4. THE MEDIUM ACCESS CONTROL SUBLAYER

Rakesh Matam

Indian Institute of Information Technology Guwahati

rakesh@iiitg.ac.in

September 10, 2021

Fast Ethernet

- As the speed of 10Mbps ethernet was increasingly insufficient, IEEE reconvened the 802.3 committee in 1992 to come up with a faster LAN.
- Two options were considered: 1) Keep 802.3 exactly as it is, just make it faster. 2) Redo it totally with many new features.
- The committee decided to keep 802.3 as it was, and just make it go faster.

Fast Ethernet

- The basic **idea behind fast Ethernet was simple**: keep all the old frame formats, interfaces, and procedural rules, but reduce the bit time from 100 nsec to 10 nsec.
- Technically, it would have been possible to copy 10-Mbps classic Ethernet and still detect collisions on time by just **reducing the maximum cable length** by a factor of 10.
- But, the advantages of twisted-pair wiring were so overwhelming that fast Ethernet is based entirely on this design. Thus, all fast Ethernet systems use hubs and switches;

Fast Ethernet

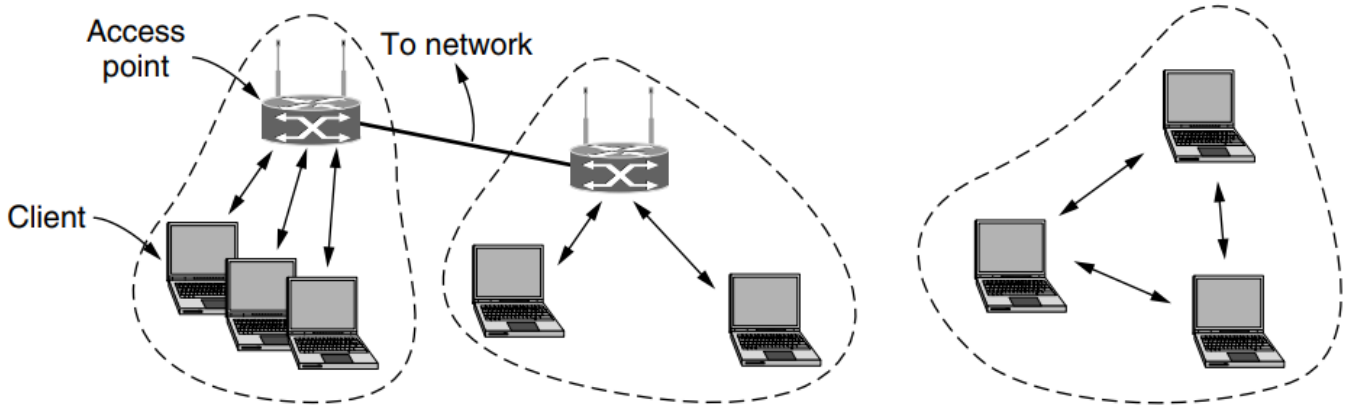
- Some design choices that had to be made, are which wire types to support.
- Category 3: Most western offices had Cat 3 twisted pairs running from it to a telephone wiring closet within 100 meters.
- The main disadvantage of a Category 3 twisted pair is its inability to carry 100 Mbps over 100 meters. [Remember 100 mts is the maximum computer-to-hub distance specified for 10-Mbps hubs.]
- However, Cat 5 can handle 100m easily and fiber can go much farther. Finally, all 3 were chosen.

Fast Ethernet

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

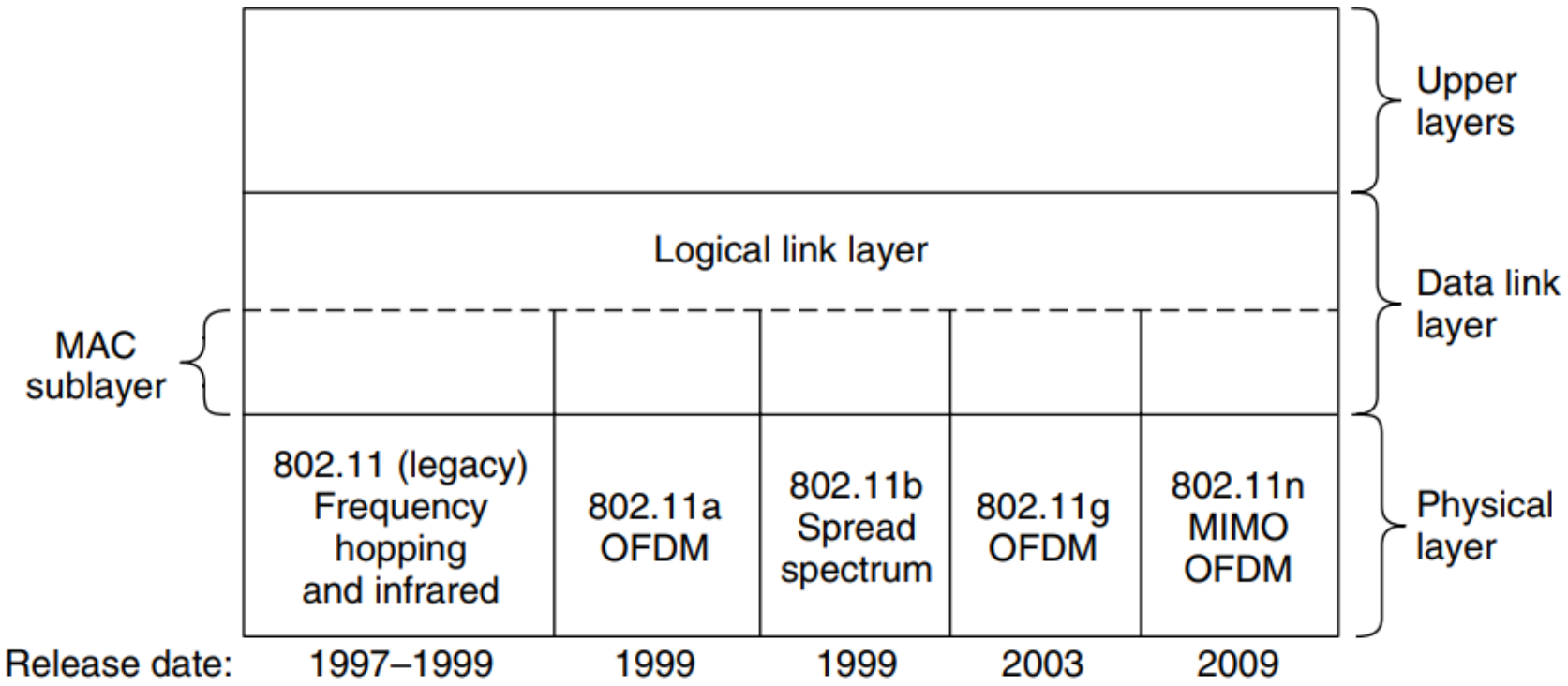
- 100Base-T4 requires four twisted pairs. Of the four pairs, one is always to the hub, one is always from the hub, and the other two are switchable to the current transmission direction.
- 100Base-Tx uses only two twisted pairs per station, one to the hub and one from it.
- 100Base-FX, uses two strands of multimode fiber, one for each direction, so it, too, can run full duplex with 100 Mbps in each direction.

802.11 Architecture and Protocol Stack



- In infrastructure mode, each client is associated with an AP (Access Point) that is in turn connected to the other network.
- The ad hoc mode mode is a collection of computers that are associated so that they can directly send frames to each other.

