Layer 2
Ethernet and Wi-Fi (802.11)

Fundamentos de Redes

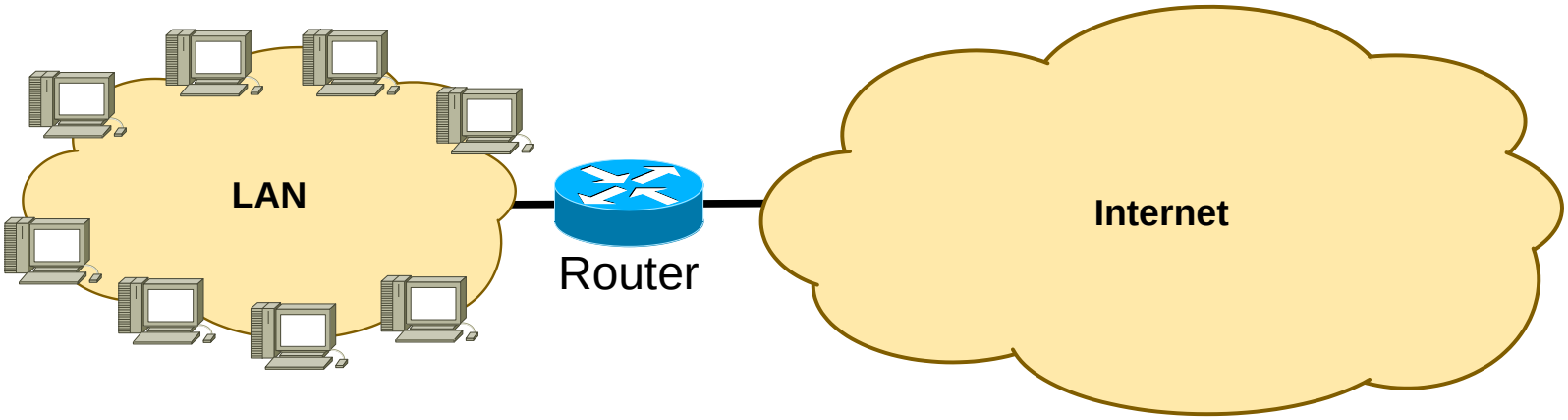
Mestrado Integrado em
Engenharia de Computadores e Telemática
DETI-UA

universidade de aveiro
deti.ua.pt

Local Area Network (LAN)

- Is a computer network within a small geographical area.
  - Home, school, room, office building or group of buildings.
- Is composed of inter-connected hosts capable of accessing and sharing data, network resources and Internet access.
  - Host refers generically to a PC, server, or any other terminal.
- Technologies
  - Current: Ethernet, 802.11 (Wi-Fi)

    Legacy: Token Ring, FDDI, …

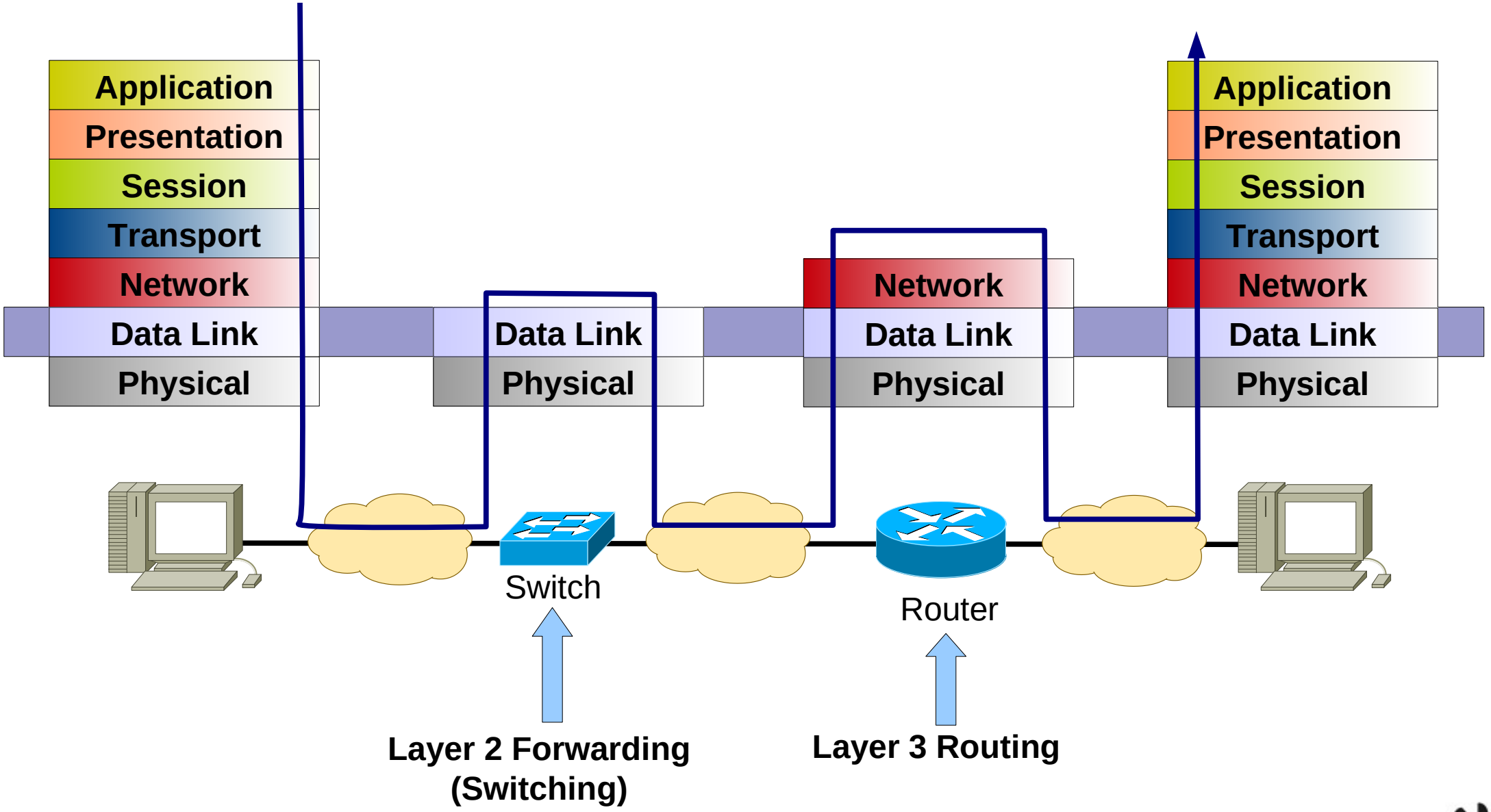


Ethernet

Ethernet (802.3)

- Most successful LAN technology.
- Invented at Xerox Palo Alto Research Center (PARC).
- Xerox, DEC and Intel defined in 1978 the standard for Ethernet 10Mbps.
- Uses “Carrier Sense/Multiple Access” with “Collision Detect” (CSMA/CD)
  - Carrier Sense: hosts can perceive is the communication channel is being used.
  - Multiple Access: multiple host can access simultaneously
  - Collision Detect: host “listen” the communication channel while transmitting to detect transmission collisions.
    - Collision: multiple physical signals overlapping and interfering with each other.

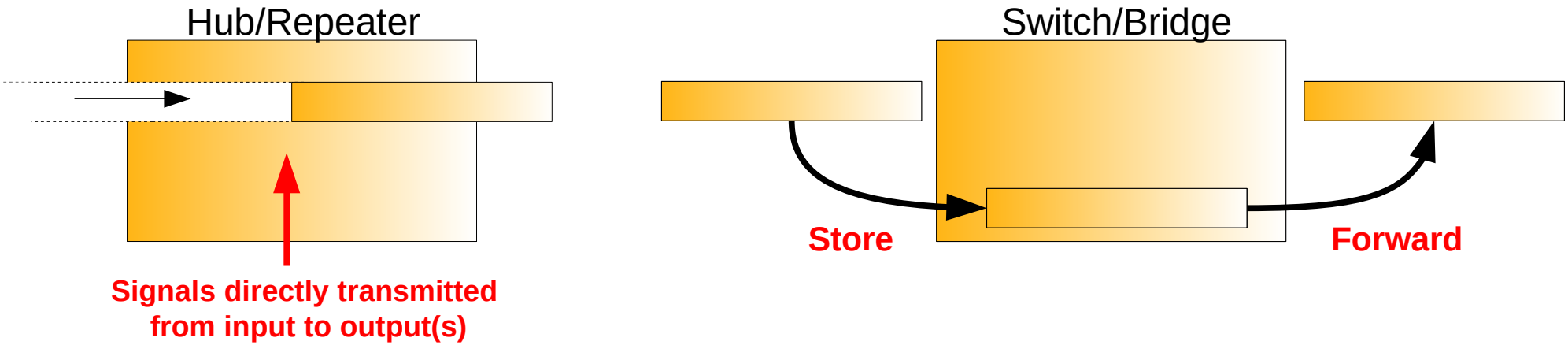
Ethernet based LAN



Ethernet Equipment

- Hub/Repeater:
  - Operates only at the physical level (OSI Layer 1).
  - Replicates and regenerates electrical signals.
  - Hub = repetidor com múltiplas portas.
  - **Não é usado nas redes locais actuais!**
- Switch/Bridge:
  - Store-and-forward operation.
  - Operates only at the data link level (OSI Layer 2).
  - Physically separates (and logically interconnects) different collision domains
    - Nowadays all Ethernet hosts are connected to a switch → There no Ethernet collision domains!
  - Forwards frames based on MAC addresses.
  - Switch = bridge with multiple ports.
- Router:
  - Store-and-forward operation.
  - Operates only at the network level (OSI Layer 3).
  - Routes packets based on network addresses (e.g., IPv4 and IPv6).

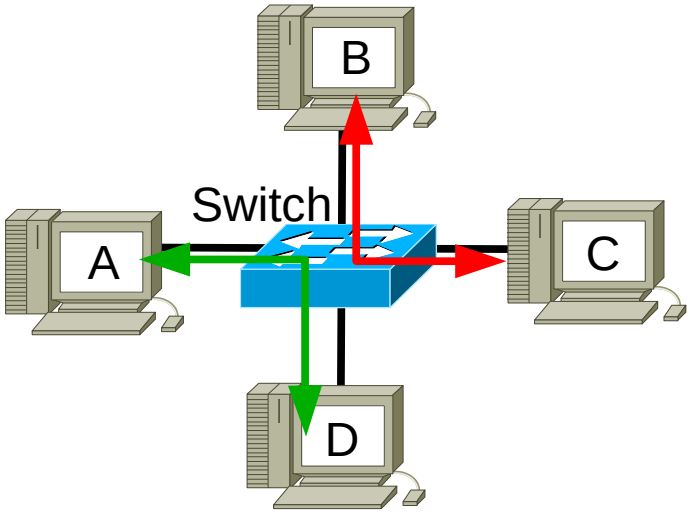
Switches/Bridges vs. Hubs/Repeaters

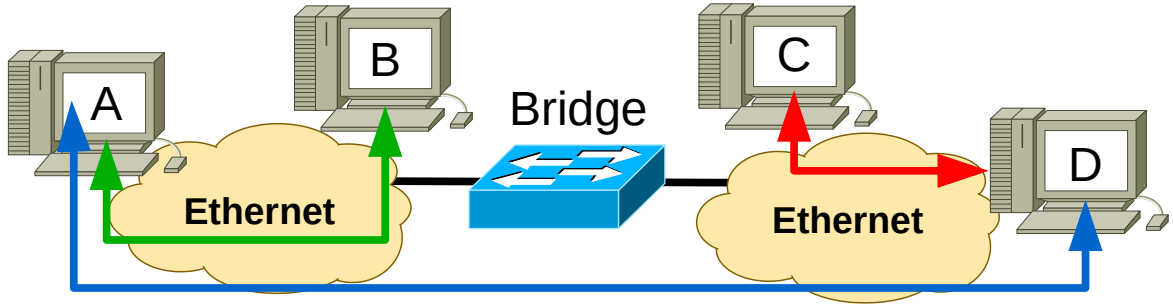


- Bridges/switches interconnect different local networks.
- Bridges/switches additional functions:
  - Store & Forward + Filtering
    - The Forwarding process decides to send a frame to a specid port based on the destination MAC address of the frame.
    - Ports may operate a different speeds.

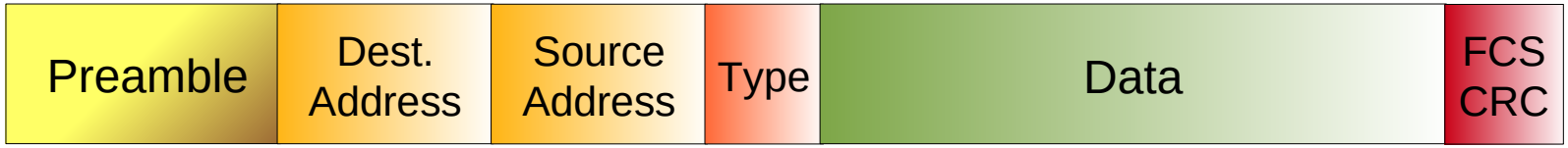
Switching

- With Switches/Bridges
  - Interconnection done at OSI Layer 2.
  - Hosts can transmit simultaneously.
  - A network of Switches is a **Broadcast Domain**
    - An Ethernet frame with destination FF:FF:FF:FF:FF:FF (Broadcast) will reach all connected switches and hosts.





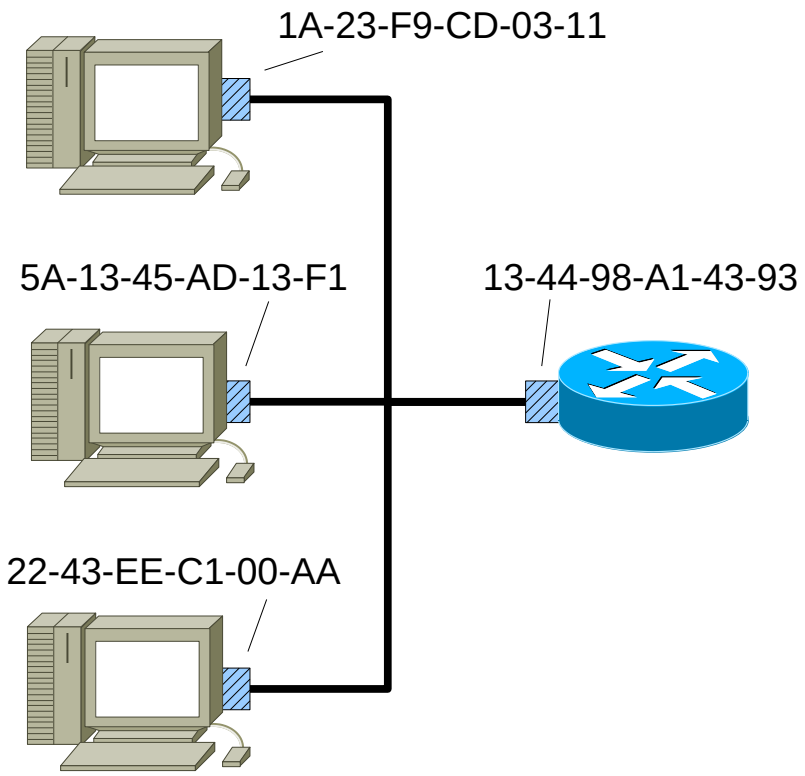
Ethernet Frame



- The sender's network card encapsulates an IP datagrama (or any other network protocol) in an Ethernet frame.
- Preamble:
  - 7 bytes with pattern 10101010 followed by one byte with pattern10101011.
  - Used to sincronize the sending and receiving clocks.
- Destination and Source addresses: 6 bytes Physical (MAC) address
  - If the network card receives a frame with destination equal to its own address or its the broadcast address, it will pass data to the network level process.
  - If not, drops the frame.
- Type defines which protocol is encapsulated in the frame (usually IPv4 or IPV6).
- The frame check sequence (FCS) is a four-octet cyclic redundancy check (CRC) that allows detection of corrupted data within the entire frame as received on the receiver side.

MAC Addresses

- MAC (Physical, Ethernet or LAN) Address:
  - Function: Allow the exchange of data between network interfaces connected using a Layer 2 network.
  - Have 6 bytes/48 bits.
  - Are unique.
  - Each network card has its own address.
  - Defined by manufacturer
    - Some hardware allows change.
    - First 24-, 28-, or 36-bits assign to manufacturer.
  - Hexadecimal notation
    - Broadcast: FF-FF-FF-FF-FF-FF



Ethernet Frame Minimum Size

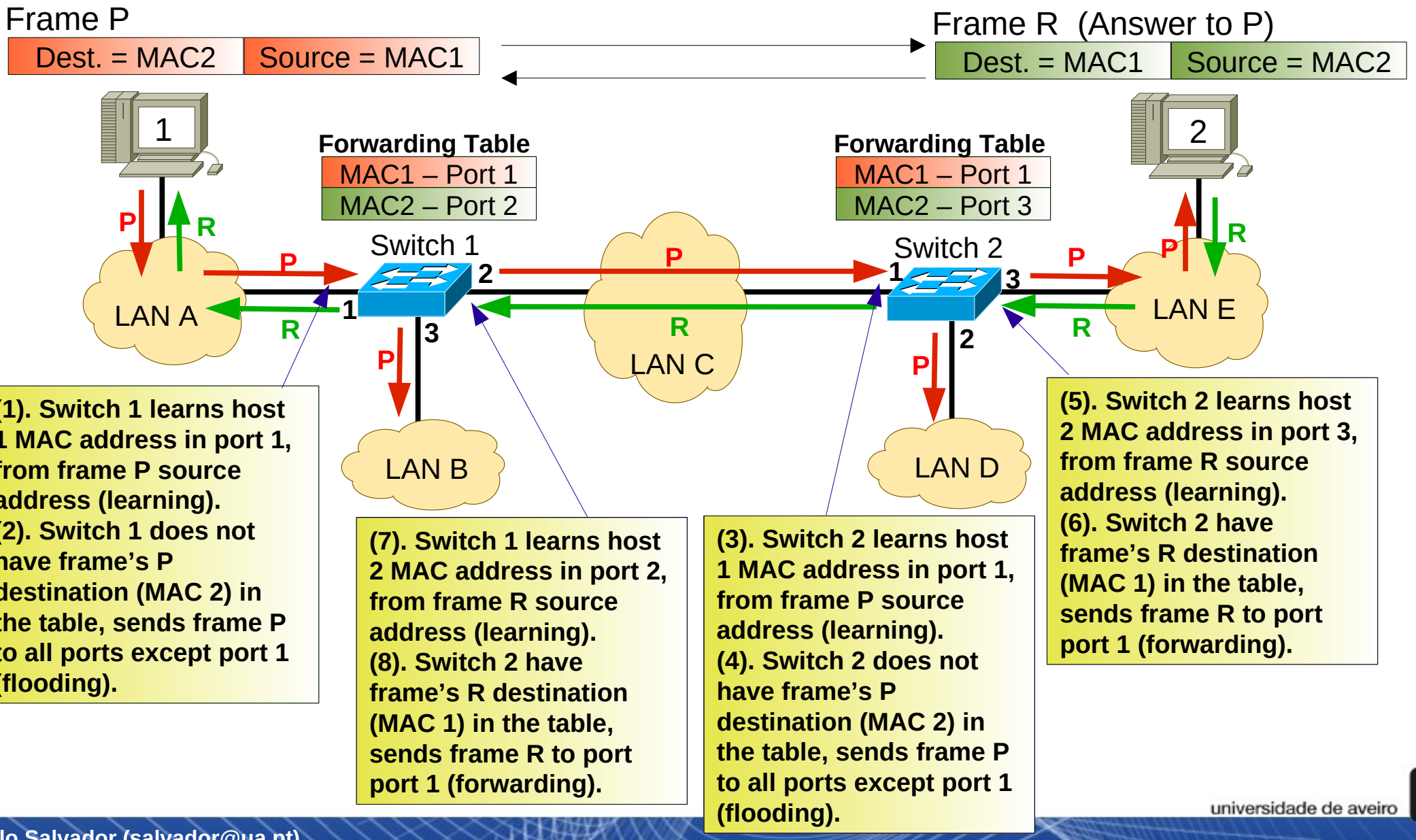
- Historically there were Ethernet technologies that allowed collisions and a collision detection mechanism had to be present (CSMA/CD).
- Depending on the technology and maximum cable size, the Ethernet frame had to be big enough to allow the collision detection mechanism to detect a frame being transmitted before the last frame byte leaving the source host.
- By legacy (it is possible to merge different Ethernet technologies) the **minimum frame size is 64 bytes**.
- If the frame's header plus data do not reach 64 bytes, a set of zeros must be added to the end of the frame to reach 64 bytes.
  - This is called **padding**.

