

CCNA TECHNOLOGIES SERIES

ONLINE TRAINING CLASS – CHAPTER 01



BURMESE VERSION

Phyo Phyo Hein

B. C. Tech (hons)

MTCNA, MTCRE, MTCWE, MTCTCE, MTCUME, MTCINE

CCNA R&S, CCNP R&S, CCIP, JNCIA-Junos, JNCDA

May 15, 2017

ABOUT ME



○ Phyto Phyto Hein

- B. C. Tech (hons)
- MikroTik Certified Trainer & Consultant
- Director of Information Beam Co., Ltd.
- Experiences:
 - Cisco instructor since 2005 at i-BEAM Co., Ltd
 - SingTel Mobile Support Network Engineer at NCS Co., Ltd (2008-2010)
 - Nera Telecommunications (Singapore) (2011-2012)
 - System Integration Manager at Yatanarpon Teleport (2012-2014)
 - Enterprise/ISP Manager at Kinetic Myanmar Technology (2014-2016)
- Certifications:
 - Cisco CCNA R&S, CCNP R&S, CCIP, CCIE R&S Written
 - Juniper JNCIA-Junos, JNCDA





SWITCHING AND VLANs

What is Switching?

Layer 2/3 Switching Functions

VLANs

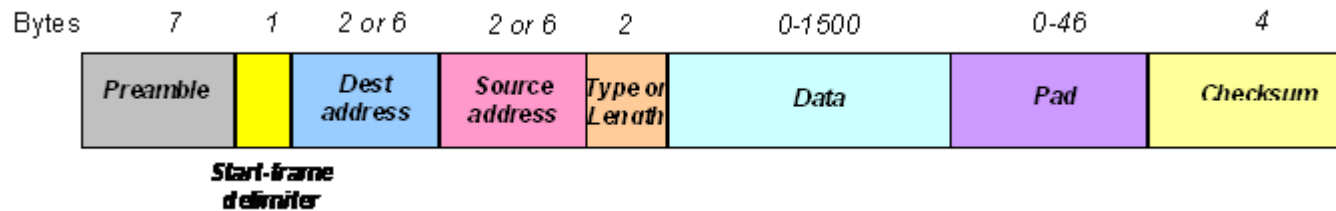
Lab 1: VLAN LAB

DATA LINK LAYER (LAYER 2)

- The communication point between Physical layer and upper layers
- Responsible to deliver the data to upper layers and send load the data from upper layers onto the physical media.
- Responsible to creating data frames and error checking (data checksum), flow control on physical link.
- There are two sub layers
 - ✓ LLC (Logical Link control) – creating frames, deliver the frames to upper layers and error checking and flow control mechanisms and encapsulating the frames
 - ✓ MAC – attach the physical layer address (L2 MAC address) into the frames and loading the frame onto the physical layer via Network Interface Card.
- Data Link Layer Protocols – Ethernet IEEE 802.3, HDLC, PPP, PPPoE and Frame-Relay, X.25, ISDN..etc
- Switches and Bridges are layer 2 devices .
- LANs and WANs Technologies are classified according to their Physical Layer transmission media and their L2 encapsulation protocol.



IEEE 802.3 ETHERNET FRAME FORMAT



- The *Preamble* consists of seven bytes all of the form 10101010, and is used by the receiver to allow it to establish bit synchronisation
- The *Start frame delimiter* is a single byte, 10101011, which is a frame flag, indicating the start of a frame.
- 48-bit (6 bytes) Destination Address
- 48-bit (6 bytes) Source Address
- The *Length/EtherType* field is the only one which differs between 802.3 and Ethernet II. In 802.3 it indicates the number of bytes of data in the frame's payload, and can be anything from 0 to 1500 bytes. Frames must be at least 64 bytes long



SWITCHING

- By Default Switches and Bridges are functioning as Layer 2 (Data Link Layer Devices)
- Bridges are software based and Switches are Hardware based.
- They have the intelligence of keeping MAC Address (Layer 2 Physical Address) Table.
- Both Switches and Bridges can still forward Layer 2 Broadcast Address.
- They cannot manage the broadcast domain (the area which can receive the broadcast frames).

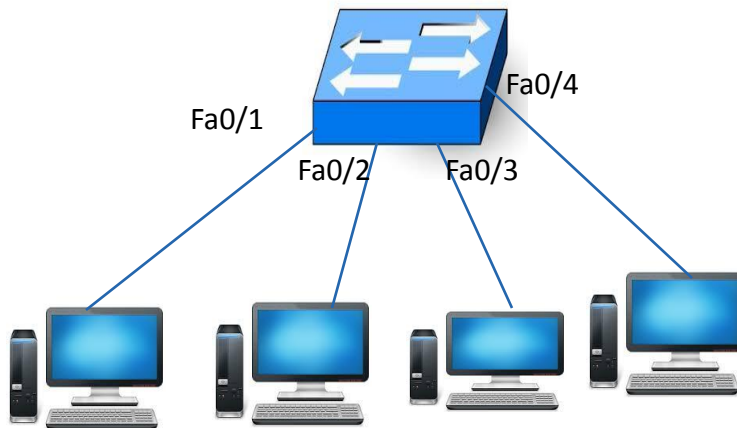


SWITCHING CONTD

- Each interface ports of Switches have one collision domain (the area which data can be collide due to sharing the same media like bus topology) per each port (i.e If a switch has active interface 12 ports , the switches have 12 collision domains)
- The switches ports can operate in Full Duplex mode which can turn of CSMA/CD IEEE 802.3 Standard Feature unlike the behavior of a hub/repeater.



LAYER 2 MAC TABLE



MAC Address Table inside L2 Switch

Port	Vlans	MAC
0/1	1	001c-ac92-12a5
0/2	1	001c-1233-ab97
0/3	1	002d-1265-a2af
0/4	1	0935-62a1-120F



CSMA/CD

- Carrier Sense Multiple Access/Collision Detection
 - IEEE 802.3 Standard for Ethernet Technology to avoid the data collision on the the network
 - Three functions according to the name
 - Carrier Sense : the host node on the network listens on the shared medium if the line is free or busy.
 - Multiple Access : Multiple Devices can access the shared medium once free
 - Collision Detection :When two host nodes send the data on the shared medium simultaneously, the collision will occur. Then the two sending nodes receive a notification signal that alarm the collision. They stop sending data and wait random period of time by setting a timer and counting down the timer. Once the timer count down to zero, the host node can resend the data by using CSMA/CD again.

