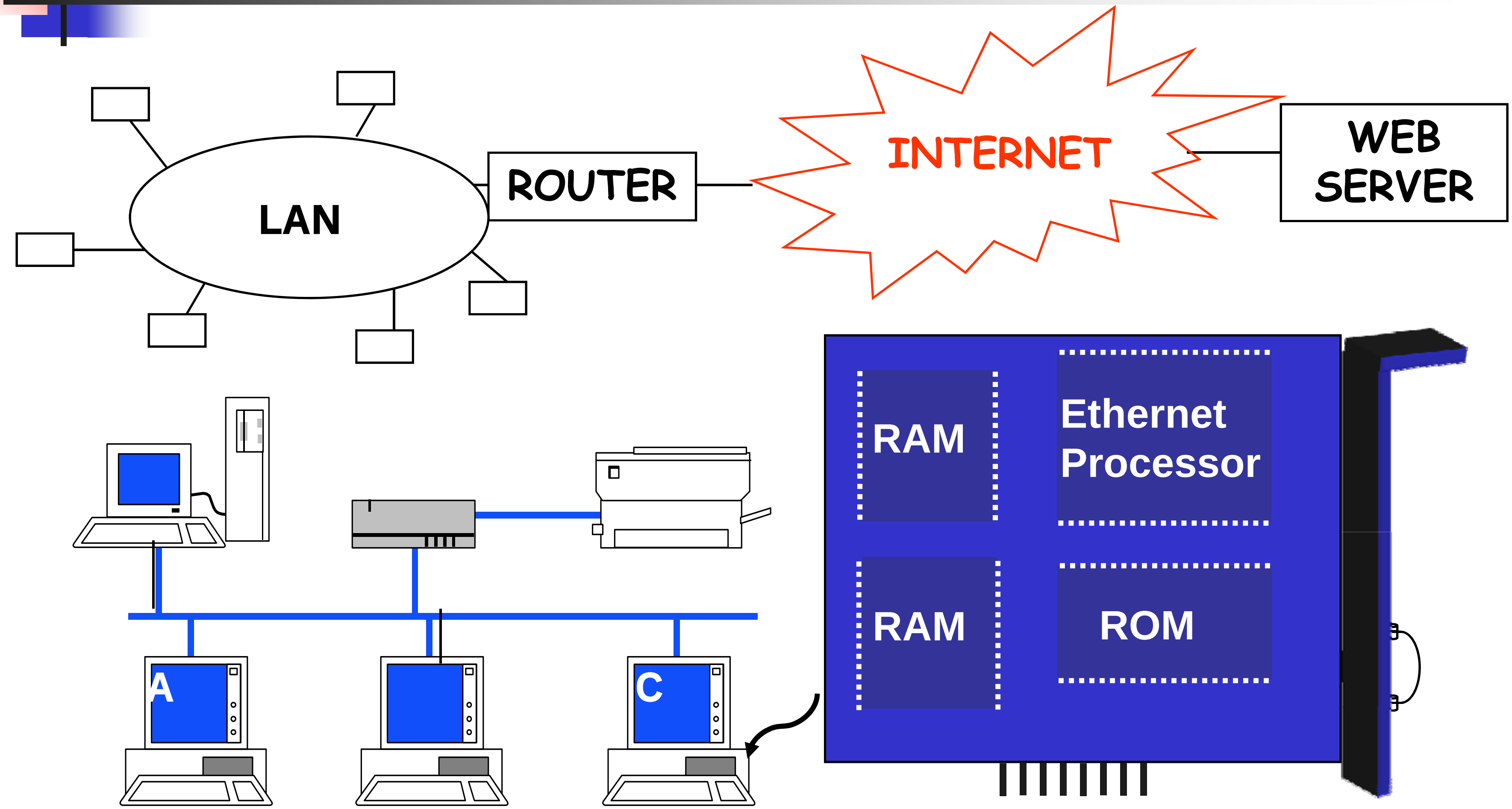
WLAN Technology:

LAN: a review
WLAN: applications & key parameters
IEEE 802.11 protocol architectures

LOCAL AREA NETWORKS



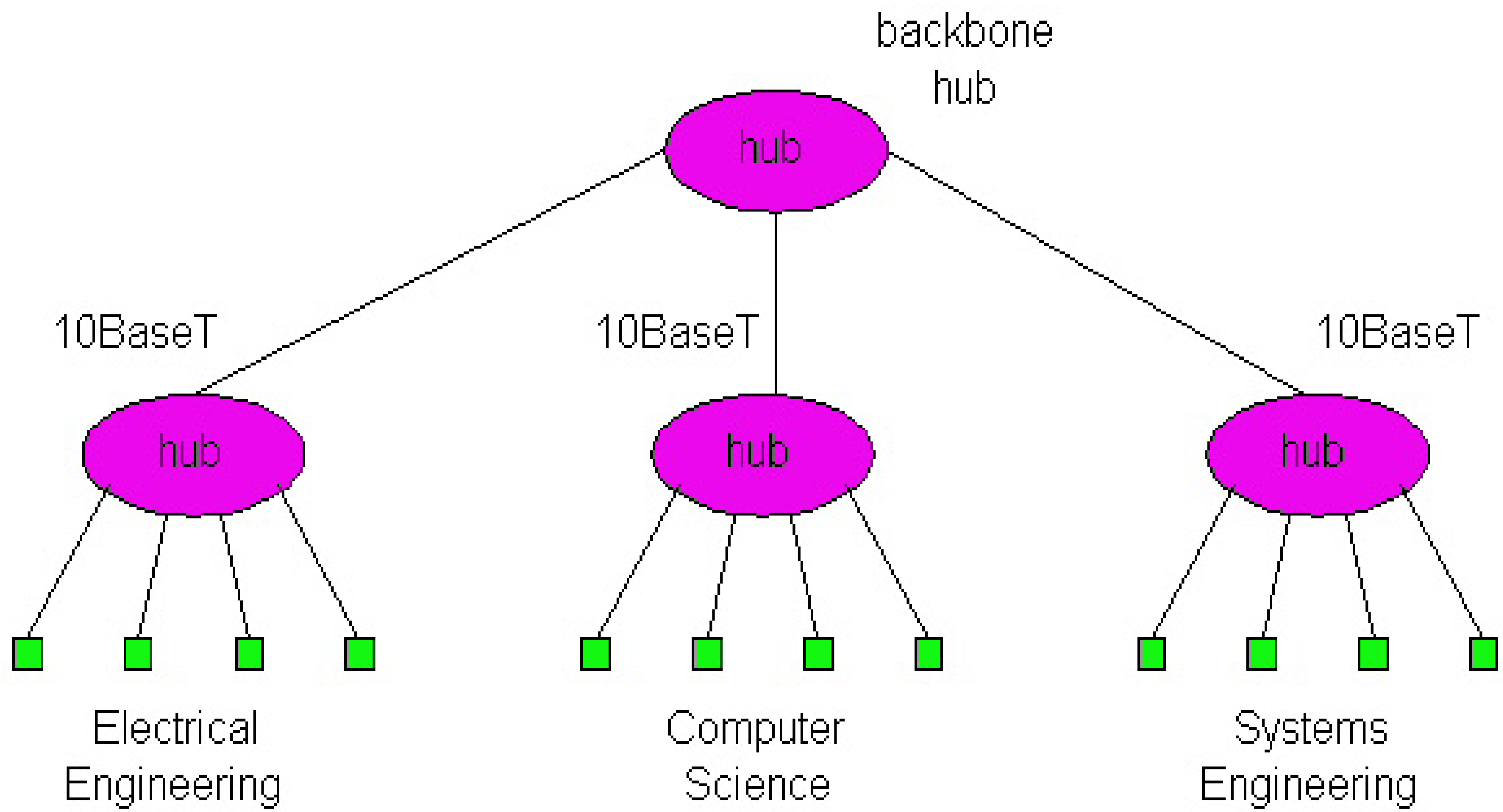
NIC with unique physical add in ROM

LAN INTERCONNECTION

WHY NOT JUST ONE BIG LAN?

- Limited amount of supportable traffic: on single LAN, all stations must share bandwidth
- limited length: 802.3 specifies maximum cable length
- large “collision domain” (can collide with many stations)
- limited number of stations: 802.5 have token passing delays at each station

LAN INTERCONNECTION WITH HUBS



HUBS

- Physical layer devices: essentially repeaters operating at bit levels: repeat received bits on one interface to all other interfaces
- Hubs can be arranged in a hierarchy (or multi-tier design), with backbone hub at its top
- Each connected LAN referred to as LAN segment
- Hubs do not isolate collision domains: node may collide with any node residing at any segment in LAN

Hub advantages:

  - Simple, inexpensive device
  - Multi-tier provides graceful degradation: portions of the LAN continue to operate if one hub malfunctions
  - Extends maximum distance between node pairs (100m per hub)

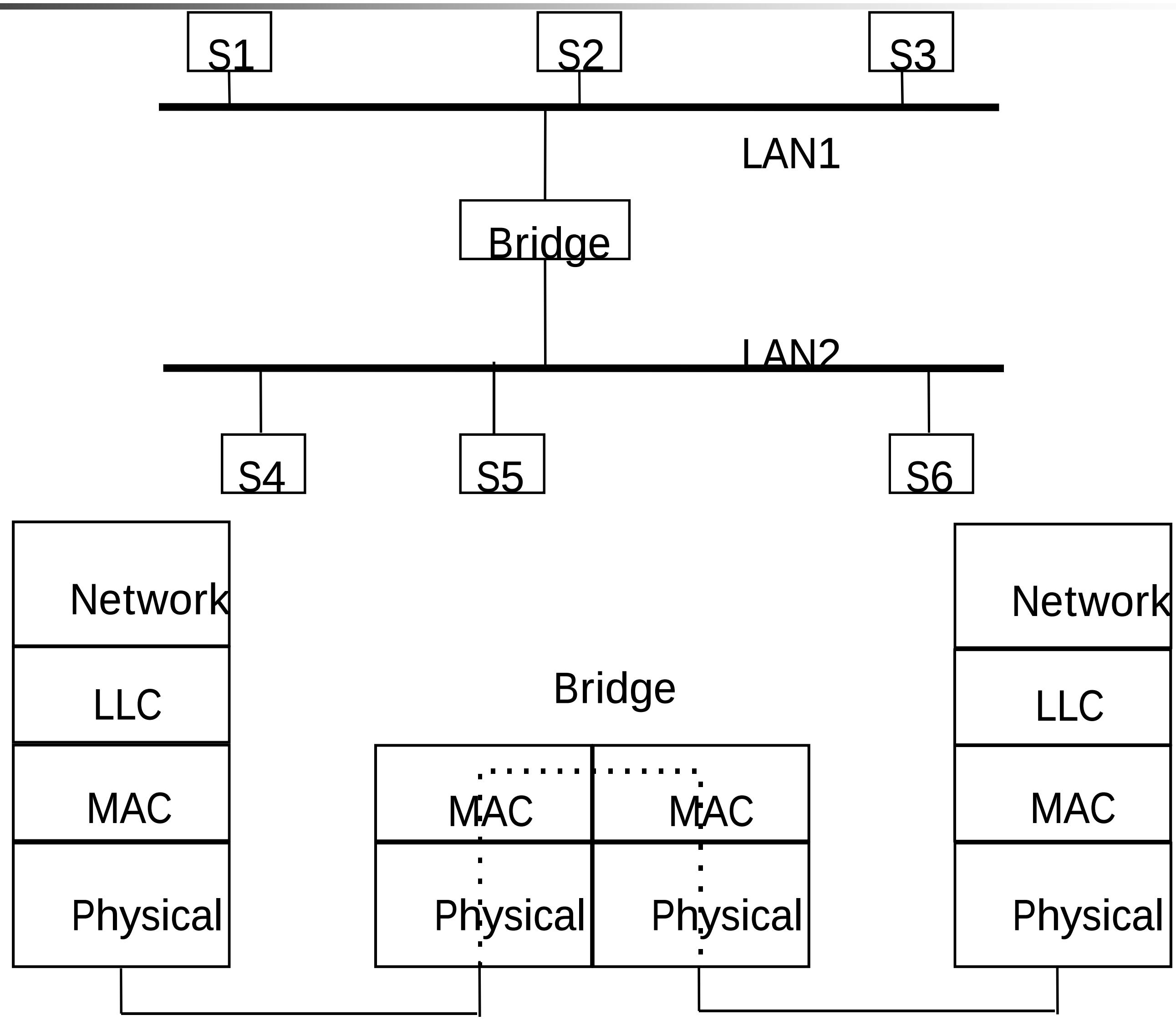
Hub limitations:

- Single collision domain results in no increase in max throughput
  - Multi-tier throughput same as single segment throughput
- Individual lan restrictions pose limits on number of nodes in same collision domain and on total allowed geographical coverage
- Cannot connect different ethernet types (e.G., 10baset AND 100baset)

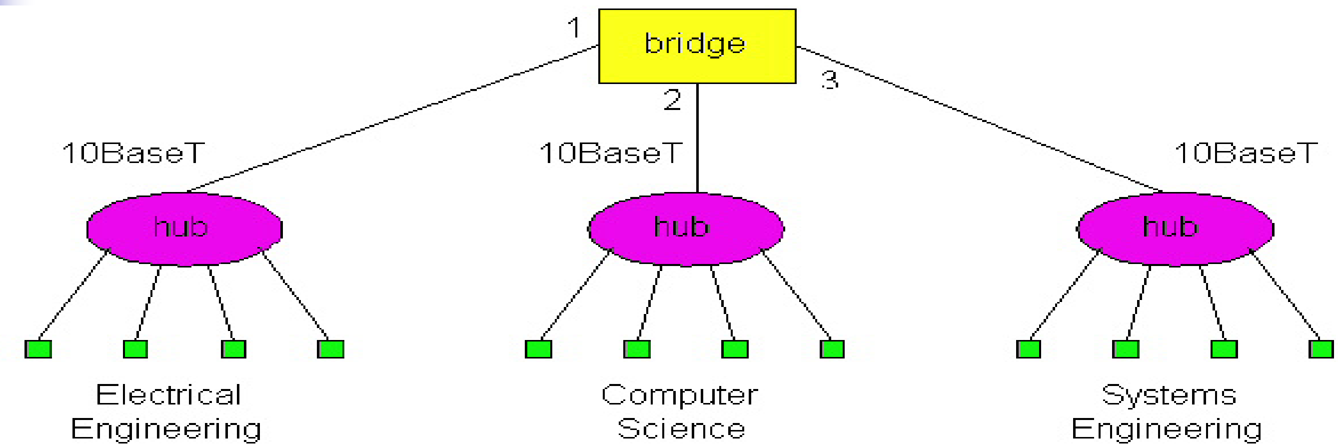
LAN BRIDGES

- Link Layer devices: operate on Ethernet frames, examining frame header and selectively forwarding frame based on its destination
- Bridge isolates collision domains since it buffers frames
- When frame is to be forwarded on segment, bridge uses CSMA/CD to access segment and transmit
- Bridge advantages:
  - Isolates collision domains resulting in higher total max throughput, and does not limit the number of nodes nor geographical coverage
  - Can connect different type Ethernet since it is a store and forward device
  - Transparent: no need for any change to hosts LAN adapters
- bridges filter packets
  - same-LAN -segment frames not forwarded onto other LAN segments
- forwarding:
  - how to know which LAN segment on which to forward frame?
  - looks like a routing problem (more shortly!)

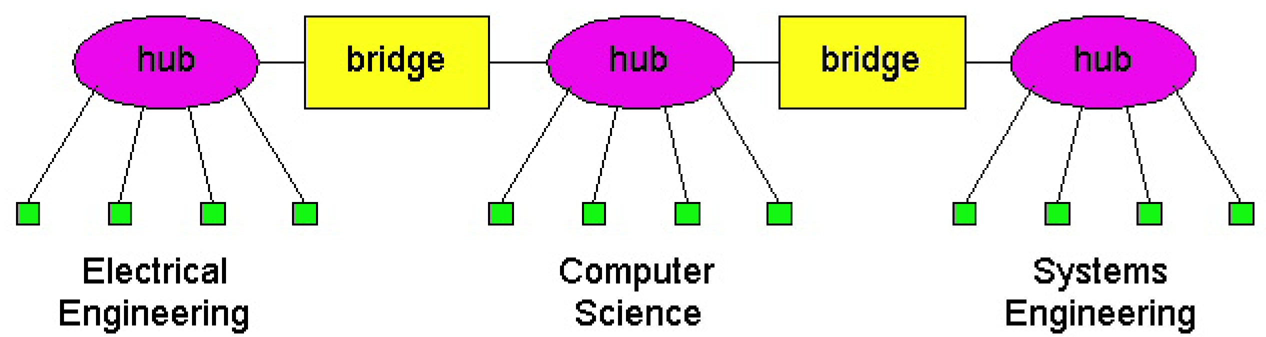
LAN INTERCONNECTION WITH BRIDGES



Backbone Bridge



Interconnection Without Backbone



- Not recommended for two reasons:
  - single point of failure at Computer Science hub
  - all traffic between EE and SE must path over CS segment

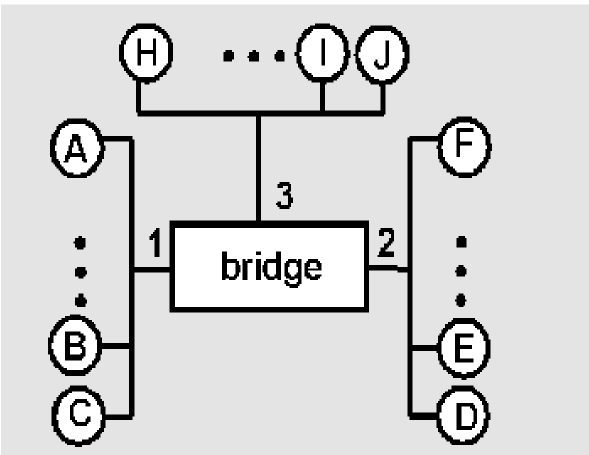
BRIDGE FILTERING

- bridges learn which hosts can be reached through which interfaces: maintain filtering tables
  - when frame received, bridge "learns" location of sender: incoming LAN segment
  - records sender location in filtering table
- filtering table entry:
  - (Node LAN Address, Bridge Interface, Time Stamp)
  - stale entries in Filtering Table dropped (TTL can be 60 minutes)
- filtering procedure:

```
if destination is on LAN on which frame was received
    then drop the frame
    else { lookup filtering table
        if entry found for destination
          then forward the frame on interface indicated;
          else flood;    /* forward on all but the interface on
                             which the frame arrived*/
      }
```

BRIDGE LEARNING: EXAMPLE

SUPPOSE C SENDS FRAME TO D AND D REPLIES BACK WITH FRAME TO C



address	port
A	1
B	1
E	2
H	3
J	3

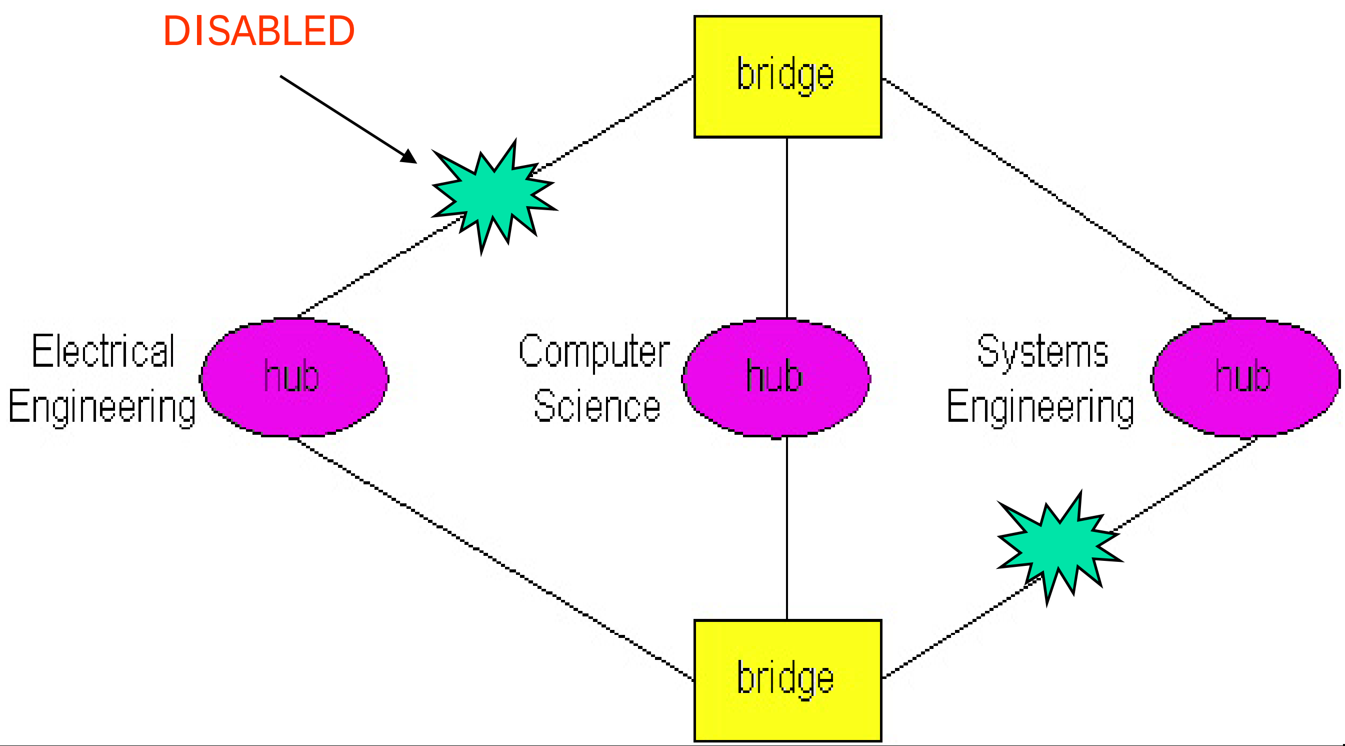
FORWARDING TABLE

- C sends frame, bridge has no info about D, so floods to both LANs
  - bridge notes that C is on port 1
  - frame ignored on upper LAN
  - frame received by D
- D generates reply to C, sends
  - bridge sees frame from D
  - bridge notes that D is on interface 2
  - bridge knows C on interface 1, so selectively forwards frame out via interface 1

(NETWORK CONTAINS NO LOOPS: ONLY 1 PATH BETWEEN ANY 2 LANs)

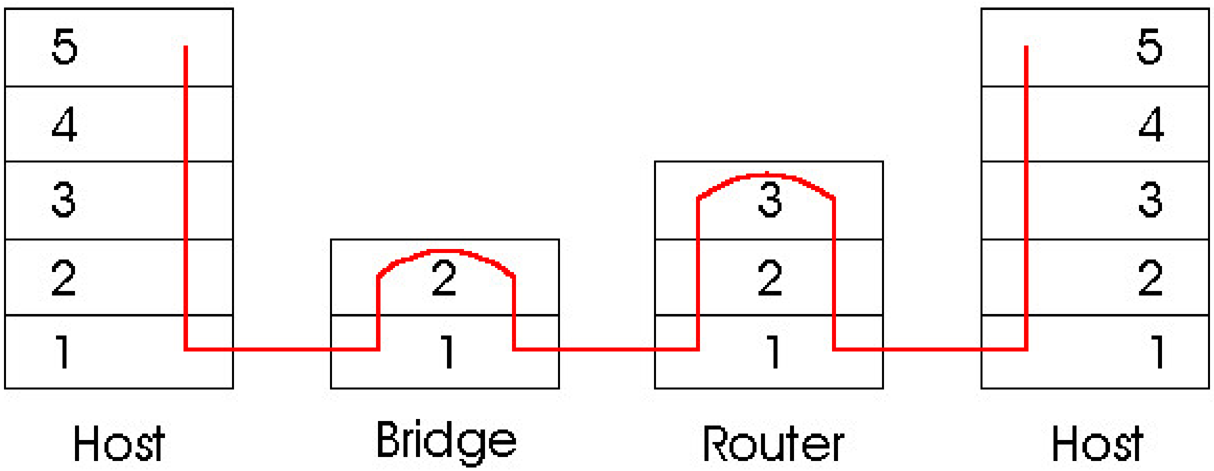
BRIDGES: SPANNING TREE

- for increased reliability, desirable to have redundant, alternate paths from source to destination
- with multiple simultaneous paths, cycles result - bridges may multiply and forward frame forever
- solution: organize bridges in a spanning tree (removing all possible loops) by disabling subset of interfaces