802.11 Protocol Stack



- LLC is a glue layer that identifies the protocol (e.g., IP) that is carried within an 802.11 frame.

802.11 Physical Layer

- All of the 802.11 techniques use short-range radios to transmit signals in either the 2.4-GHz or the 5-GHz ISM frequency bands
- NICs are compatible with multiple physical layers.
  E.g., 802.11 a/b/g

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

802.11 MAC sub-layer protocol

- The 802.11 MAC sub-layer protocol is quite different from that of Ethernet, due to **two factors** that are fundamental to wireless communication.
- **First**, radios are nearly always half duplex, meaning that they cannot transmit and listen for noise bursts at the same time on a single frequency.
- The received signal can easily be a million times weaker than the transmitted signal, so it cannot be heard at the same time.
- With wireless, collision detection mechanism does not work.

802.11 MAC sub-layer protocol

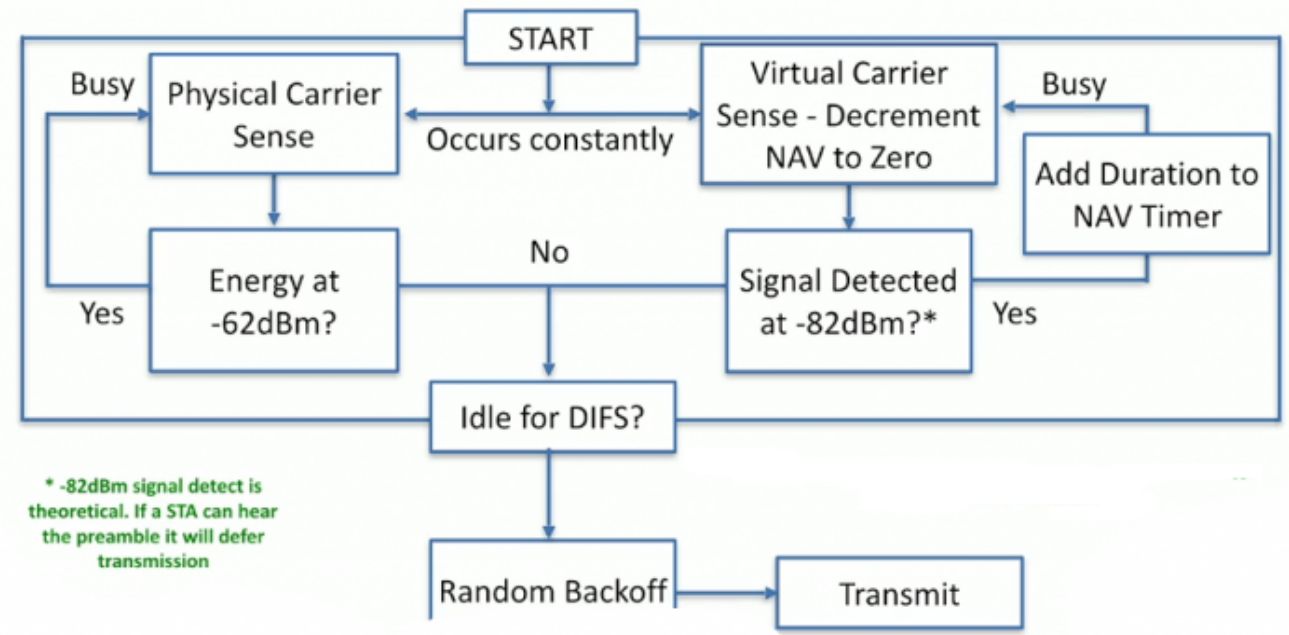
- 802.11 tries to avoid collisions with a protocol called **CSMA/CA** (CSMA with Collision Avoidance).
- CSMA/CA conceptually similar to Ethernet's CSMA/CD, with channel sensing before sending and exponential back off after collisions.
- However, a station that has a frame to send starts with a random backoff (except in the case that it has not used the channel recently and the channel is idle). It does not wait for a collision.

802.11 MAC sub-layer protocol

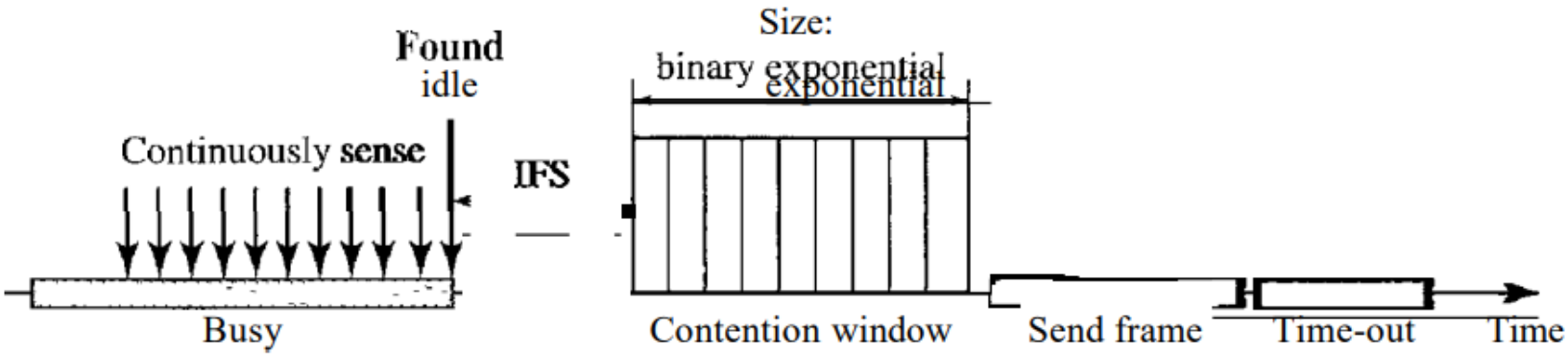
- The number of slots to backoff is chosen in the range 0 to, say, 15 in the case of the OFDM physical layer.
- The station waits until the channel is idle, by sensing that there is no signal for a short period of time (called the DIFS), and counts down idle slots, pausing when frames are sent.
- It sends its frame when the counter reaches 0. If the frame gets through, the destination immediately sends a short acknowledgement.
- Lack of an acknowledgement is inferred to indicate an error, whether a collision or otherwise.
- In this case, the sender doubles the backoff period and tries again, continuing with exponential backoff as in Ethernet until the frame has been successfully transmitted or the maximum number of re-transmissions has been reached.