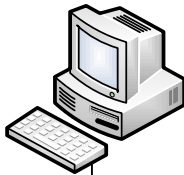


CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION

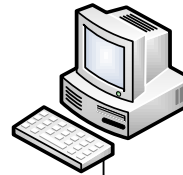
Carrier Sense

Host A is checking the medium is free or not

Host A

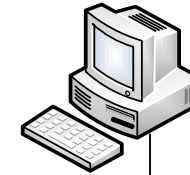


Host B

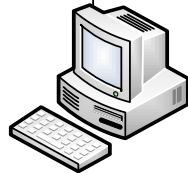


Host C is checking the medium is free or not

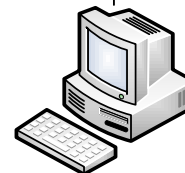
Host C



Host D

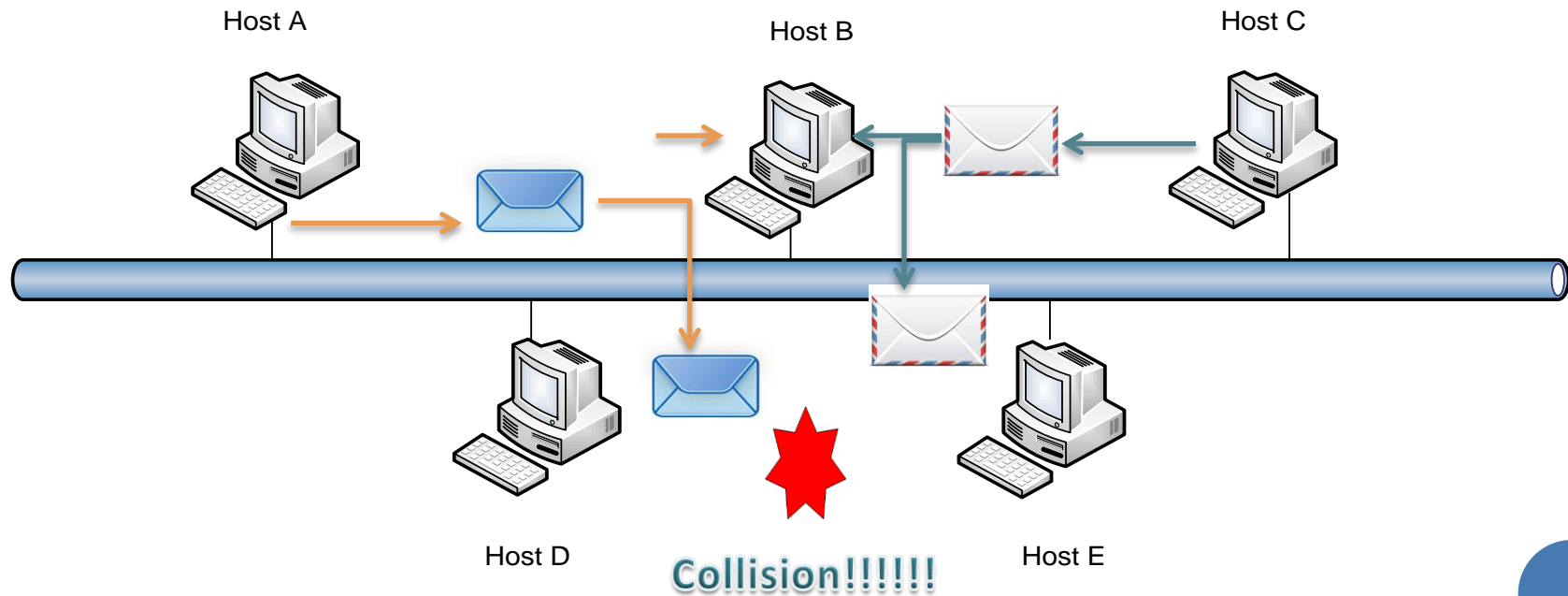


Host E



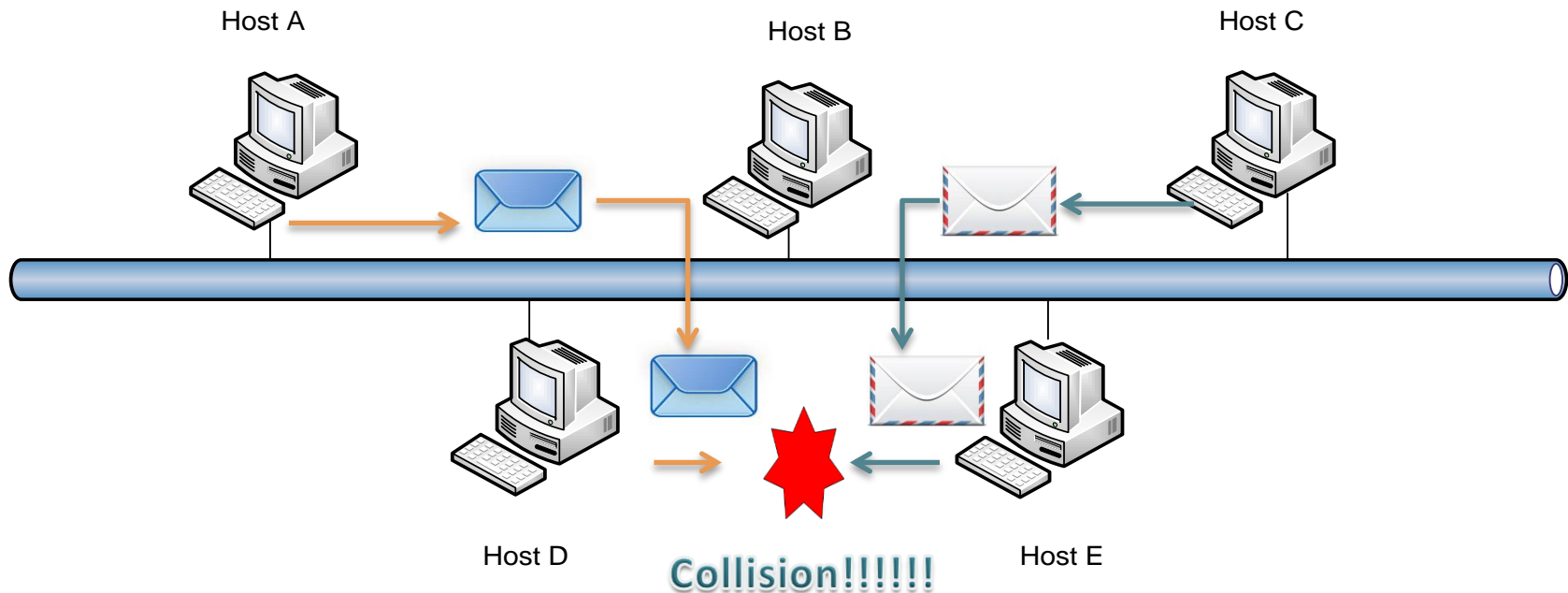
CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION

Multiple Access with Collision Detection

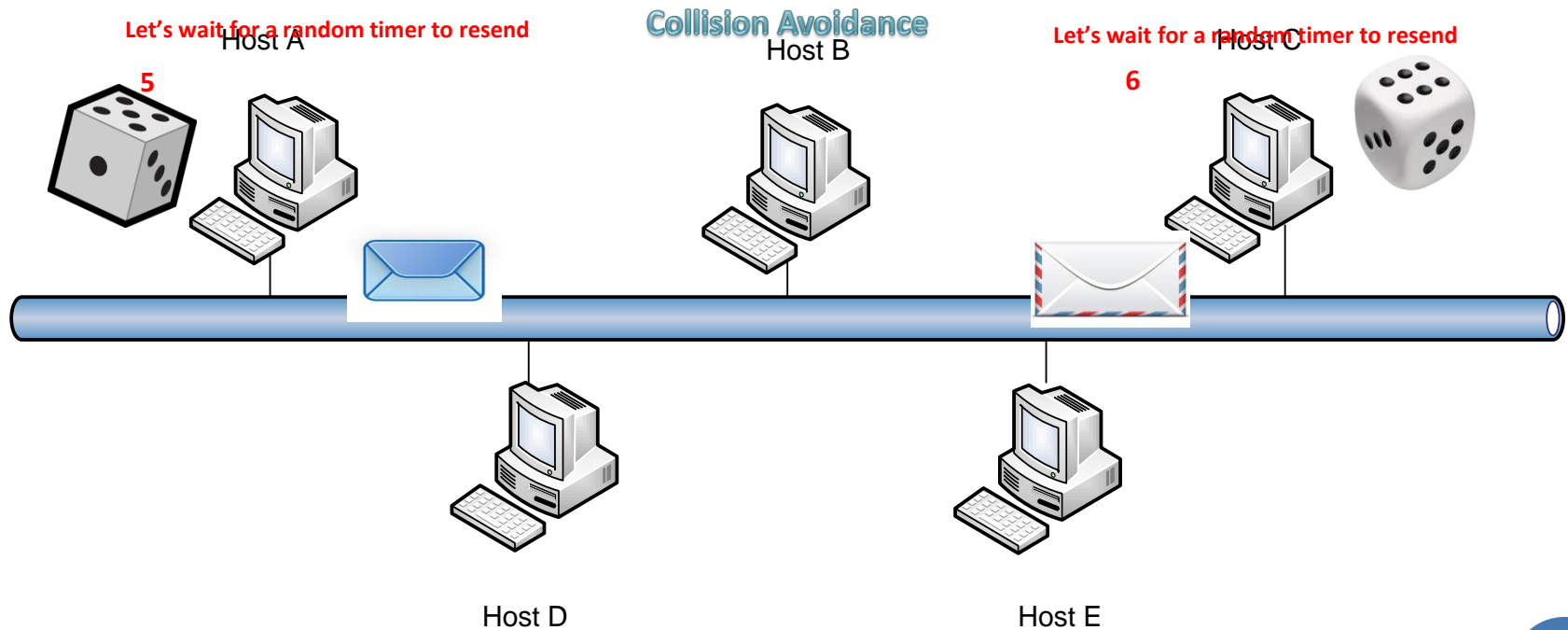


CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION

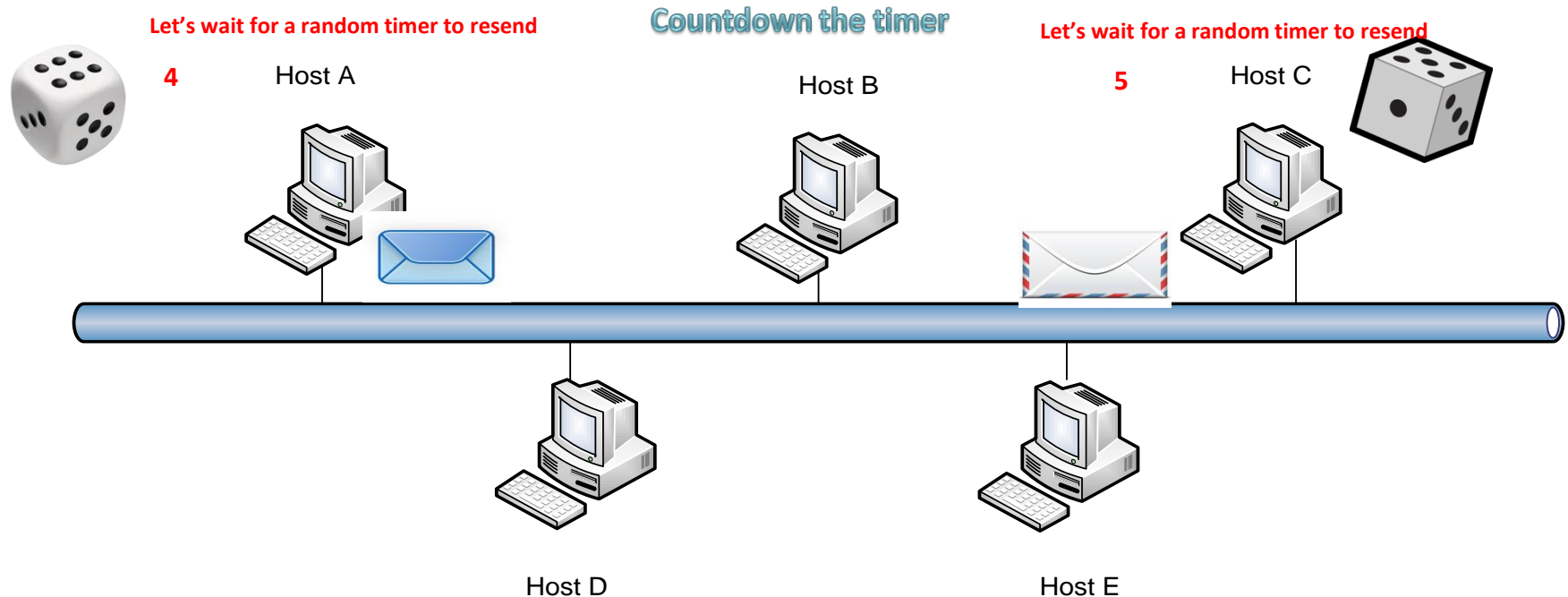
Back off



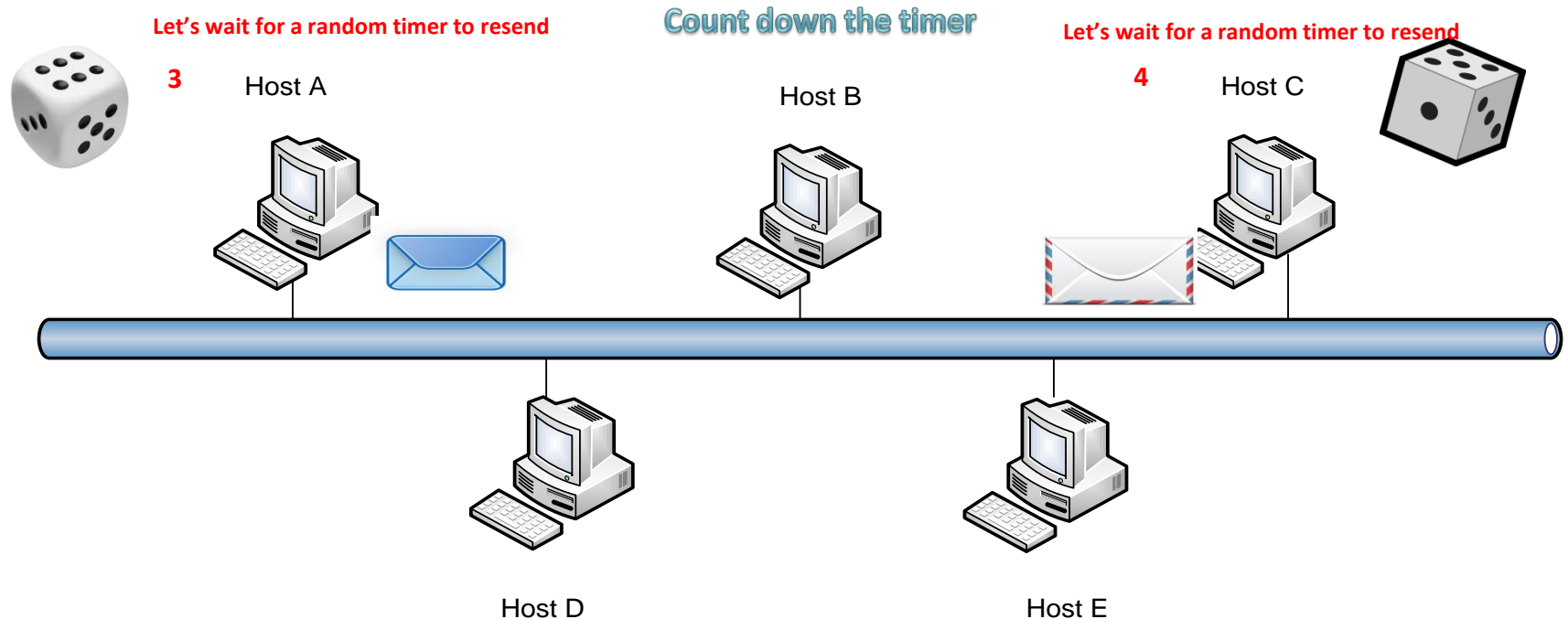
CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION



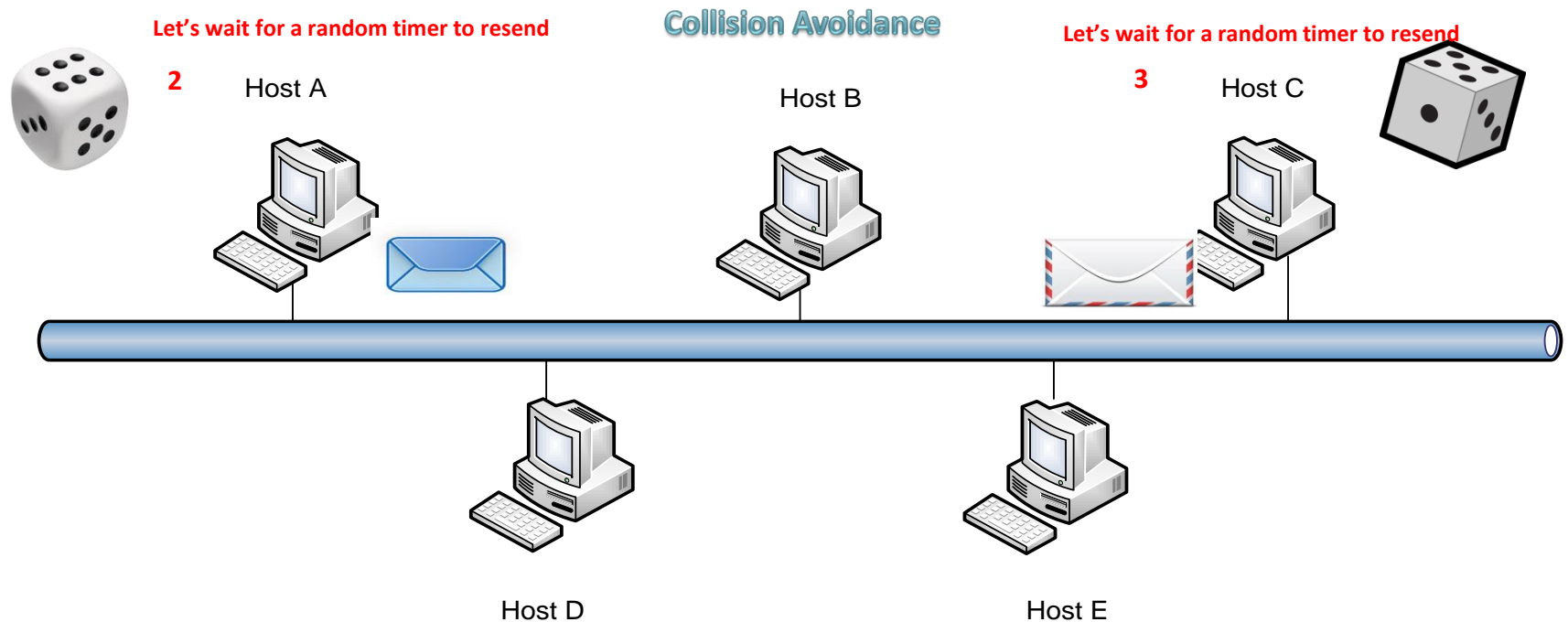
CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION



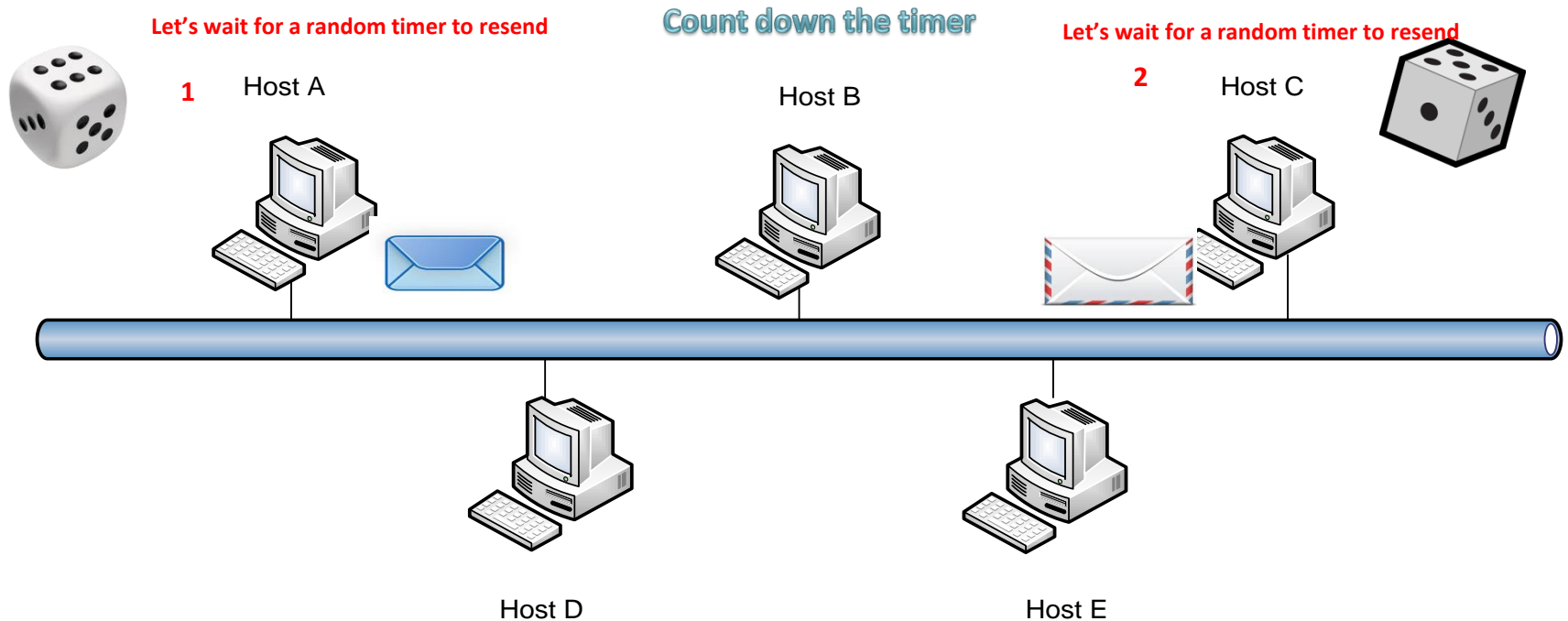
CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION



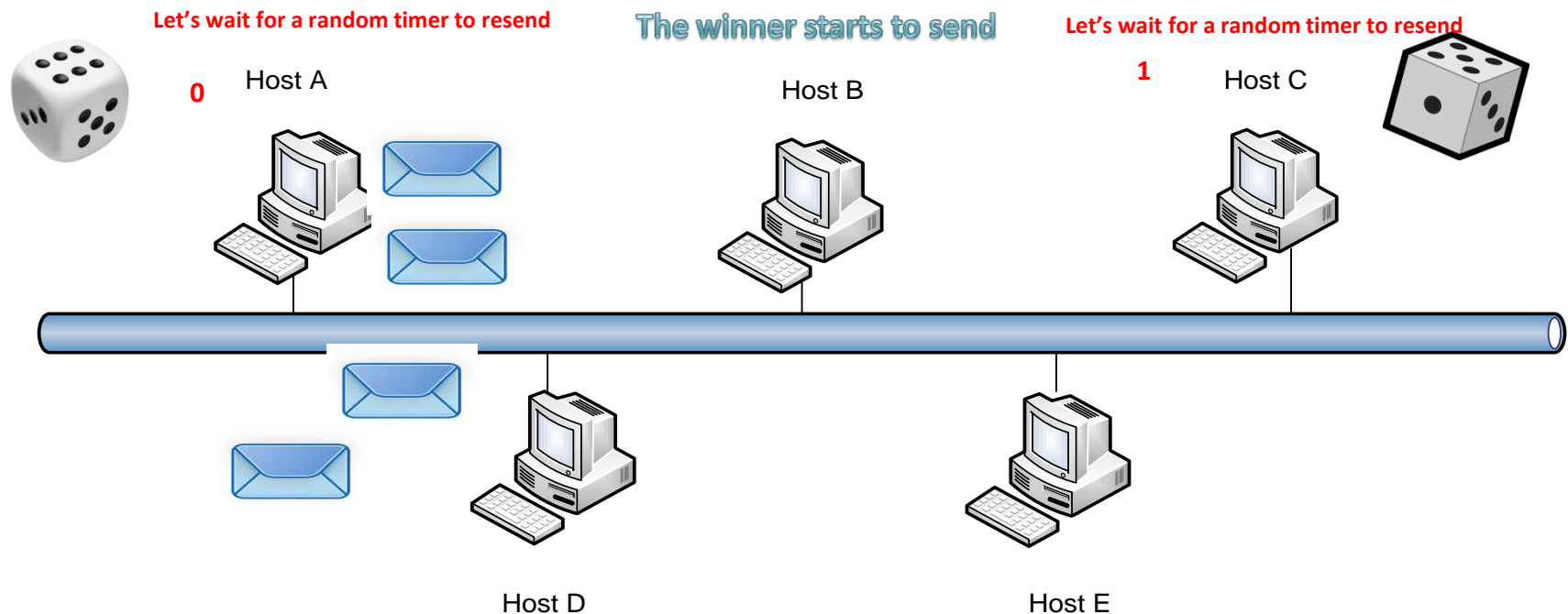
CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE



CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION



CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION



CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECTION

The CSMA/CD circle begins at Host C again

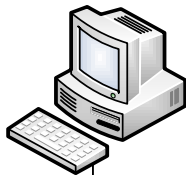
Host A might be sending or finish sending

Host C needs to wait again until the line is free again and then send the data

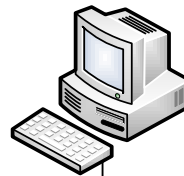


0

Host A

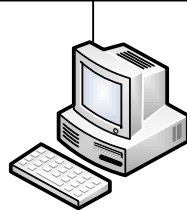
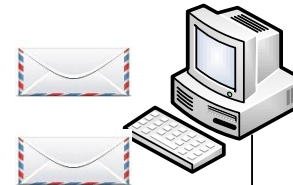


Host B

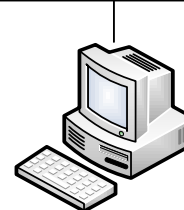


0

Host C



Host D



Host E



SWITCHING FUNCTIONS

○ Address Learning

- MAC-Table is empty when it is firstly turned on.
- When a host is sending a frame to destination, it records the source MAC address in MAC Table
- It sends the broadcast frames (FF:FF:FF:FF:FF:FF) flooding to look for the destination address.
- The destination host which is hearing the broadcast reply the MAC address and record it in the MAC Table.



SWITCHING FUNCTIONS

○ Forwarding

- When a host is sending to a destination , it looks up the MAC table to know the exact location of the destination hosts.
- If MAC Table has the destination host MAC address, it forwarded it.

