4. THE MEDIUM ACCESS CONTROL SUBLAYER

Rakesh Matam

Indian Institute of Information Technology Guwahati

rakesh@iiitg.ac.in

September 3, 2021

Objective

- Network links can be divided into two categories: those using point-to-point connections and those using broadcast channels.
- This chapter deals with broadcast links and their protocols.

MAC

- In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it.
- Broadcast channels are sometimes referred to as multi-access channels or random access channels.
- The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called the MAC (Medium Access Control) sublayer.
- The MAC sublayer is especially important in LANs, particularly wireless ones because wireless is naturally a broadcast channel.

The Channel Allocation Problem

How to allocate a single broadcast channel among competing users?

Channel: The channel might be a portion of the wireless spectrum in a geographic region, or a single wire or optical fiber to which multiple nodes are connected.

Static Channel Allocation:

- Traditional Way: FDM
- If there are N users, the bandwidth is divided into N equal-sized portions, with each user being assigned one portion.
- Disadvantages: Wastage of spectrum if Idle users/bursty traffic

Static Channel Allocation

The poor performance of static FDM can easily be seen with a simple queueing theory calculation.

Let us start by finding the mean time delay, **T**, to send a frame onto a channel of capacity **C** bps.

We assume that the frames arrive randomly with an average arrival rate of λ frames/sec, and that the frames vary in length with an average length of $1/\mu$ bits.

With these parameters, the service rate of the channel is μC frames/sec.

Static Channel Allocation

A standard queueing theory result is
T = 1 / μC - λ

It requires that the randomness of the times between frame arrivals and the frame lengths follow an exponential distribution, or equivalently be the result of a Poisson process.

if C is 100 Mbps, the mean frame length, $1/\mu$, is 10,000 bits, and the frame arrival rate, λ, is 5000 frames/sec, then T=?

Now let us divide the single channel into N independent subchannels, each with capacity C/N bps. The mean input rate on each of the subchannels will now be λ/N. Recomputing T, we get
T_N = 1 / μ(C/N) - λ/N

The mean delay for the divided channel is N times worse than if all the frames were somehow magically arranged orderly in a big central queue.

Assumptions of Dynamic Channel Allocation

Independent Traffic:

The model consists of N independent stations, where each station generates frames for transmission. The expected number of frames generated in an interval of length Δt is $\lambda \Delta t$. Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

Single Channel

A single channel is available for all communication. All stations can transmit on it and all can receive from it. The stations are assumed to be equally capable, though protocols may assign them different roles (e.g., priorities).

Assumptions of Dynamic Channel Allocation

Observable Collisions.

If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled. This event is called a collision. All stations can detect that a collision has occurred. A collided frame must be transmitted again later. No errors other than those generated by collisions occur.

Continuous or Slotted Time

Time may be assumed continuous, in which case frame transmission can begin at any instant. Alternatively, time may be slotted or divided into discrete intervals (called slots). Frame transmissions must then begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

Assumptions of Dynamic Channel Allocation

Carrier Sense or No Carrier Sense

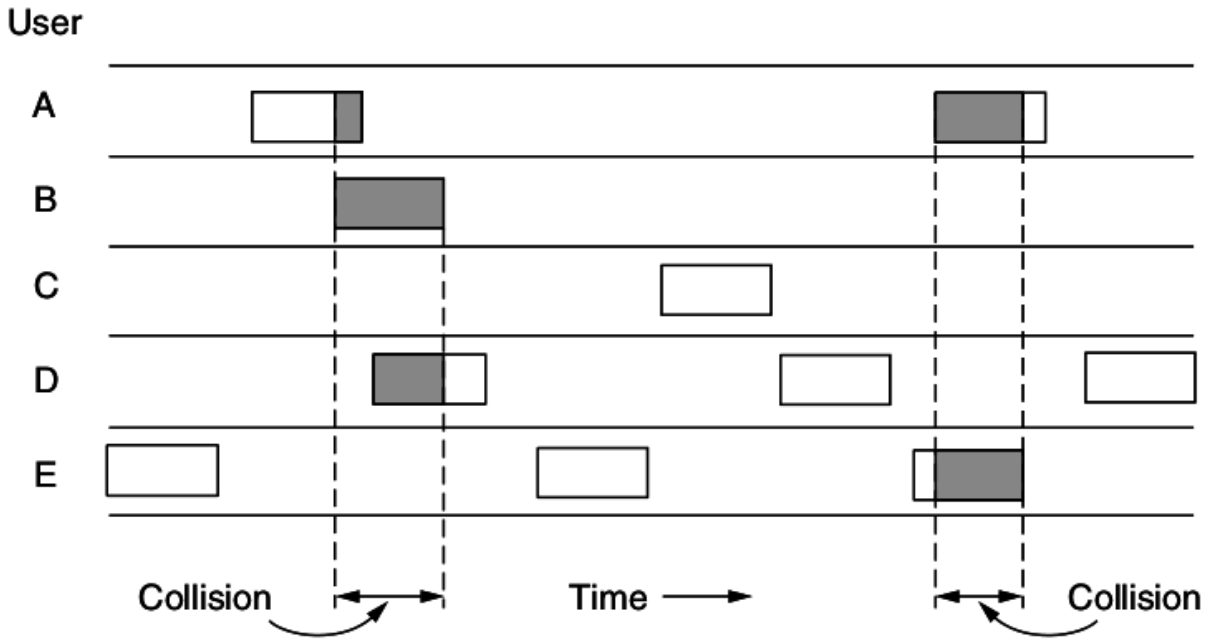
With the carrier sense assumption, stations can tell if the channel is in use before trying to use it. No station will attempt to use the channel while it is sensed as busy. If there is no carrier sense, stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

Pure Aloha

- Basic Idea: Let users transmit whenever they have data to be sent.
- There will be collisions, of course, and the colliding frames will be damaged. Senders need some way to find out if this is the case.
- After each station has sent its frame to the central computer, this computer rebroadcasts the frame to all of the stations.
- A sending station can thus listen for the broadcast from the hub to see if its frame has gotten through.
- If the frame was destroyed, the sender just waits a random amount of time and sends it again.

Pure Aloha

- The waiting time must be random or the same frames will collide over and over, in lockstep.



Pure Aloha

So what is the efficiency of an ALOHA channel?

- In other words, what fraction of all transmitted frames escape collisions under these chaotic circumstances?

Pure Aloha: Efficiency

Let us consider an infinite collection of users typing at their terminals (stations).

- A user is always in one of two states: typing or waiting. Initially, all users are in the typing state. When a line is finished, the user stops typing, waiting for a response.
- The station then transmits a frame containing the line over the shared channel to the central computer and checks the channel to see if it was successful.
- If so, the user sees the reply and goes back to typing. If not, the user continues to wait while the station retransmits the frame over and over until it has been successfully sent.

Pure Aloha: Efficiency

Let the "frame time" denote the amount of time needed to transmit the standard, fixed-length frame

- We assume that the new frames generated by the stations are well modeled by a **Poisson distribution** with a **mean of N frames** per frame time.
- If $N > 1$, the user community is generating frames at a higher rate than the channel can handle, and nearly every frame will suffer a collision.
- For reasonable throughput, we would expect $0 < N < 1$.

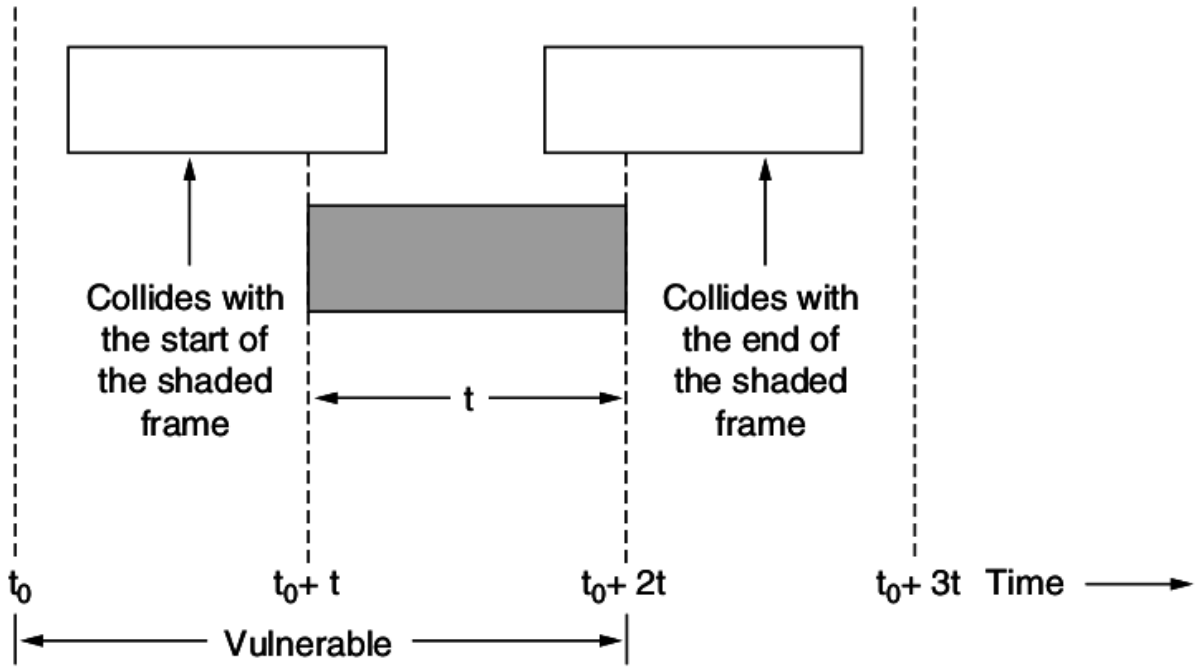
Pure Aloha: Efficiency

In addition to the new frames, the stations also generate retransmissions of frames that previously suffered collisions.