802.11 MAC sub-layer protocol

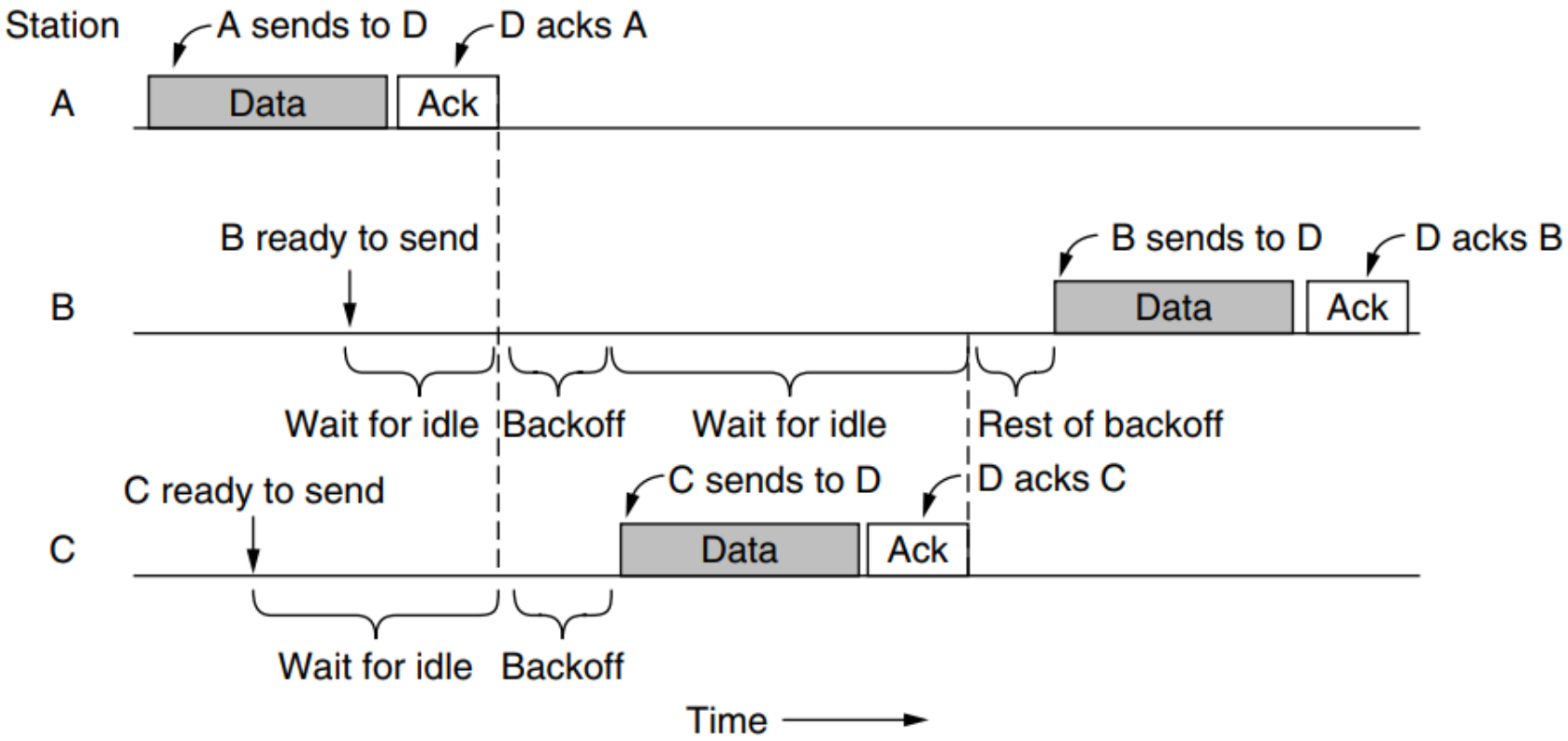
- Compared to Ethernet, there are two main differences. First, starting back-offs early helps to avoid collisions.
- Second, acknowledgements are used to infer collisions because collisions cannot be detected.
- This is called DCF (Distributed Coordination Function) because each station acts independently, without any kind of central control.



802.11 MAC sub-layer protocol

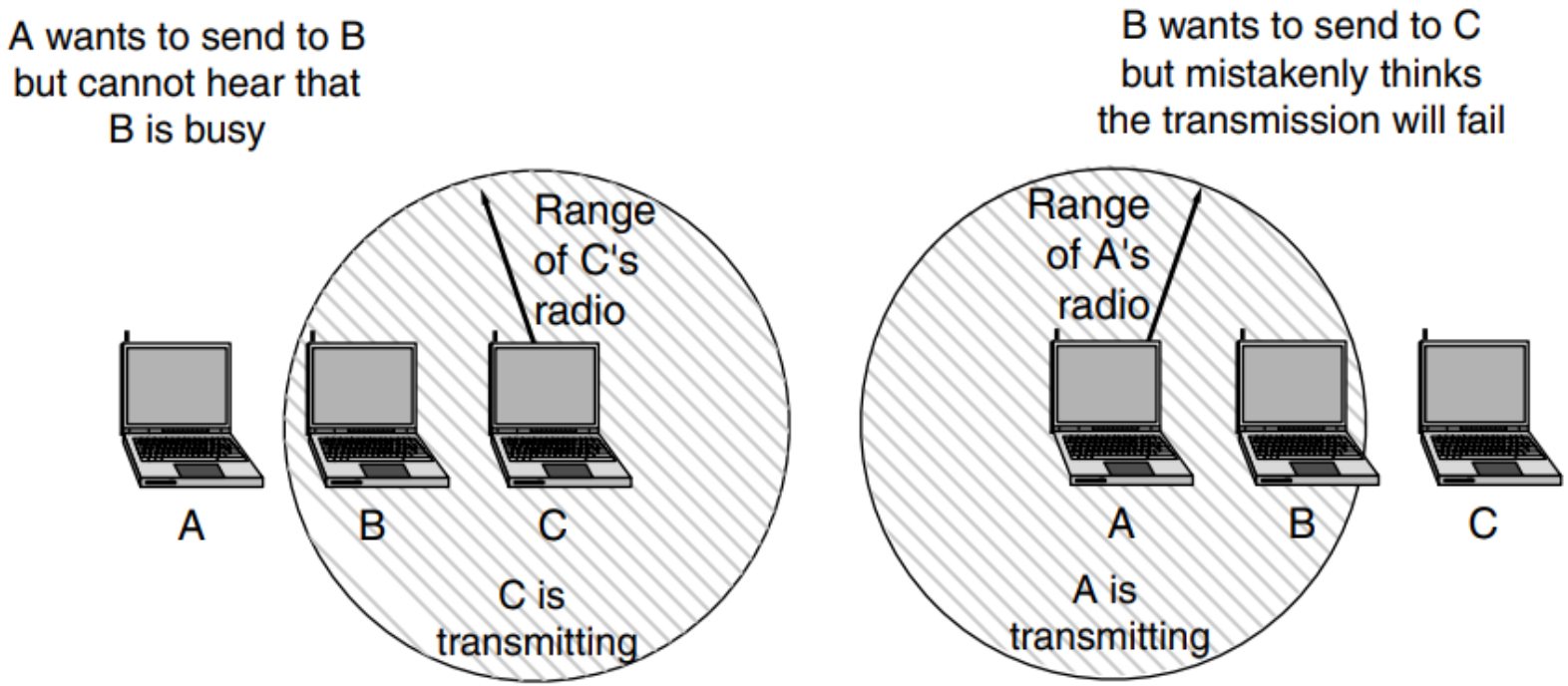


802.11 MAC sub-layer protocol



802.11 MAC sub-layer protocol

- The standard also includes an optional mode of operation called PCF (Point Coordination Function) in which the access point controls all activity in its cell.
- However, PCF is not used in practice because there is normally no way to prevent stations in another nearby network from transmitting competing traffic.