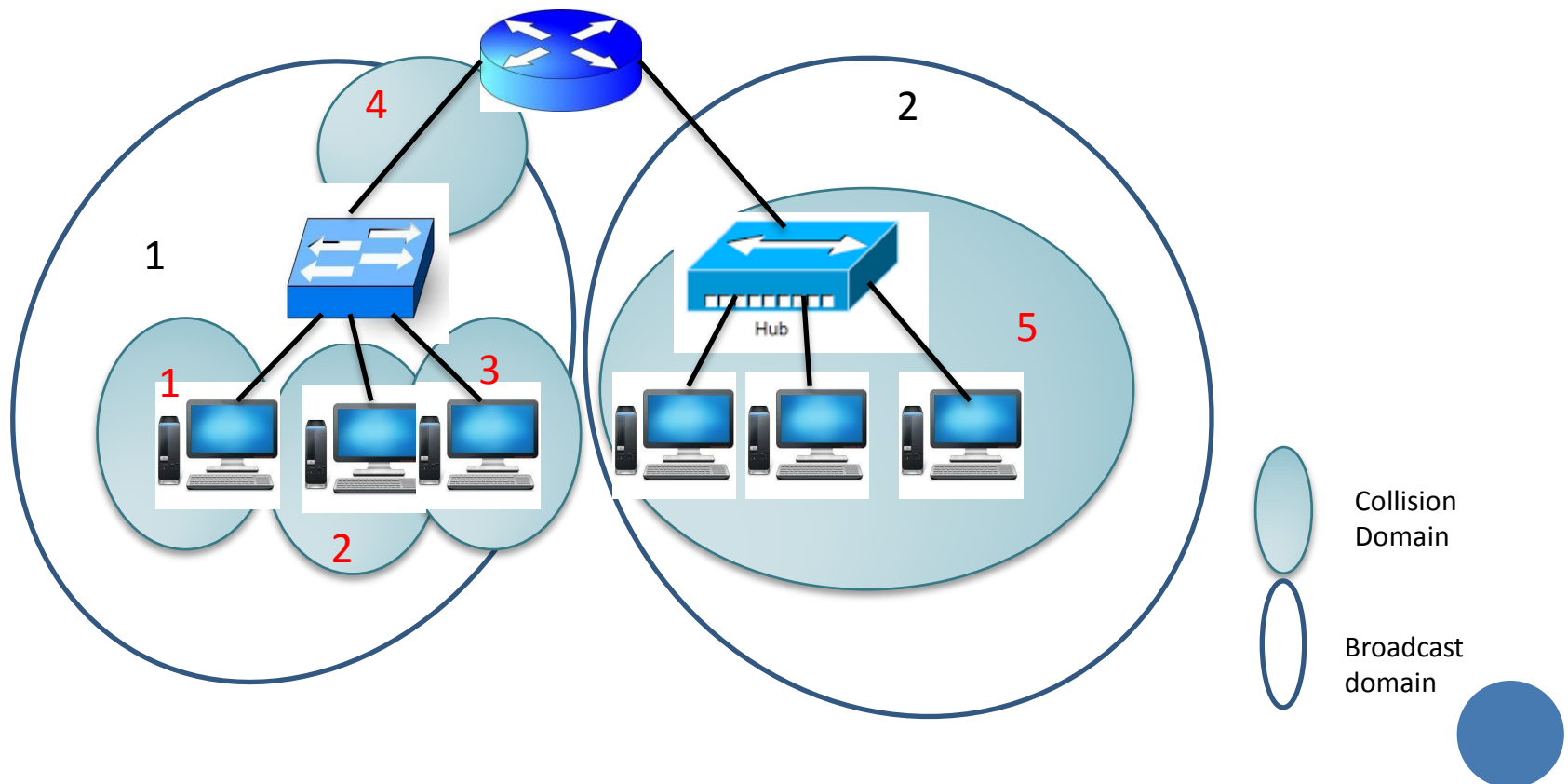
○ Loop Avoidance

- If there is the redundant physical link, it will help to have redundancy but It can cause Layer 2 Broadcast loop and Unicast Flooding.
- To avoid the Layer 2 Loop, Spanning Tree Protocol is the solution for solving the loop issue.



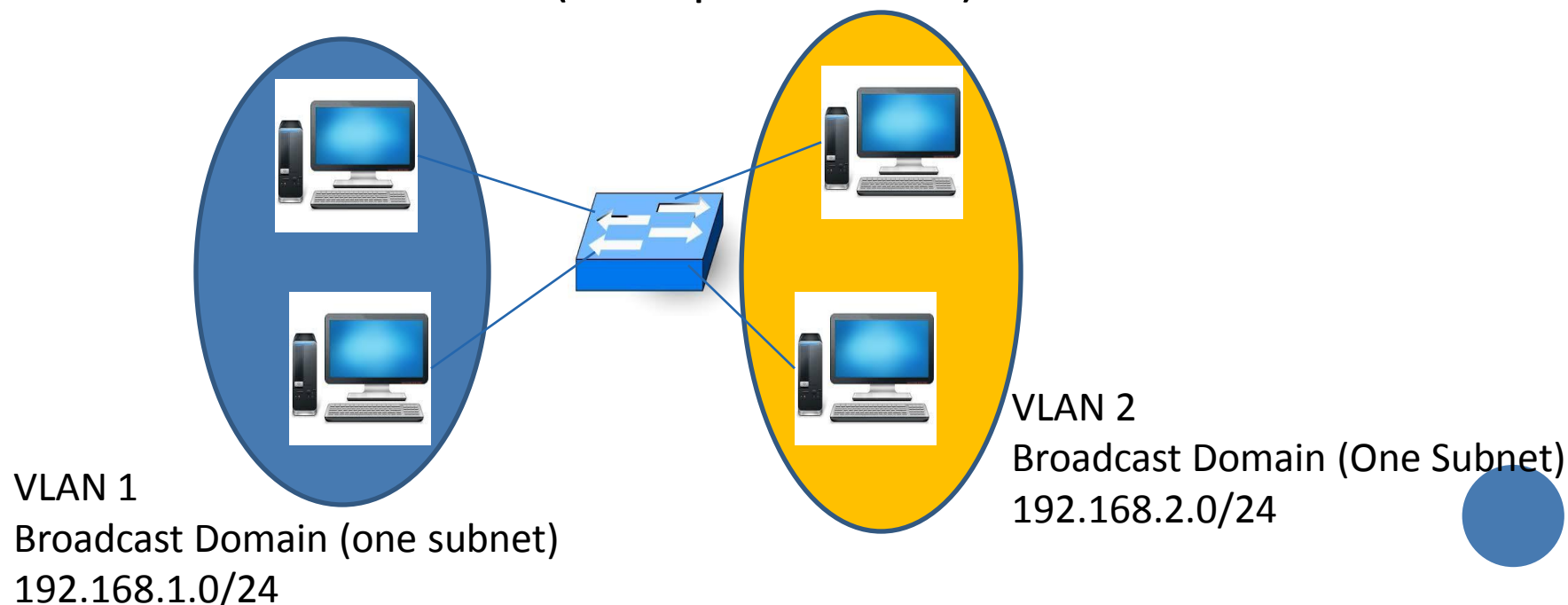
HOW MANY COLLISION DOMAINS AND BROADCAST DOMAINS

5 collision domains and 2 broadcast domains



VIRTUAL LOCAL AREA NETWORK

- LAN means one Single Broadcast Domain.
- By default the Switches have only one LAN.
- Creating Multiple VLANs in Switches means Multiple Broadcast Domains (Multiple Subnets) in Switches.



BENEFITS OF VLANs

- To reduce CPU overhead on each device by reducing the number of devices that receive
- each broadcast frame
- To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood (broadcasts, multicasts, and unknown unicasts)
- To improve security for hosts that send sensitive data by keeping those hosts on a separate VLAN



BENEFITS OF VLANS CONT'D

- To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
- To solve problems more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain
- To reduce the workload for the Spanning Tree Protocol (STP) by limiting a VLAN to a single access switch



ACCESS PORTS AND TRUNK PORTS

○ Access Ports

- Belong to only one single VLAN except for voice VLAN
- Single Access Port can belong to two vlans : Data VLAN and VOICE VLANs in Cisco switches.
- End User Device will be connected to access ports.