BRIDGES & ROUTERS

- both store-and-forward devices
  - routers: network layer devices (examine network layer headers)
  - bridges are Link Layer devices
- routers maintain routing tables, implement routing algorithms
- bridges maintain filtering tables, implement filtering, learning and spanning tree algorithms



BRIDGES DO WELL IN SMALL (FEW HUNDRED HOSTS) WHILE ROUTERS USED IN LARGE NETWORKS (THOUSANDS OF HOSTS)

BRIDGES: advantages & disadvantages

ADVANTAGES:

- Bridge operation is simpler requiring less processing bandwidth

DISADVANTAGES:

- Topologies are restricted with bridges: a spanning tree must be built to avoid cycles
- Bridges do not offer protection from broadcast storms (endless broadcasting by a host will be forwarded by a bridge)

ROUTERS: advantages & disadvantages

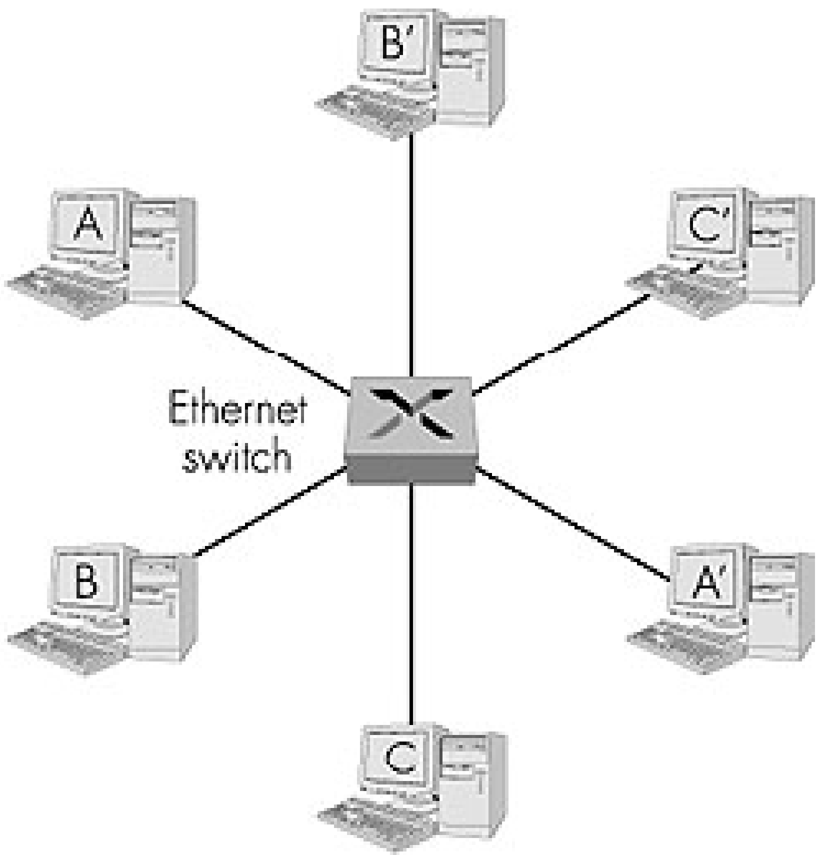
ADVANTAGES:

- arbitrary topologies can be supported, cycling is limited by TTL counters (and good routing protocols)
- provide firewall protection against broadcast storms

DISADVANTAGES:

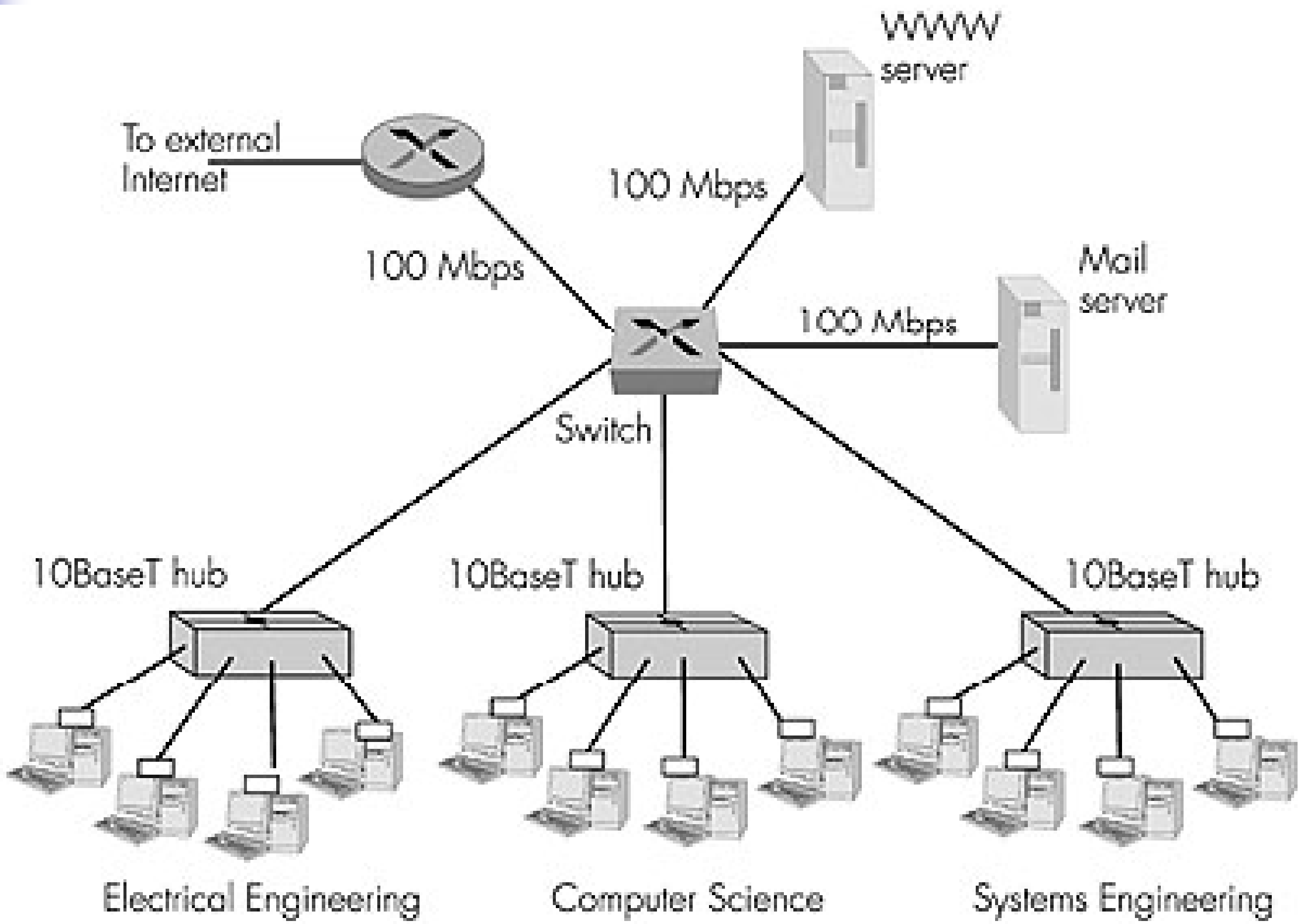
- require IP address configuration (not plug and play)
- require higher processing bandwidth

ETHERNET SWITCHES



- layer 2 (frame) forwarding, filtering using LAN addresses
- Switching: A-to-B and A'-to-B' simultaneously, no collisions
- large number of interfaces
- often: individual hosts, star-connected into switch
  - Ethernet, but no collisions!
- cut-through switching: frame forwarded from input to output port without awaiting for assembly of entire frame
  - slight reduction in latency
- combinations of shared/dedicated, 10/100/1000 Mbps interfaces

SWITCH INTERCONNECTION



WLAN Applications

LAN Extension: linked into a wired LAN on same premises

- Wired LAN
  - Backbone
  - Support servers and stationary workstations
- Wireless LAN
  - Stations in large open areas
  - Manufacturing plants, stock exchange trading floors, and warehouses

Cross-Building Interconnect: Wired or wireless LANs

- Point-to-point wireless link is used
- Devices connected are typically bridges or routers

Nomadic Access: to hub from laptop computer or notepad computer:

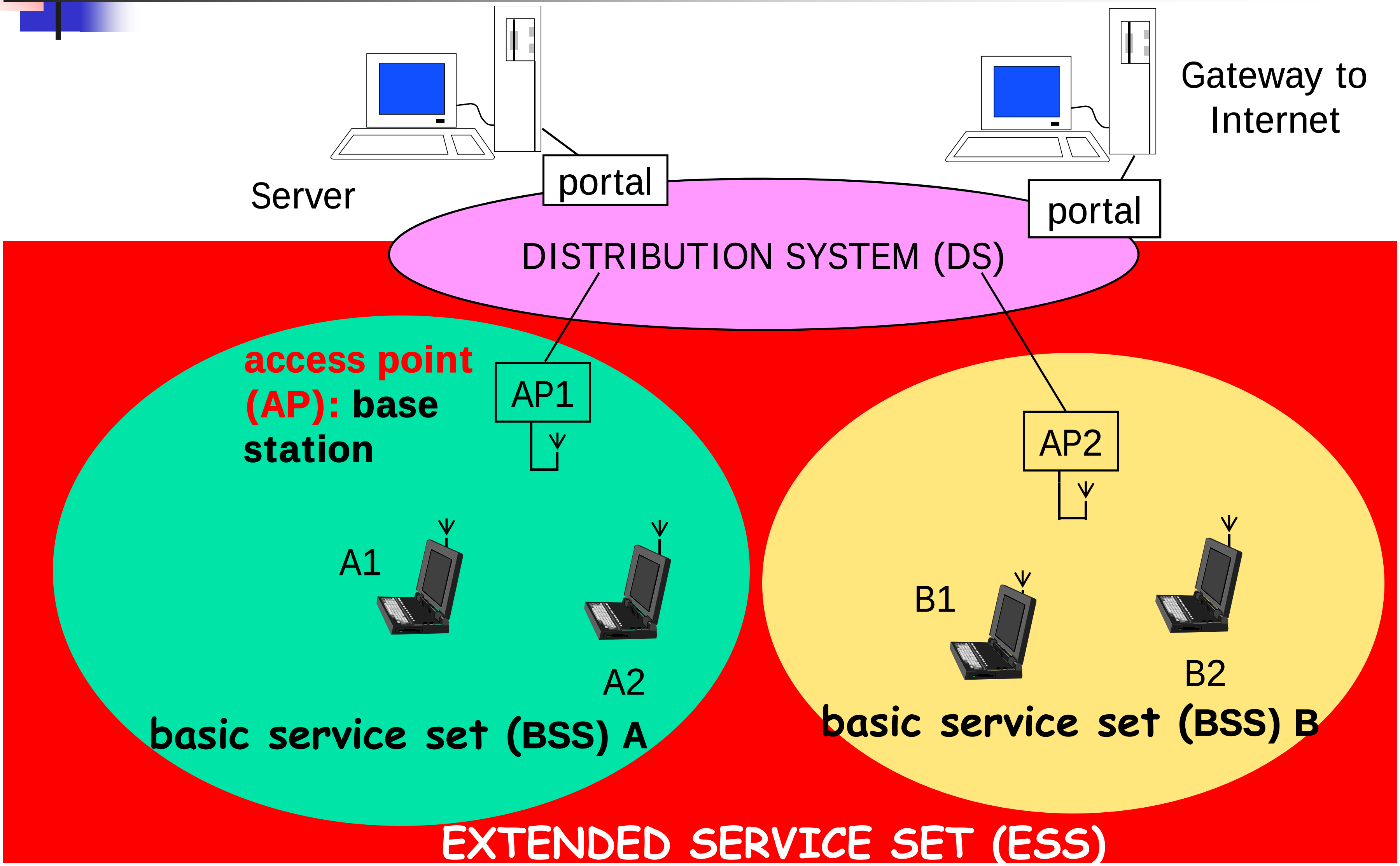
- Transfer data from portable computer to office server
- Extended environment such as campus