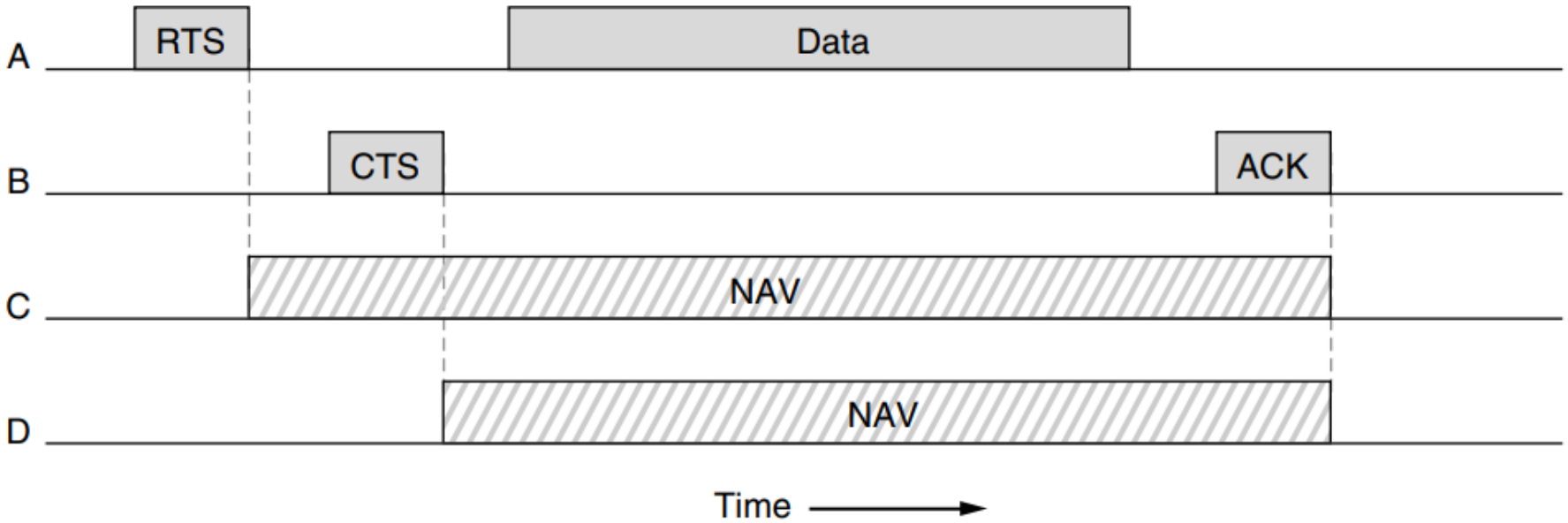


NAV - Network Allocation Vector

- To reduce ambiguities about which station is sending, 802.11 defines channel sensing to consist of both physical sensing and virtual sensing.
- Physical sensing simply checks the medium to see if there is a valid signal.
- With virtual sensing, each station keeps a logical record of when the channel is in use by tracking the NAV (Network Allocation Vector).
- Each frame carries a NAV field that says how long the sequence of which this frame is part will take to complete.
- Stations that overhear this frame know that the channel will be busy for the period indicated by the NAV, regardless of whether they can sense a physical signal.

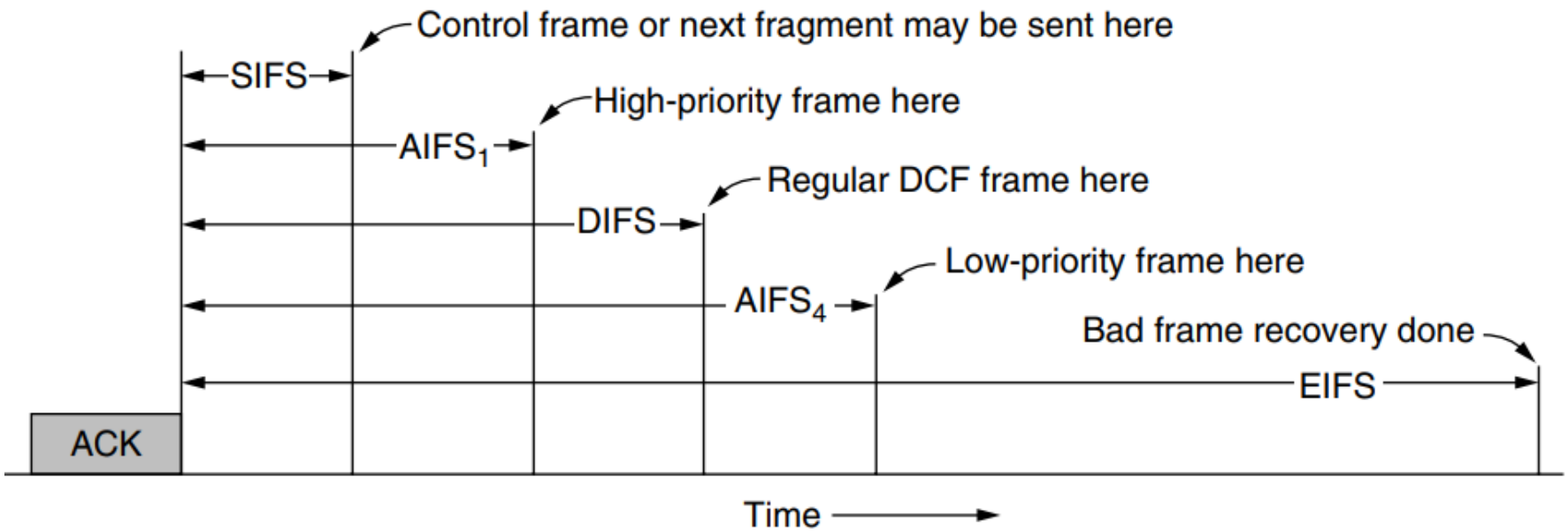
RTS/CTS uses NAV

- An **optional** RTS/CTS mechanism uses the NAV to prevent terminals from sending frames at the same time as hidden terminals.