- Let us further assume that the old and new frames combined are well modeled by a Poisson distribution, with mean of **G** frames per frame time.
- Clearly, $G \geq N$. At low load (i.e., $N \approx 0$), there will be few collisions, hence few retransmissions, so $G \approx N$.
- At high load, there will be many collisions, so $G > N$.
- Under all loads, the throughput, S, is the offered load(G) times the probability P_0, of a transmission succeeding-that is, $S = GP_0$, where P_0 is the probability that a frame does not suffer a collision.

Pure Aloha: Efficiency

- A frame will not suffer a collision if no other frames are sent within one frame time of its start



Pure Aloha: Efficiency

The probability that **k** frames are generated during a given frame time, in which **G** frames are expected, is given by the Poisson distribution

$$\Pr[k] = \frac{G^k \, e^{-G}}{k!}$$

so the probability of zero frames is just e^{-G}.

In an interval two frame times long, the mean number of frames generated is 2G.

The probability of no frames being initiated during the entire vulnerable period is thus given by $P_0 = e^{-2G}$.

Using S $=$GP_0, we get S$=$Ge^{-2G}. The maximum throughput occurs at G $= 0.5$, with S $= 1/2$e, which is about 0.184.

Slotted Aloha

Slotted Aloha divides time into discrete intervals called slots, each interval corresponding to one frame.

- In slotted ALOHA, a station is not permitted to send whenever the user types a line. Instead, it is required to wait for the beginning of the next slot.
- Thus, the continuous time ALOHA is turned into a discrete time one. This halves the vulnerable period.
- The probability of no other traffic during the same slot as our test frame is then e^{-G}, which leads to S=Ge^{-G}.

Carrier Sense Multiple Access Protocols

Protocols in which stations listen for a carrier (i.e., a transmission) and act accordingly are called carrier sense protocols.

1-persistent CSMA:

- When a station has data to send, it first listens to the channel to see if anyone else is transmitting at that moment.
- If the channel is idle, the stations sends its data. Otherwise, if the channel is busy, the station just waits until it becomes idle. Then the station transmits a frame.
- If a collision occurs, the station waits a random amount of time and starts all over again.
- The protocol is called 1-persistent because the station transmits with a probability of 1 when it finds the channel idle.

1-persistent CSMA:

What would be the prob. of collision?

1-persistent CSMA:

What would be the prob. of collision?

- If two stations become ready in the middle of a third station's transmission, both will wait politely until the transmission ends, and then both will begin transmitting exactly simultaneously, resulting in a collision.
- If they were not so impatient, there would be fewer collisions.
- The propagation delay has an important effect on collisions.
- There is a chance that just after a station begins sending, another station will become ready to send and sense the channel.

1-persistent CSMA:

- If the first station's signal has not yet reached the second one, the latter will sense an idle channel and will also begin sending, resulting in a collision.
- This chance depends on the number of frames that fit on the channel, or the bandwidth-delay product of the channel.
- If only a tiny fraction of a frame fits on the channel, which is the case in most LANs since the propagation delay is small, the chance of a collision happening is small.

nonpersistent CSMA

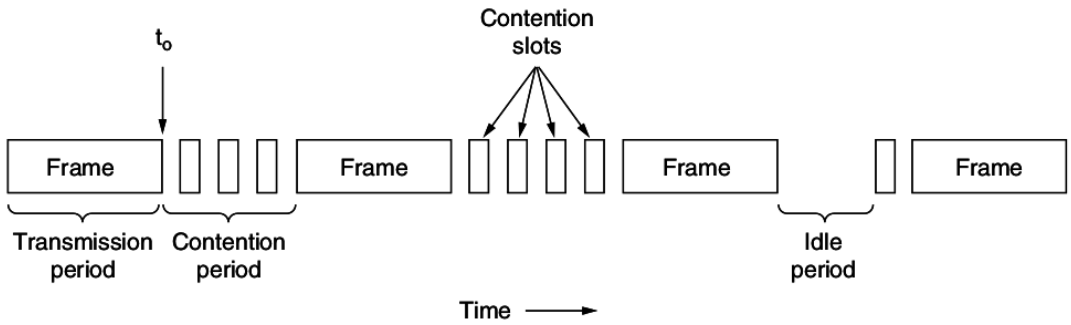
- A conscious attempt is made to be less greedy.
- A station senses the channel when it wants to send a frame, and if no one else is sending, the station begins doing so itself.
- If the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the previous transmission.
- Instead, it waits a random period of time and then repeats the algorithm.

p-persistent CSMA

- When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p.
- With a probability q = 1 - p, it defers until the next slot.
- If that slot is also idle, it either transmits or defers again, with probabilities p and q.
- This process is repeated until either the frame has been transmitted or another station has begun transmitting.

CSMA with Collision Detection: CSMA-CD

- Stations quickly detect collision and abruptly stop transmitting. Strategy saves time and bandwidth.
- At the point marked t_0, a station finished transmitting, other station having a frame to send may now attempt. If two or more stations decide to transmit simultaneously, there will be a collision.
- On detecting a collision transmission is aborted, waits a random period of time, and then tries again.



How long will it take them to realize that they have collided?

CSMA with Collision Detection: CSMA-CD

- Collision detection is an analog process.
- The station's hardware must listen to the channel while it is transmitting. If the signal it reads back is different from the signal it is putting out, it knows that a collision is occurring.
- The implications are that a received signal must not be tiny compared to the transmitted signal.
- It is difficult for wireless, as received signals may be 1,000,000 times weaker than transmitted signals and that the modulation must be chosen to allow collisions to be detected.

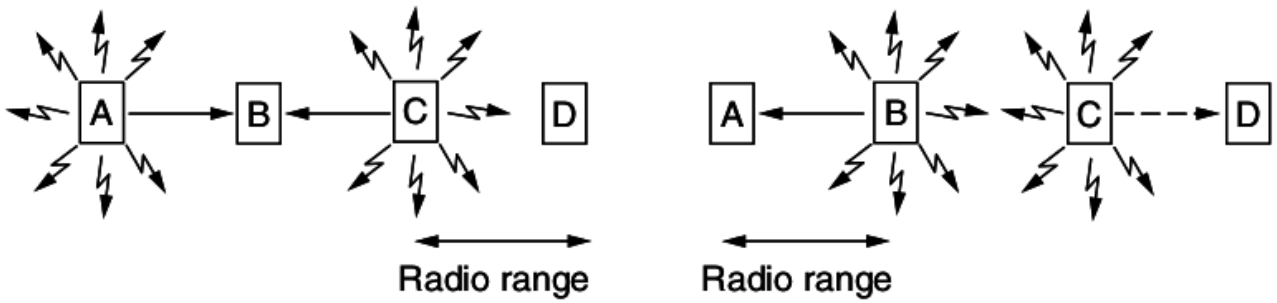
Wireless LAN Protocols

- A system of laptop computers that communicate by radio can be regarded as a wireless LAN
- Wireless systems cannot normally detect a collision while it is occurring. The received signal at a station may be tiny, perhaps a million times fainter than the signal that is being transmitted.
- A station on a wireless LAN may not be able to transmit frames to or receive frames from all other stations because of the limited radio range of the stations.
- In wired LANs, when one station sends a frame, all other stations receive it.

Wireless LAN Protocols

A naive approach to using a wireless LAN might be to try CSMA: just listen for other transmissions and only transmit if no one else is doing so.

- What matters for reception is interference at the receiver, not at the sender.