Ad Hoc Networking: Temporary peer-to-peer network set up to meet immediate need, e.g., meeting

Key parameters:

- Throughput
- Number of nodes
- Connection to backbone LAN
- Service area
- Battery power consumption
- Transmission robustness and security
- Collocated network operation
- License-free operation
- Handoff/roaming
- Dynamic configuration

WLAN: BSS, ESS & INFRASTRUCTURE NETWORK



WLAN SYSTEM: COMPONENTS

Distribution system (DS):
- Distribution service:from station in one BSS to station in another BSS
- Integration service: between station on IEEE 802.11 LAN and station on integrated IEEE 802.x LAN

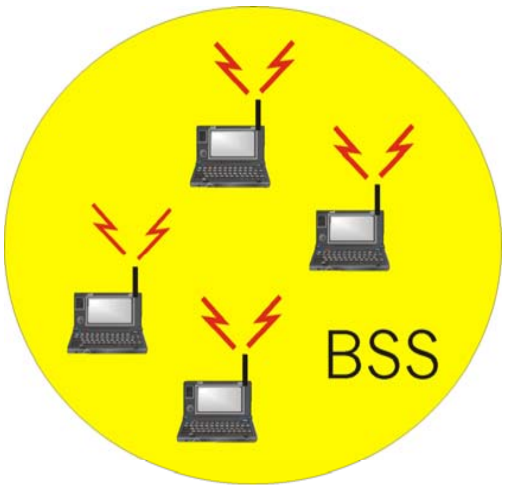
Access point (AP)

Basic service set (BSS)
  - Stations competing for access to shared wireless medium
  - Isolated or connected to backbone DS through AP

Extended service set (ESS) :Two or more basic service sets interconnected by DS

Transition types:
- No transition: Stationary or moves only within BSS
- BSS transition: Station moving from one BSS to another BSS in same ESS
- ESS transition: Station moving from BSS in one ESS to BSS within another ESS

AD HOC NETWORKING

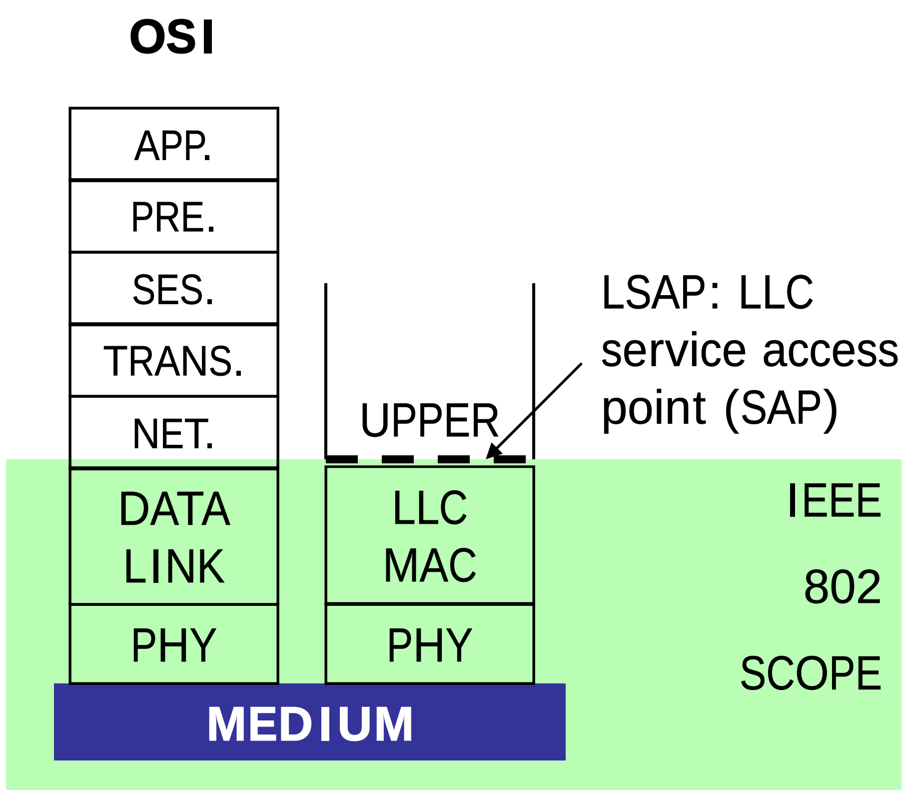


- Temporary peer-to-peer network set up to meet immediate need
- Applications:
  - "laptop" meeting in conference room, car
  - interconnection of "personal" devices
  - battlefield
- Ad hoc network: IEEE 802.11 stations can dynamically form network without AP
- IETF MANET (Mobile Ad hoc Networks) working group

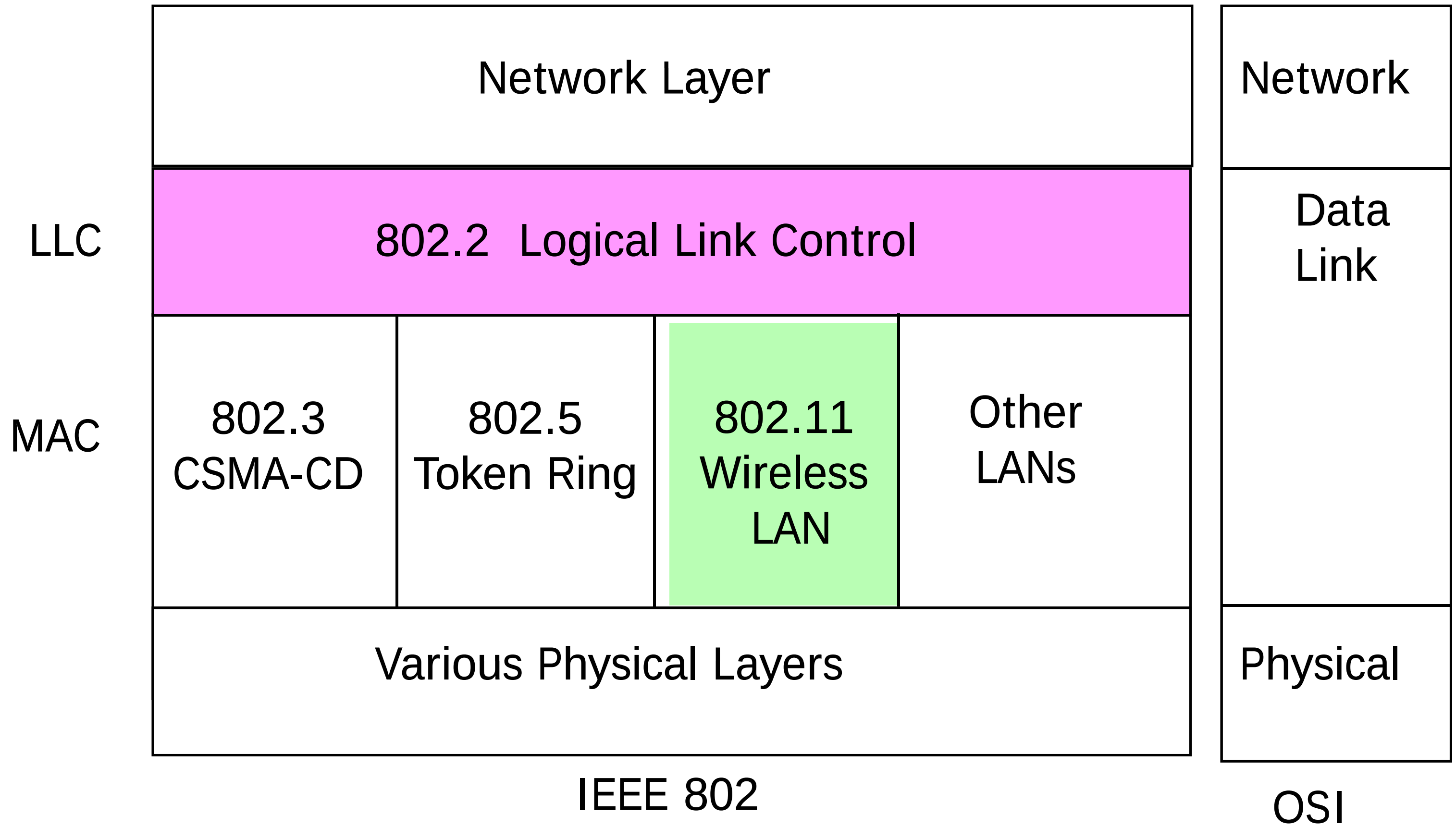
Services

- **Association:** Establishes initial association between station and AP
- **Reassociation:** Enables transfer of association from one AP to another, allowing station to move from one BSS to another
- **Disassociation:** Association termination notice from station or AP
- **Authentication:** Establishes identity of stations to each other
- **Deathentication:** Invoked when existing authentication is terminated
- **Privacy:** Prevents message contents from being read by unintended recipient