Switches Basic Operations

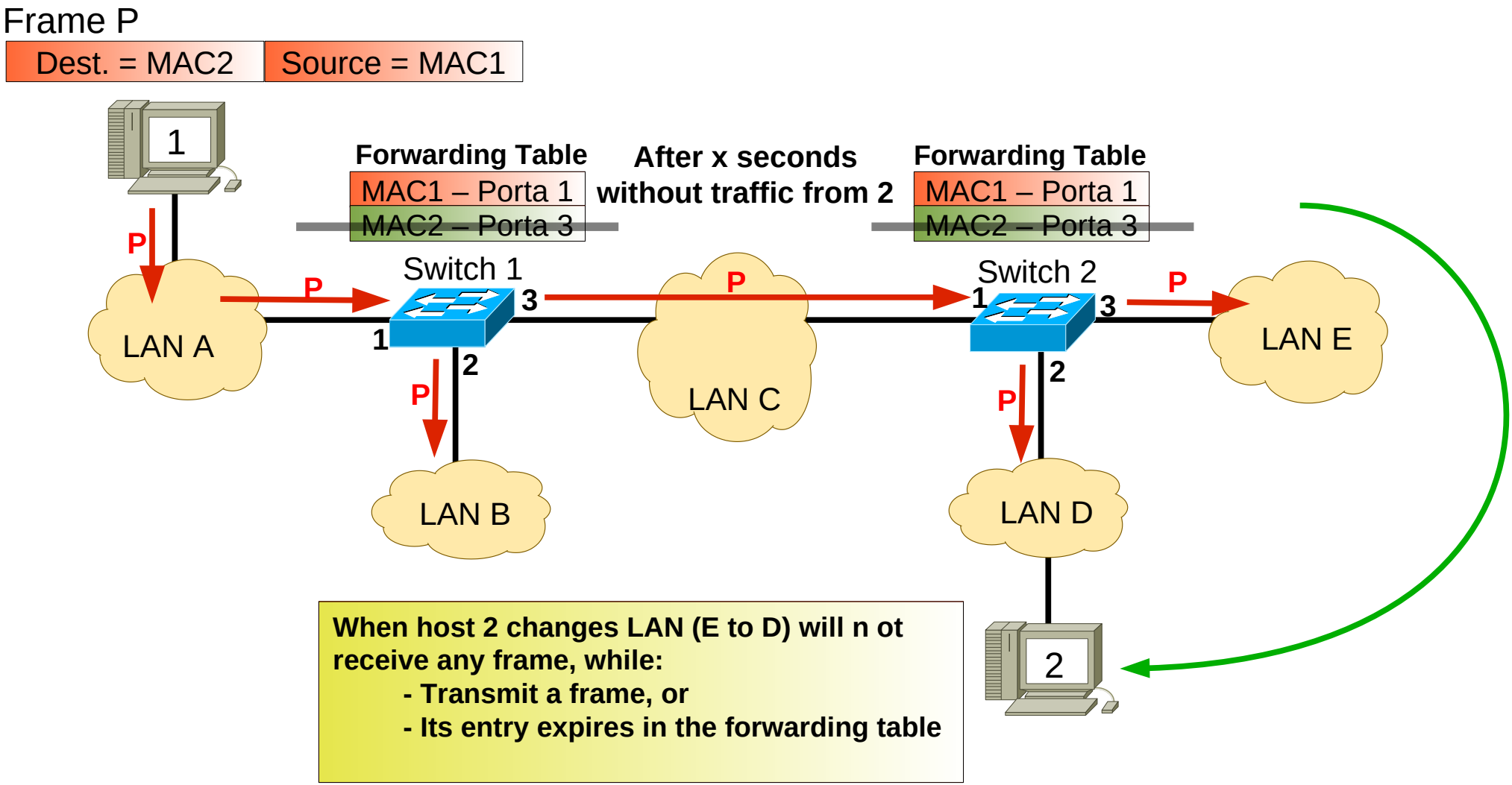
MAC	Porta
00:11:11:11:11:11	1
00:22:22:22:22:22	1
A1:33:33:33:33:33	2
44:44:44:44:44:44	3
55:55:55:00:00:55	3

- Switches have a **Forwarding Table**.
- When a switch receives an Ethernet frame:
  - Registers an entry at the Forwarding Table the frame's source MAC address and the port where the frame was received.
    - If no frames are received from that MAC address after some time (**aging time**) the entry is removed.
  - Searches the Forwarding Table for the frame's destination MAC address and forwards the packet according:
    - **Forwarding** mechanism:
      - If the frame's destination MAC address exists in the table, the switches forwards the frame through the port associated with that MAC address.
    - **Flooding** mechanism:
      - If the frame's destination MAC address DOES NOT exist in the table, the switches forwards the frame through all active ports (except the one where it was received).
        - » Note: Just within the same VLAN (more details later).

Learning, Flooding and Forwarding

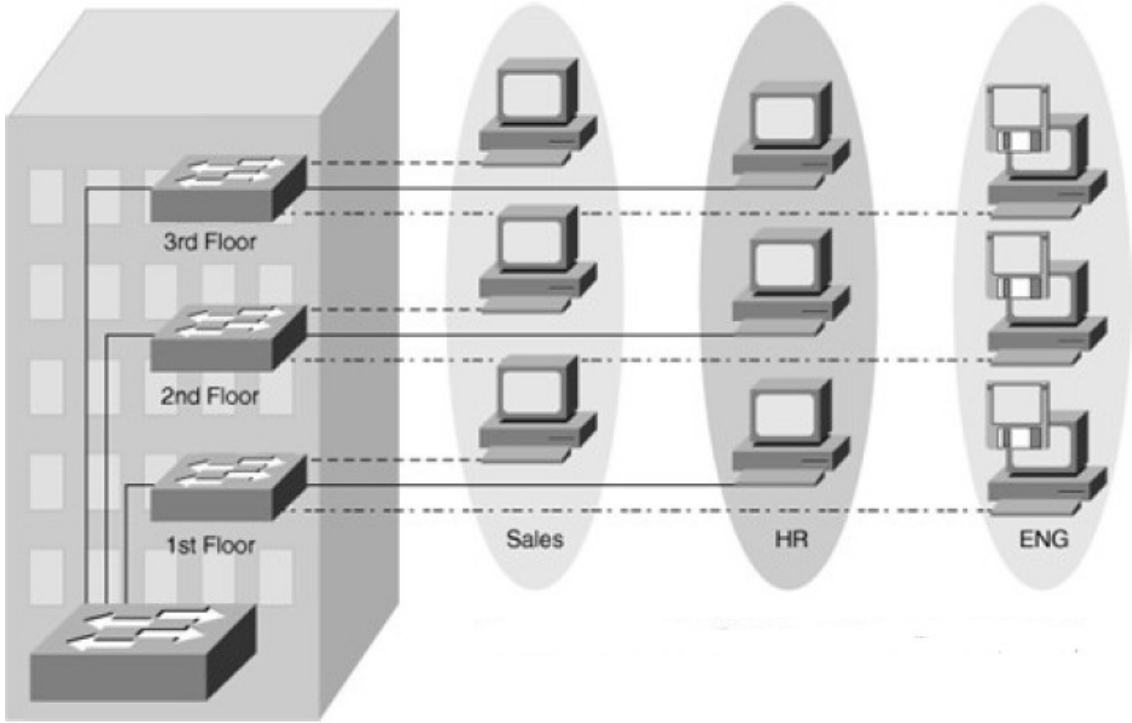


Forwarding Table Aging Time



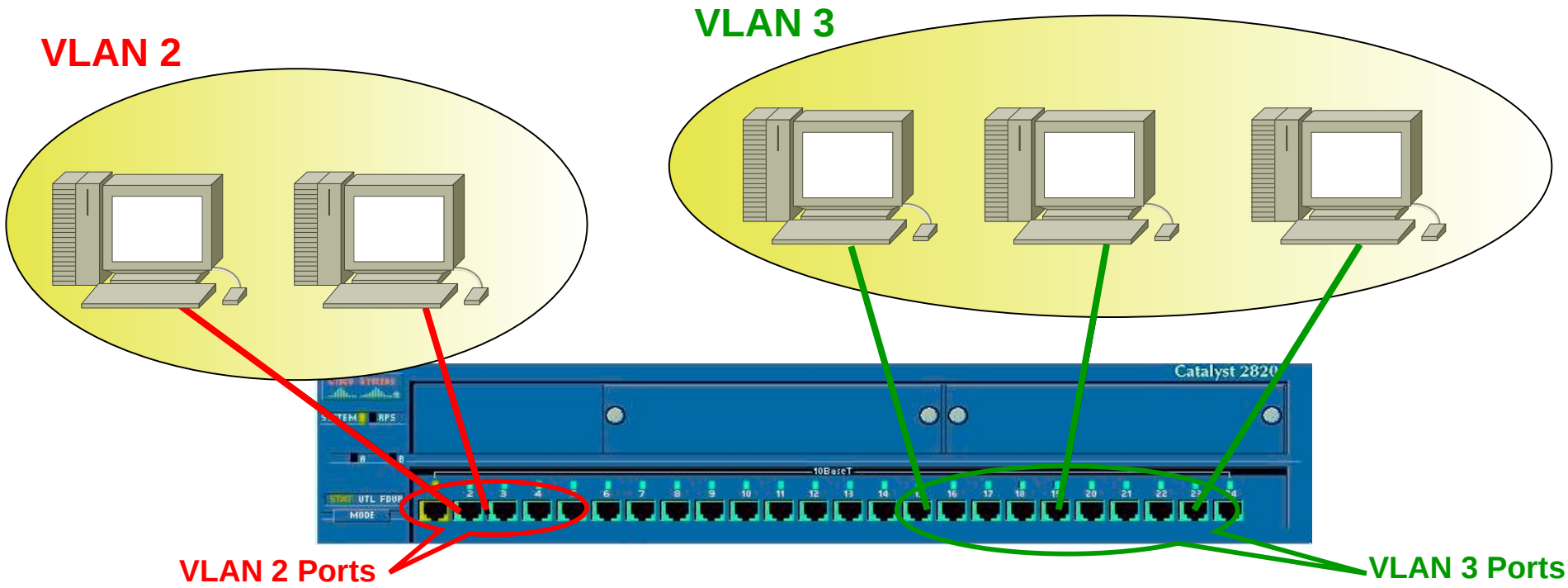
Virtual LAN (VLAN)

- A Virtual LAN (VLAN) is a group of hosts/users with a common set of requirements or characteristics in the same broadcast domain.
  - Independent of their physical location.
- Solves the scalability problems of large networks.
  - By breaking a single broadcast domain into several smaller broadcast domains.
  - Allows better/simpler network administration and security deployment.
- Hosts in different VLAN do not communicate by Layer 2.
  - Its communications are done at Layer 3 (with IP routing).



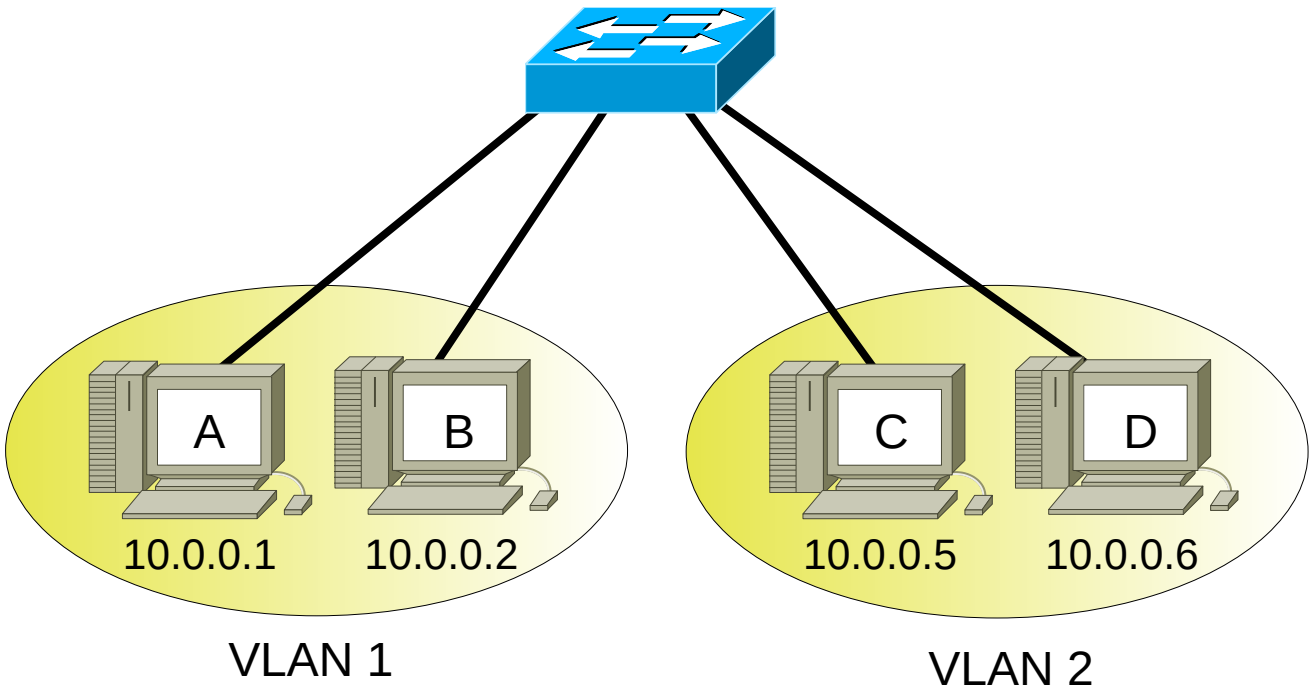
Defining Host VLAN

- The VLAN to which a host belongs depends only on the port of the switch.
  - Configured only in the switch.
  - Example: If port 1 is configure as VLAN 2, and port 20 is configured as VLAN 3:
    - If host is connected to port 1 it is on VLAN 2,
    - If host is connected to port 20 it is on VLAN 3.
- VLAN 1 is usually reserved to network administration.
  - Used to access configurations remotely via IP.