WLAN Requirement

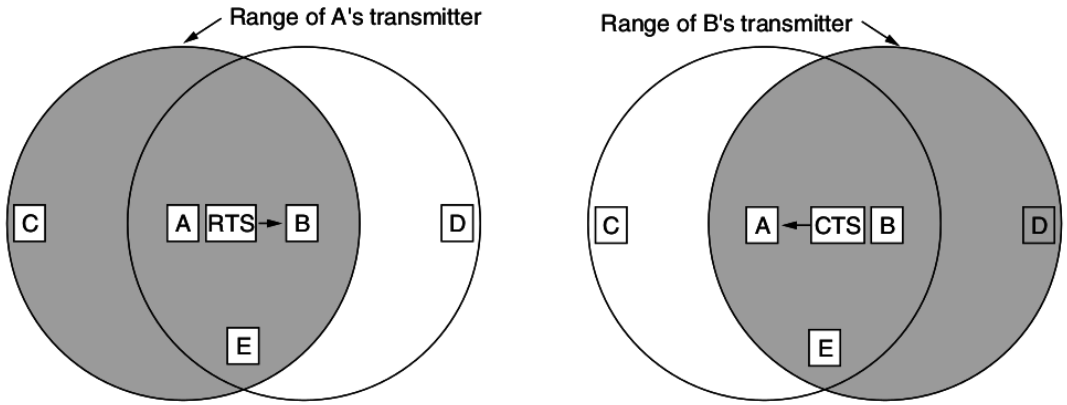
Before starting a transmission, a station really wants to know whether there is radio activity around the receiver.

- CSMA merely tells it whether there is activity near the transmitter by sensing the carrier.
- With a wire, all signals propagate to all stations, so this distinction does not exist.
- For short-range radio waves, multiple transmissions can occur simultaneously if they all have different destinations and these destinations are out of range of one another.

MACA

The basic idea behind it is for the sender to stimulate the receiver into outputting a short frame, so stations nearby can detect this transmission and avoid transmitting for the duration of the upcoming (large) data frame.

- This technique is used instead of carrier sense.



In the event of a collision, an unsuccessful transmitter (i.e., one that does not hear a CTS within the expected time interval) waits a random amount of time and tries again later.

MAC protocols in Real Systems

Many designs for personal, local, and metropolitan area networks have been standardized under the name of IEEE 802.

- Only 802.3 (Ethernet), 802.11 (wireless LAN), IEEE 802.15 (WPAN) are active.
- Bluetooth (wireless PAN) is widely deployed, but has now been standardized outside of 802.15.
- IEEE 802.2 (LLC), 802.4 (Token bus), 802.5 (Token Ring) etc. are now disbanded.

Ethernet

Two kinds of Ethernet exist: classic Ethernet and switched Ethernet

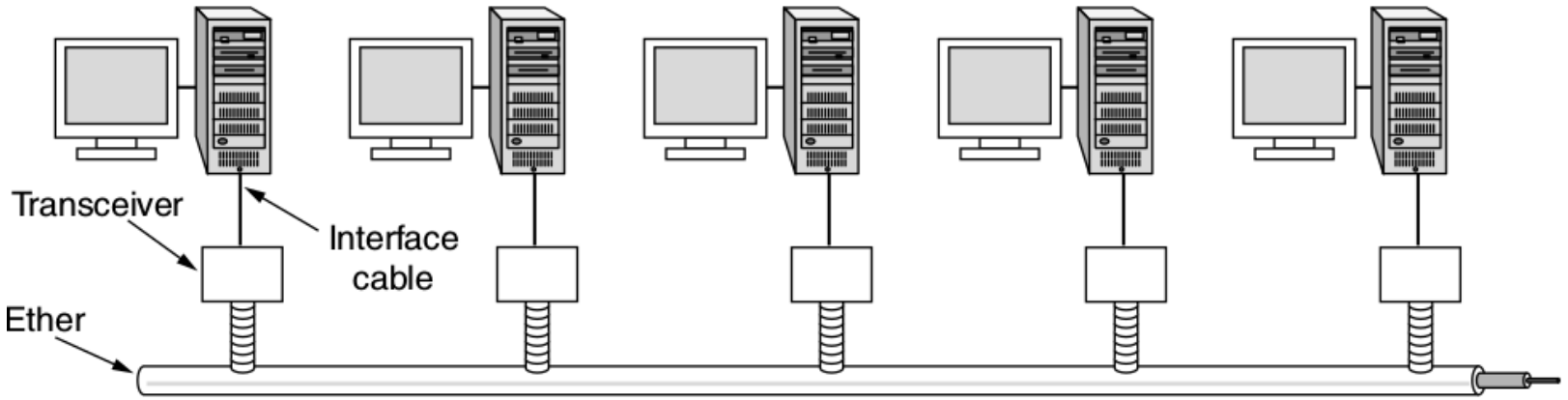
- Classic Ethernet solves the multiple access problem using the techniques we just studied. It is the original form and ran at rates from 3 to 10 Mbps.
- In switched Ethernet devices called **switches** are used to connect different computers. It runs at 100, 1000, and 10,000 Mbps, in forms called fast Ethernet, gigabit Ethernet, and 10 gigabit Ethernet.

Classic Ethernet Physical Layer

- At Xerox (PARC), Bob Metcalfe and David Boggs designed and implemented the first LAN (1976).
- It used a single long, thick coaxial cable that ran at 3 Mbps.
- The Xerox Ethernet was so successful that DEC, Intel, and Xerox drew up a standard in 1978 for a 10-Mbps Ethernet, called the **DIX standard**.
- With a minor change, the DIX standard became the IEEE 802.3 standard in 1983.
- Classic Ethernet snaked around the building as a single long cable to which all the computers were attached.

Classic Ethernet Physical Layer

- The first variety, popularly called thick Ethernet, resembled a yellow garden hose, with markings every 2.5 meters to show where to attach computers.
- It was succeeded by thin Ethernet, which bent more easily and made connections using industry-standard BNC connectors.



BNC Connector

Classic Ethernet Physical Layer

- Thin Ethernet was much cheaper and easier to install, but it could run for only 185 meters per segment (instead of 500 m with thick Ethernet), each of which could handle only 30 machines (instead of 100).
- Each version of Ethernet has a maximum cable length per segment (i.e., un-amplified length) over which the signal will propagate.
- To allow larger networks, multiple cables can be connected by repeaters.

Classic Ethernet Physical Layer

- A repeater is a physical layer device that receives, amplifies (i.e., regenerates), and re-transmits signals in both directions.
- Over each of these cables, information was sent using the Manchester encoding.
- An Ethernet could contain multiple cable segments and multiple repeaters, but no two transceivers could be more than **2.5 km** apart and no path between any two transceivers could traverse more than **four repeaters**.

Classic Ethernet MAC Sub-layer Protocol

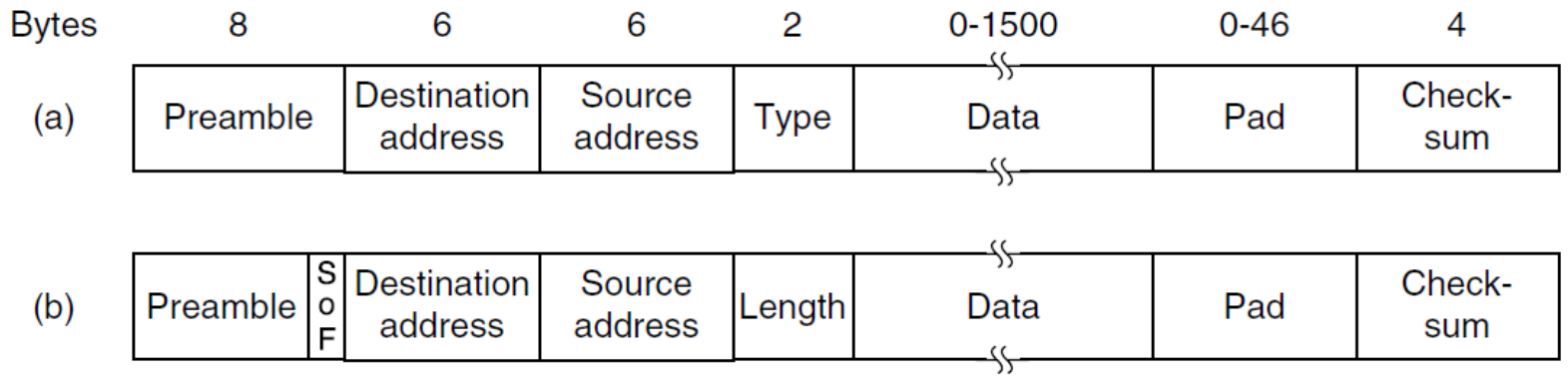
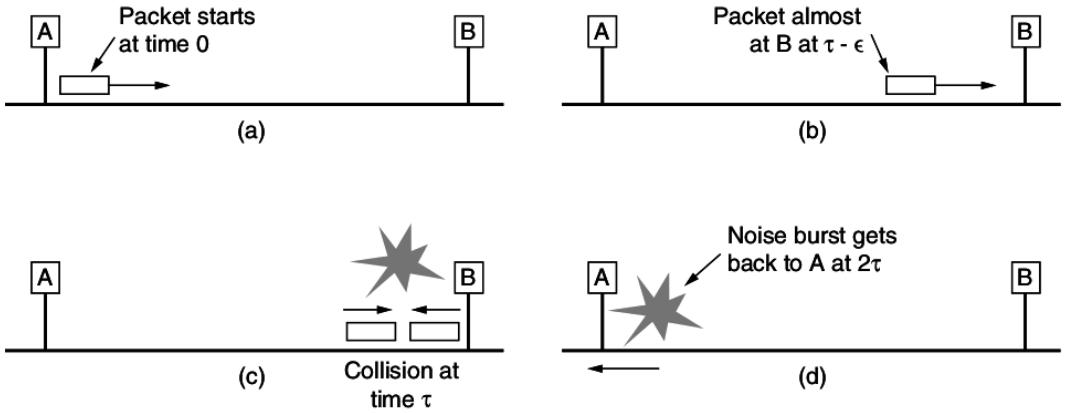


Figure 4-14. Frame formats. (a) Ethernet (DIX). (b) IEEE 802.3.