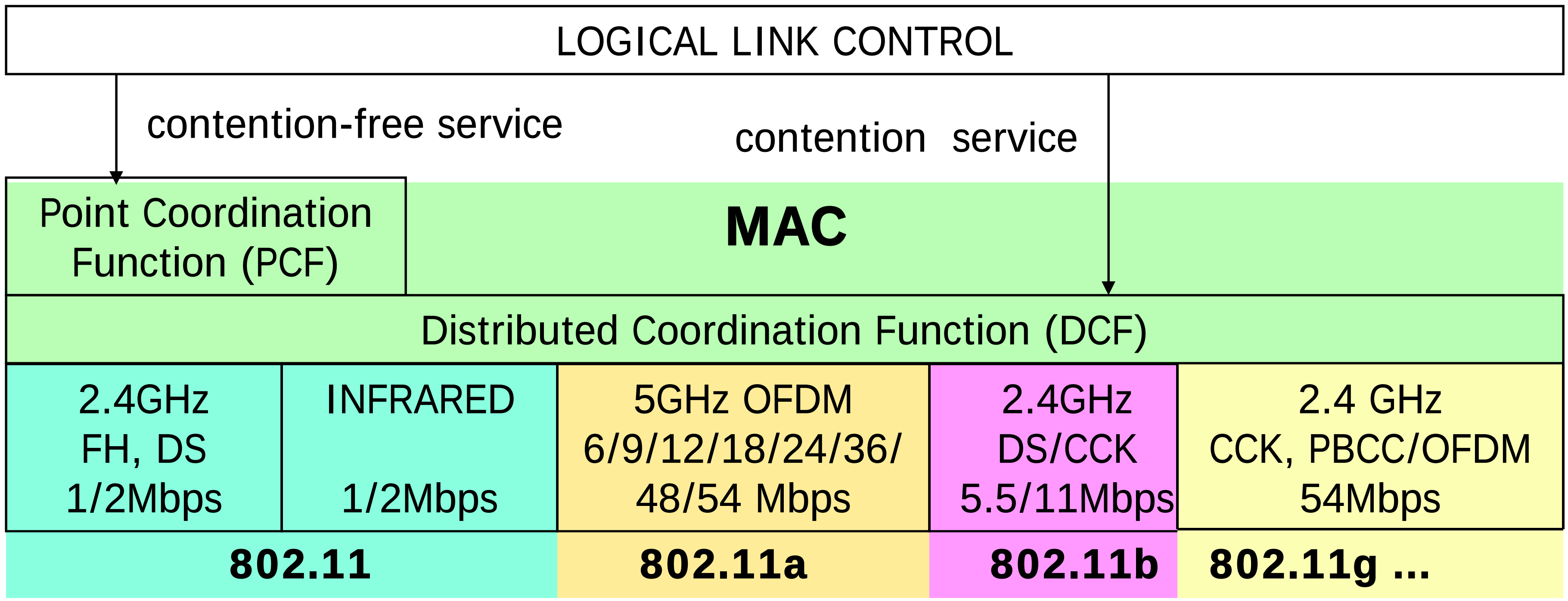
OSI AND IEEE 802 LAYERS



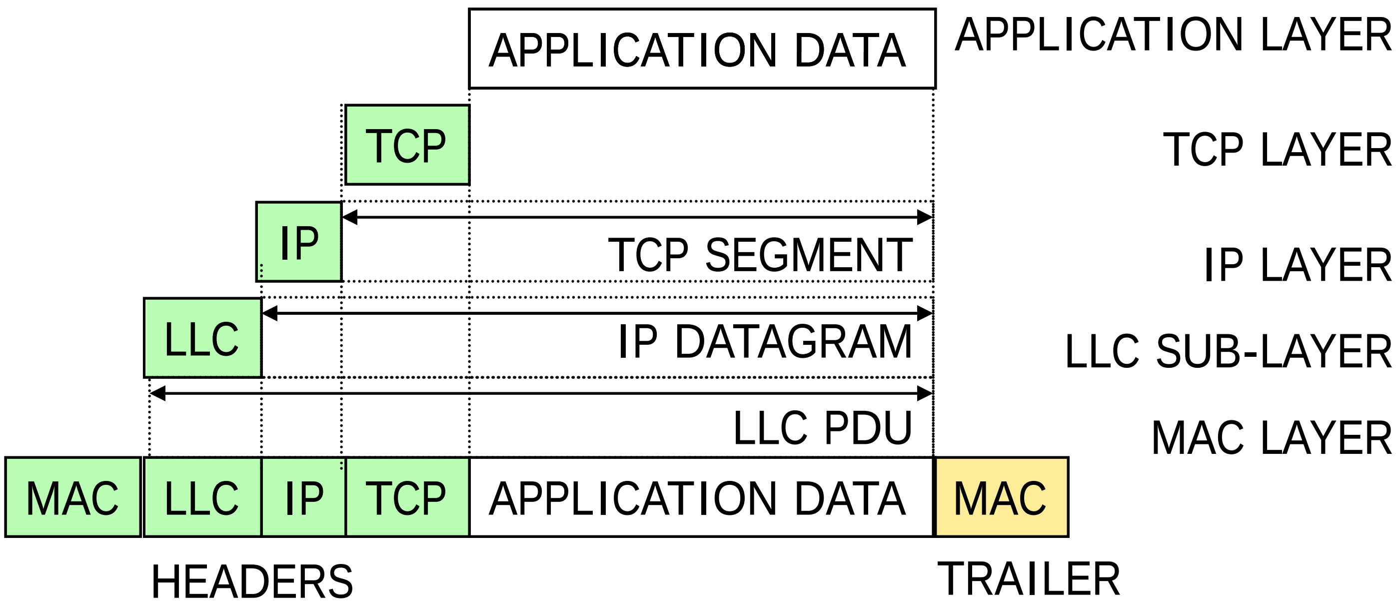
IEEE 802 LAN STANDARDS



802.11 ARCHITECTURE

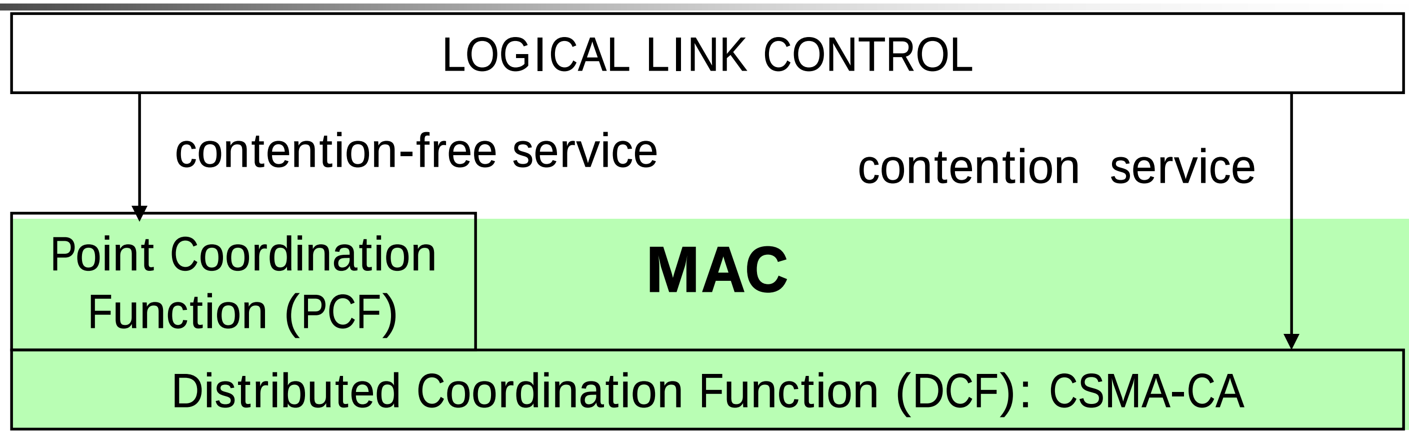


MAC FRAME



APPLICATION DATA
APPLICATION LAYER
TCP
TCP LAYER
IP
TCP SEGMENT
IP LAYER
LLC
IP DATAGRAM
LLC SUB-LAYER
LLC PDU
MAC LAYER
MAC
LLC
IP
TCP
APPLICATION DATA
MAC
HEADERS
TRAILER

MAC & LLC SUB-LAYERS



LOGICAL LINK CONTROL (LLC):

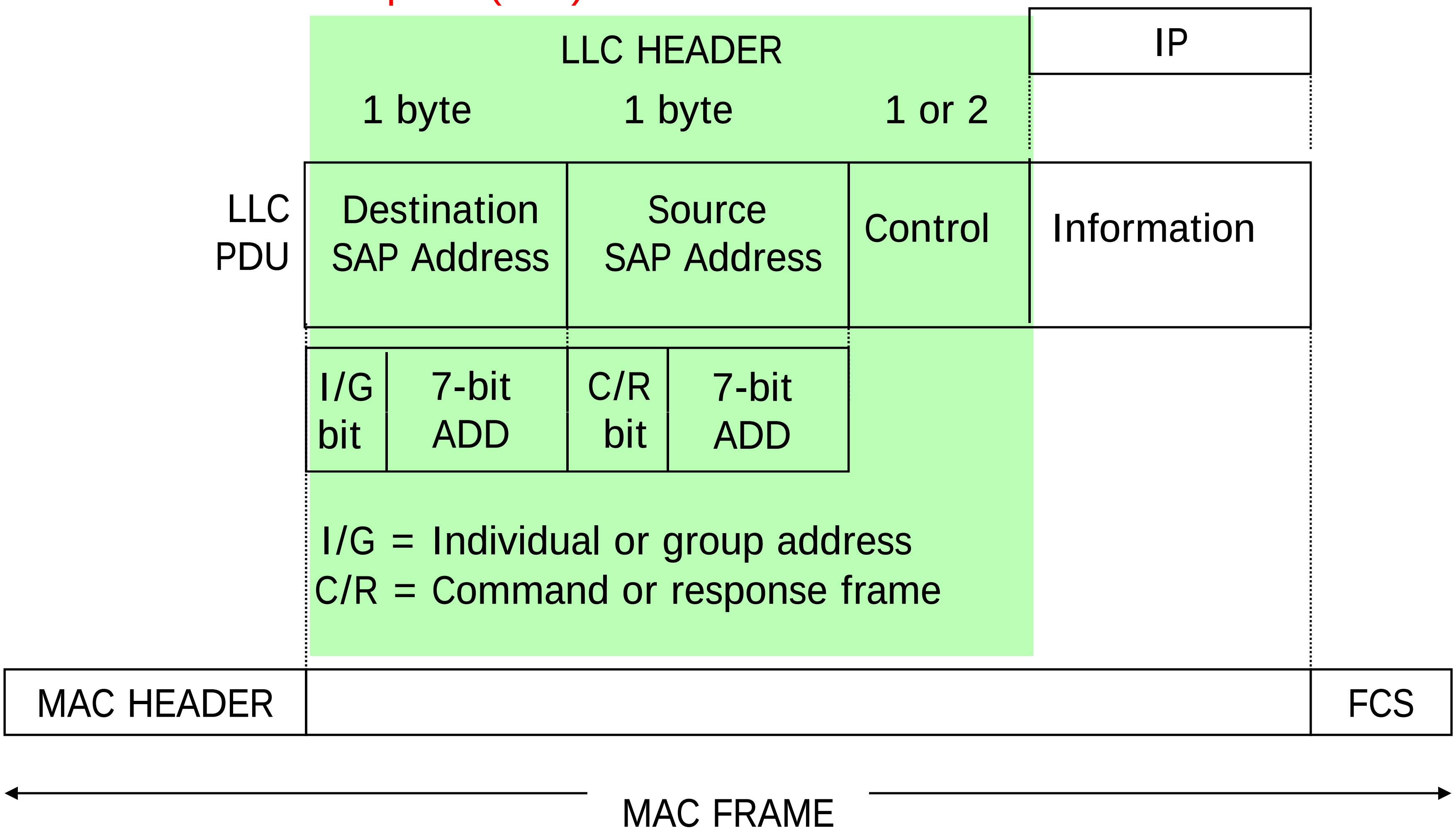
- Provide an interface to higher layers and perform flow and error control
- LLC permits multiplexing by the use of LLC service access points (LSAPs)
- For the same LLC, several MAC options may be provided

MEDIUM ACCESS CONTROL (MAC):

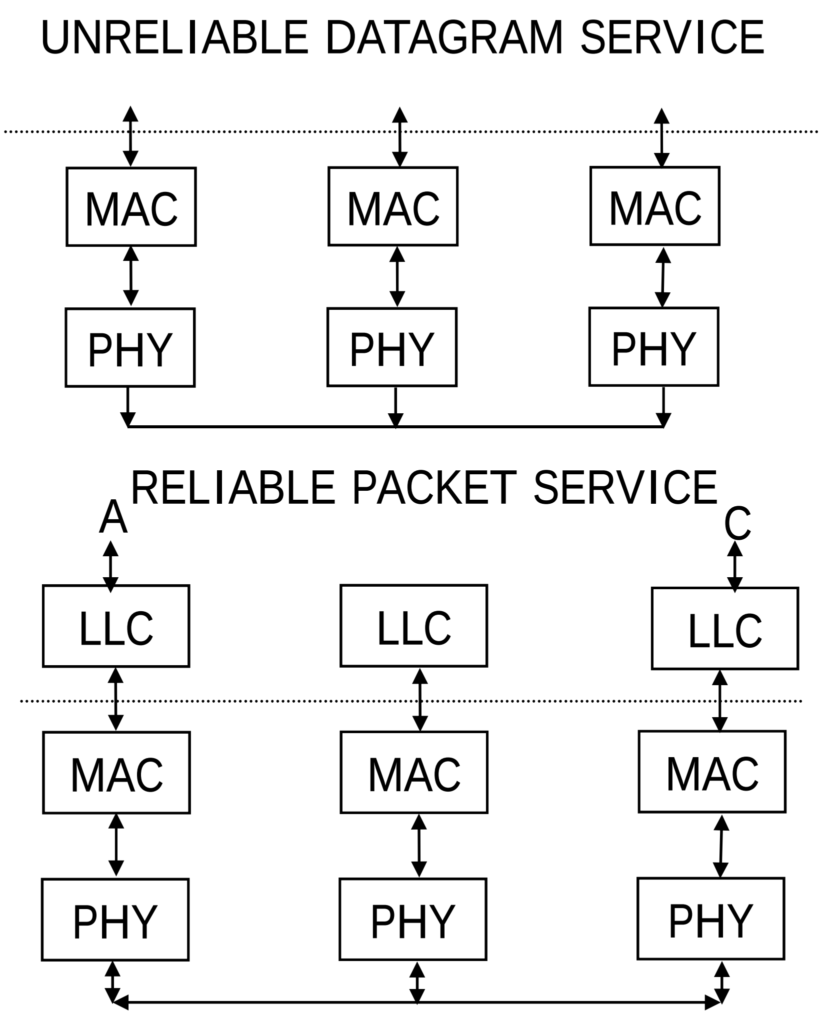
- On transmission, assemble data into a frame with address and error detection fields
- On reception, disassemble frame and perform address recognition and error detection
- Govern access to the LAN transmission medium