Example – VLAN

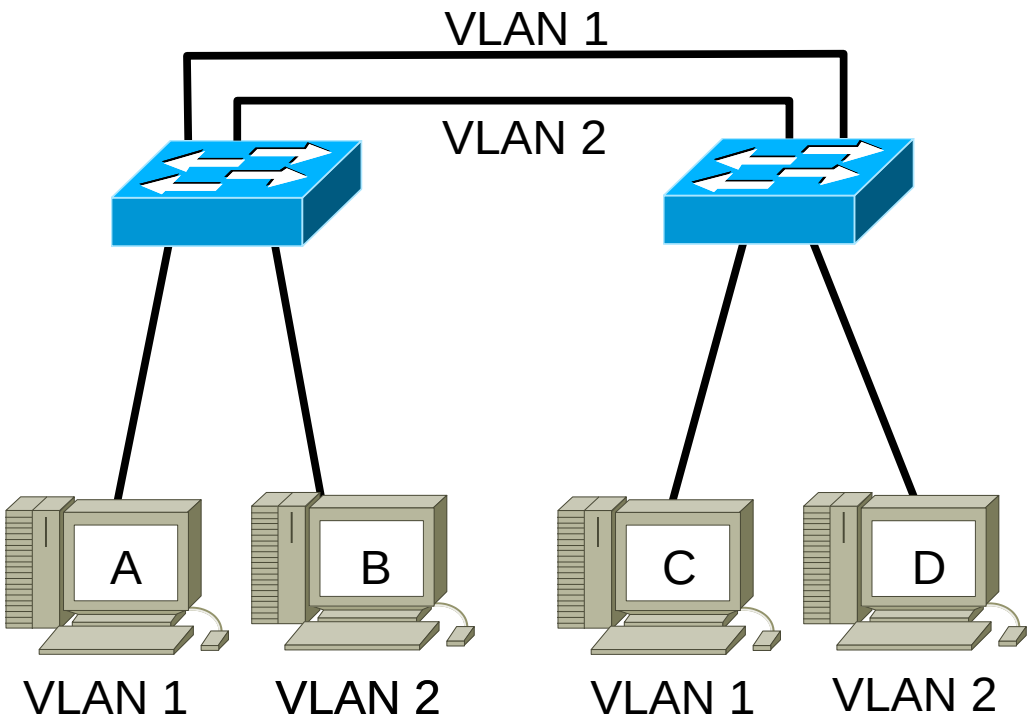
Pings sent by 10.0.0.1



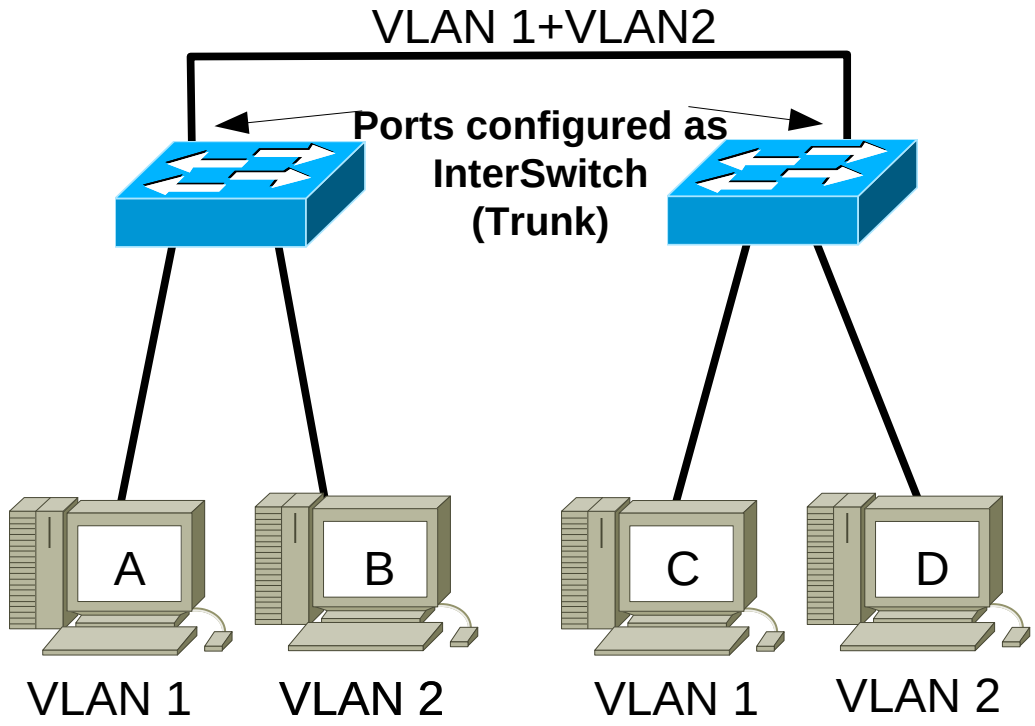

```
# ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128
Reply from 10.0.0.2: bytes=32 time<10ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

# ping 10.0.0.5

Pinging 10.0.0.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

# ping 10.0.0.6

Pinging 10.0.0.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

Interconnection of Switches

- Physical link per VLAN

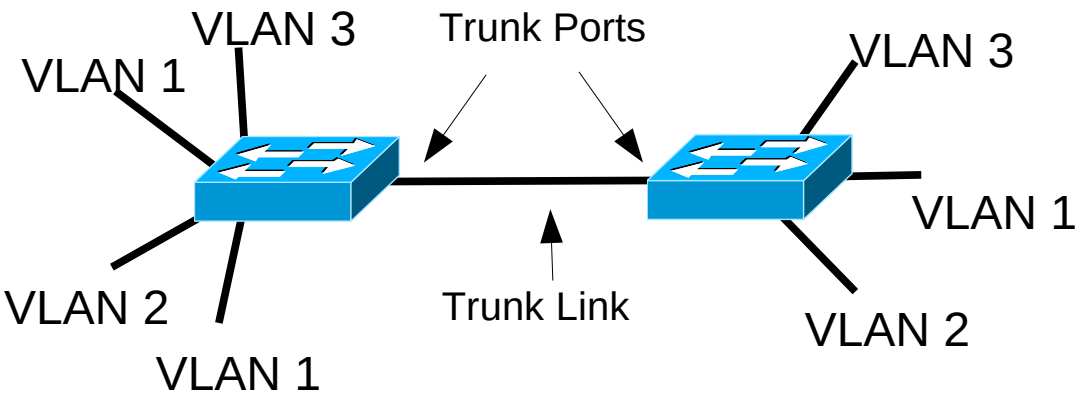


- With a single physical link.
- Using InterSwitch/Trunk port(s).

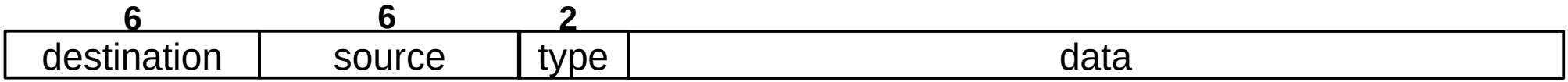


- Using a single physical link requires a mechanism to differentiate frames from different VLAN.
  - Frames must have a tagged
    - Added when forwarding to a trunk port.
    - Read and removed when receiving a frame from a trunk port

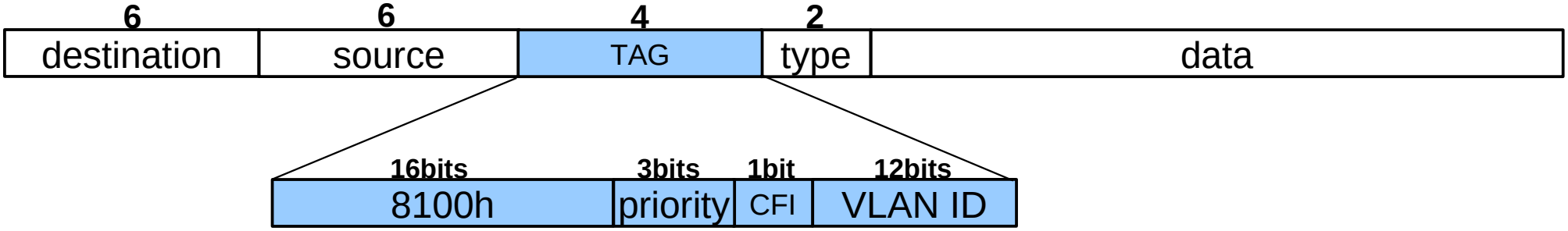
IEEE802.1Q Standard



Ethernet frame without a VLAN tag



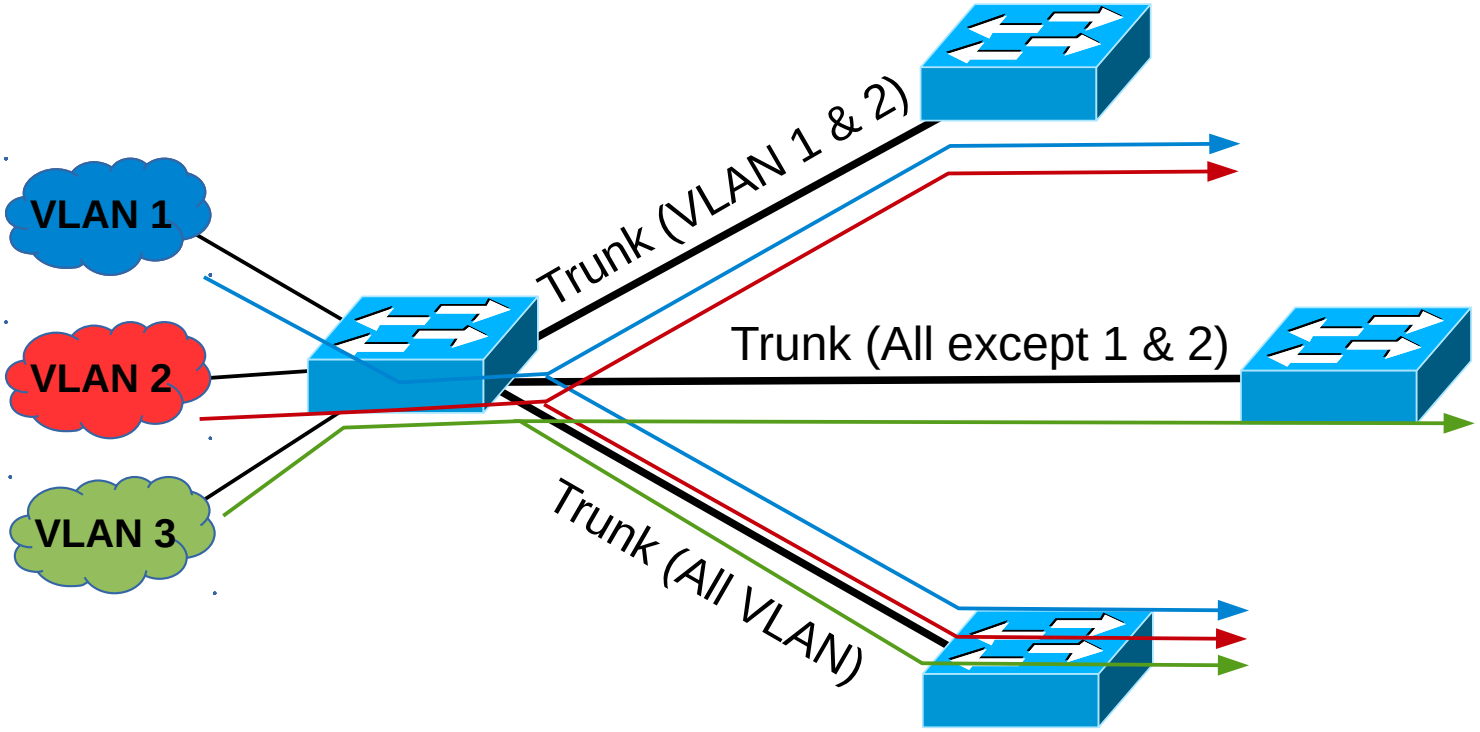
Ethernet frame with a VLAN tag



- Priority: Traffic relative priority according to standard 802.1q (0 to 7 values).
- CFI: Used to guarantee compatibility with older technologies (always zero in Ethernet).
- VLAN ID: VLAN identifier.

Trunk Links

- The physical link between two Trunk ports is called a Trunk link.
- A trunk carries traffic for multiple VLANs using IEEE 802.1Q.
  - Inter-Switch Link (ISL) encapsulation is an alternative but it getting obsolete.
- Trunks may transport all VLAN or only some!



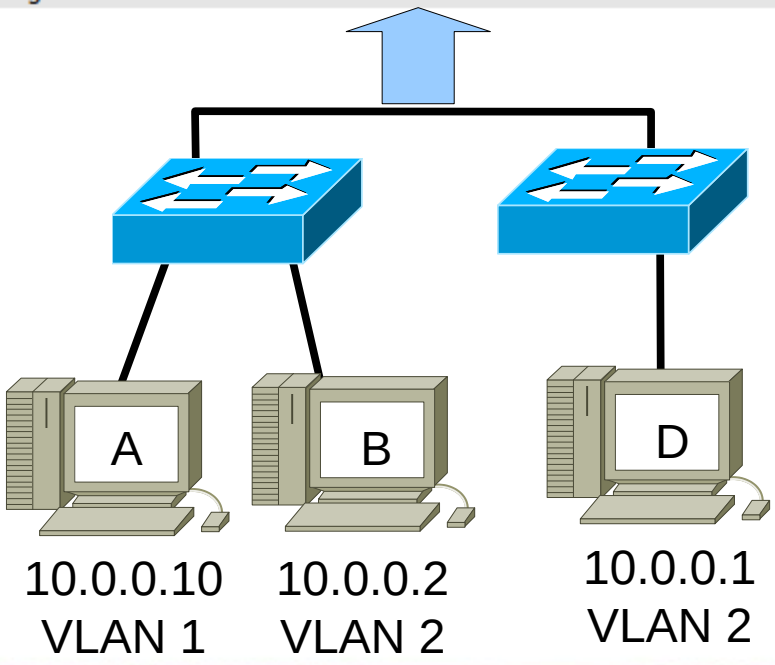
Example – InterSwitch/Trunk Ports

Filter: icmp | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Info
23	11.535990	10.0.0.2	10.0.0.1	ICMP	Echo (ping) request
24	11.536995	10.0.0.1	10.0.0.2	ICMP	Echo (ping) reply
27	12.538443	10.0.0.2	10.0.0.1	ICMP	Echo (ping) request
28	12.539186	10.0.0.1	10.0.0.2	ICMP	Echo (ping) reply

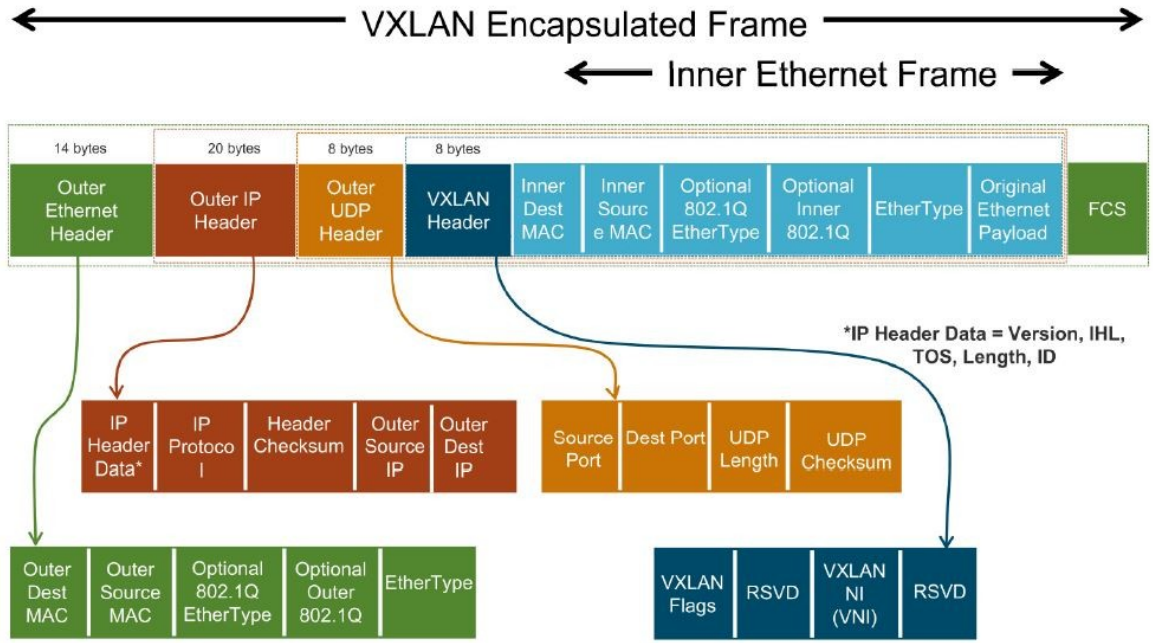
```
▷ Frame 23 (102 bytes on wire, 102 bytes captured)
▷ Ethernet II, Src: 00:aa:00:53:7c:00 (00:aa:00:53:7c:00), Dst: 00:aa:00:fa:67:00 (00:aa:00:fa:67:00)
▽ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0010 = ID: 2
    Type: IP (0x0800)
▷ Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.1 (10.0.0.1)
▷ Internet Control Message Protocol
```

ID:2 == VLAN 2



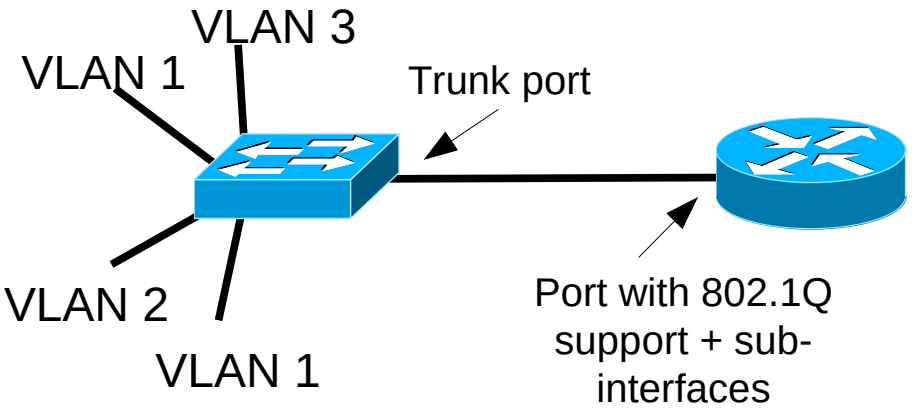
Virtual Extensible LAN (VXLAN)

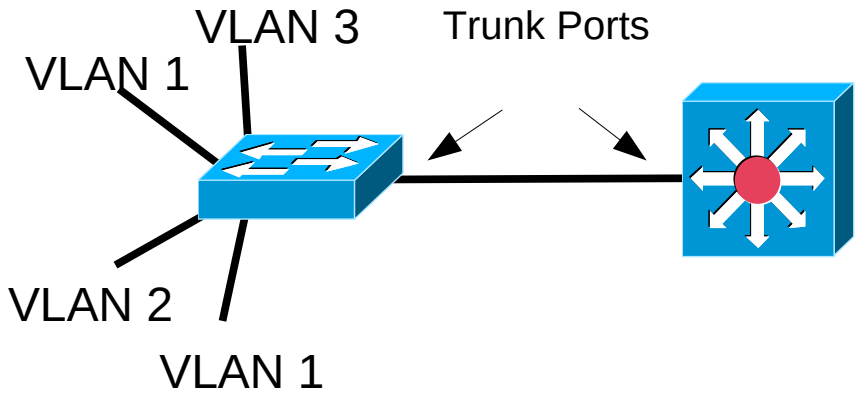
- Alternative/Complement to 802.1Q in Layer3 Switches.
- Encapsulates OSI Layer 2 Ethernet frames within Layer 4 UDP/IP datagrams .
  - Default port 4789.
- VLAN may be additionally identified by a VNI field with 24 bits.
  - 802.1Q tag only as 12 bits.
  - Allows for a very large number of VLAN.
- Usually used when connecting remote VLAN (connected only via IP) in Datacenter and Cloud scenarios.



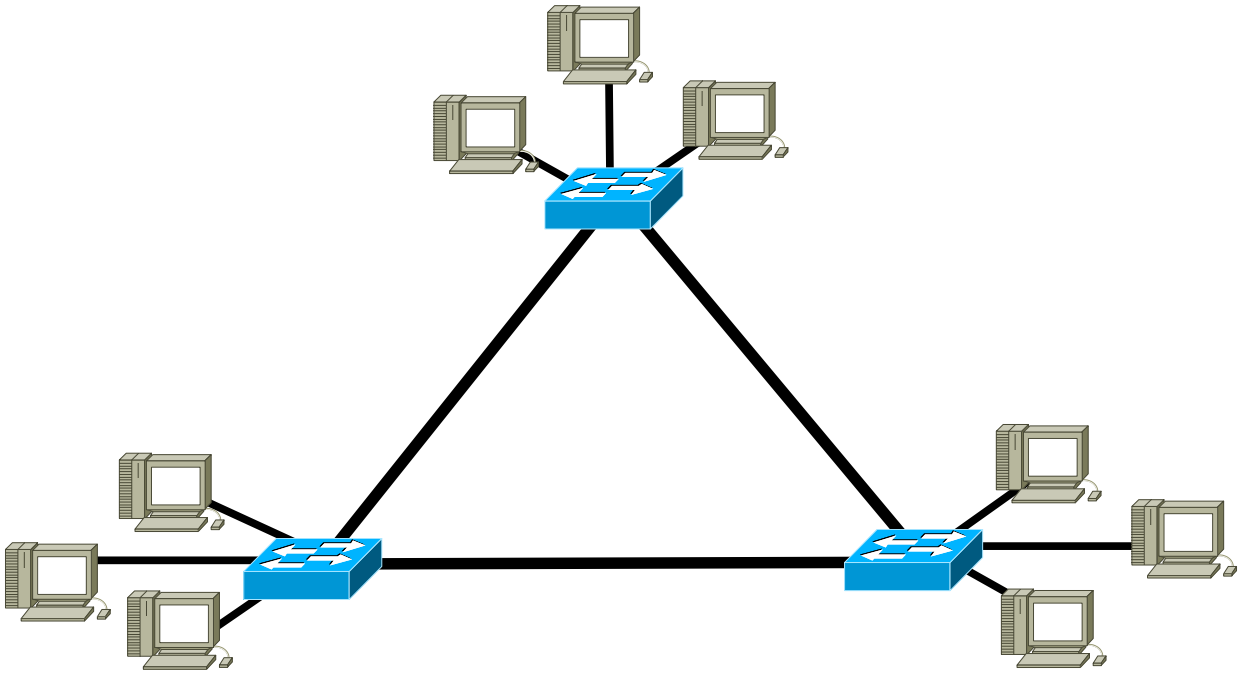
IP Connection between VLANs

- To communicate between different VLAN it is required to use Layer 3 (IP Routing).
- Common solutions:
  - A router with support to 802.1Q,
    - Connecting the physical router interface to a Trunk port.
    - The router's physical interface is sub-divided in sub-interfaces (one for each VLAN).