- First comes a Preamble of 8 bytes, each containing the bit pattern 10101010 (with the exception of the last byte, in which the last 2 bits are set to 11).
- This last byte is called the Start of Frame delimiter for 802.3.
- The Manchester encoding of this pattern produces a 10-MHz square wave for 6.4 micro sec to allow the receiver's clock to synchronize with the sender's.

- In addition to there being a maximum frame length, there is also a minimum frame length.
- When a transceiver detects a collision, it truncates the current frame, which means that stray bits and pieces of frames appear on the cable all the time.
- Ethernet requires that valid frames must be at least 64 bytes long, from destination address to checksum, including both.
- If the data portion of a frame is less than 46 bytes, the Pad field is used to fill out the frame to the minimum size.

Classic Ethernet MAC Sublayer Protocol



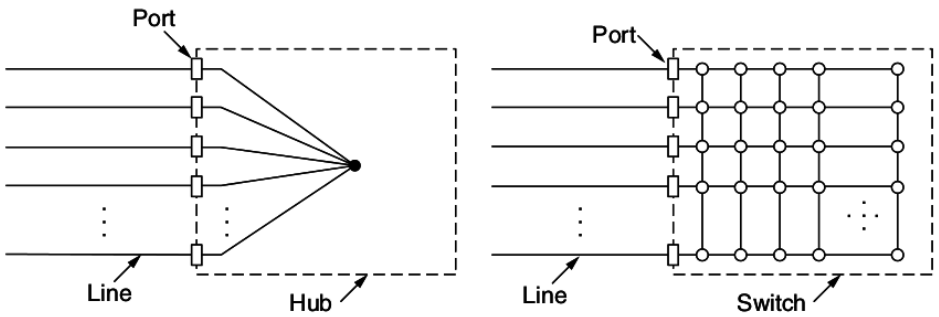
- For a 10-Mbps LAN with a maximum length of 2500 meters and four repeaters the round-trip time (including time to propagate through the four repeaters) has been determined to be nearly 50 μsec in the worst case.
- At 10 Mbps, a bit takes 100 nsec, so 500 bits is the smallest frame that is guaranteed to work. To add some margin of safety, this number was rounded up to 512 bits or 64 bytes.

CSMA-CD with BEB

- Classic Ethernet uses the 1-persistent CSMA/CD algorithm.
- If there is a collision, they abort the transmission with a short jam signal and retransmit after a random interval.
- After the first collision, each station waits either 0 or 1 slot times at random before trying again.
- If two stations collide and each one picks the same random number, they will collide again.
- After the second collision, each one picks either 0, 1, 2, or 3 at random and waits that number of slot times.
- After 10 collisions have been reached, the randomization interval is frozen at a maximum of 1023 slots.

Switched Ethernet

- Single long cable architecture of classic Ethernet had issues.
- The problems associated with finding breaks or loose connections motivated the architecture in which each station has a dedicated cable running to a central hub.
- A hub simply connects all the attached wires electrically, as if they were soldered together.
- The wires were **telephone company twisted pairs**, spares were readily available.
- This reuse was a win, but it reduced the maximum cable run from the hub to 100 meters.

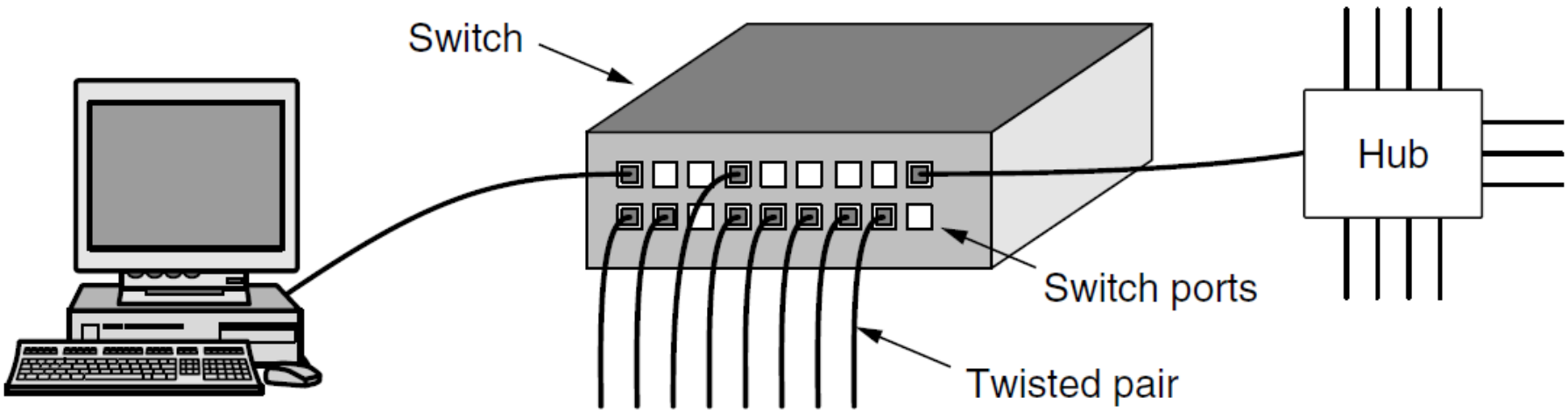


Switched Ethernet: Hub

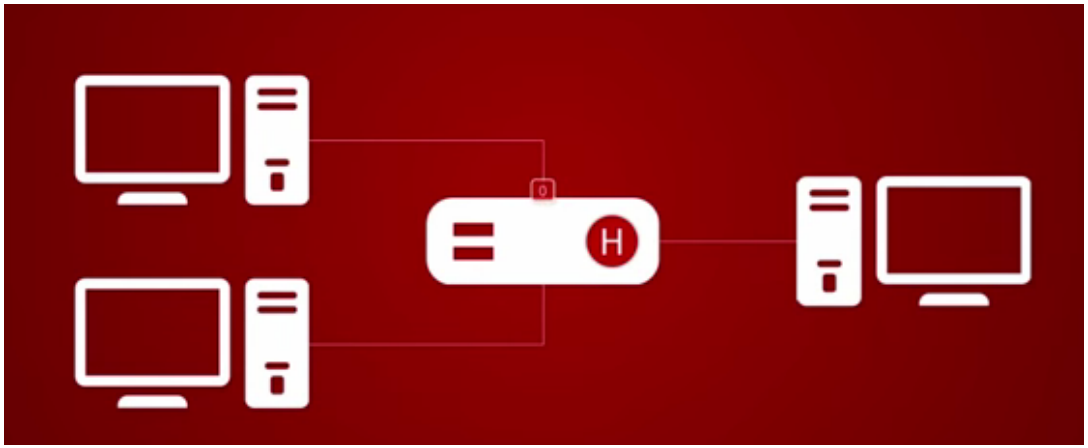
- Hubs do not increase capacity because they are logically equivalent to the single long cable of classic Ethernet.
- As more and more stations are added, each station gets a decreasing share of the fixed capacity.
- One way out is to go to a higher speed, say, from 10 Mbps to 100 Mbps, 1 Gbps, or even higher speeds. But with the growth of multimedia and powerful servers, even a 1-Gbps Ethernet can become saturated.

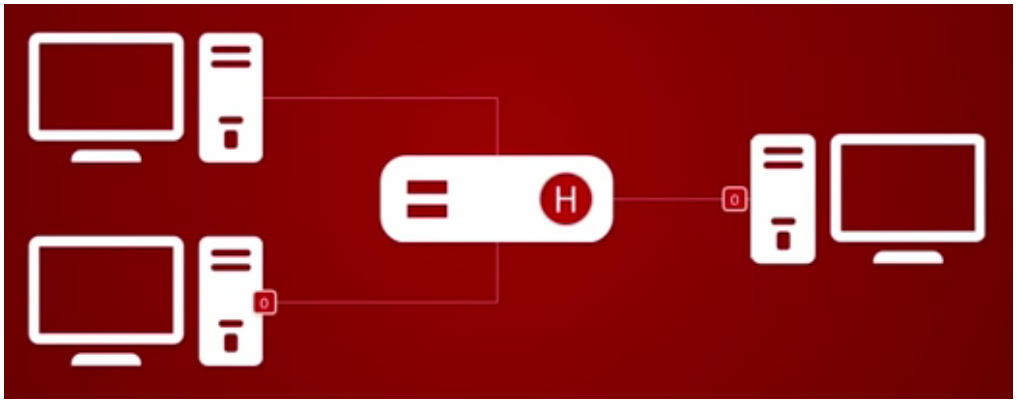
Switched Ethernet

- Switched ethernet is an another way to deal with increased load.
- The heart of this system is a switch containing a high-speed backplane that connects all of the ports
- From the outside, a switch looks just like a hub. They are both boxes, typically with 4 to 48 ports, each with a standard RJ-45 connector for a twisted-pair cable.