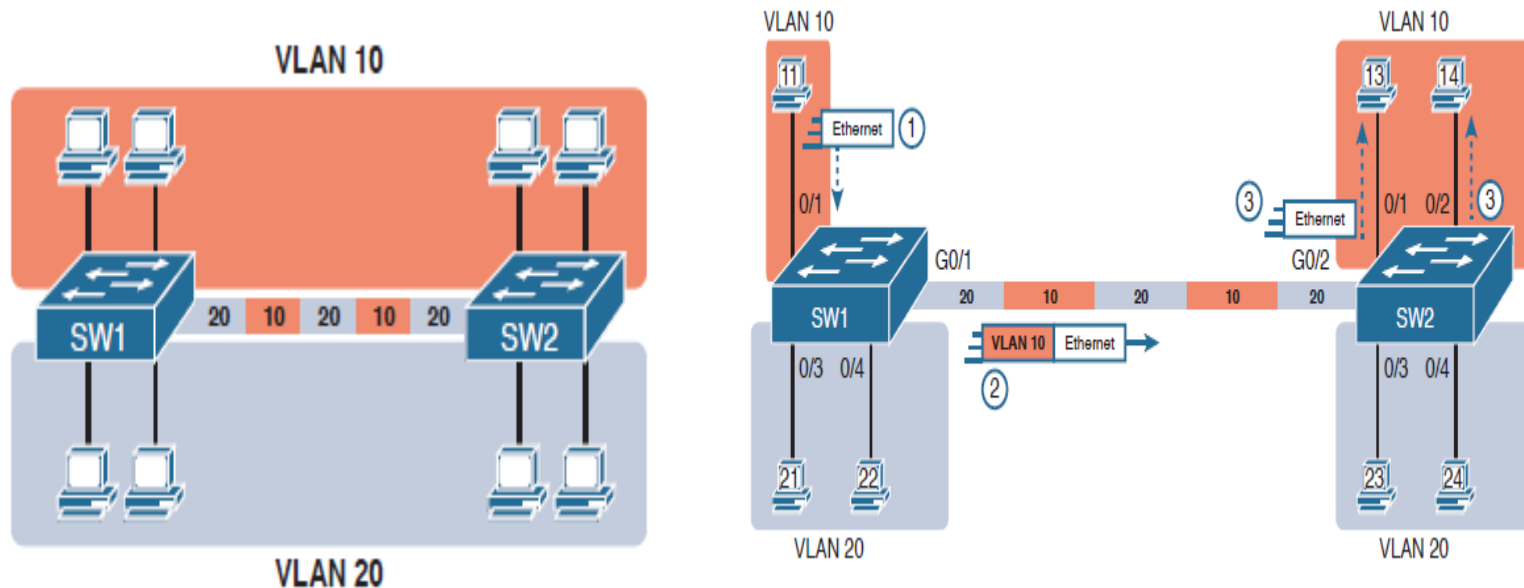
○ Trunk Ports

- The ports that can carry multiple VLANs
- By default, Cisco Switches allow all vlans on Trunk Ports
- Specific VLANs can be allowed on the trunk also.
- Switch to Switch, Switch to Router, Switch to Server



VLAN TAGGING

- VLANs need to be marked (flagged/tagged) on Trunk link so that where the traffic will go to which vlan.



VLAN TAGGING METHOD ENCAPSULATION PROTOCOLS



- There are two VLAN tagging Encapsulation Protocols
 - ISL (Cisco Proprietary)
 - IEEE 802.1Q
- ISL – Cisco Proprietary Encapsulation Protocol
 - Nowadays Cisco no longer use this protocol in new IOS.
 - They support 802.1Q Trunking Protocol only.
- IEEE802.1Q (Dot1q)
 - Inserts an extra 4-byte 802.1Q VLAN header into the original frame's Ethernet header
 - Out of 4 byte – 12 bits are for VLAN ID.
 - $2^{12} = 4096$, Therefore Total VLAN (0-4095) will be able to exist in a switch.



802.1Q TRUNKING PROTOCOL

Preamble	Destination MAC address	Source MAC address	Type	PayLoad	CRC/FCS
----------	-------------------------------	--------------------------	------	---------	---------

Preamble	Destination MAC address	Source MAC address	802.1Q header (VLAN ID)	Type	PayLoad	Recalculated field CRC/FCS
----------	-------------------------------	--------------------------	--	------	---------	----------------------------------

Insertion of 802.1Q Tag (VLAN ID) in Ethernet-II frame



DYNAMIC TRUNKING PROTOCOL

- There are 4 Switchport modes
 - Access
 - Trunk
 - Dynamic Auto
 - Dynamic Desirable
- DTP auto negotiates the operational status of the port with the other end of the ports.



DYNAMIC TRUNKING PROTOCOL

	Access	Trunk	Dynamic Auto	Dynamic Desirable
Access	Access	-	Access	Access
Trunk	-	Trunk	Trunk	Trunk
Dynamic Auto	Access	Trunk	Access	Trunk
Dynamic Desirable	Access	Trunk	Access	Trunk

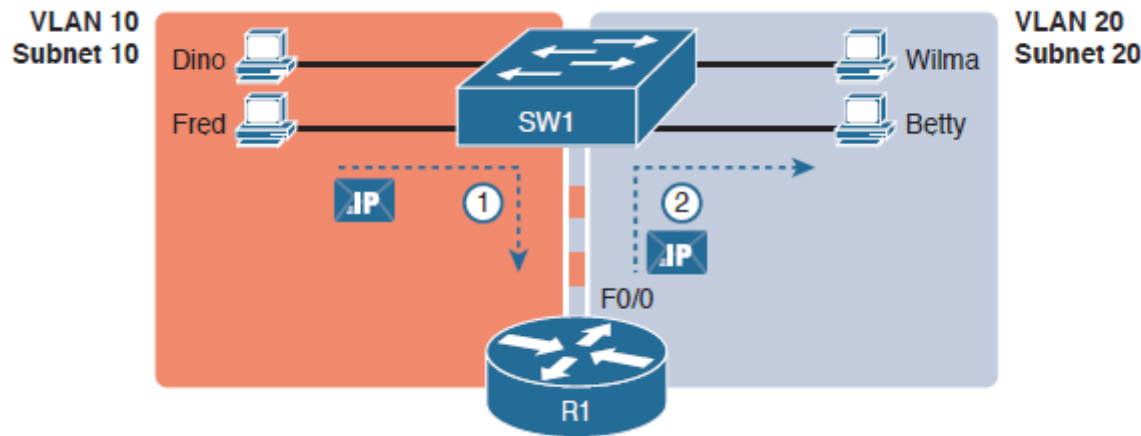


INTERVLAN ROUTING

- For Routing between two VLANs
- By default, hosts between same VLAN only can communicate each other.
- For going to other VLANs, We need to route between VLANs with a Layer 3 Device either a Router or a Multilayer (L3 Switch).
- There are two methos
 - Router on a Stick
 - Switch Virtual Interface