    - The IP gateway for a VLAN host is the IP address of the respective sub-interface in the Router.
  - A Layer 3 switch,
    - Connecting both switches (L3 and L2) using Trunk ports.
    - Each VLAN is mapped to a virtual Layer 3 interface.
    - The IP gateway for a VLAN host is the IP address of the respective virtual interface in the L3 switch.





Redundant Layer 2 Network

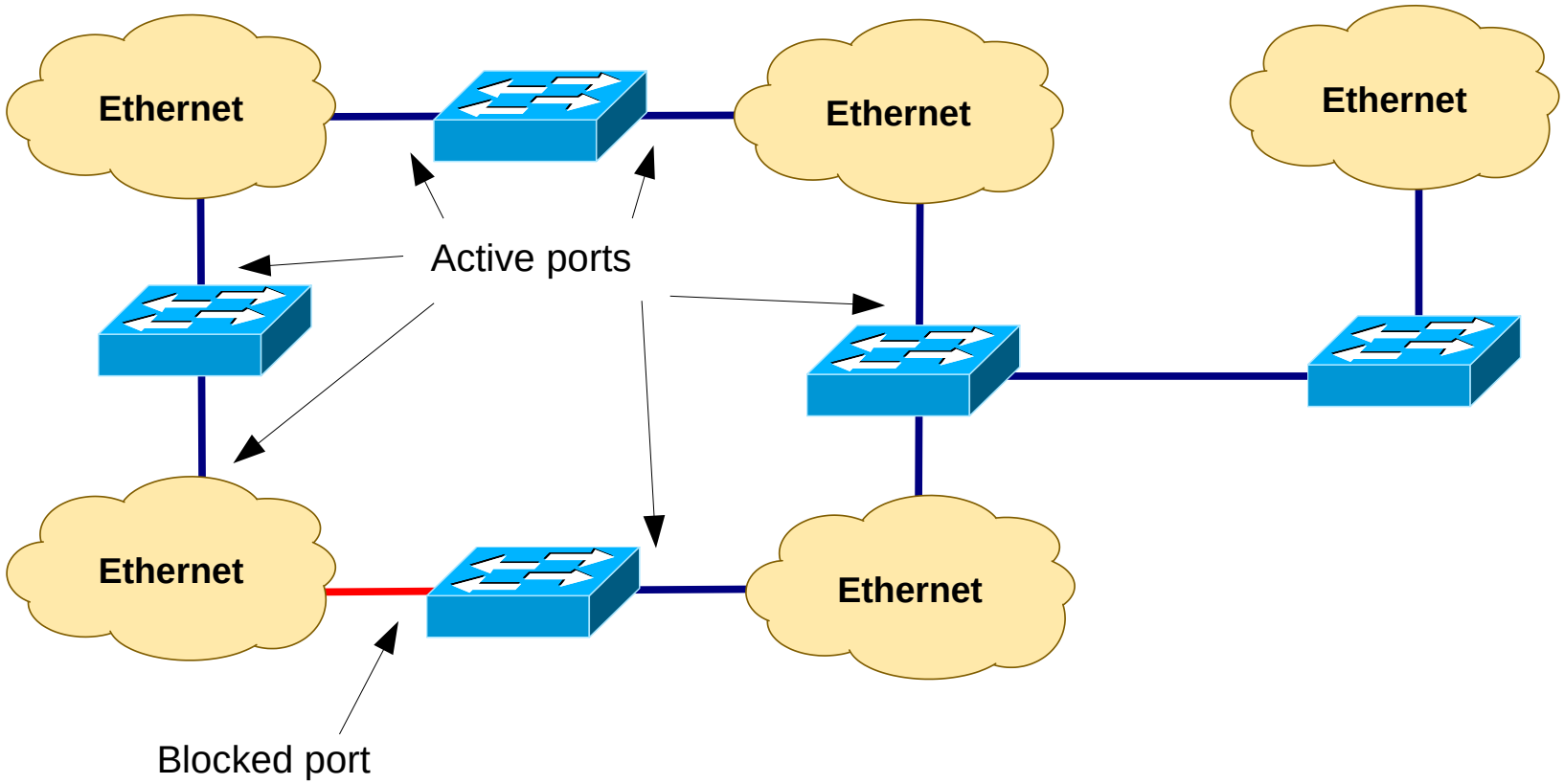


- Objective: Allow the network for dynamically recover from network failures.
- Problem: Link redundancy creates Layer 2 loops. Causes the collapse of communications when MAC frames with broadcast address are sent by any host due to infinite frame flooding.

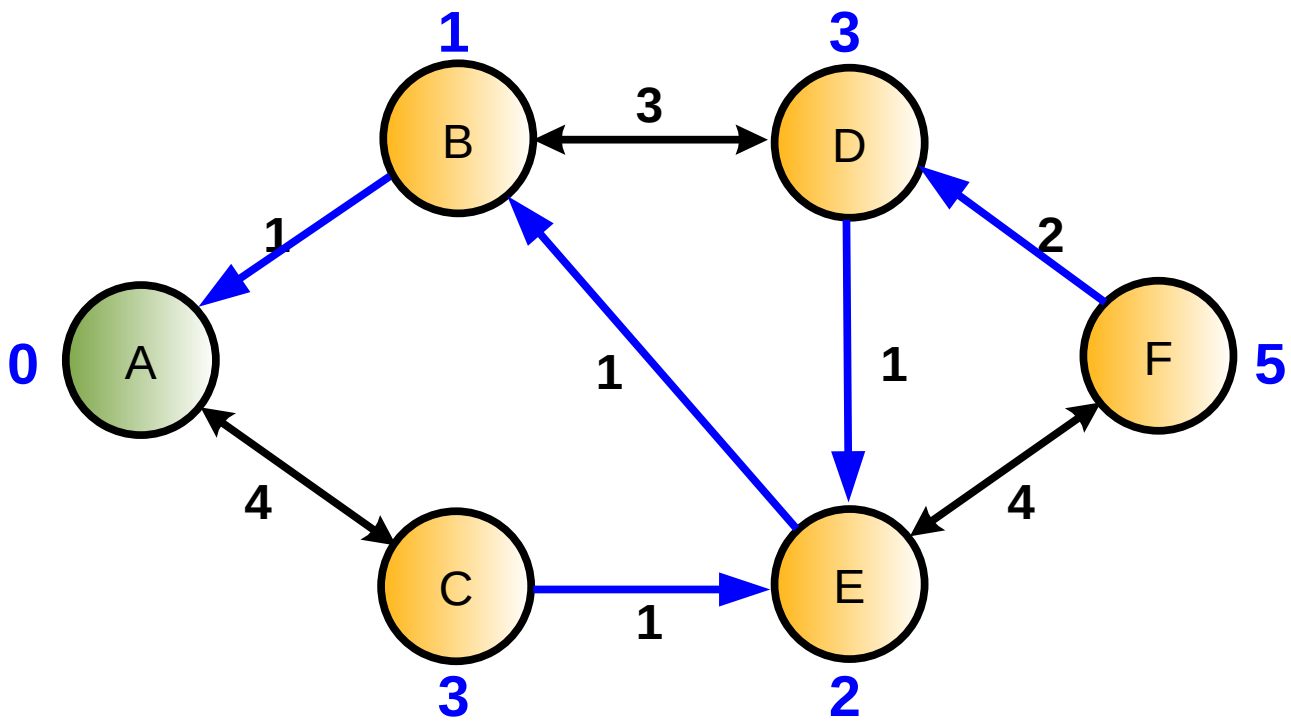
Spanning Tree Protocol (SPT)

- STP enables the network to deterministically block ports and provide a loop-free topology in a network with redundant links.
- There are several STP Standards and Features:
  - STP is the original IEEE 802.1D version (802.1D-1998) that provides a loop-free topology in a network with redundant links.
  - RSTP, or IEEE 802.1W, is an evolution of STP that provides faster convergence of STP.
  - Multiple Spanning Tree (MST) is an IEEE standard. MST maps multiple VLANs into the same spanning-tree instance.
  - Per VLAN Spanning Tree Plus (PVST+) is a Cisco enhancement of STP that provides a separate 802.1D spanning-tree instance for each VLAN configured in the network.
  - RPVST+ is a Cisco enhancement of RSTP that uses PVST+. It provides a separate instance of 802.1W per VLAN.

Spanning-Tree



Bellman Equations



- When link cost are not negative, then:

Shortest path from one node X to node A

=

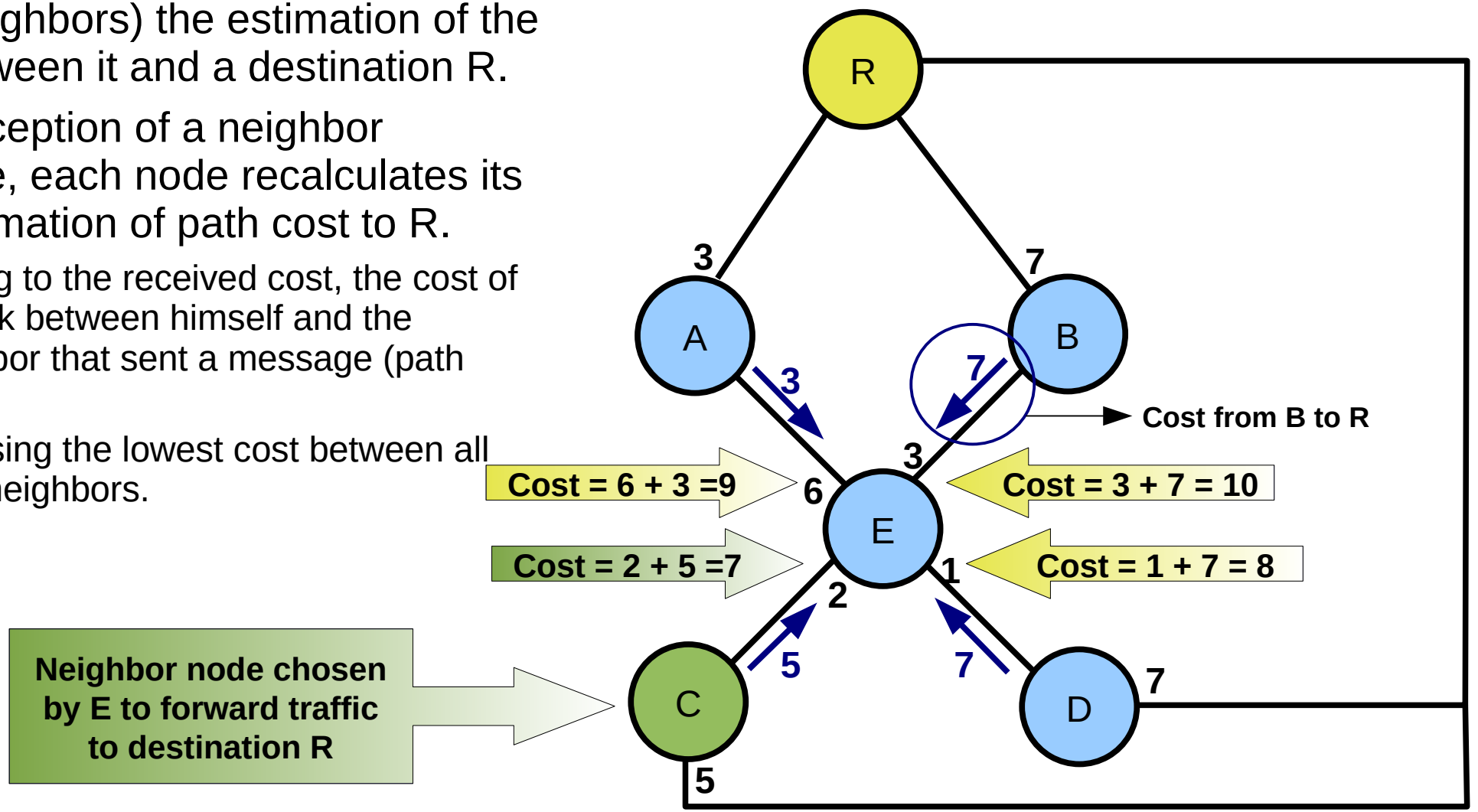
Cost of the link from that node X to the node that follows it in the shortest path to A

+

Shortest path from that node to node A

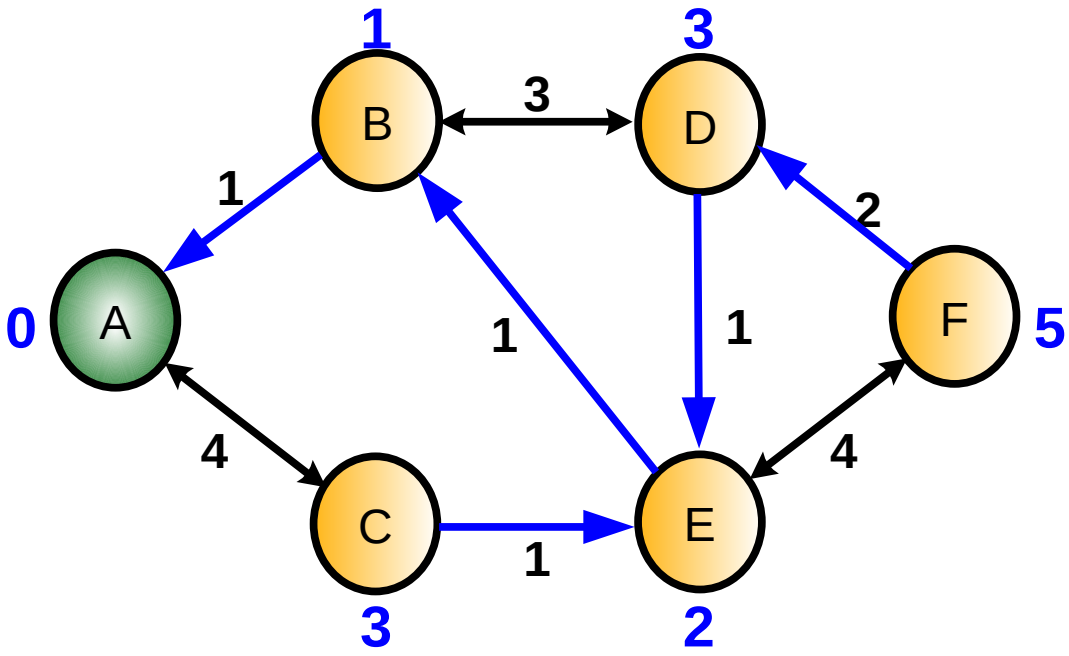
Bellman-Ford Distributed and Asynchronous Algorithm

- Each node transmits periodically (to all its neighbors) the estimation of the cost between it and a destination R.
- Upon reception of a neighbor message, each node recalculates its own estimation of path cost to R.
  - Adding to the received cost, the cost of the link between himself and the neighbor that sent a message (path cost).
  - Choosing the lowest cost between all links/neighbors.

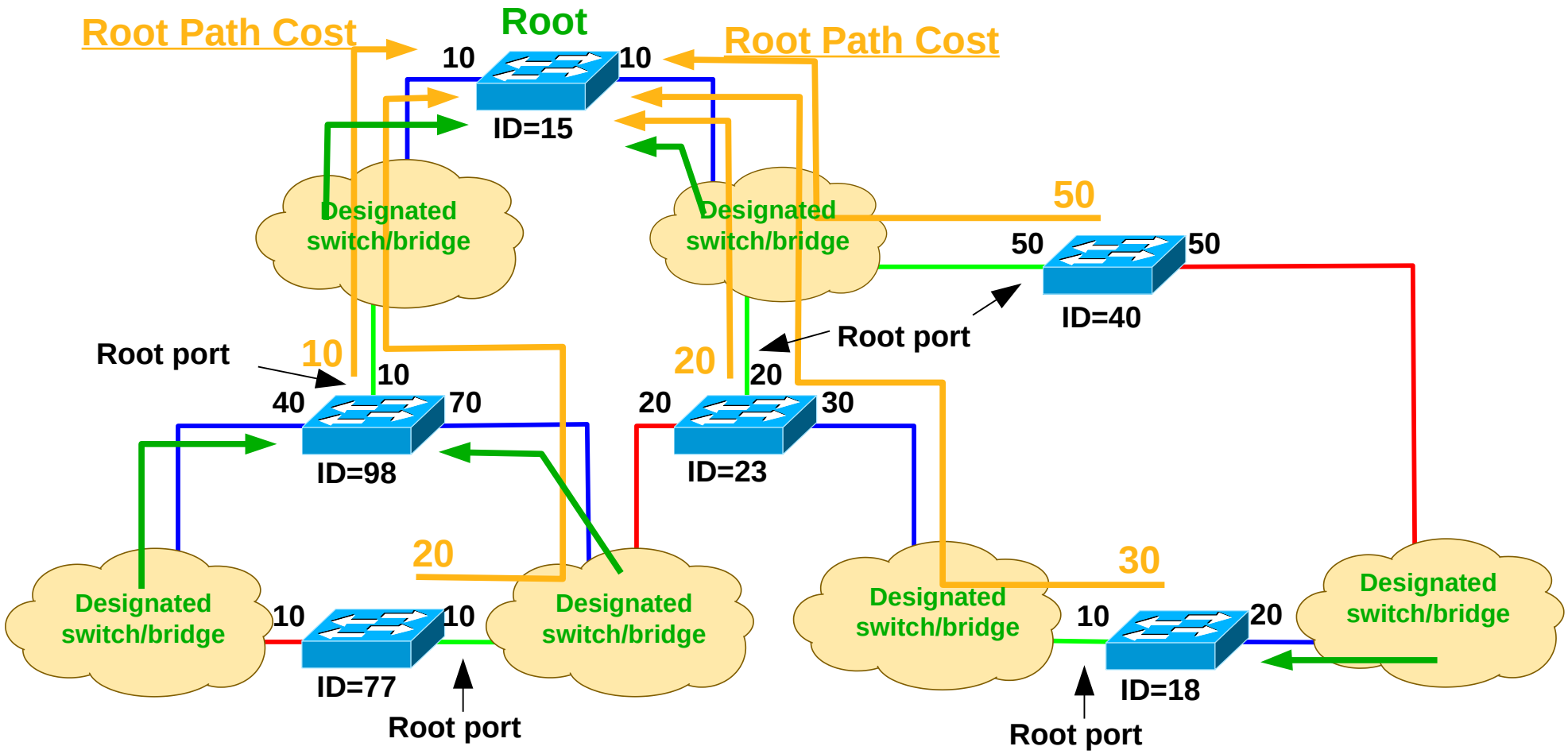


Routing based on Spanning Trees

- It is chosen an origin/root node.
- All nodes use the **Bellman-Ford Distributed and Asynchronous Algorithm** to calculate the neighbored node (and respective path cost) that provide the smallest cost to the origin/root node.
- The set of links used by all nodes to provide the shortest paths to the origin/root node is called the **Spanning Tree**.
- It is required a criteria to solve ties.

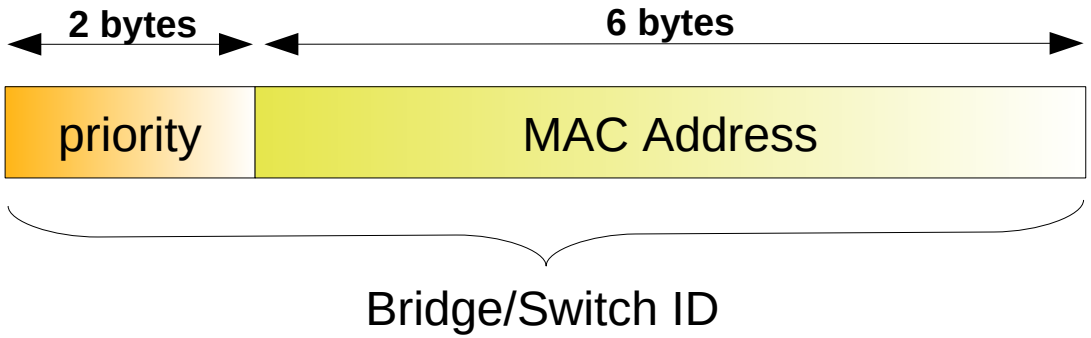


Spanning Tree Basic Concepts (1)



Spanning Tree Basic Concepts (2)

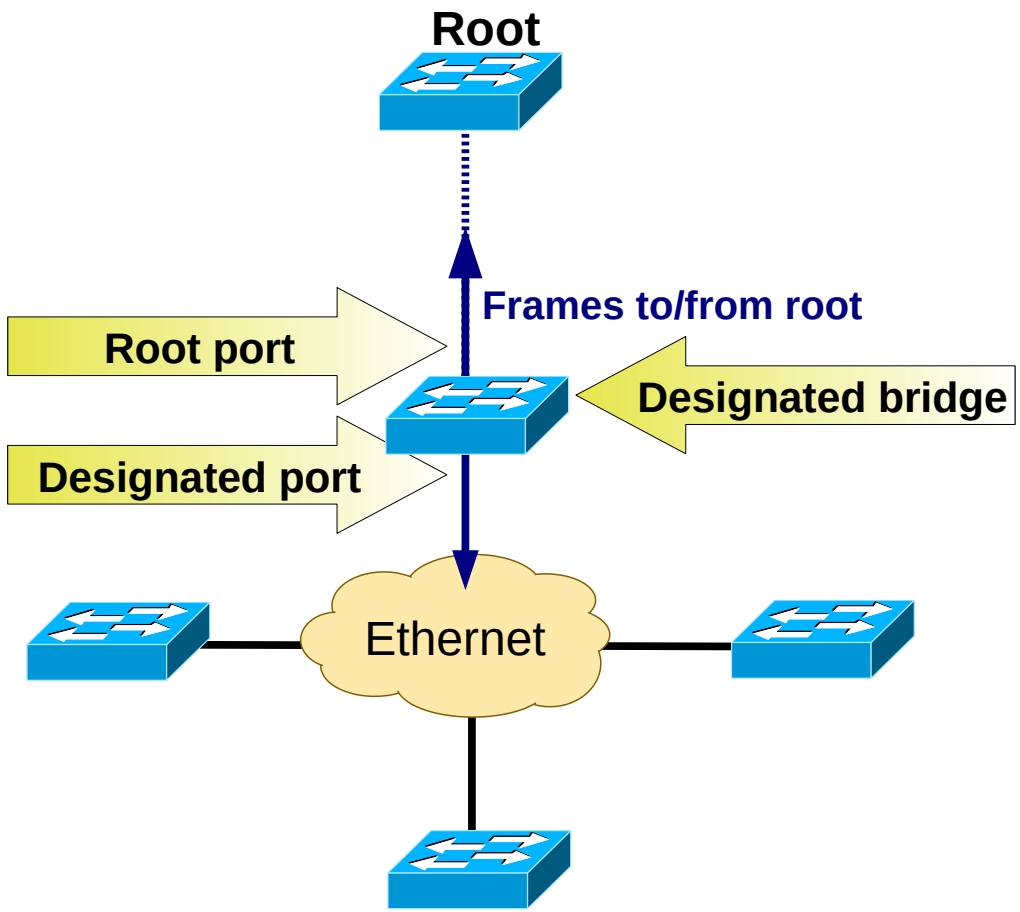
- Bridge/Switch ID – each switch is identified by an 8 bytes identifier based on:
  - 2 **Priority** bytes, defined by configuration.
  - 6 bytes (one of the **MAC Address** of the switch, or any other unique 48 bit sequence).