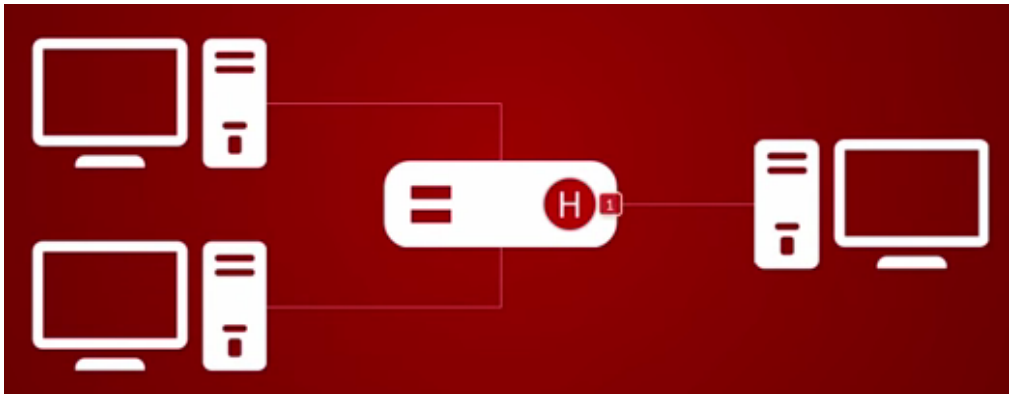


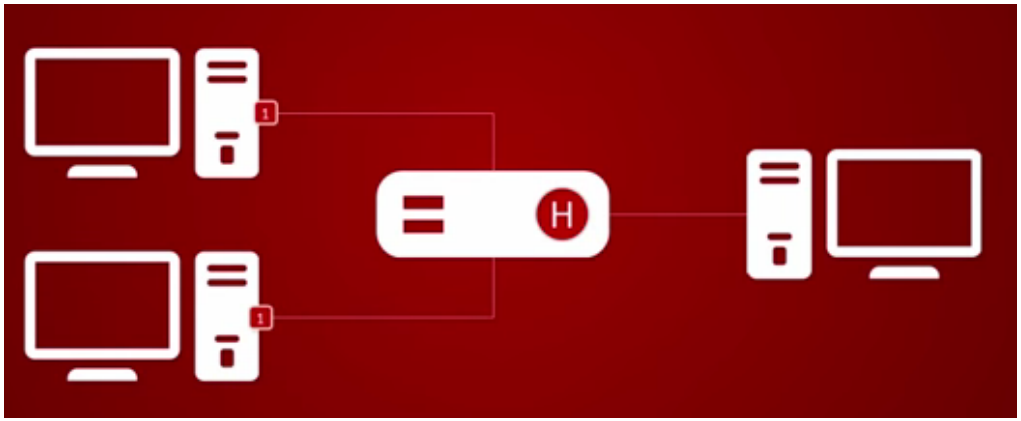
Switched Ethernet



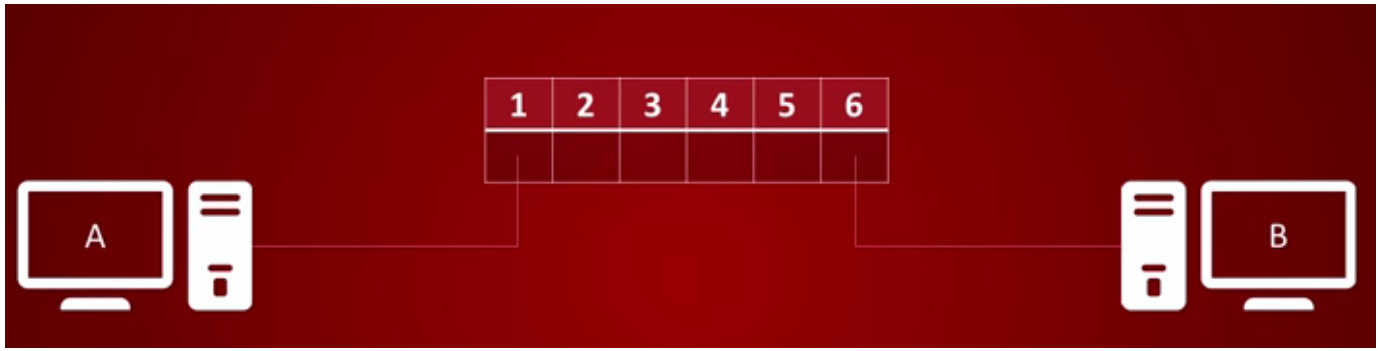


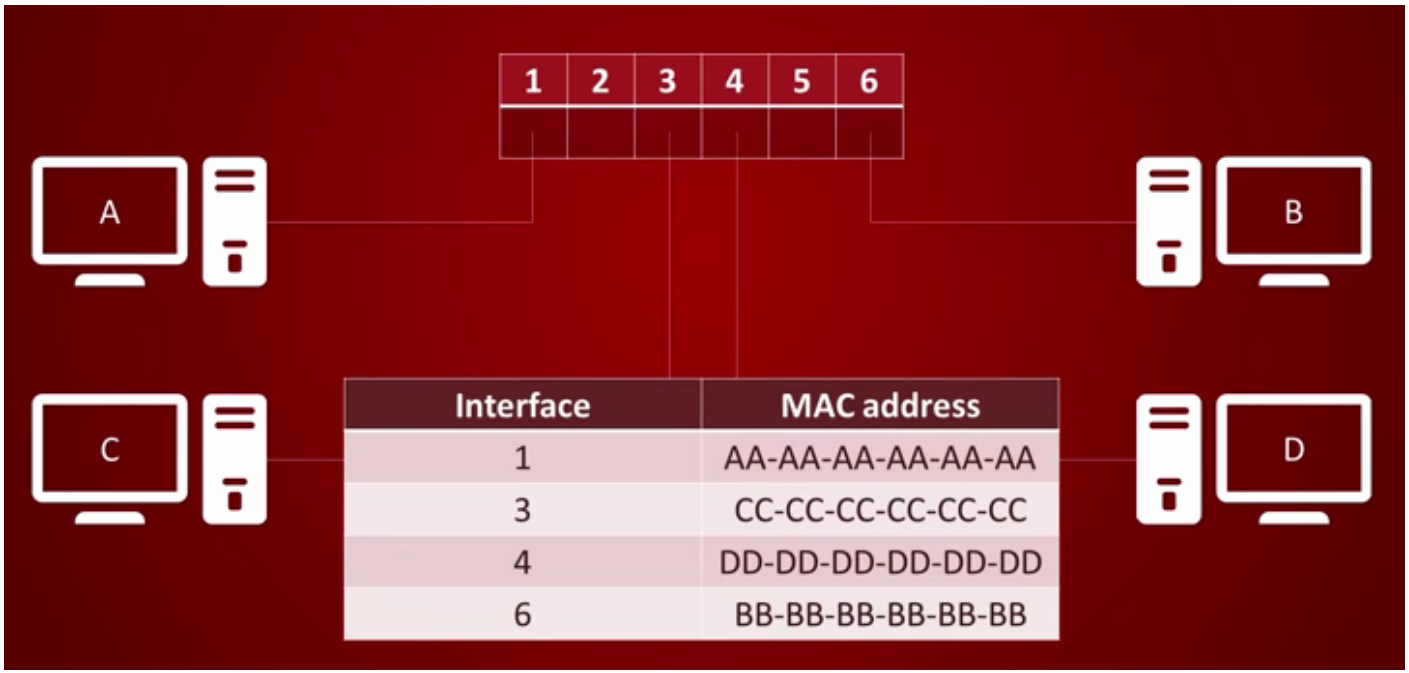
Switched Ethernet



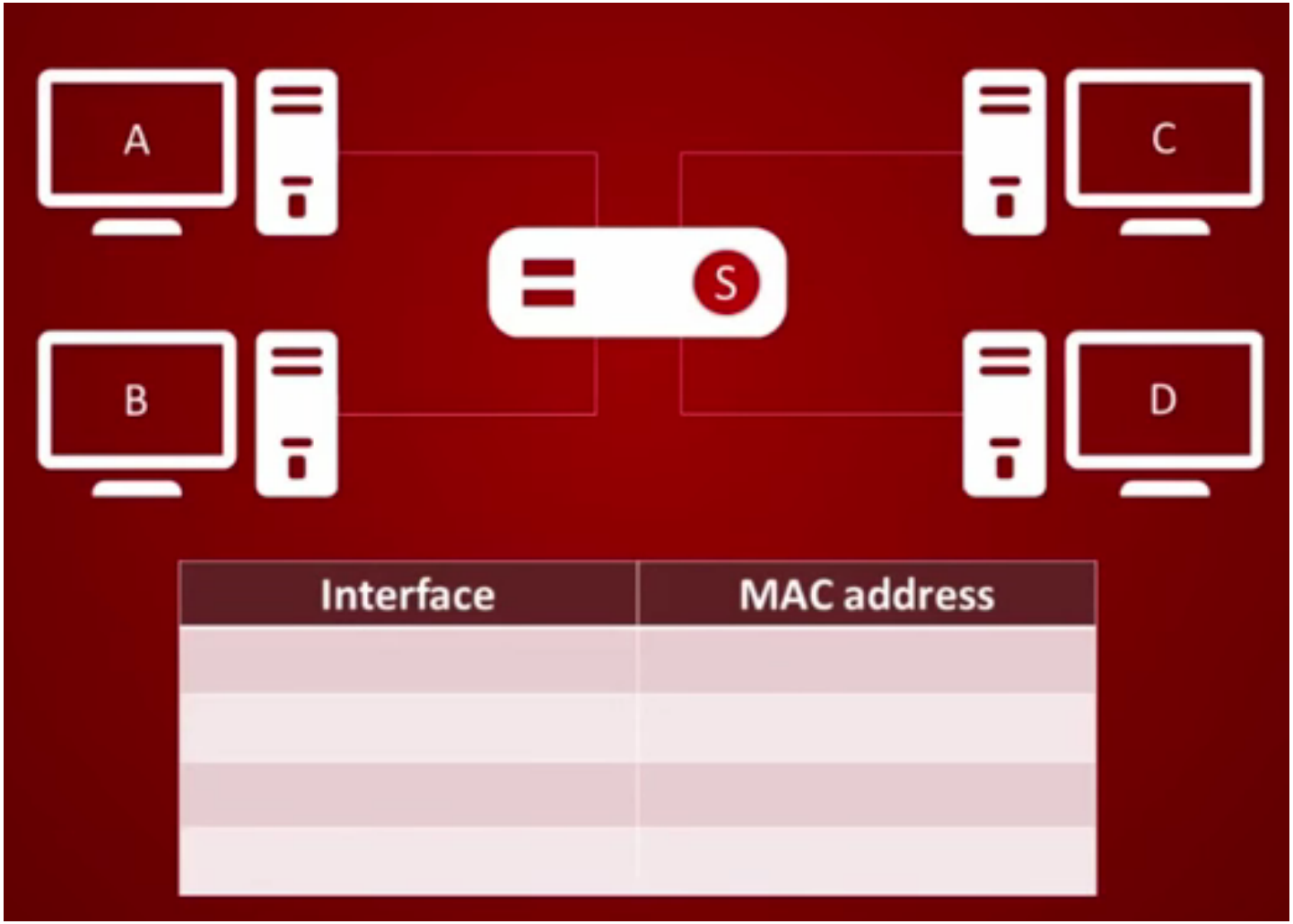