MAC FRAME & LLC PDU

Single MAC (PHY) add supports different logical connections, each with its service access point (SAP)



LLC FUNCTIONS:



Interaction between MAC entities is not between pairs of peers, but rather all entities must monitor all frames that are transmitted onto the shared medium

LLC can enhance the service offered by the MAC layer to provide 3 services of HDLC:

TYPE 1: UNACK. CONNECTIONLESS SERVICE (UNNUMBERED FRAMES):

- No flow- and error-control mechanisms
- Data delivery not guaranteed,

TYPE 2: RELIABLE CONNECTION-ORIENTED (ASYNC BALANCED MODE OF HDLC):

- Logical connection set up between two users
- Flow- and error-control provided

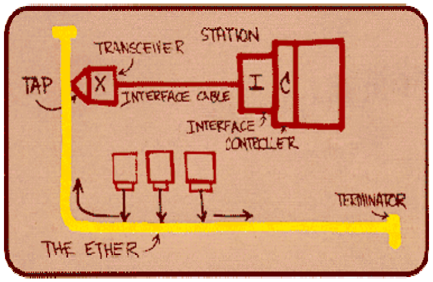
TYPE 3: ACK CONNECTIONLESS SERVICE:

- Cross between previous two
- Datagrams acknowledged
- No prior logical setup

ETHERNET FRAME STRUCTURES (wireline LAN)

developed in the early 1970's by Xerox (and DEC, Intel), standardized as 802.3 in 1985

Metcalfe's Ethernet sketch



802.3 LLC FRAME WITHOUT SNAP

SAP add $\neq AA_{16}$, e.g. 06:IP, 98:ARP, E0: Novell, F0: Net BIOS, 7E:x.25

LLC PDU

D	S	C	43 to 1497 data bytes
1	1	1	

802.3 WITH SNAP

ORG	TYPE
3	2

SNAP PDU

SNAP Header	Information

⇩

LLC PDU

AA	AA	03	
1	1	1	

MAC HEADER

X: **LENGTH** (IEEE 802.3) UP TO 1500 ($05DC_{16}$),
X: **TYPE** (DIX): 0800_{16}:IP, 0850_{16}:X25, 0806_{16}:ARP

7	1	2 or 6	2 or 6	2	← 46 to 1500 →		4
Preamble	SFD	Dest. Add.	S. Add.	X	Information	Pad	FCS

SFD: Start frame Delimiter:10101011

Sync: 7 bytes, each: 10101010

FCS: CCITT 32-bit CRC covers all except preamble+SFD

← 802.3 MAC Ethernet Frame →

- Destination address is either single address or group address (broadcast = 111...111)
- Addresses are defined on local or universal basis
- 2^{46} possible global addresses

0	Single address
1	Group address

0	Local add.
1	Global add.

Ethernet: CSMA/CD

Procedure:

A: sense channel, **if** idle

then { transmit and monitor the channel;

If detect another transmission

then { abort and send jam signal; update # collisions; delay as required by exponential backoff algorithm; goto A}

else {done with the frame; set collisions to zero}

}

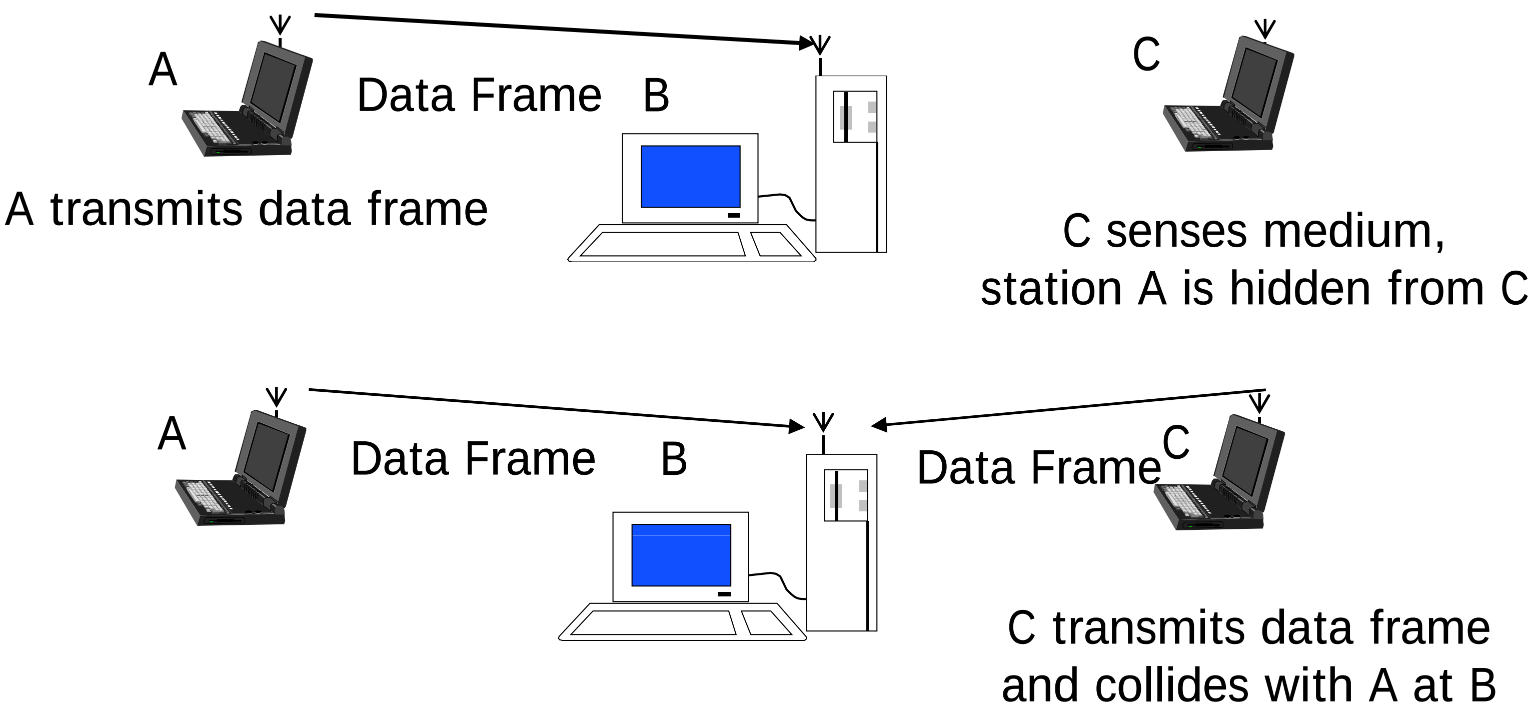
else {wait until ongoing transmission is over and goto A}

Jam Signal: make sure all other transmitters are aware of collision; 48 bits;

Exponential Backoff: adapt retransmission attempts to estimated current load (heavy load: random wait will be longer)

- first collision: choose K from {0,1}; delay is K x 512 bit transmission times
- after second collision: choose K from {0,1,2,3}...
- after ten or more collisions, choose K from {0,1,2,3,4,...,1023}

WLAN:HIDDEN-STATION PROBLEM



MAC FUNCTIONS

Reliable data delivery:

- More efficient to deal with errors at the MAC level than higher layer (such as TCP)
- Frame exchange protocol
  - Source station transmits data
  - Destination responds with acknowledgment (ACK)
  - If source doesn't receive ACK, it retransmits frame
- Four frame exchange
  - Source issues request to send (RTS)
  - Destination responds with clear to send (CTS)
  - Source transmits data
  - Destination responds with ACK

Access control

Security

802.11 MAC FRAME STRUCTURE

- **Frame Control** – frame type, control information
- **Duration/connection ID** – channel allocation time
- **Addresses** – context dependant, types include source and destination
- **Sequence Control** – numbering and reassembly
- **Frame Body** – MSDU or fragment of MSDU
- **FCS: Frame Check Sequence** – 32-bit CRC

MAC Header (bytes)

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

2bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	MF	R	PM	MD	WEP	O

Frame Control (FC)

2bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	MF	RT	PM	MD	WEP	O

Protocol version

Type – control, management, or data

Subtype – identifies function of frame:

- Power save – poll (PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment
- Contention-free (CF)-end
- CF-end + CF-ack

To DS =1 if destined for DS

From DS =1 if leaving DS

MF: More fragments =1 if fragments follow

RT: Retry =1 if retransmission of previous frame

PM: Power management =1 if transmitting station is in sleep mode

MD: More data =1, Indicates that station has more data to send

WEP wired equivalent privacy =1 if info of frame body is processed by the crypto. algorithm

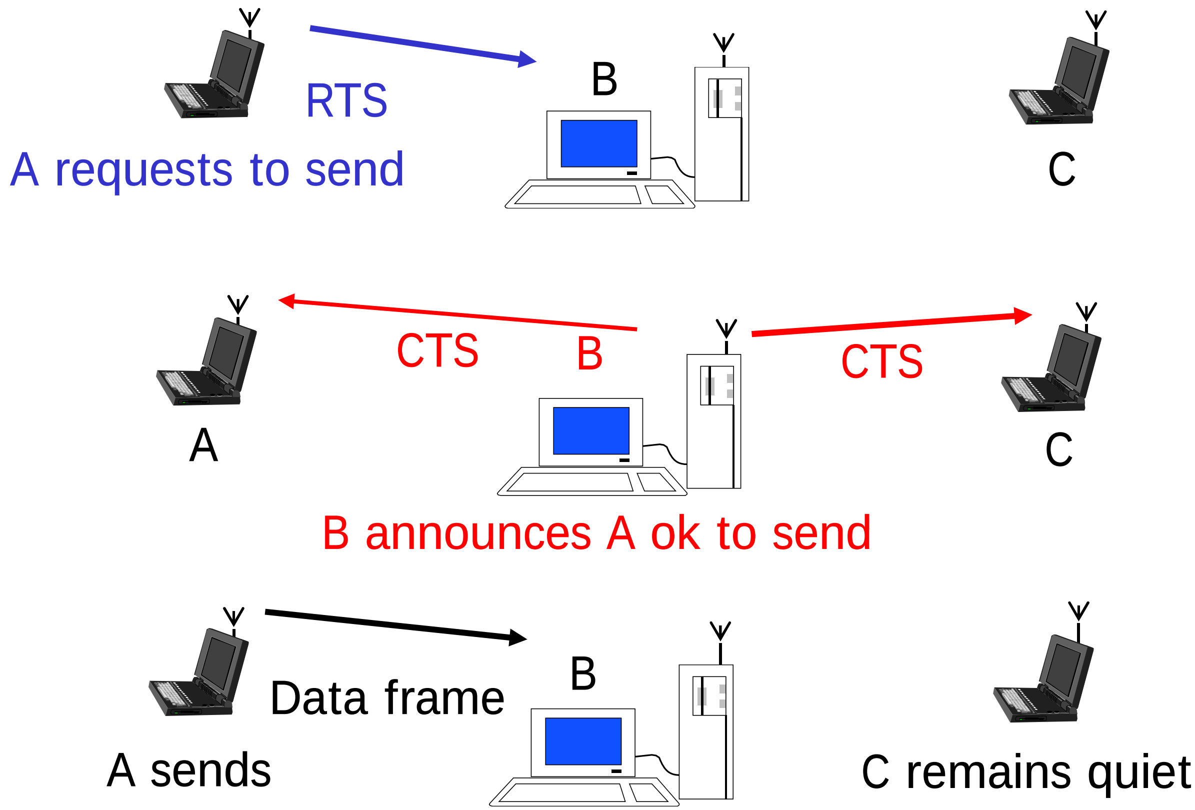
O: Order =1 if any data frame is sent using the Strictly Ordered service