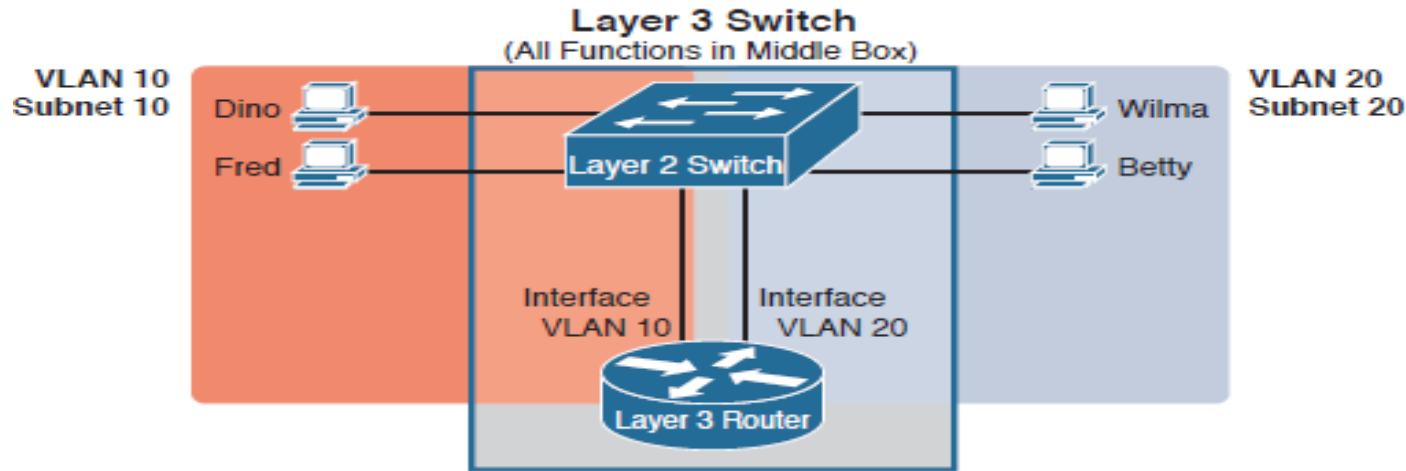
ROUTER ON A STICK



- The Switch is connected with single router interface
- The router port needs to support 802.1q protocol so that it can route multiple vlan traffic.
- Create Sub-interfaces on the interface
- Encapsulation dot1q <vlan-id>



SVI



- Create Multiple Logical VLAN Interface on Layer 3 Switches.
- Set IP on this interface
- Enable IP Routing on Layer 3 Switches.
- Route the traffic between the vlans by setting the gateway ip of SVI interface in the end devices



CREATING VLAN

- Switch> enable
- Switch# configure terminal
- Switch(config)# vlan 2
- Switch(config-vlan)# name Marketing



ASSING THE VLAN ID ON ACCESS PORT

- Switch(config)# interface fa0/1
- Switch(config-if)# switchport mode access
- Switch(config-if)#switchport access vlan 2



TRUNK PORT CONFIGURATION

○ Manual On Mode

- Switch(config)# interface gig0/1
- Switch(config-if)#switchport trunk encapsulation dot1q
- Switch(config-if)#switchport mode trunk

○ Dyanmic Auto

- Switch(config)# interface gig0/1
- Switch(config-if)#switchport mode dynamic auto

○ Dynamic Desirable

- Switch(config)# interface gig0/1
- Switch(config-if)#switchport mode dynamic desirable



VLAN VERIFICATION COMMANDS

- Verify VLAN information
 - Show vlan brief
- Verify VLAN Trunking information
 - show interface trunk
 - Show interface gig0/1 switchport

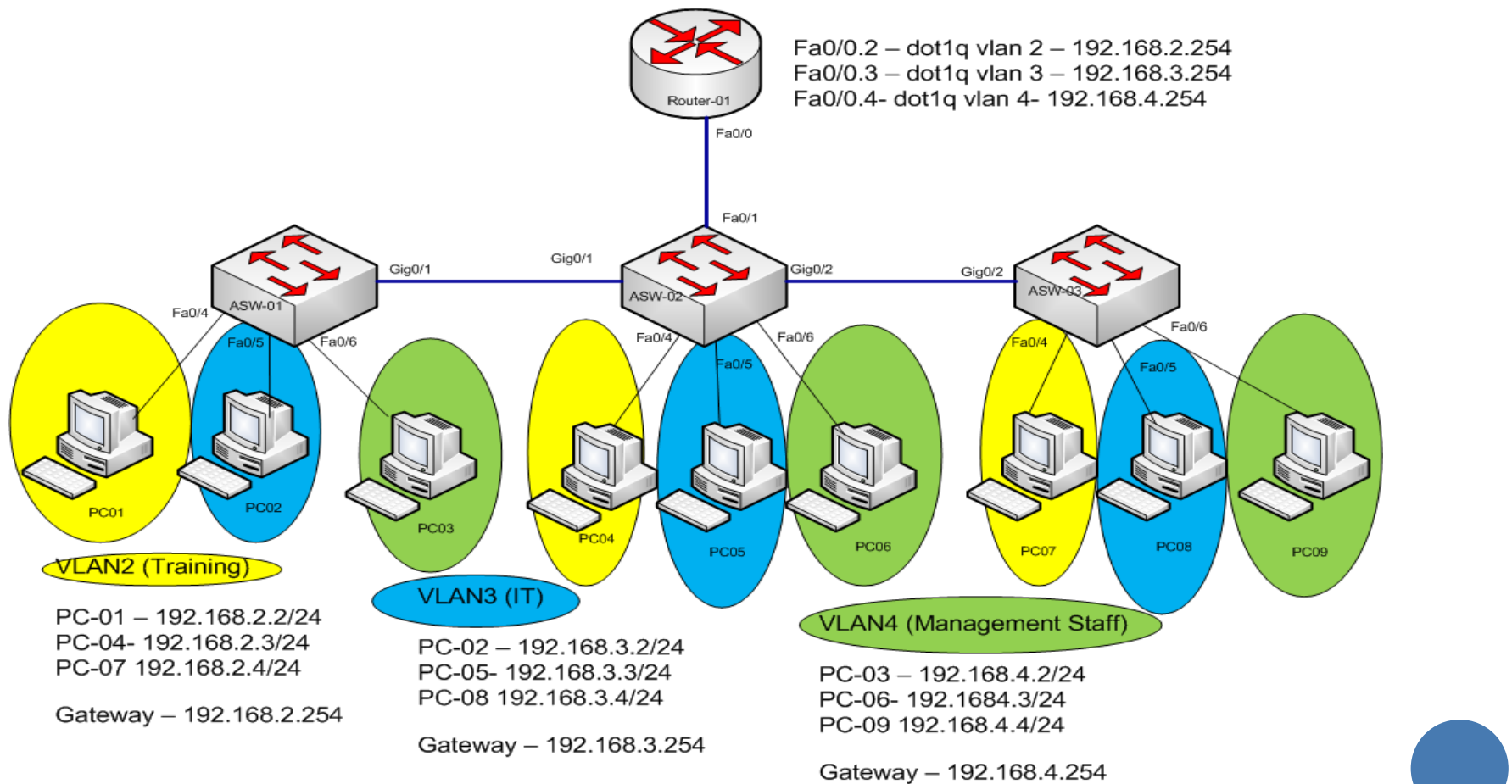


ROUTER ON A STICK CONFIGURATION

- Router(config)# interface fa0/0
- Router (config-if)#no shut
- Router (config-if)# interface fa0/0.2
- Router(config-subif)#encapsulation dot1q 2
- Router(config-subif)#ip address 192.168.2.254
255.255.255.0



LAB: VLAN



ASK QUESTIONS?



- Comment on this training video
- YouTube Channel: **Information Beam**
 - Subscribe our channel to get the latest update!
- Post in social networks
 - Information Beam Facebook Group:
<https://www.facebook.com/groups/1481854632142914/>
- Send me an email directly
 - phyo@informationbeam.net





TO BE CONTINUED...

THANKS FOR YOUR ATTENTION!

Contact Me

phyo@informationbeam.net

Skype: pphein82