  - Priority has precedence over the 6 bytes sequence (usually MAC address).



- Root Switch/bridge – Switch chosen as origin/root of the spanning tree.
  - Switch com **lowest ID**.
- Path cost – Cost associated with each port.
  - Has a default value, but can be changed by configuration.

Spanning Tree Basic Concepts (3)

- Designated Bridge – Switch responsible to forward the packets from an Ethernet segment to and from the root.
  - The root bridge is the designated bridge to all Ethernet segments connected to it.
- Designated Port – Port of the designated bridge that connects an Ethernet segment (to which is designated).
- Root Port – Port of the designated bridge that provides the path to the root.



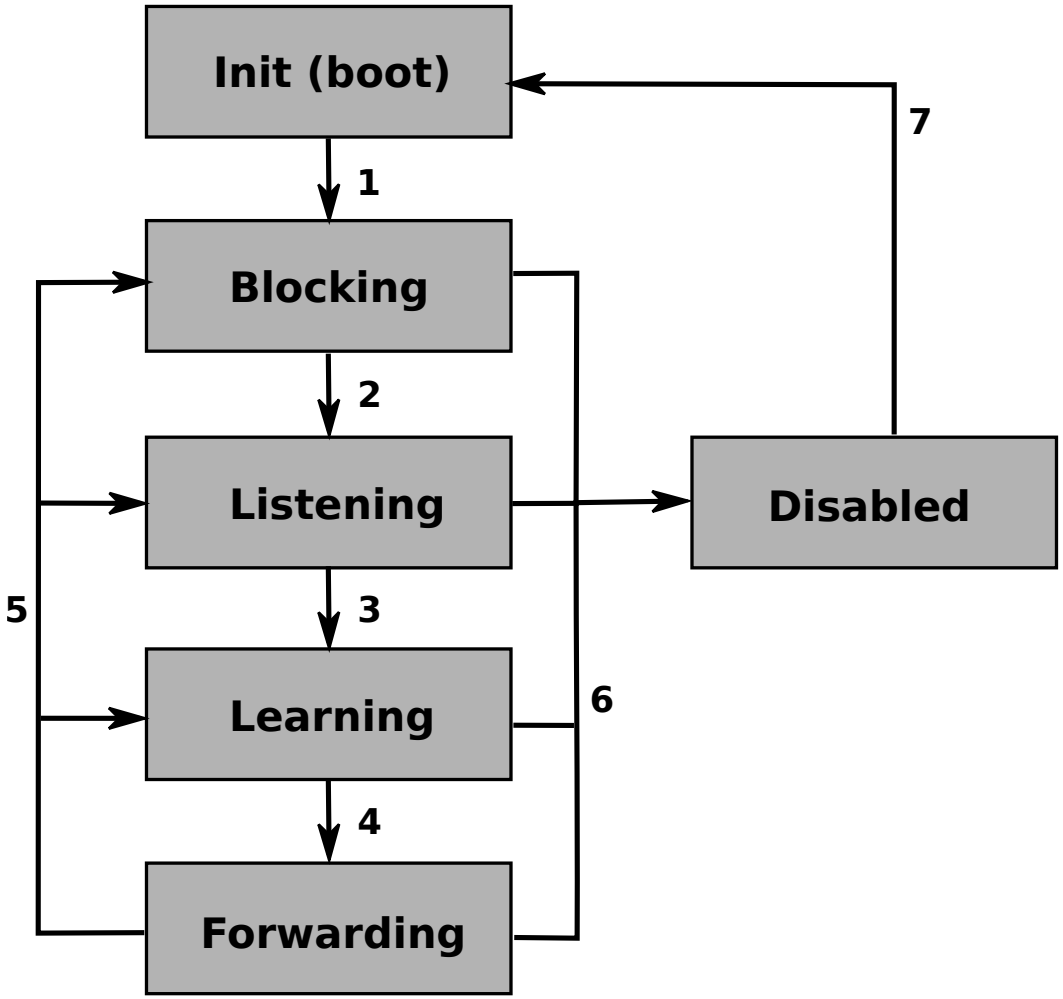
Spanning Tree Basic Concepts (4)

- Possible Port States
  - **Blocking** state:
    - MAC address learning and packet forwarding are disabled;
    - Receives and processes BPDU.
    - After *MaxAge* time without receiving BPDU, it transitions to Listening state.
  - **Listening** state:
    - MAC address learning and packet forwarding are disabled;
    - Receives and processes BPDU.
    - When *ForwardDelay* timer expires the port transitions to Learning state.
  - **Learning** state:
    - Learns MAC address;
    - Packet forwarding are disabled;
    - Receives and processes BPDU.
    - When *ForwardDelay* timer expires the port transitions to Forwarding state.
  - **Forwarding** state:
    - MAC address learning and packet forwarding are enabled;
    - Receives and processes BPDU.
  - **Disabled** state:
    - MAC address learning and packet forwarding are disabled;
    - Does not receive BPDU.

Spanning Tree Basic Concepts (5)

- Each switch has an associated cost of the shortest path to the root (Root Path Cost), given by the sum of the costs of all root ports along the path to the root.
- The Root Port, in each switch, is the port that provides the best path to the root (**lowest** Root Path Cost).
  - If more than one have the lowest cost, it is chosen the one with the neighbor with the lowest ID.
  - If more of one link is used to connect to the “best” neighbor it is used the one with the lowest (neighbor) port identifier.
- The Designated Bridge, from each Ethernet segment, is the switch with the **lowest** Root Path Cost from all connected to that segment.
  - If more than one have the lowest cost, it is chosen the one with the with the lowest ID.
- The Designated Port, from each Ethernet segment, is the port that connects it to its Designated Bridge.
- The root and designated ports will be in Forwarding state.
- All remaining ports will be in Blocking state.

Port States Diagram

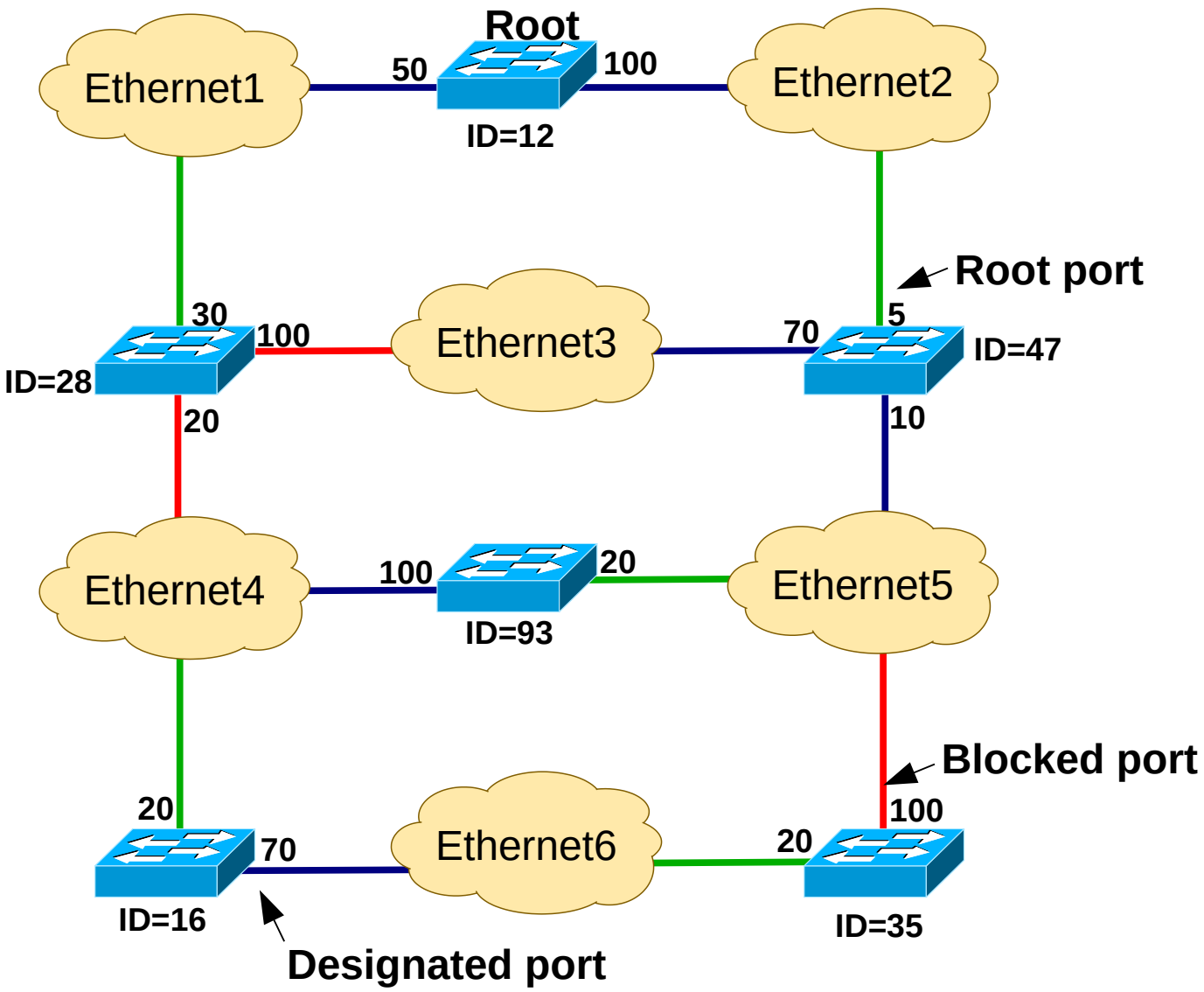


1) A port boots up and transitions to **Blocking** state.
2) When *MaxAge* timer expires the port transitions to **Listening** state.
3) When *ForwardDelay* timer expires the port transitions to **Learning** state.
4) When *ForwardDelay* timer expires the port transitions to **Forwarding** state.
5) After a topology change the port transitions immediately to **Blocking** state.
6) and 7) Administrative actions.

Example – Spanning Tree (1)

Designated bridges

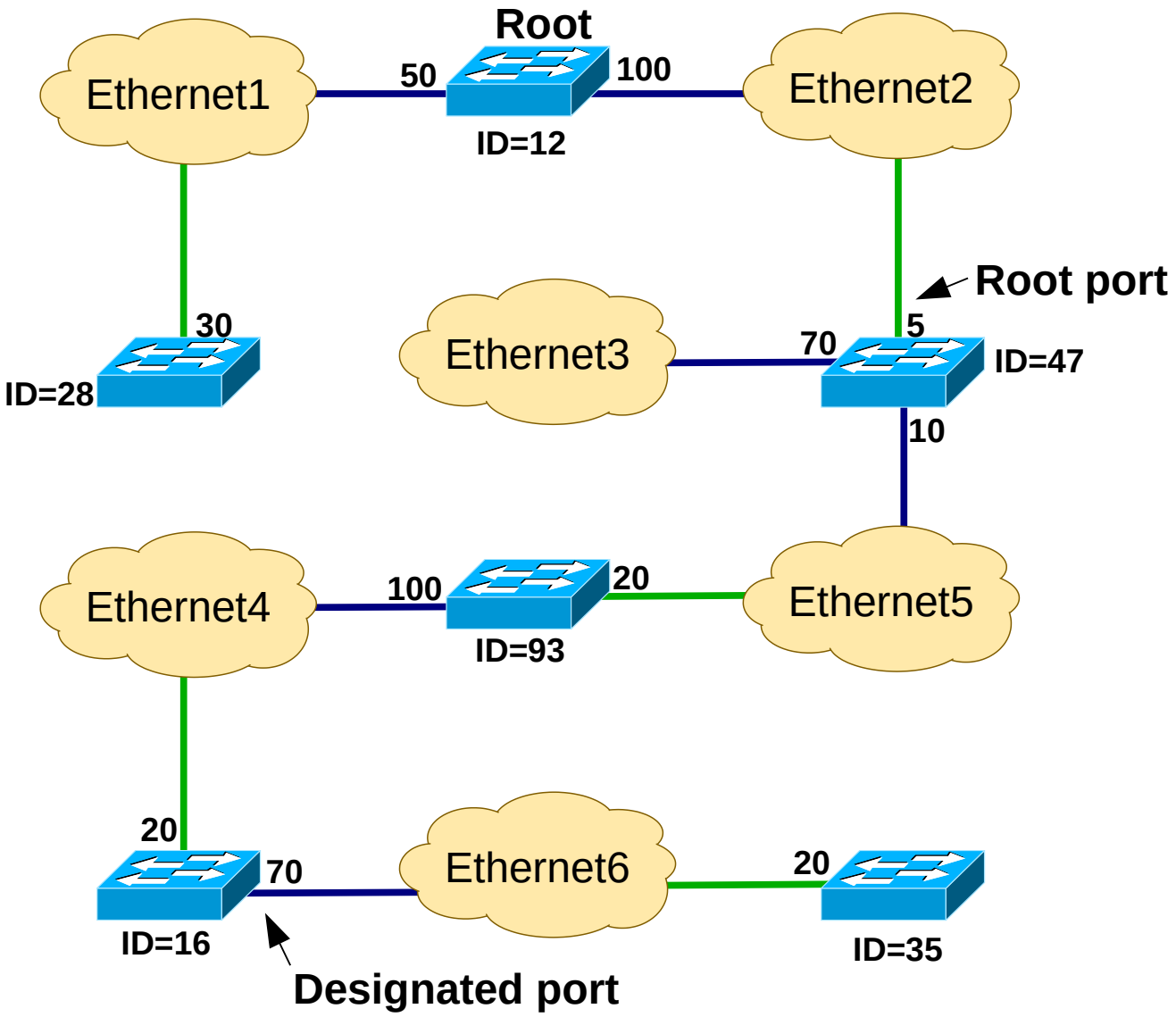