MAC FRAME: TO DS & FROM DS FIELDS

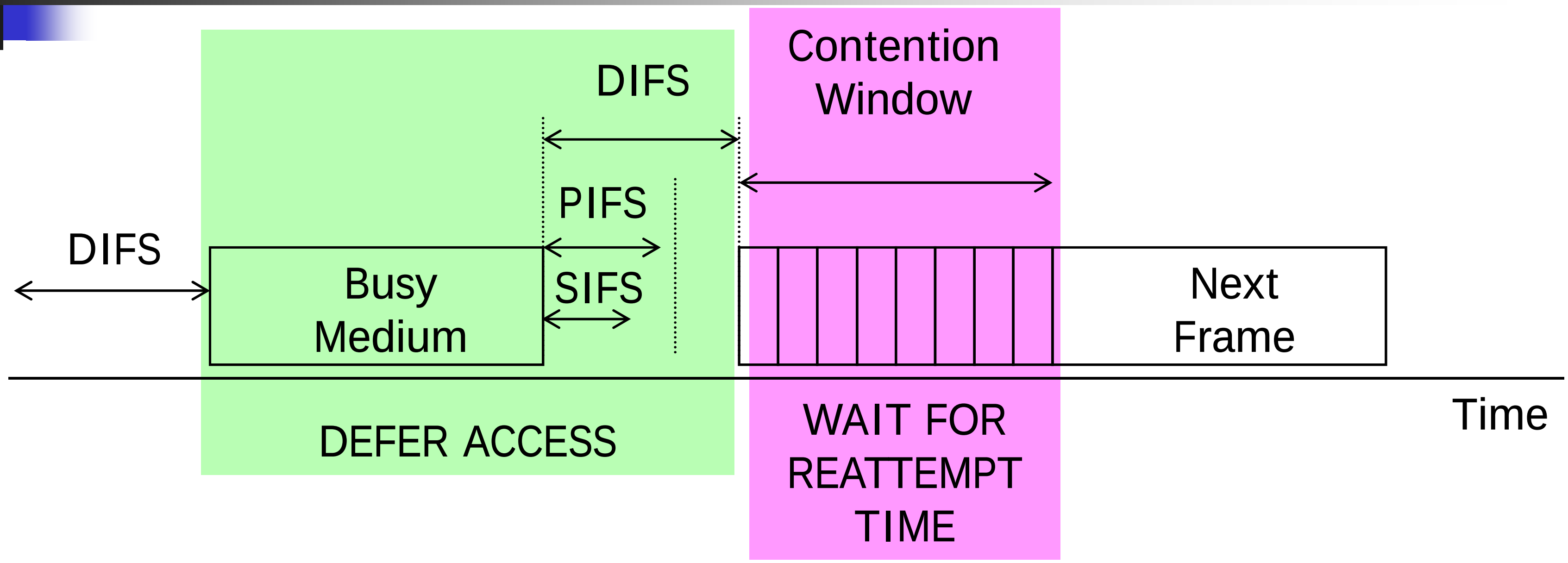
To DS	From DS	Address 1	Address 2	Address 3	Address 4	Meaning
0	0	Destination Address	Source Address	BSSID	N/A	Data frame from station to station within a BSS
0	1	Destination Address	BSSID	Source Address	N/A	Data frame exiting the DS
1	0	BSSID	Source Address	Destination Address	N/A	Data frame destined for the DS
1	1	Receiver Address	Transmitter Address	Destination Address	Source Address	WDS frame being distributed from AP to AP

DS: DISTRIBUTION SYSTEM
AP: ACCESS POINT

CARRIER SENSE MULTIACCESS with COLLISION AVOIDANCE (CSMA-CA)



Interframe Space (IFS):



IFS: INTERFRAME SPACE: QUIET INTERVAL AFTER A Tx COMPLETED

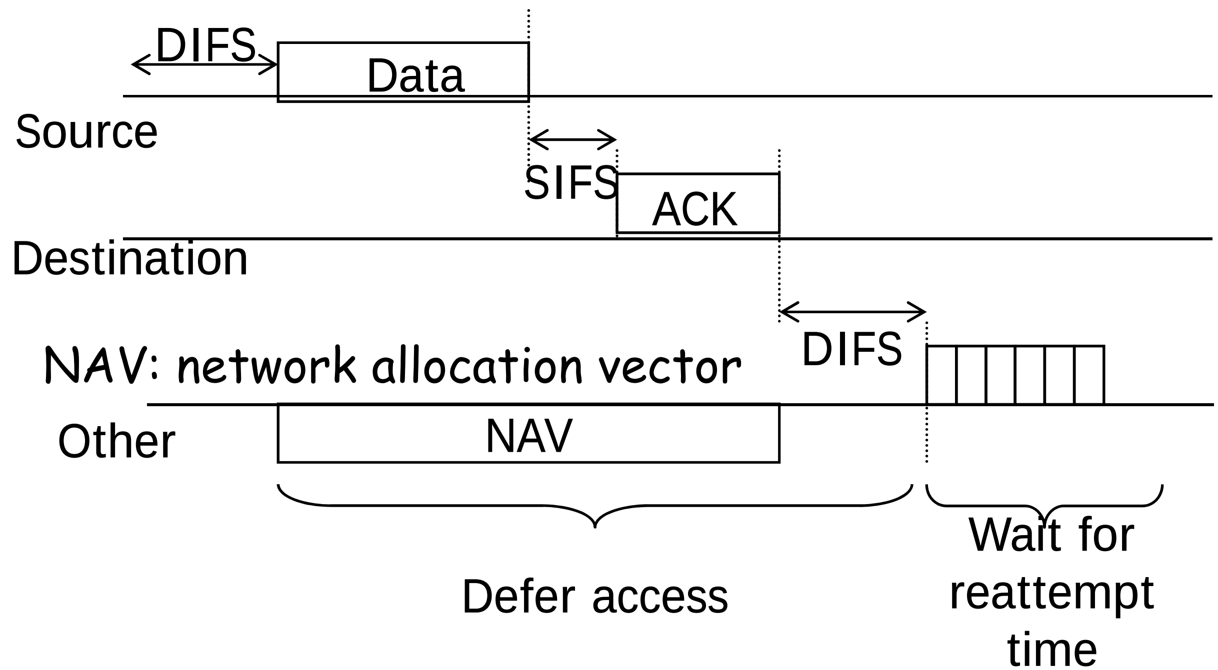
Short IFS (SIFS) shortest IFS for hi-priority frames: ACK, CTS, Poll response

Point coordination function (PCF) IFS (PIFS): mid-size, used by centralized controller in PCF scheme when using polls to gain priority access (takes precedence over normal contention traffic) for contention-free service

Distributed coordination function (DCF) IFS (DIFS): longest IFS, used by DCF to Tx ordinary asynchronous data & MGT for contention service