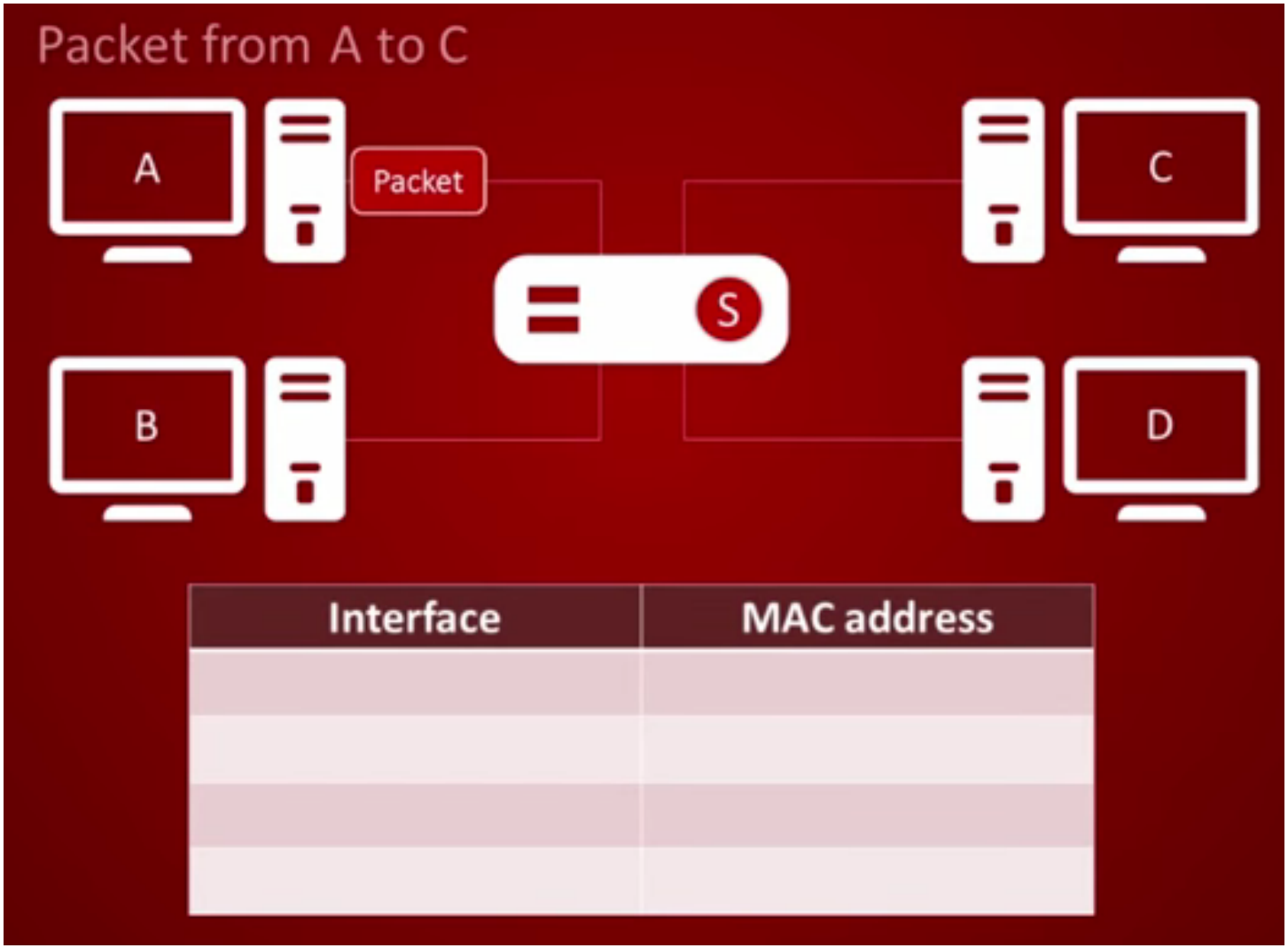
Switched Ethernet:Switch

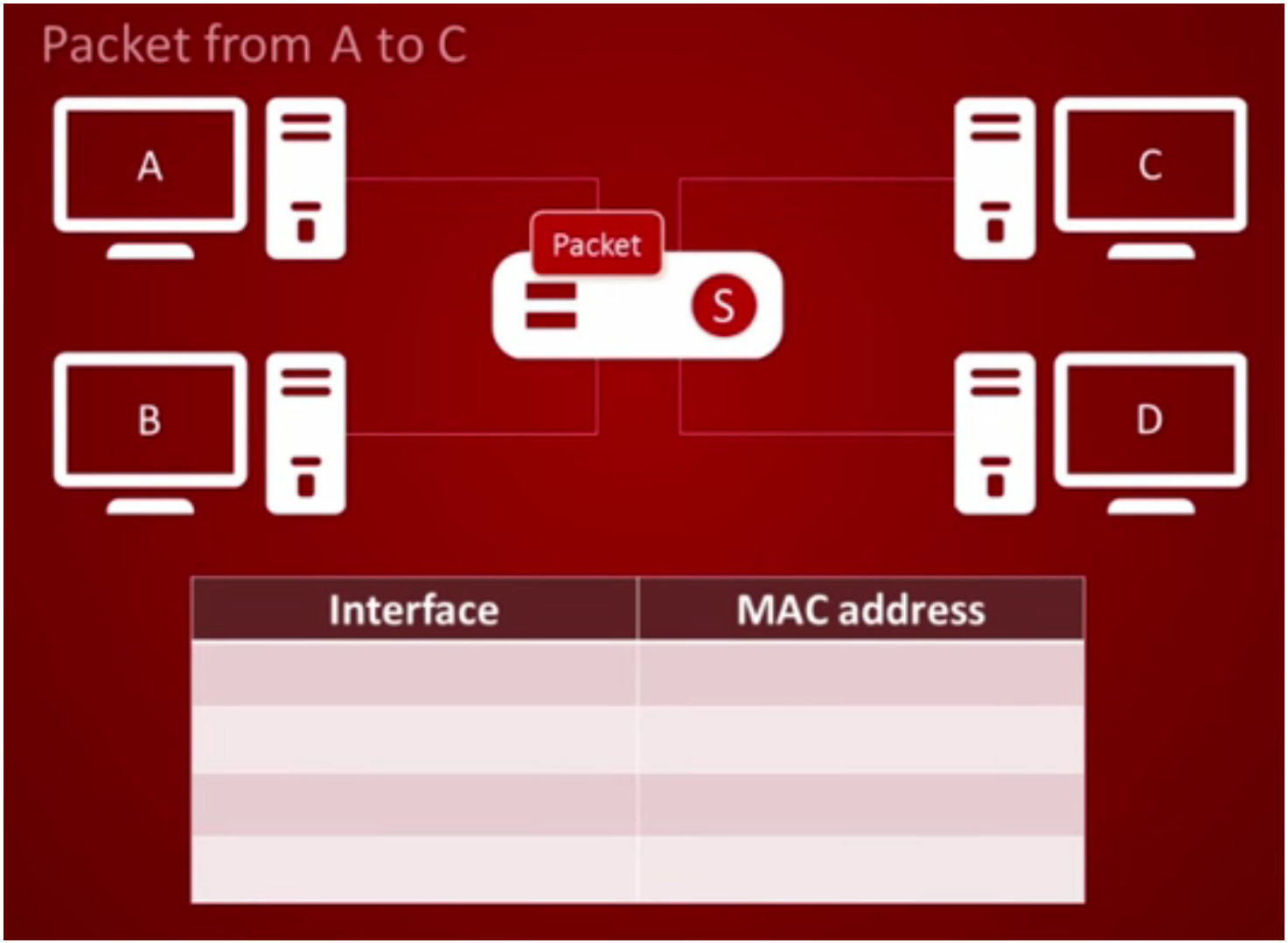


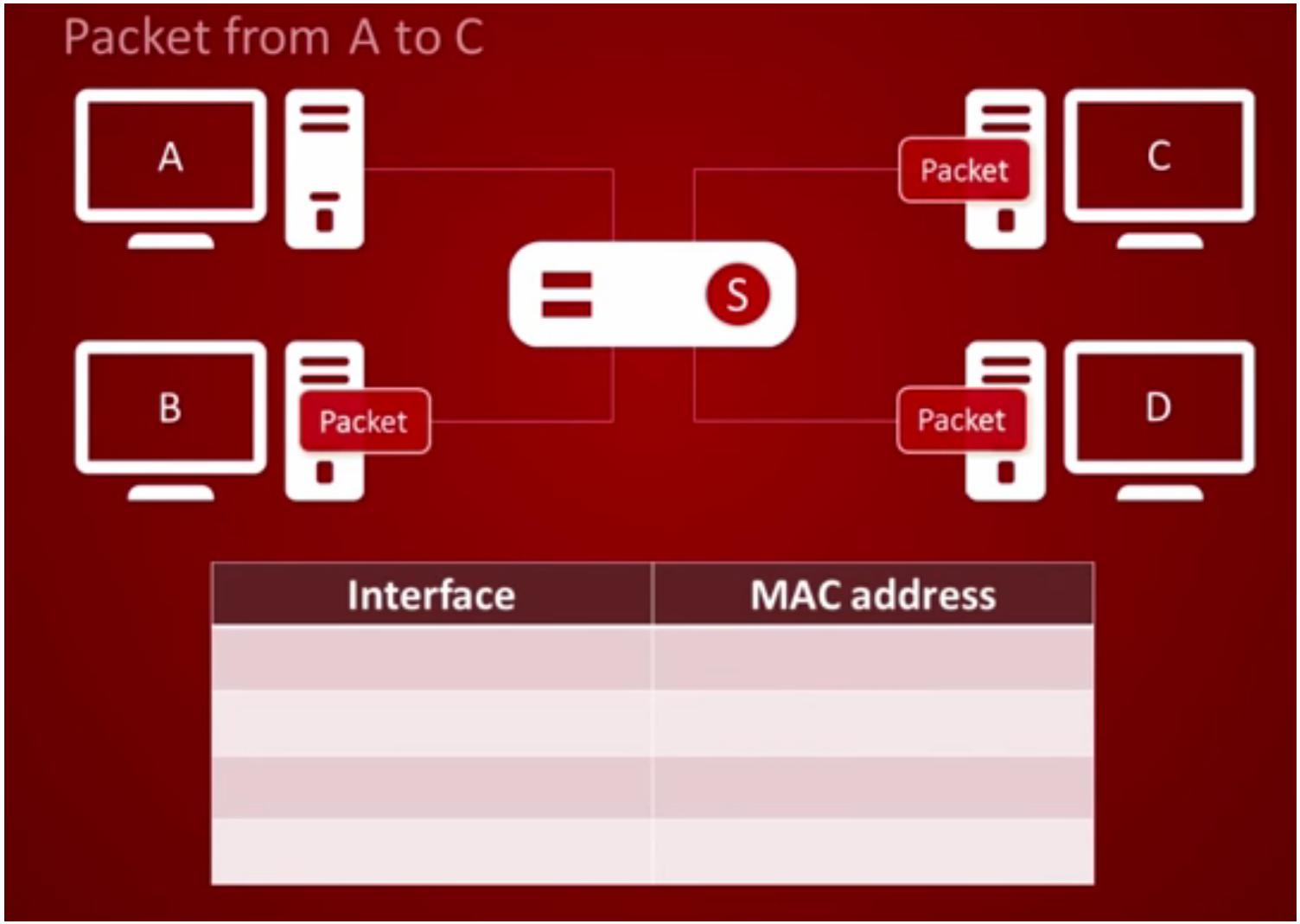


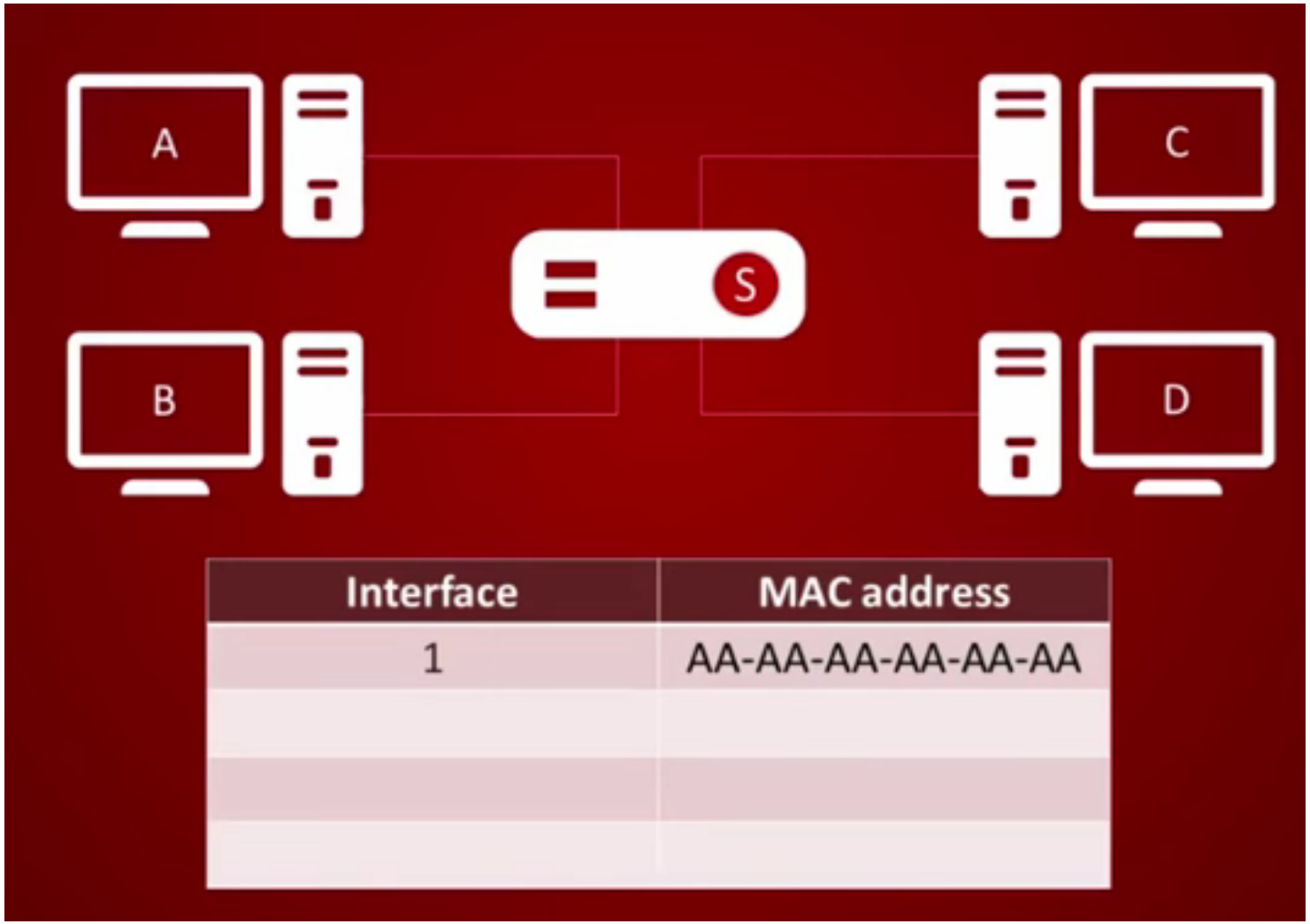
Switched Ethernet:Switch