Eth1	12
Eth 2	12
Eth 3	47
Eth 4	93
Eth 5	47
Eth 6	16



Example – Spanning Tree (2)

Designated bridges

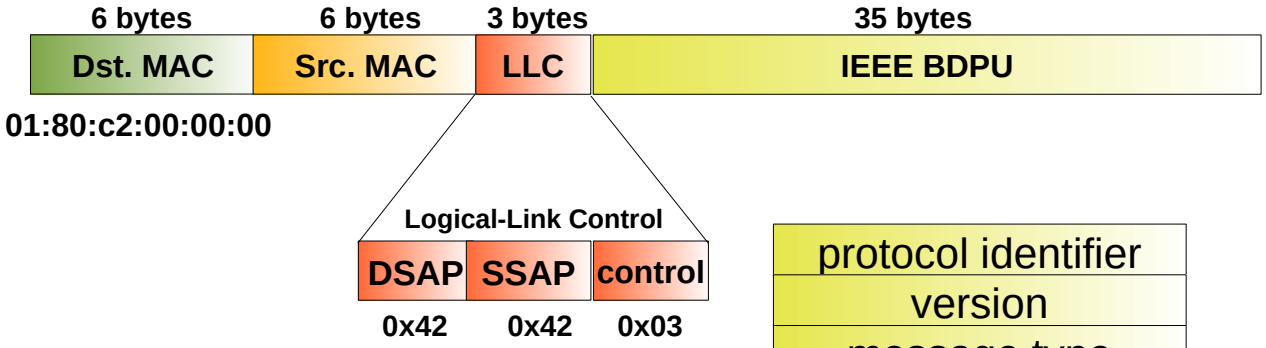
Eth1	12
Eth 2	12
Eth 3	47
Eth 4	93
Eth 5	47
Eth 6	16



Protocolo IEEE 802.1D
BPDUs (Bridge Protocol Data Units)

- To build the spanning tree, switches exchange special messages between them called Bridge Protocol Data Units (BPDU).
- There are two types: *Configuration* e *Topology Change Notification.*

IEEE 802.3 Ethernet
Destination: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
Source: 00:16:e0:9a:c3:92 (00:16:e0:9a:c3:92)
Length: 39
Logical-Link Control
DSAP: Spanning Tree BPDU (0x42)
SSAP: Spanning Tree BPDU (0x42)
Control field: U, func=UI (0x03)
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Spanning Tree (0)
BPDU Type: Configuration (0x00)
Root ID: 32768 / 00:05:1a:4e:fd:58
Root Path Cost: 200004
Bridge ID: 32768 / 00:16:e0:9a:c3:80
Port ID: 0x8012
Message Age: 1
Max Age: 20
Hello Time: 2
Forward Delay: 15



protocol identifier		
version		
message type		
TCA	reserved	TC
root ID		
root path cost		
bridge ID		
port ID		
message age		
max age		
hello time		
forward delay		

Configuration BPDU

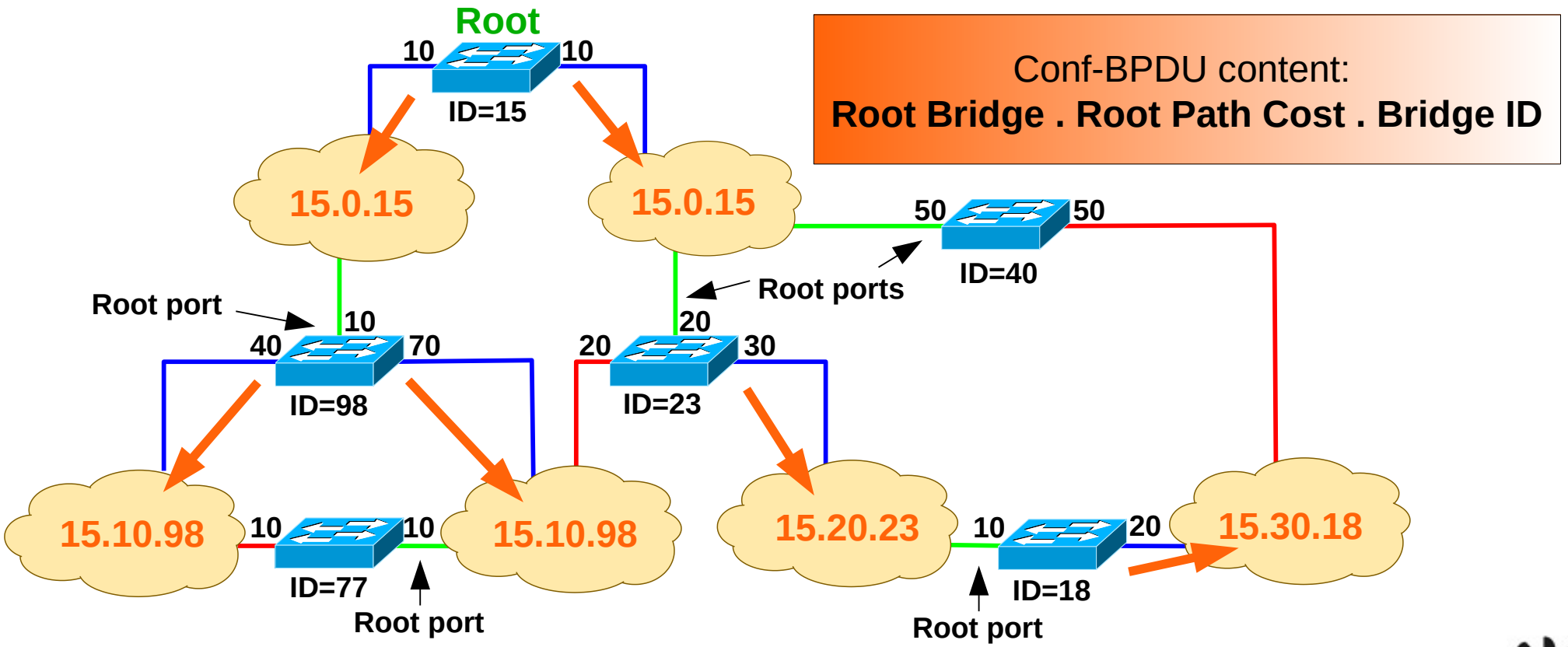
- The setup of the Spanning Tree id dune using Conf - BPDU (configuration messages).

IEEE 802.3 Ethernet
Destination: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
Source: 00:16:e0:9a:c3:92 (00:16:e0:9a:c3:92)
Length: 39
Logical-Link Control
DSAP: Spanning Tree BPDU (0x42)
SSAP: Spanning Tree BPDU (0x42)
Control field: U, func=UI (0x03)
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Spanning Tree (0)
BPDU Type: Configuration (0x00)
Root ID: 32768 / 00:05:1a:4e:fd:58
Root Path Cost: 200004
Bridge ID: 32768 / 00:16:e0:9a:c3:80
Port ID: 0x8012
Message Age: 1
Max Age: 20
Hello Time: 2
Forward Delay: 15

- More relevant fields:
  - Root ID: ID of the current root bridge.
  - Root Path Cost: estimation of the cost to the root.
  - Bridge ID: own bridge identifier.
  - Port ID: identifier of the port by which the BPDU was sent.
    - Port priority (1 byte) + Port number

Spanning Tree Maintenance

- Periodically switches sent Conf-BPDUs by its Designated Ports.
  - Periodicity of Conf-BPDU messages = hello time
    - Recommended Hello time: 2 seconds.
    - Defined at the root bridge.



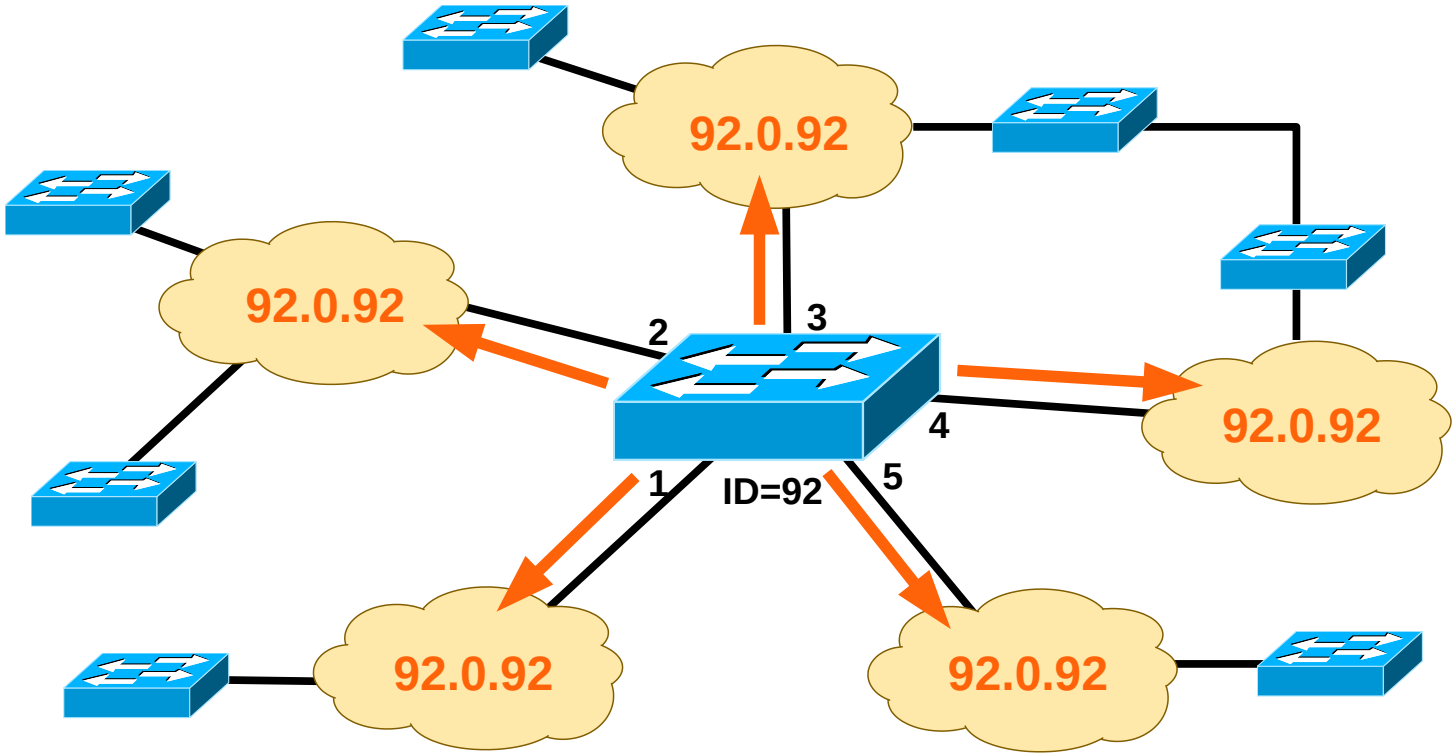
Sorting of Best BPDU

- A Conf-BPDU C1 is considered better than a Conf-BPDU C2 if:
  - The Root ID of C1 is lower than the one in C2,
  - With equal Root ID, if Root Path Cost of C1 is lower than the one in C2,
  - With equal Root ID and Root Path Cost, if the Bridge ID of C1 is lower than the one in C2,
  - With equal Root ID, Root Path Cost and Bridge ID, if the Port ID of C1 is lower than the one in C2.

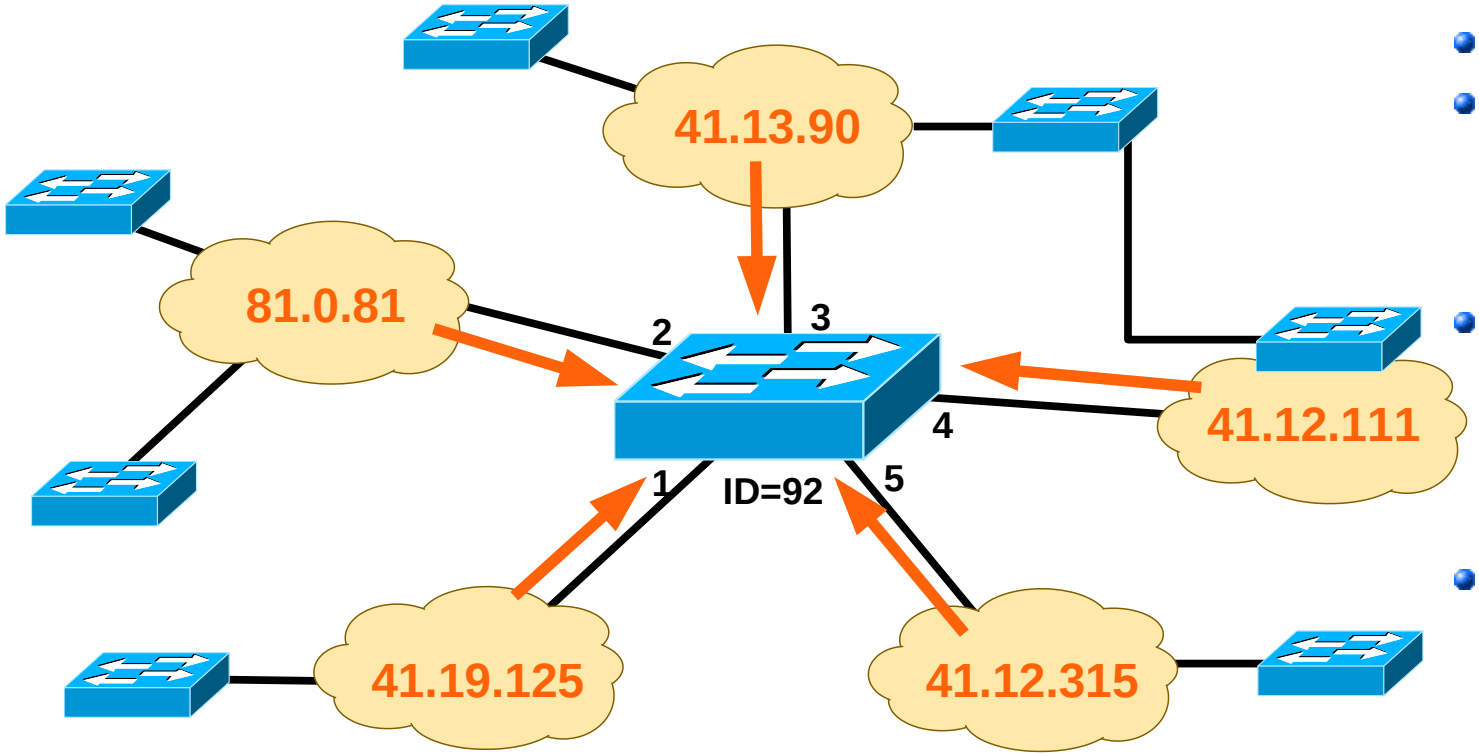
Root ID	Root Path Cost	Bridge ID	Port ID
18	27	32	2
18	27	32	4
18	27	43	1
18	35	23	3
23	31	45	2

Building the Spanning Tree (1)

- Each switch initially assumes to be the Root Bridge.
  - Assumes Root Path Cost = 0,
  - Sends Conf-BPDU to all its ports.



Building the Spanning Tree (2)



- Bridge92 is not root (BridgeID 92>41)
- Bridge 92 Root Port is 4.
  - Lowest RootID (41).