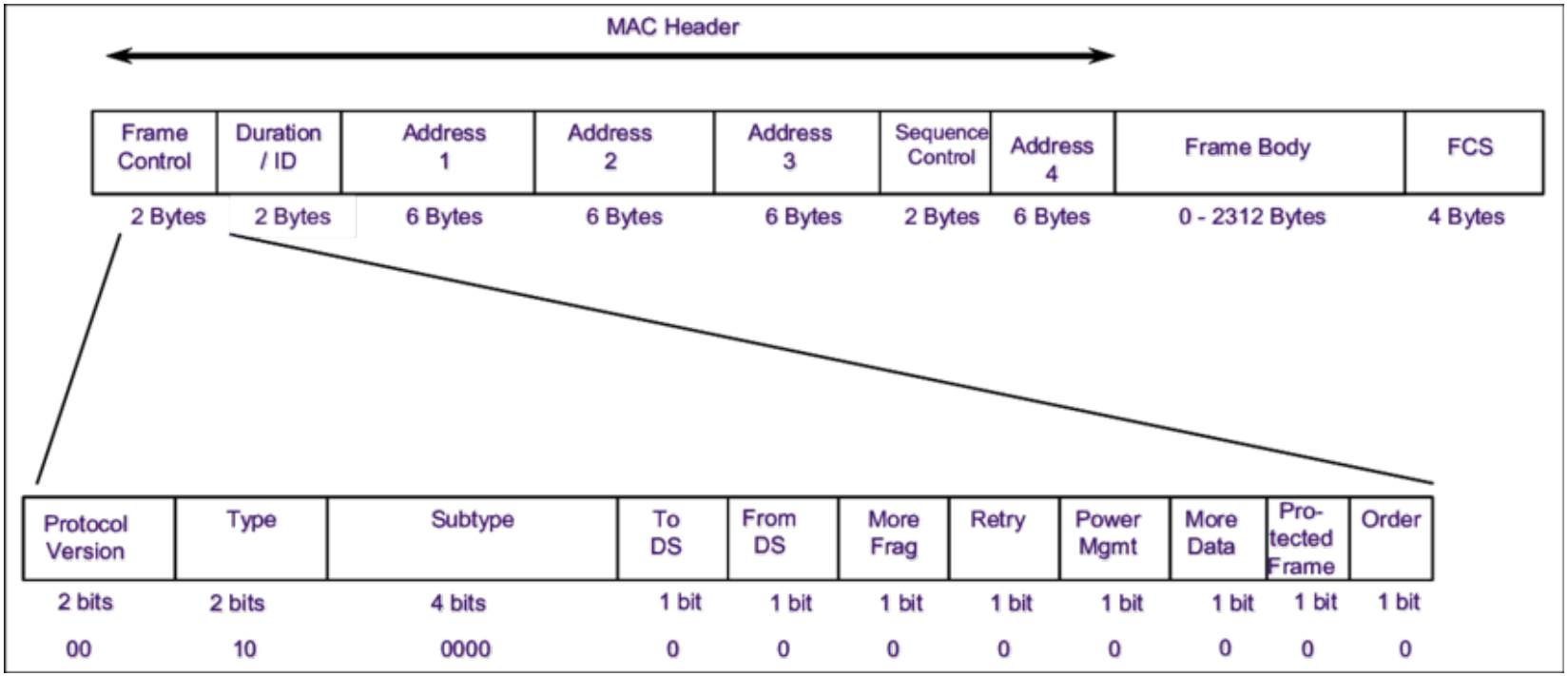


802.11 MAC (Frame Spacing)

- After a frame has been sent, a certain amount of idle time is required before any station may send a frame to check that the channel is no longer in use.
- The trick is to define different time intervals for different kinds of frames.



802.11 MAC Frame Structure



- Type (data, control, or management) and Sub-type fields (e.g., ACK, RTS or CTS)

802.11 MAC Frame Structure

- Duration field, tells how long the frame and its acknowledgement will occupy the channel, measured in microseconds.
- Data frames sent to or from an AP have three addresses, all in standard IEEE 802 format.

Function	ToDS	FromDS	Address 1 (receiver)	Address 2 (transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	Not used
To AP (infra.)	1	0	BSSID	SA	DA	Not used
From AP (infra.)	0	1	DA	BSSID	SA	Not used
WDS (bridge)	1	1	RA	TA	DA	SA

802.11 MAC Frame Structure - Address Fields

- In the case of frames bound for a destination on the distribution system, the client is both source and transmitter.

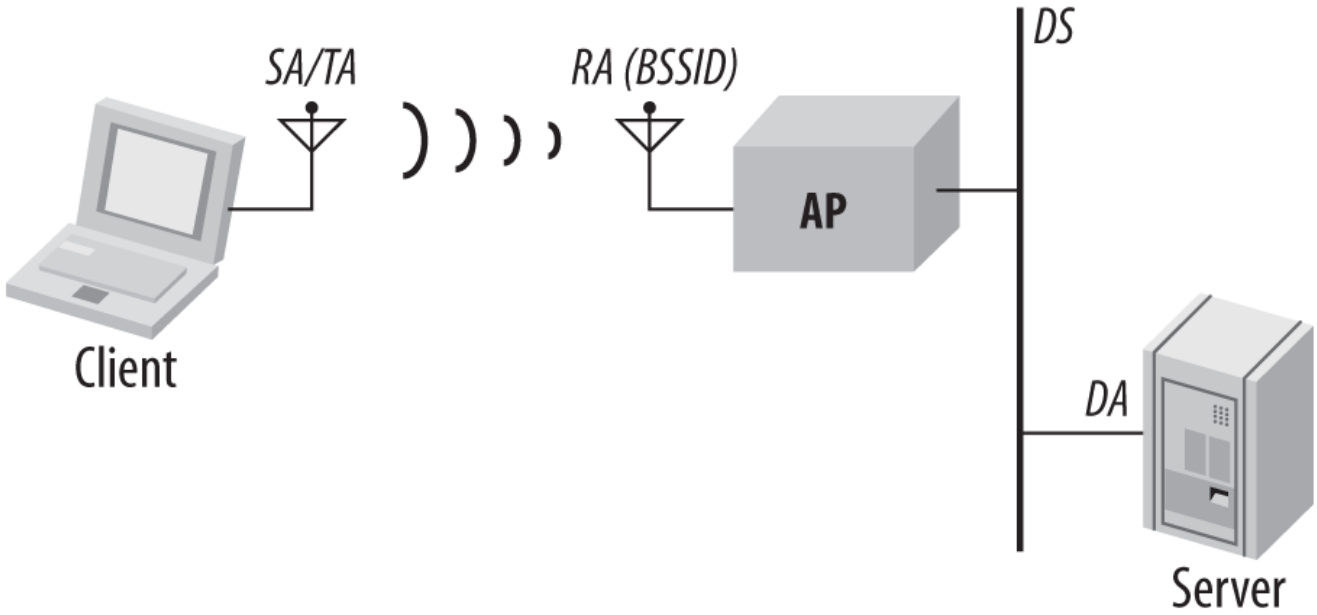


Figure: Address fields usage to the DS

802.11 MAC Frame Structure - Address Fields

- Frames are created by the server, so the server's MAC address is the source address for frames.

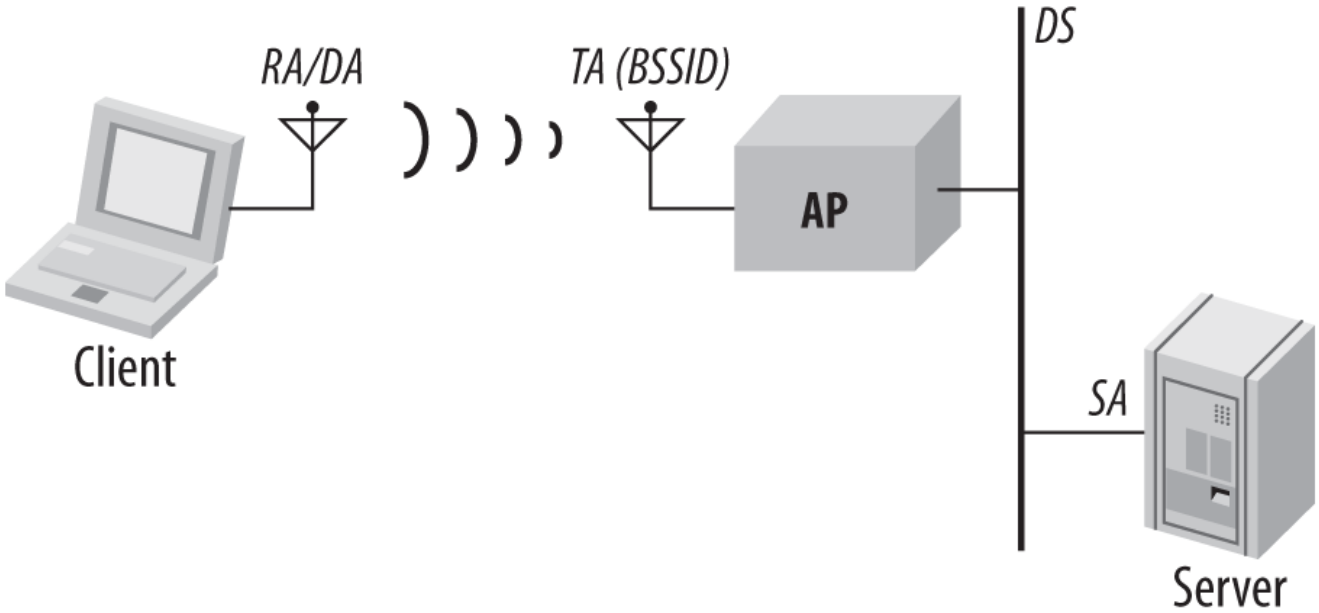


Figure: Address fields usage from the DS

802.11 MAC Frame Structure - Address Fields

- For frames bound from the client to the server, the transmitter is the client-side access point, and the receiver is the server-side access point.