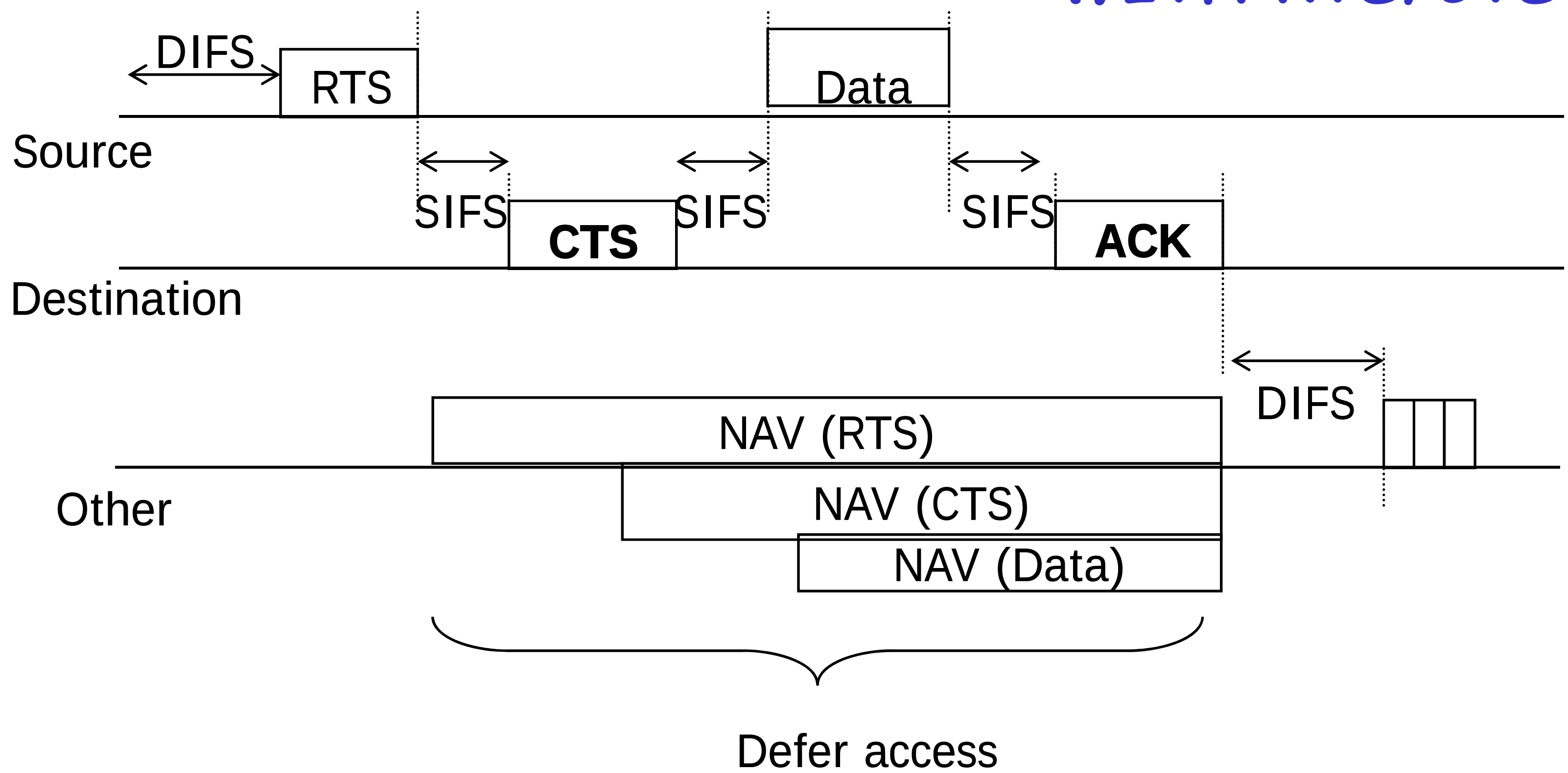
Frame exchange: Tx OF MPDU

WITHOUT RTS/CTS



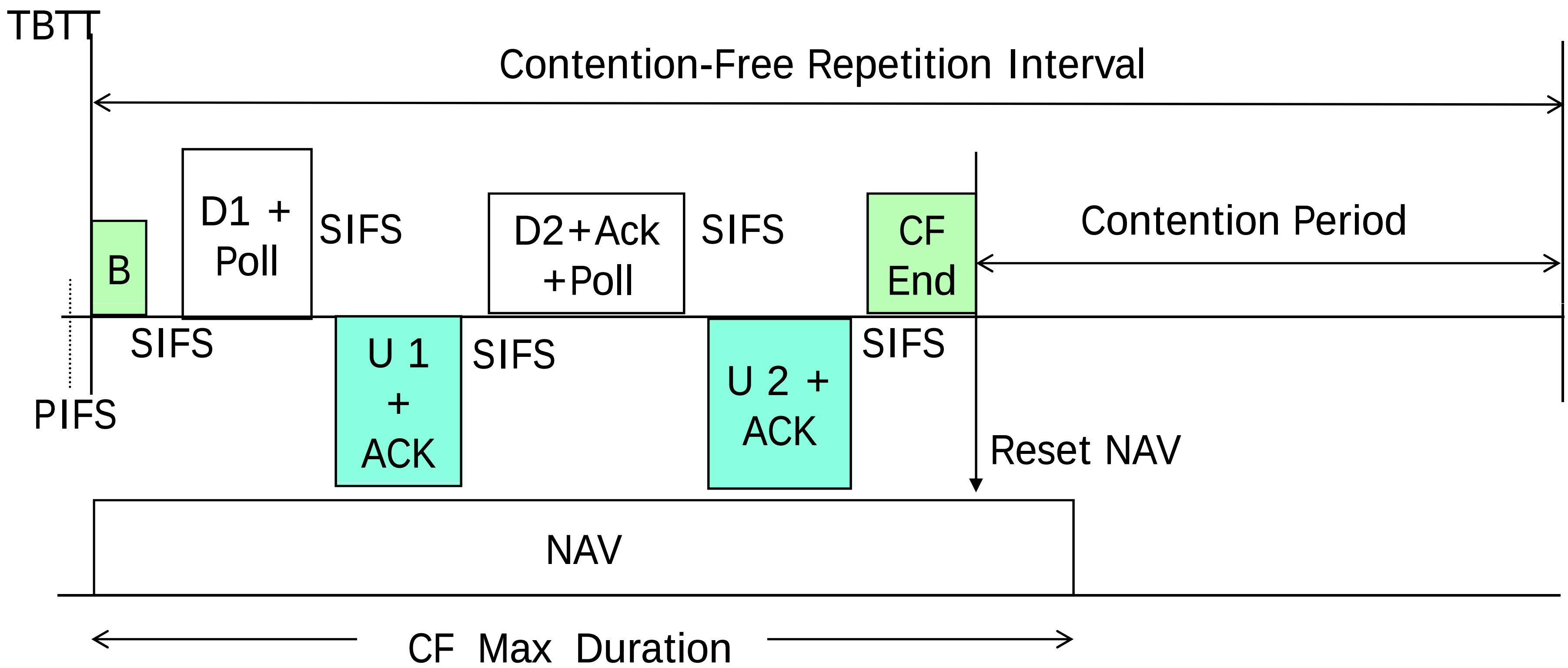
- Source station transmits data
- Destination responds with acknowledgment (ACK)
- If source doesn't receive ACK, it retransmits frame

Frame exchange: Tx OF MPDU WITH RTS/CTS



NAV: network allocation vector indicates the time amount that must elapse until the current Tx is complete and the channel can be sample again for idle status

POINT COORDINATION FRAME TRANSFER



D1, D2 = frame sent by Point Coordinator
U1, U2 = frame sent by polled station
TBTT = target beacon transmission time
B = Beacon Frame

Subtypes

Management Frame Subtypes:

- Association request
- Association response
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- Beacon
- Announcement traffic indication message
- Dissociation
- Authentication
- Deauthentication

Data-carrying frames

- Data
- Data + CF-Ack
- Data + CF-Poll
- Data + CF-Ack + CF-Poll

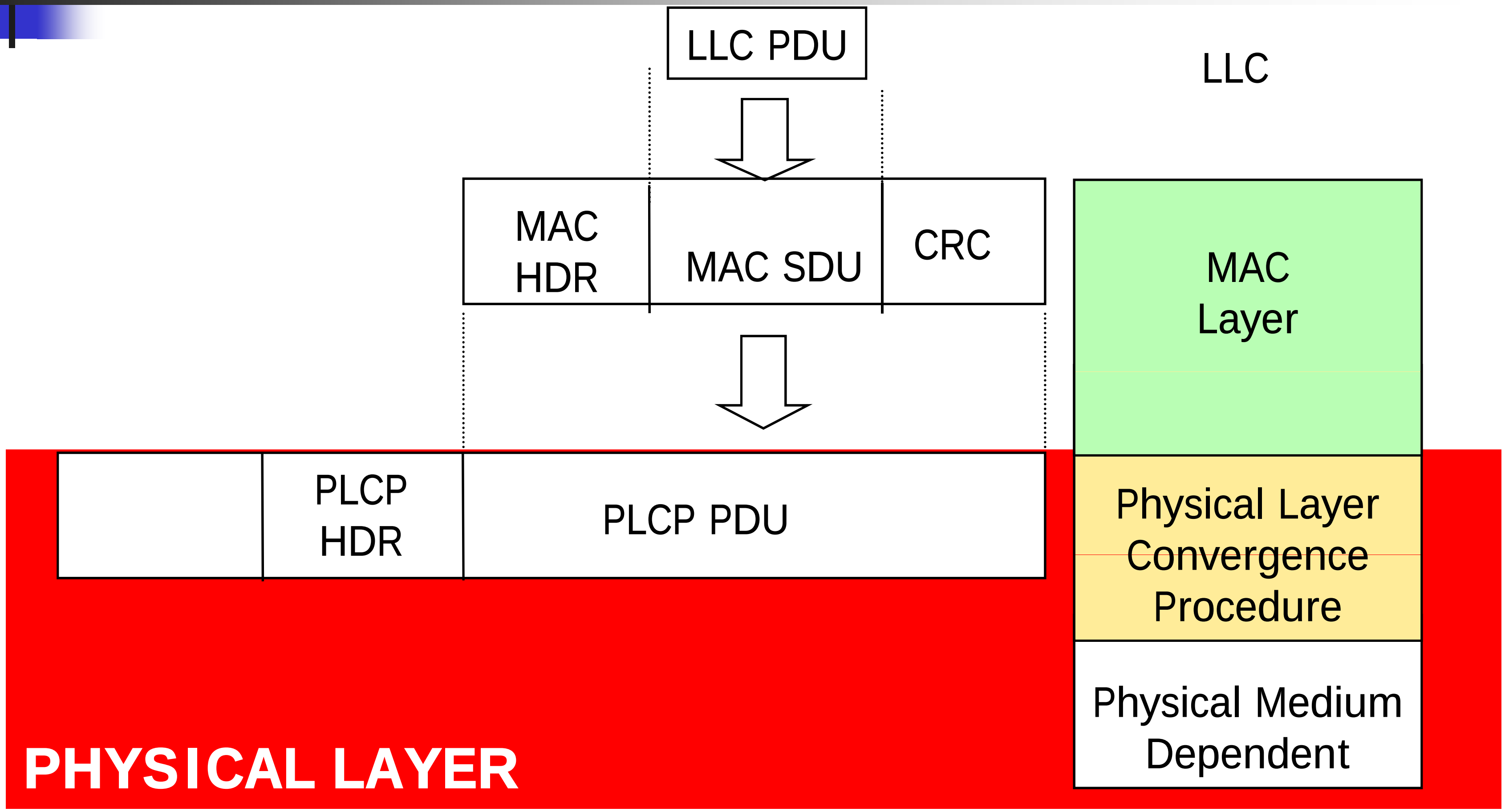
No-Data-carrying frames

- Null Function
- CF-Ack
- CF-Poll
- CF-Ack + CF-Poll

Authentication

- Open system authentication
  - Exchange of identities, no security benefits
- Shared Key authentication
  - Shared Key assures authentication

802.11: PHYSICAL LAYER



- Encoding/decoding of signals
- Preamble generation/removal (for synchronization)
- Bit transmission/reception
- Includes specification of the transmission medium

PHYSICAL LAYER CONVERGENCE PROCEDURE (PLCP)

2.4GHz FHSS

80 bits	16	12	4	16	Variable
Sync	Start Frame Delimiter	Length	Signaling	CRC	Payload data
PLCP preamble		PLCP header			

2.4GHz DSSS

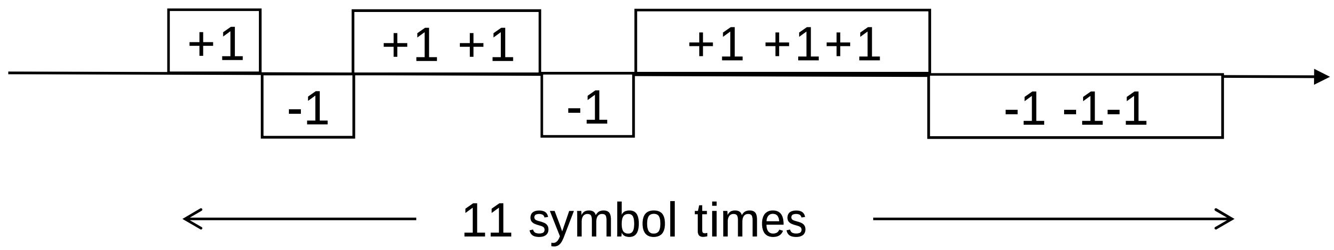
128 bits	16	8	8	16	16	Variable
Sync	SFD	Signal	Service	Length	CRC	Payload data
PLCP preamble		PLCP header				

INFRARED USING PPM (Wavelength between 850 and 950 nm)

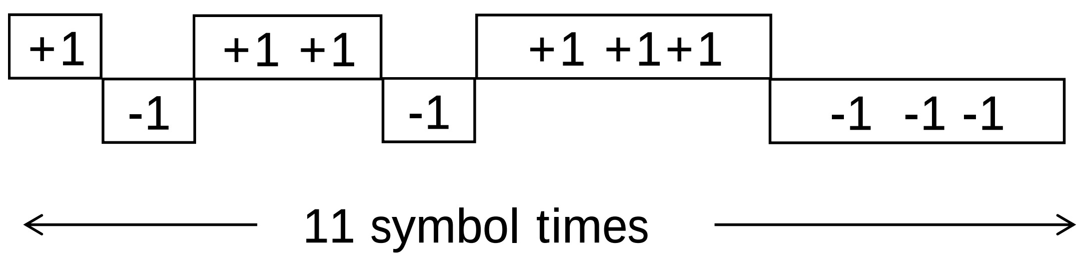
57-73 slots	4	3	32	16	16	Variable
Sync	SFD	Data rate	DC level adjust	Length	CRC	Payload data
PLCP preamble		PLCP header				

DSSS USING 11-CHIP BARKER SEQUENCE

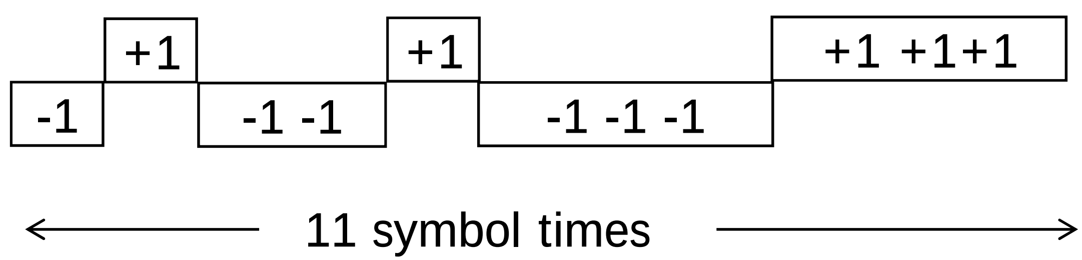
11 chip Barker sequence:



To transmit +1, send:



To transmit -1, send:



WLAN 802.11a,b,g DATA RATES

Rate, Mbps	Single/Multi Carrier	802.11b @2.4 GHz Mandatory	802.11b @2.4 GHz Optional	802.11g @2.4 GHz Mandatory	802.11g @2.4 GHz Optional	802.11a @5.2 GHz Mandatory	802.11a @5.2 GHz Optional
1	Single	Barker		Barker			
2	Single	Barker		Barker			
5.5	Single	CCK	PBCC	CCK	PBCC		
6	Multi			OFDM	CCK-OFDM	OFDM	
9	Multi				OFDM, CCK-OFDM		OFDM
11	Single	CCK	PBCC	CCK	PBCC		
12	Multi			OFDM	CCK-OFDM	OFDM	
18	Multi				OFDM, CCK-OFDM		OFDM
22	Single				PBCC		
24	Multi			OFDM	CCK-OFDM	OFDM	
33	Single				PBCC		
36	Multi				OFDM, CCK-OFDM		OFDM
48	Multi				OFDM, CCK-OFDM		OFDM
54	Multi				OFDM, CCK-OFDM		OFDM

- Packet Binary Convolutional Code (PBCC™)
- OFDM WITH BPSK, QPSK, 16-QAM or 64-QAM
- CCK: Complementary code keying