  - Lowest Root Path Cost (12+1=13).
  - Lowest Neighbor BridgeID (111<315)
- Bridge 92 is Designated Bridge via ports 1 and 2
  - Port 2, Lowest RootID (41).
  - Port 1, Same RootID (41) and Lowest Root Path Cost (13<19).
- Bridge 92 ports 3 and 5 are blocked.
  - Neighbors have the same RootID (41).
  - Via port 3, Neighbor has the same Root Path Cost (13), but lower BridgeID (90<92).
  - Via port 5, Neighbor has lower Root Path Cost (12).

Best Conf-BPDU received by Bridge 92 (until now)

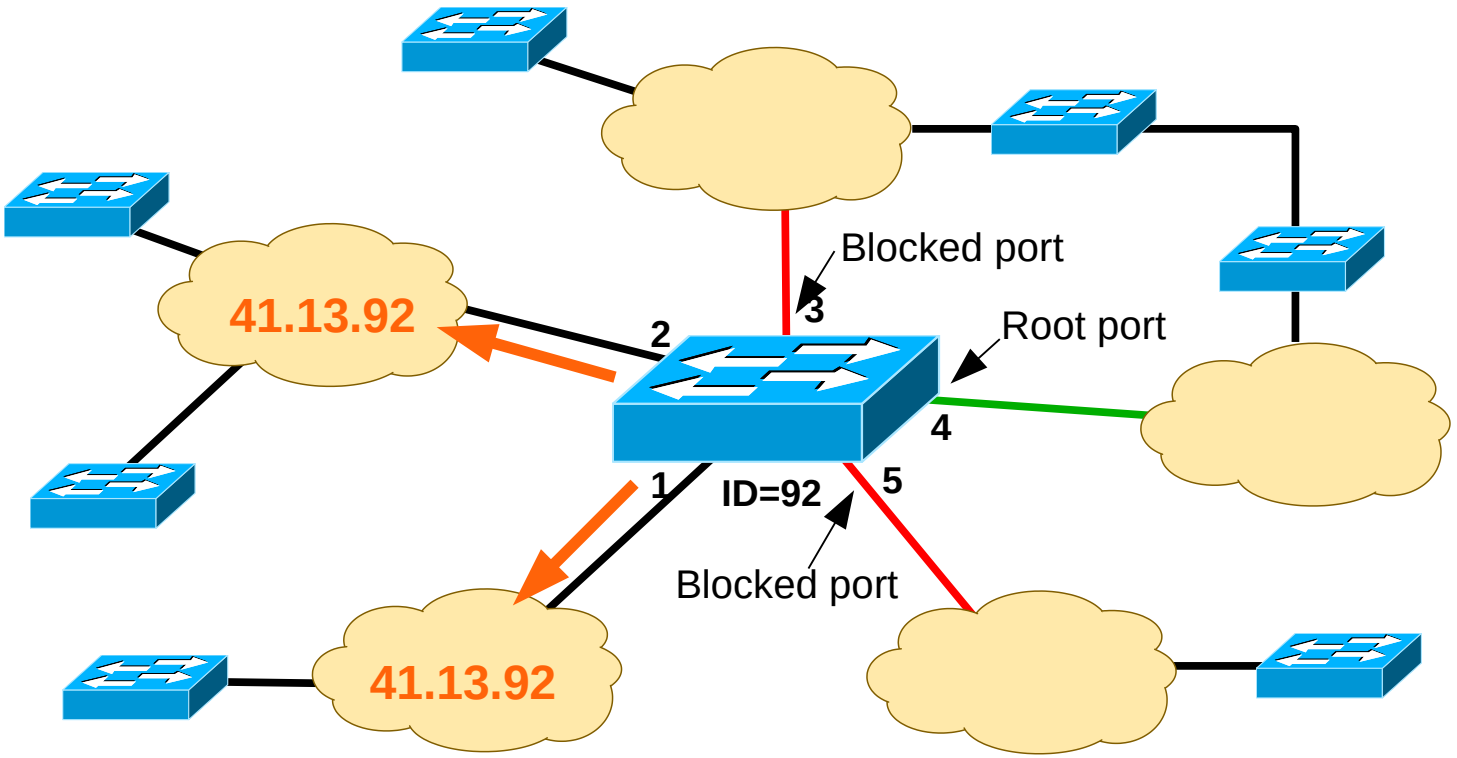
Estimations of Bridge 92 (assuming port costs equal to 1).

Root Bridge = 41

Root port = 4

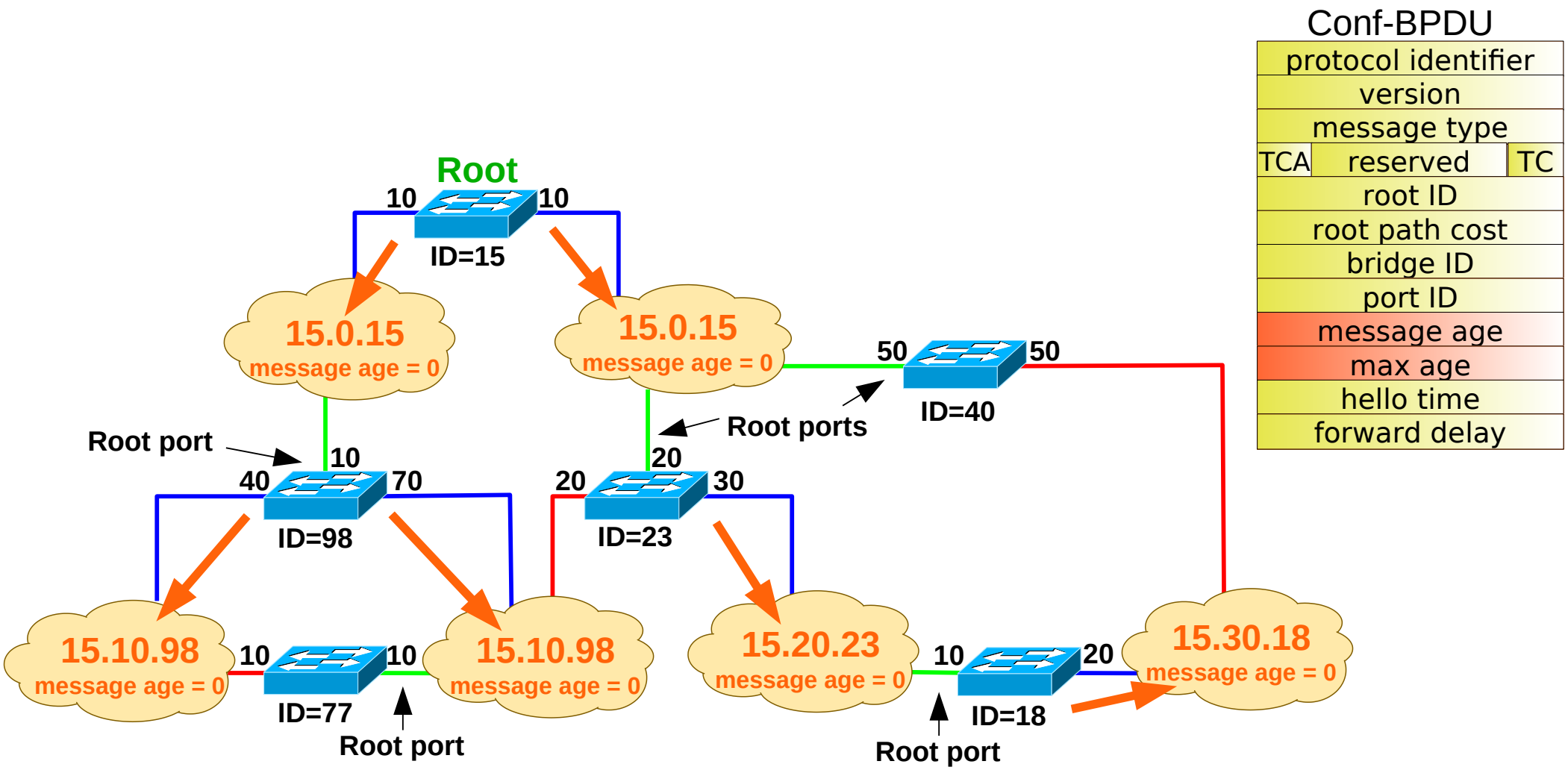
Root Path Cost = 12 + 1 **=13**

Building the Spanning Tree (3)



Conf-BPDU sent by Bridge 92 - 41.13.92

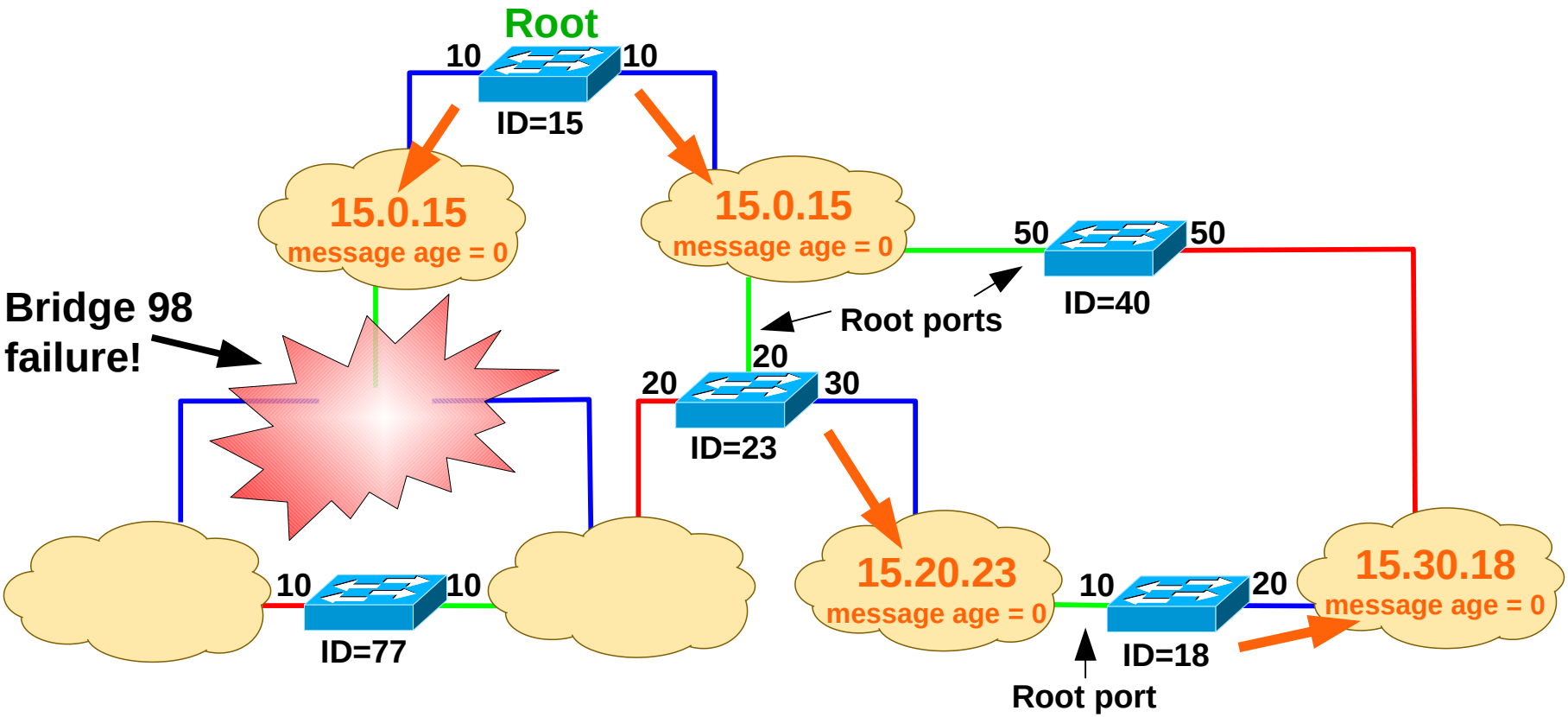
Network Failures (1)



Conf-BPDU

protocol identifier		
version		
message type		
TCA	reserved	TC
root ID		
root path cost		
bridge ID		
port ID		
message age		
max age		
hello time		
forward delay		

Network Failures (2)

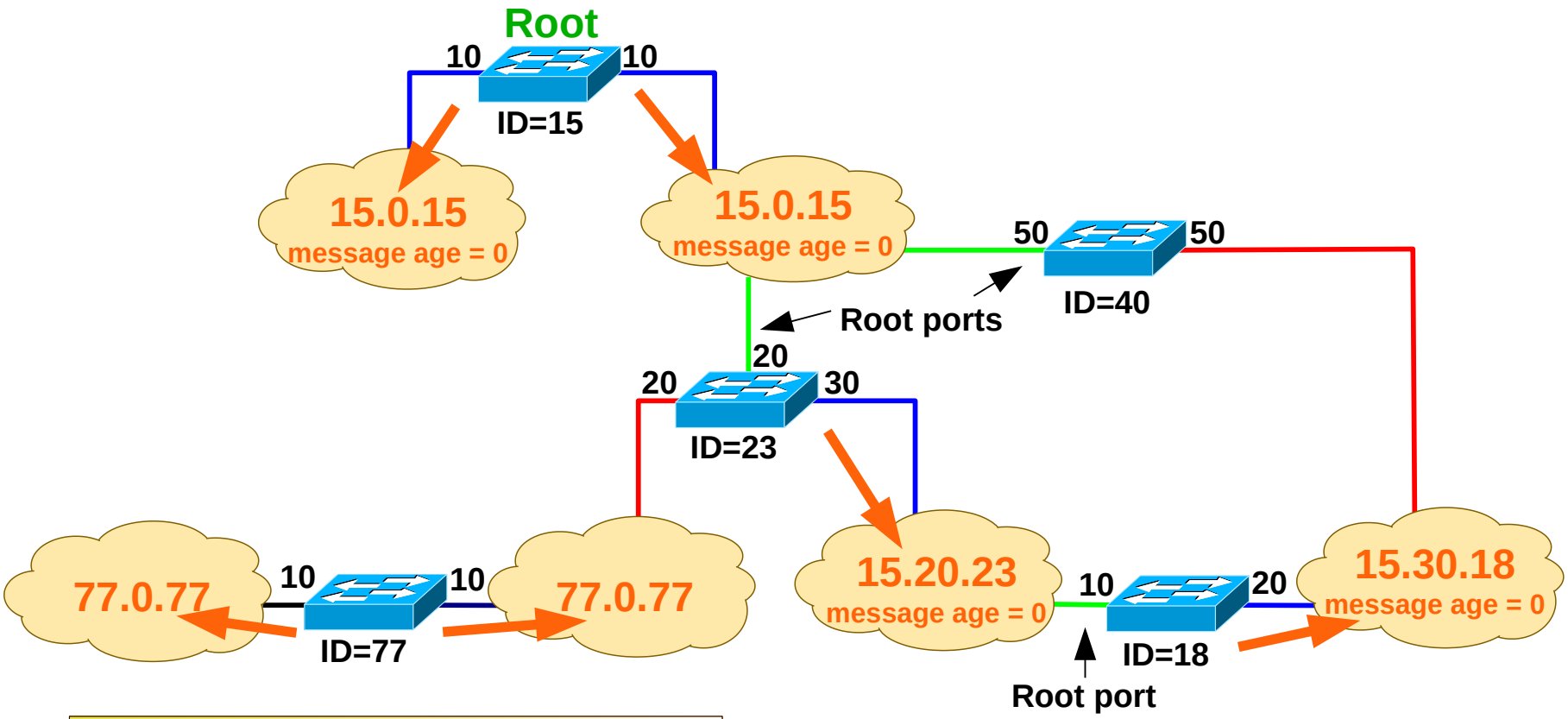


15.10.98 age = 0
15.10.98 age = 5
15.10.98 age = 10
.....
15.10.98 age = max age

15.10.98 age = 0
15.10.98 age = 5
15.10.98 age = 10
.....
15.10.98 age = max age

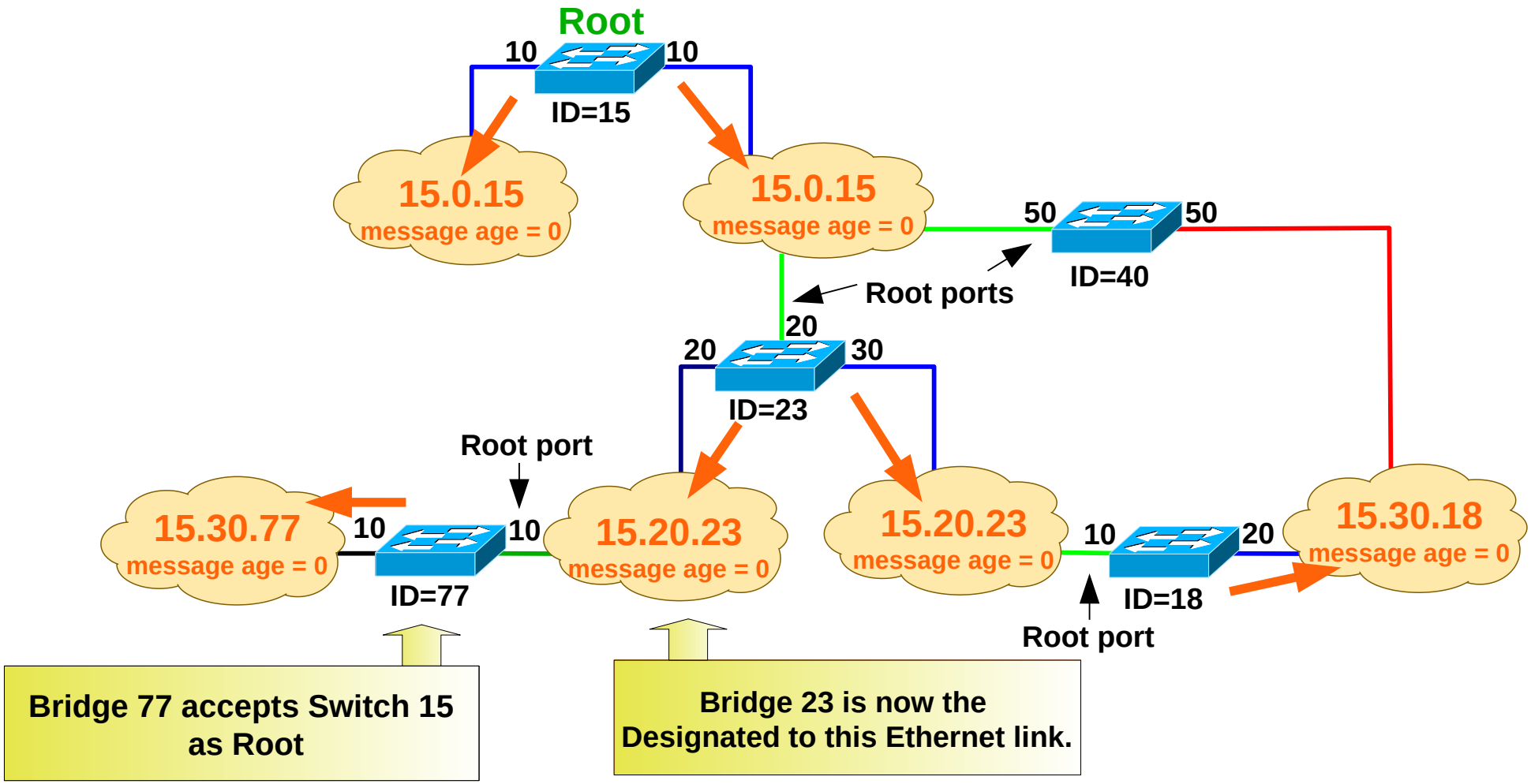
max age = 20 seconds

Network Failures (3)



Bridge 77 assumes to be Root

Network Failures (4)



Forwarding Tables Entries Lifetimes

- Forwarding Tables Long Lifetime – Many frames will be lost when network is changing topology.
- Forwarding Tables Short Lifetime – Creates to much traffic due to frequent flooding.

- There are two forwarding tables lifetimes:
  - **Long**: used by default (recommended value = 300 seconds)
  - **Short:** used when SPT is re-configuring (recommended value = 15 seconds)

Topology Change Notification

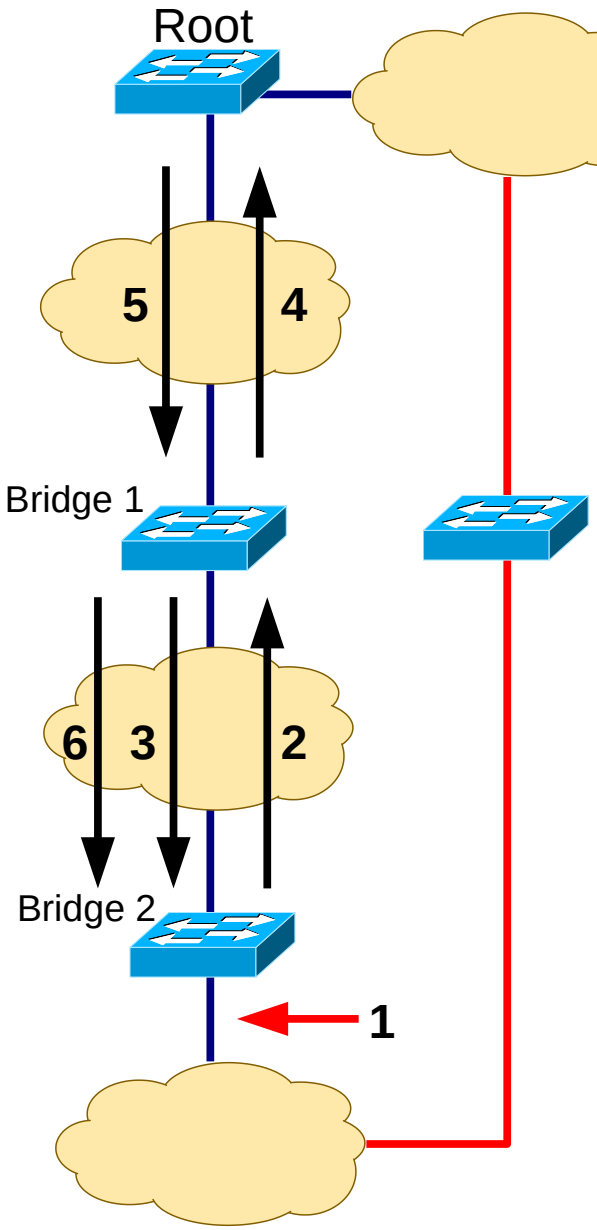
Conf (Configuration) BPDU

protocol identifier		
version		
message type = 0		
TCA	reserved	TC
root ID		
root path cost		
bridge ID		
port ID		
message age		
max age		
hello time		
forward delay		

TCA - flag Topology Change Acknowledgment
TC - flag Topology Change

TCN (Topology Change Notification) BPDU

protocol identifier
version
message type = 1



1. **Port changes state to disabled or blocking**
2. **Sends TCN-BPDU (periodicity = hello time)**
3. **Sends Conf-BPDU with TCA = 1 while receiving TCN-BPDU**
4. **Sends TCN-BPDU (periodicity = hello time)**
5. **Sends Conf-BPDU with TCA = 1 while receiving TCN-BPDU and with TC=1 for a period of time equal to *ForwardDelay* + *MaxAge***

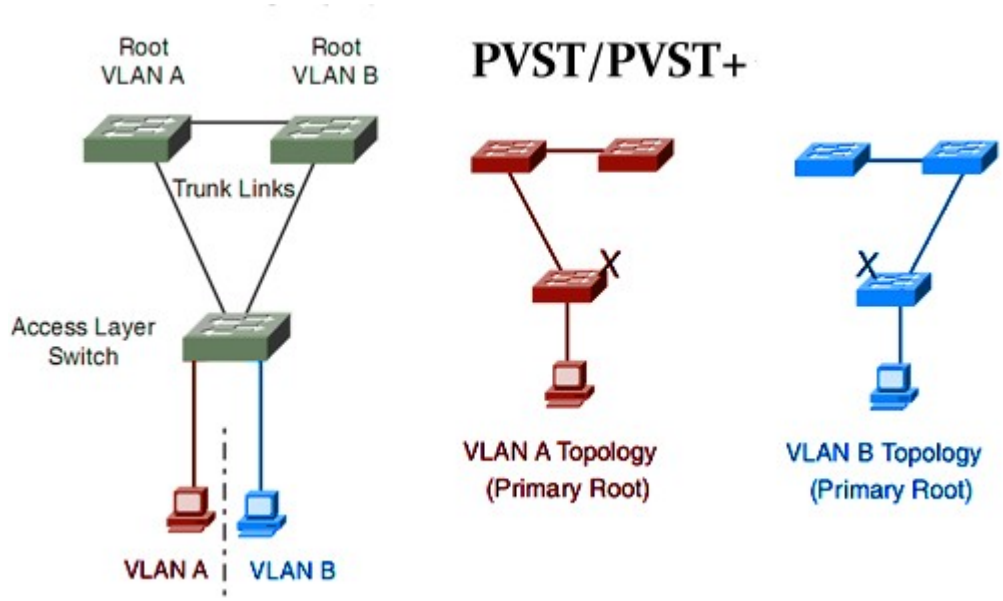
   Root bridge uses the forwarding table short lifetime during this period
6. **Sends Conf-BPDU with TC=1**

   Bridge 1 uses the forwarding table short lifetime while receiving Conf-BPDU with TC=1

   Bridge 2 uses the forwarding table short lifetime while receiving Conf-BPDU with TC=1

Other Protocols (1)

- Cisco's proprietary versions of SPT are:
  - Per-VLAN Spanning Tree (PVST).
  - Per-VLAN Spanning Tree Plus (PVST+).
- Create a different spanning tree for each VLAN.
  - Different roots, costs, blocked ports, etc...
  - In a complex switching network some switches may not have ports of all VLAN.