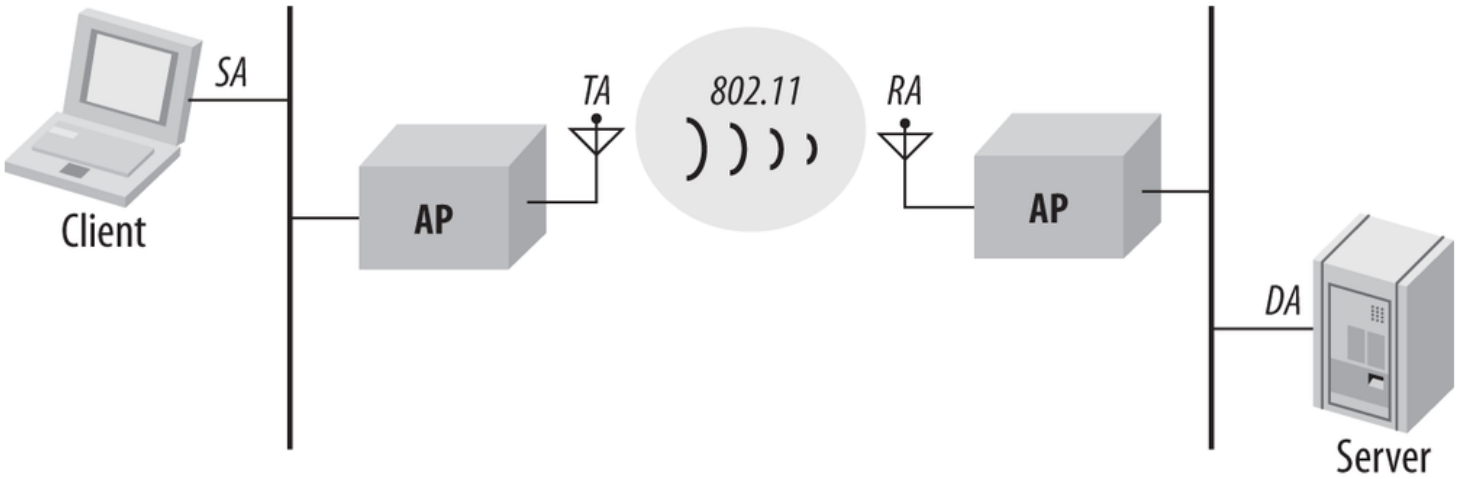


Figure: WDS

802.11 MAC Frame Structure

- The **Sequence** field numbers frames so that duplicates can be detected. Of the 16 bits available, 4 identify the fragment and 12 carry a number that is advanced with each new transmission.
- The **Data** field contains the payload, up to 2312 bytes. The first bytes of this payload are in a format known as LLC (Logical Link Control).
- Frame check sequence, which is the same 32-bit CRC.

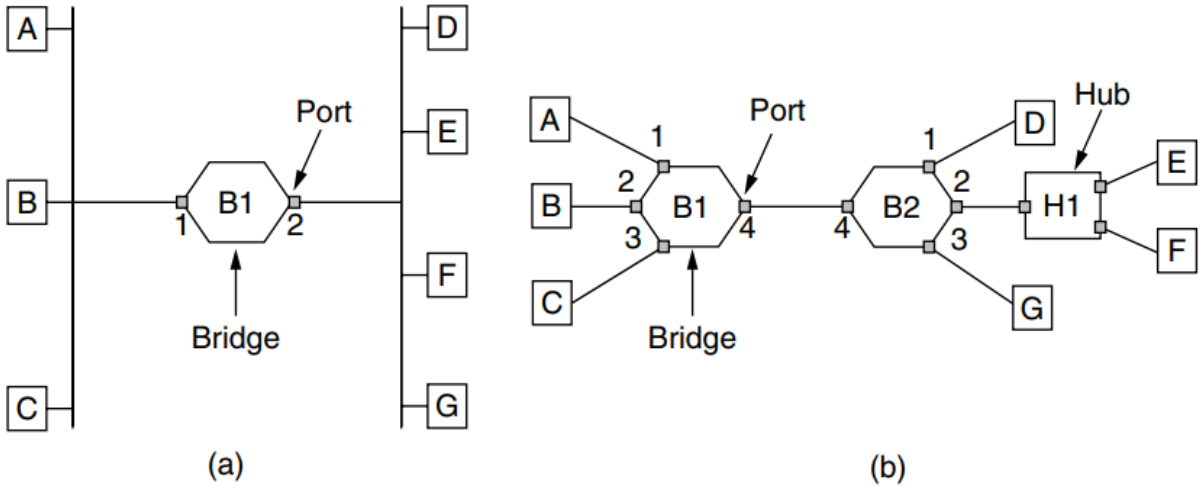
Bridges

- Many organizations have multiple LANs and wish to connect them.
- It can be done with devices called bridges.
- The Ethernet switches are a modern name for bridges;
- Bridges operate in the data link layer, so they examine the data link layer addresses to forward frames.

Uses of Bridges

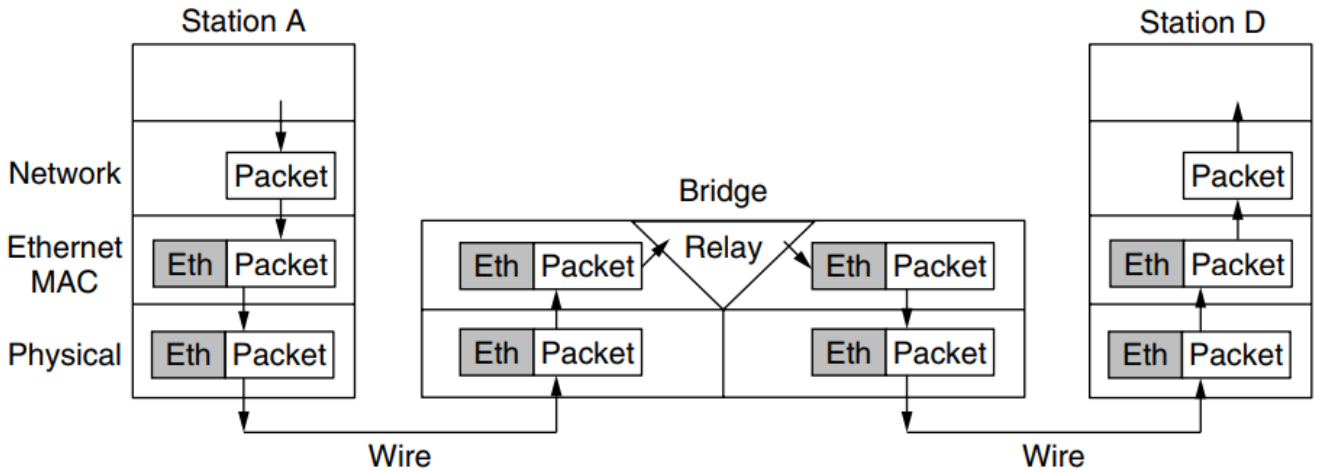
1. Multiple LANs come into existence due to the autonomy of their owners. Bridges connect them.
2. The organizations may be geographically spread over several buildings separated by considerable distances. It may be cheaper to have separate LANs in each building and connect them with bridges and a few long-distance fiber optic links than to run all the cables to a single central switch.
3. It may be necessary to split what is logically a single LAN into separate LANs (connected by bridges) to accommodate the load.