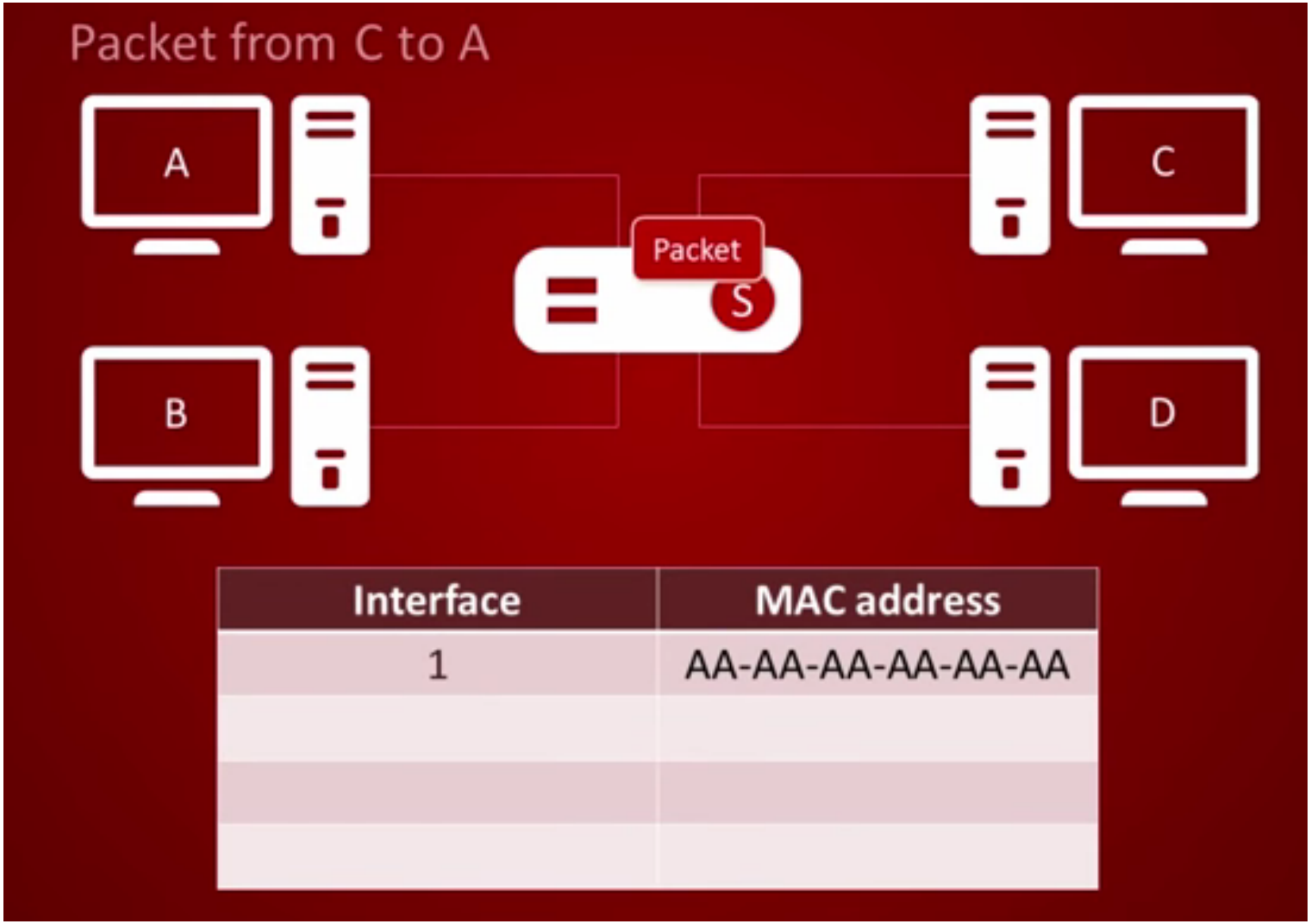


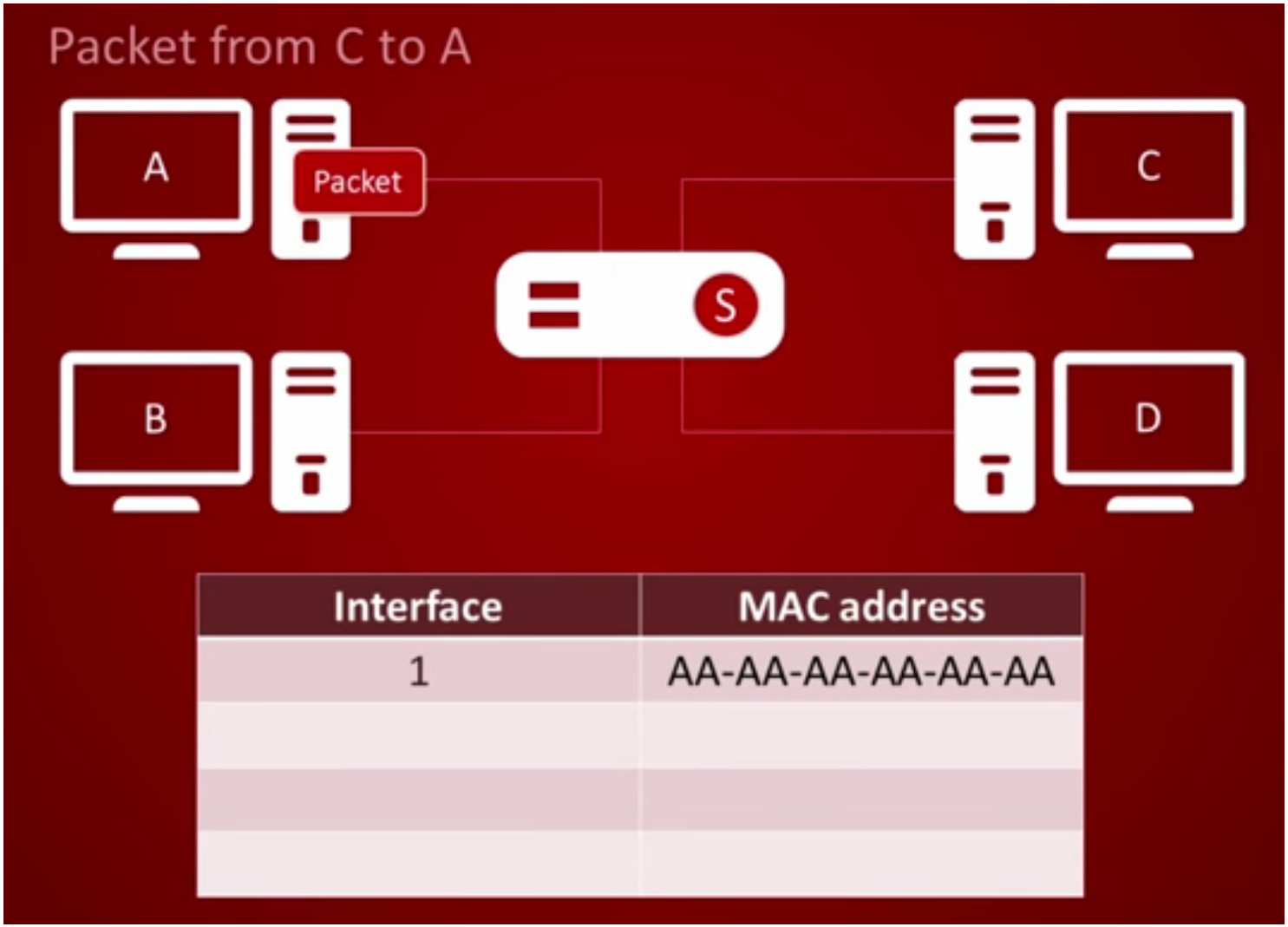

Packet from A to C
A
Packet
B
S
C
D
Interface
MAC address


Packet from A to C
A
B
C
D
Packet
S
Interface
MAC address


Packet from A to C
A
B
Packet
S
Packet
C
Packet
D
Interface
MAC address


A
B
S
C
D
Interface
MAC address
1
AA-AA-AA-AA-AA-AA


Packet from C to A
A
B
C
D
Packet
S
Interface
MAC address
1
AA-AA-AA-AA-AA-AA


Packet from C to A
A
Packet
C
S
B
D
Interface
MAC address
1
AA-AA-AA-AA-AA-AA

The End