Learning Bridges



- Backward learning algorithm picks the output port:
  - Associates source address on frame with input port
  - Frame with destination address is sent to learned port
  - Unlearned destinations are sent to all other ports

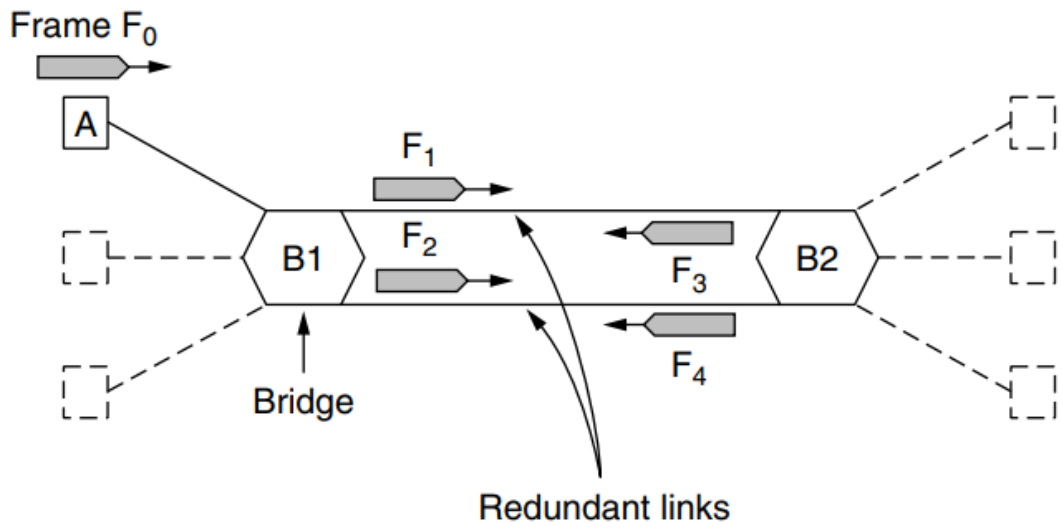
Learning Bridges



- Bridges extend the Link layer:
  - Use but don't remove Ethernet header/addresses
  - Do not inspect Network header

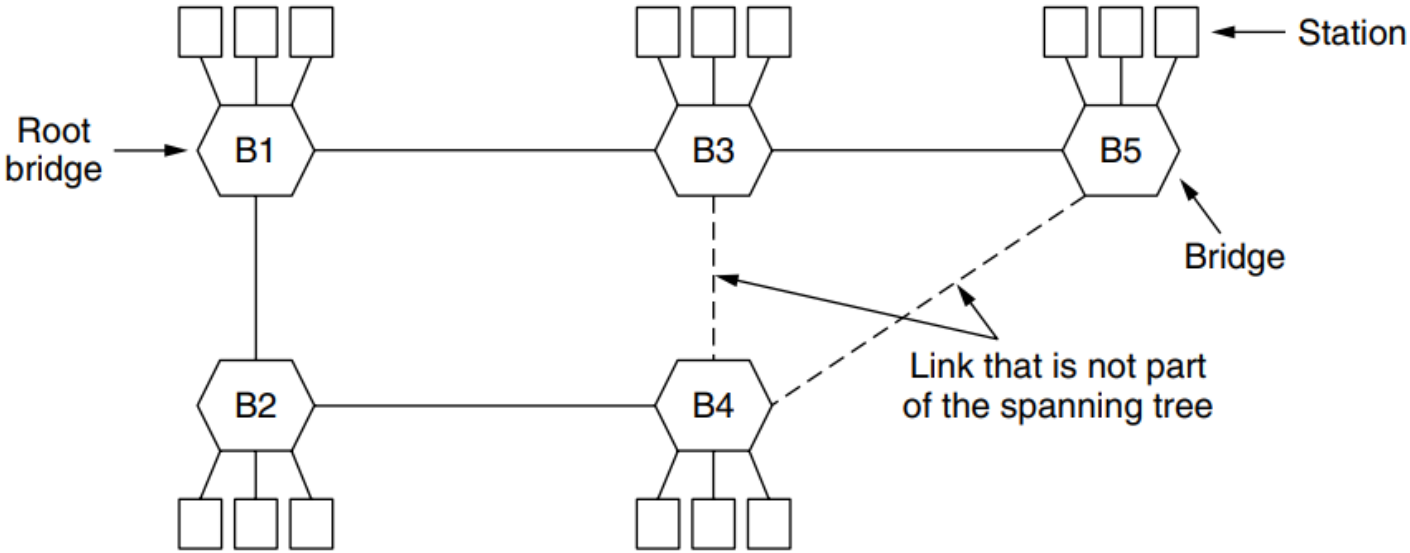
Learning Bridges:Spanning Trees

- To increase reliability, redundant links can be used between bridges.



- Bridge topology with loops and only backward learning can cause frames to circulate for ever.
- The solution to this difficulty is for the bridges to communicate with each other and **overlay the actual topology with a spanning tree** that reaches every bridge.

Learning Bridges: Spanning Trees

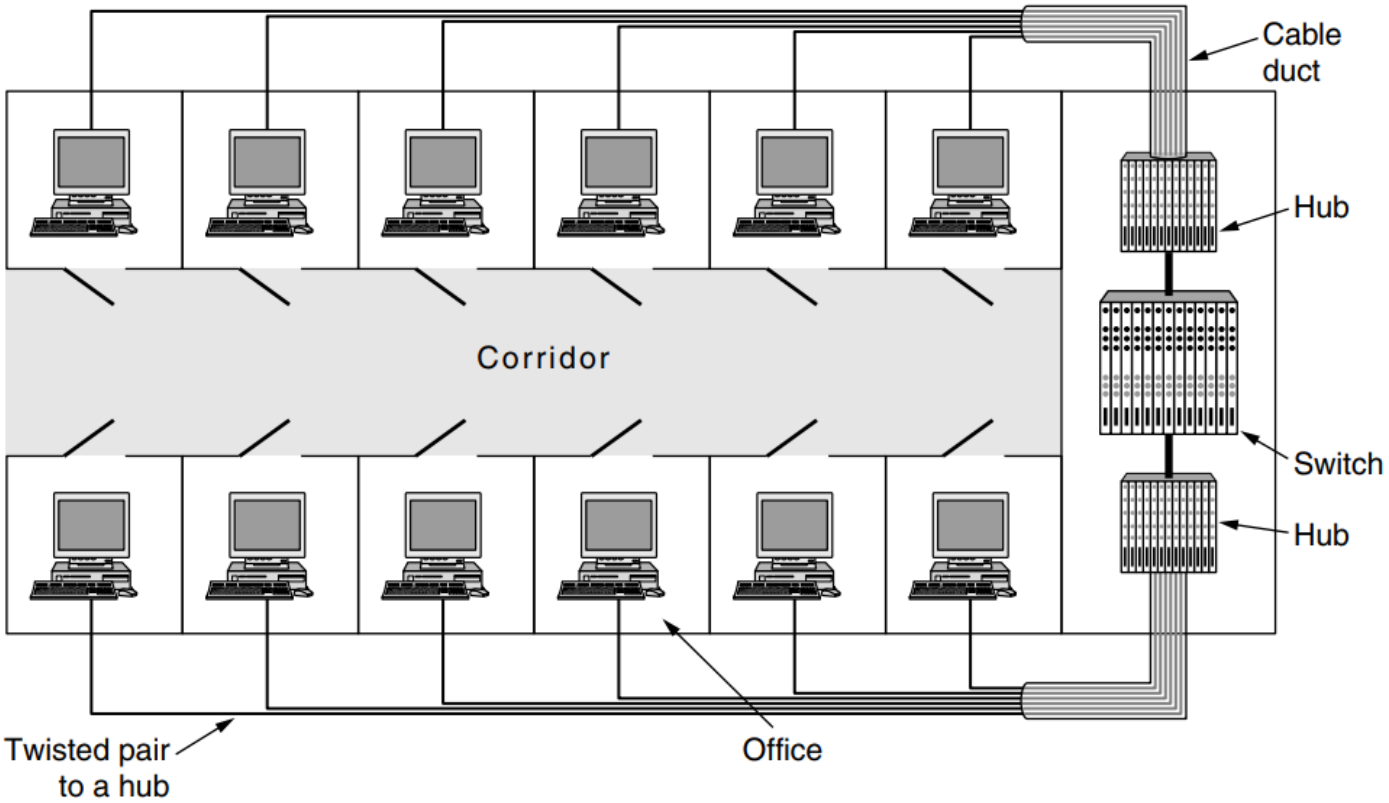


- Each bridge periodically broadcasts a configuration message out all of its ports to its neighbors and processes the messages it receives from other bridges.
- The bridges must first choose one bridge to be the root of the spanning tree.

Learning Bridges: Spanning Trees

- Each bridge include an identifier based on their MAC address in the configuration message, as well as the identifier of the bridge they believe to be the root.
- The bridges choose the bridge with the lowest identifier to be the root. After enough messages have been exchanged to spread the news, all bridges will agree on which bridge is the root.
- Next, a tree of shortest paths from the root to every bridge is constructed.
- To find shortest paths, bridges include the distance from the root in their configuration messages.
- Each bridge remembers the shortest path it finds to the root. The bridges then turn off ports that are not part of the shortest path.
- To break ties, the path via the bridge with the lowest identifier is chosen.

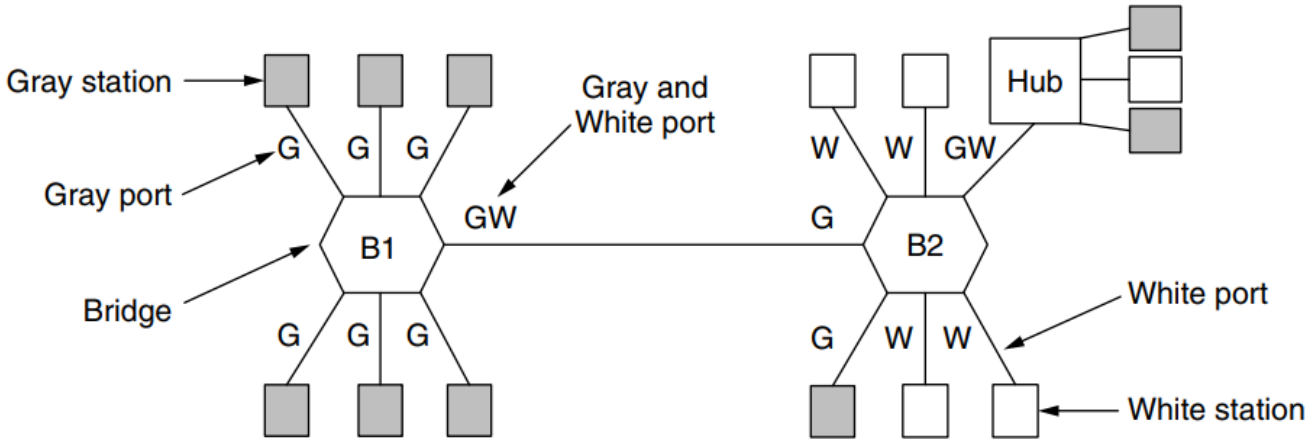
Virtual LANs



- During early days of LAN, all the people geographically close were put on the same LAN, whether they belonged together or not.
- Switches makes it possible to configure LANs logically rather than physically.

VLAN

- VLANs are based on VLAN-aware switches.
- To set up a VLAN-based network, the network administrator decides how many VLANs there will be, which computers will be on which VLAN, and what the VLANs will be called.
- Often the VLANs are (informally) named by colors.

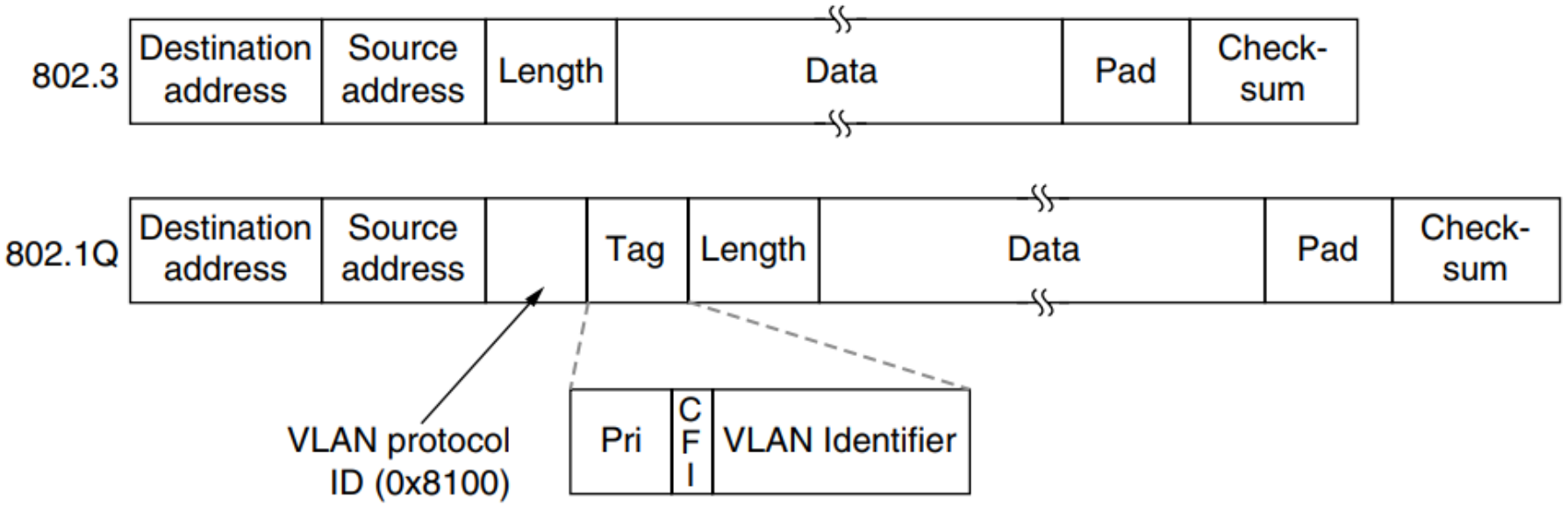


VLAN

- To make the VLANs function correctly, configuration tables have to be set up in the bridges.
- These tables tell which VLANs are accessible via which ports.
- When a frame comes in from, say, the gray VLAN, it must be forwarded on all the ports marked with a G.
- Note that a port may be labeled with multiple VLAN colors.

VLAN: IEEE 802.1Q Standard

- To implement VLANs, bridges need to know to which VLAN an incoming frame belongs.



802.1Q frames carry a color tag (VLAN identifier)
- Length/Type value is 0x8100 for VLAN protocol

The End