```
Ethernet II, Src: c2:00:05:7f:f1:01 (c2:00:05:7f:f1:01), Dst: PVST+ (01:00:0c:cc:cc:cd)
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 1
   000. .... .... .... = Priority: 0
   ...0 .... .... .... = CFI: 0
   .... 0000 0000 0001 = ID: 1
   Length: 50
Logical-Link Control
Spanning Tree Protocol
   Protocol Identifier: Spanning Tree Protocol (0x0000)
   Protocol Version Identifier: Spanning Tree (0)
   BPDU Type: Configuration (0x00)
▷  BPDU flags: 0x00
▷  Root Identifier: 32768 / 0 / c2:00:05:7f:00:00
   Root Path Cost: 0
▷  Bridge Identifier: 32768 / 0 / c2:00:05:7f:00:00
   Port identifier: 0x802a
   Message Age: 0
   Max Age: 20
   Hello Time: 2
```

Identificador da VLAN

Other Protocols (2)

- IEEE 802.1p
  - Extension of IEEE 802.1Q.
  - Provides QoS based on relative priorities.
  - Defines the field *User Priority* (3 bits) that allows 8 levels of priority.
  - The standard recommends:
    - Priority 7 : Critical traffic,
    - Priorities 5–6 : Delay sensitive traffic (voice and live video),
    - Priorities 1–4 : Delay variation sensitive traffic (*streaming*),
    - Priority 0 : Other traffic.

Other Protocols (3)

- IEEE 802.1w Rapid Spanning Tree Protocol
  - Extension of IEEE 802.1D.
  - Speeds up the convergence time of the Spanning Tree in case of topology changes
    - There are only three port states in RSTP that correspond to the three possible operational states.
    - Adds two additional port roles to a port when in blocking state
      - Alternate port: possible alternative Root port.
      - Backup port: possible alternative Designated port.
  - Adds a negotiated mechanism between switches.
    - Uses the reserved bits in the Conf-BPDU.

Conf (Configuration) BPDU

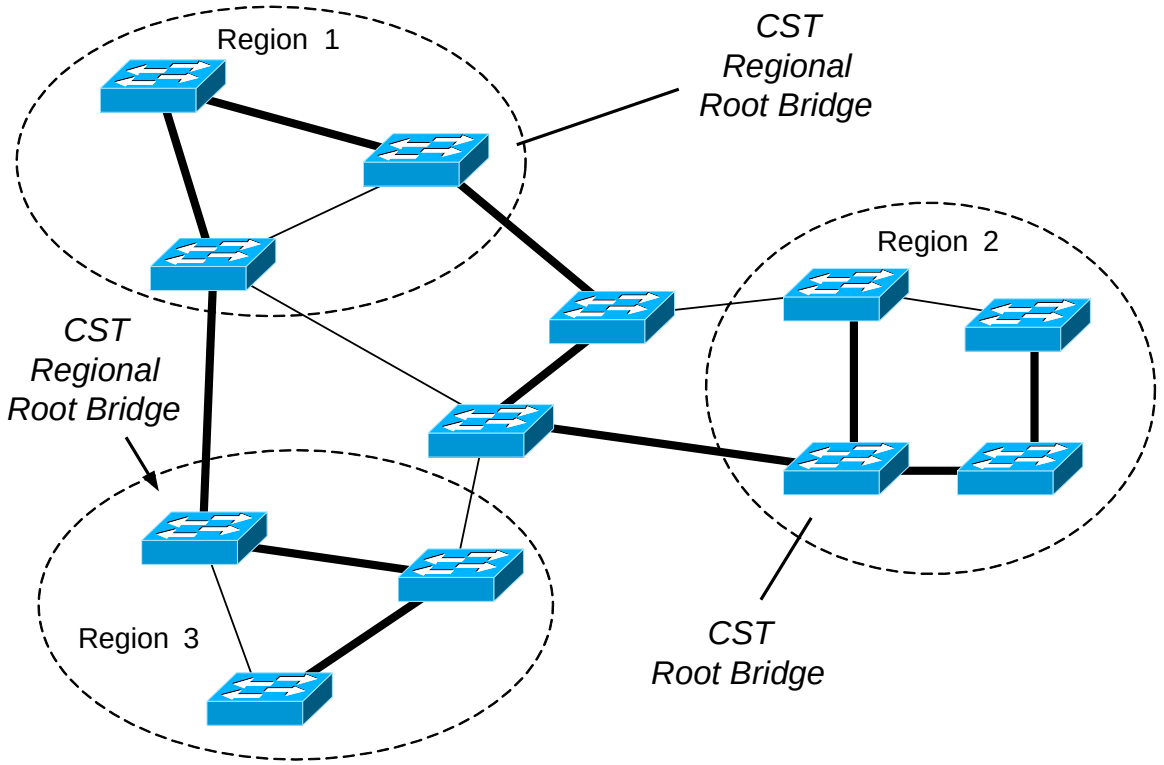
protocol identifier		
version		
message type = 0		
TCA	reserved	TC
root ID		
root path cost		
bridge ID		
port ID		
message age		
max age		
hello time		
forward delay		

STP (802.1D) Port State	RSTP (802.1w) Port State	Is Port Included in Active Topology?	Is Port Learning MAC Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

Other Protocols (4)

- IEEE 802.1s Multiple Spanning Tree Protocol
  - Creates multiple Spanning Trees.

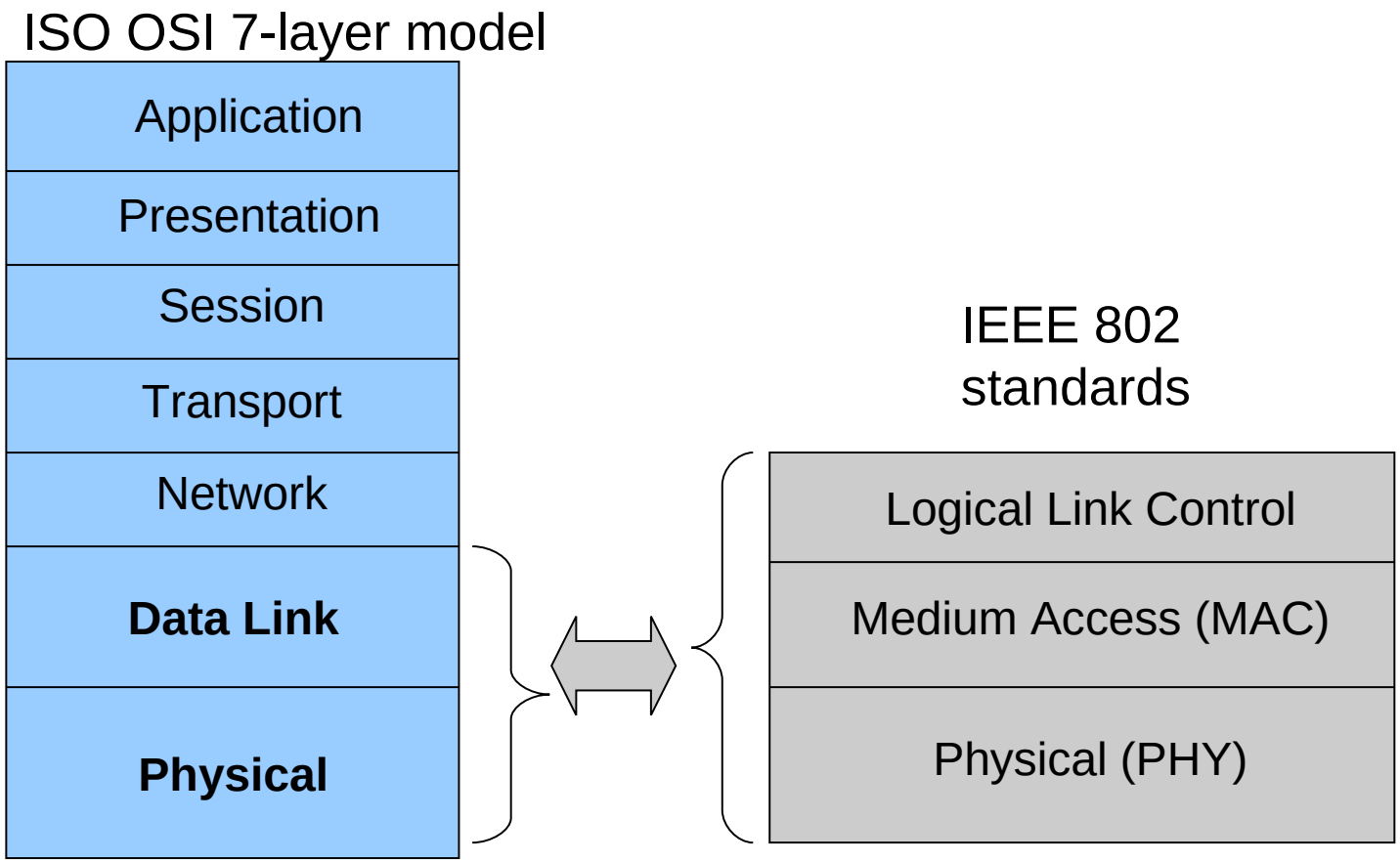
    Allows the assignment of a set of several VLAN to a specific Common Spanning Tree (CST).
    - CST are usually mapped to regions of the network.



Wi-Fi

Standardization of Wireless Networks

- Wireless networks are standardized by the IEEE under the 802 LAN MAN standards committee.



Wireless Networks

- Networks are designed according to the number of users and coverage area
- There are several scales on the number of users and coverage area
  - **Local: LANs → IEEE 802.11**
  - Personal: PANs → e.g. Bluetooth, ZigBee
  - Regional: WANs → GSM, UMTS, LTE, 5G, LoRa,...
  - Worldwide : Satellite → Iridium, SpaceX Starlink?

Wireless LAN: Oveview

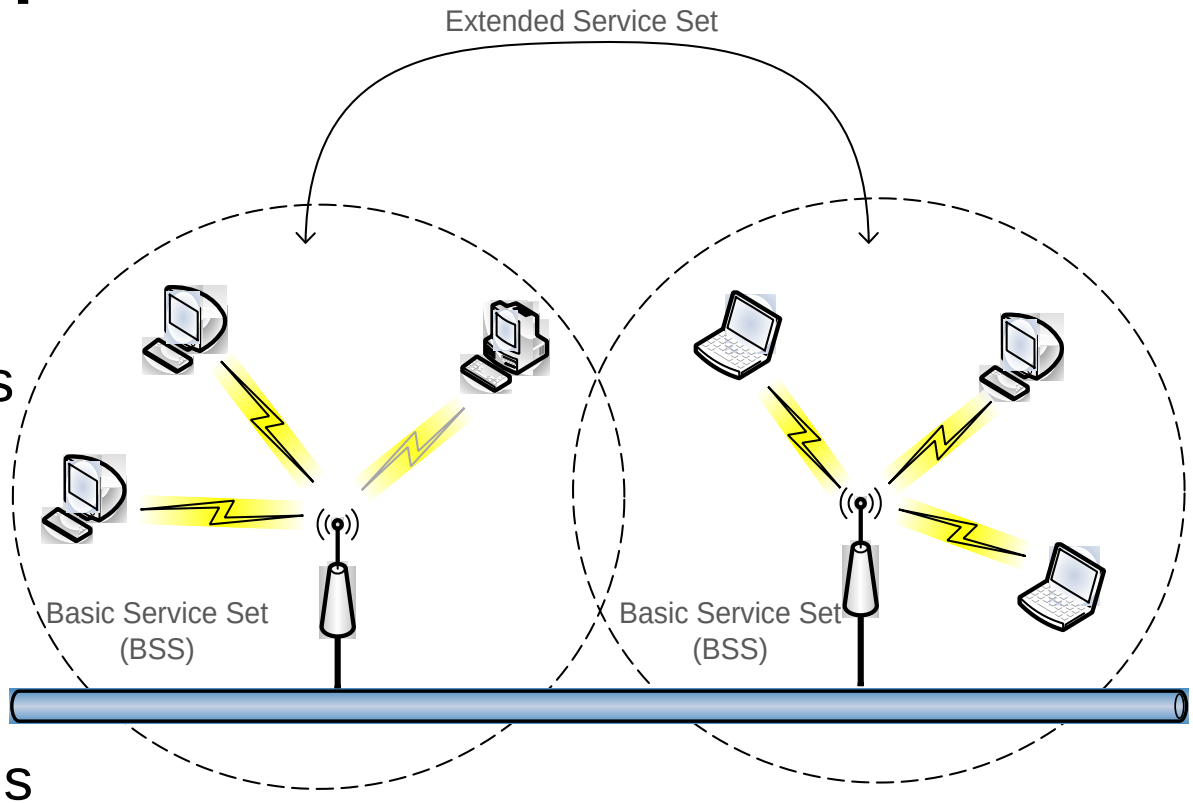
- Two Types
  - Infra-structured,
  - Ad-hoc.
- Advantages
  - Flexible installation (minimum cables).
  - More robust (no cable problems).
  - One-time installation (conferences, historic buildings).
- Problems
  - Many proprietary solutions.
  - Restrictions on the electromagnetic spectrum.
  - Subject to frame collision when accessing the transmission medium.
    - More on this later.
  - Lower bandwidths than cabled networks.

Evolution of WLAN standards

- WiFi 1 - 802.11b, 1999, 2.4 GHz band, 11 Mbps data rate
- WiFi 2 - 802.11a, 1999, 5 GHz band, 54 Mbps data rate
- WiFi 3 - 802.11g, 2003, 2.4 GHz band, 54 Mbps data rate
- WiFi 4 - 802.11n, 2009, 2.4 and 5 GHz bands, ~600 Mbps data rate
- WiFi 5 - 802.11ac, 2013, 5 GHz band, ~1.3 Gbps data rate
- WiFi 6 - 802.11ax, 2019, 1 to 7GHz bands, >11Gbps data rate

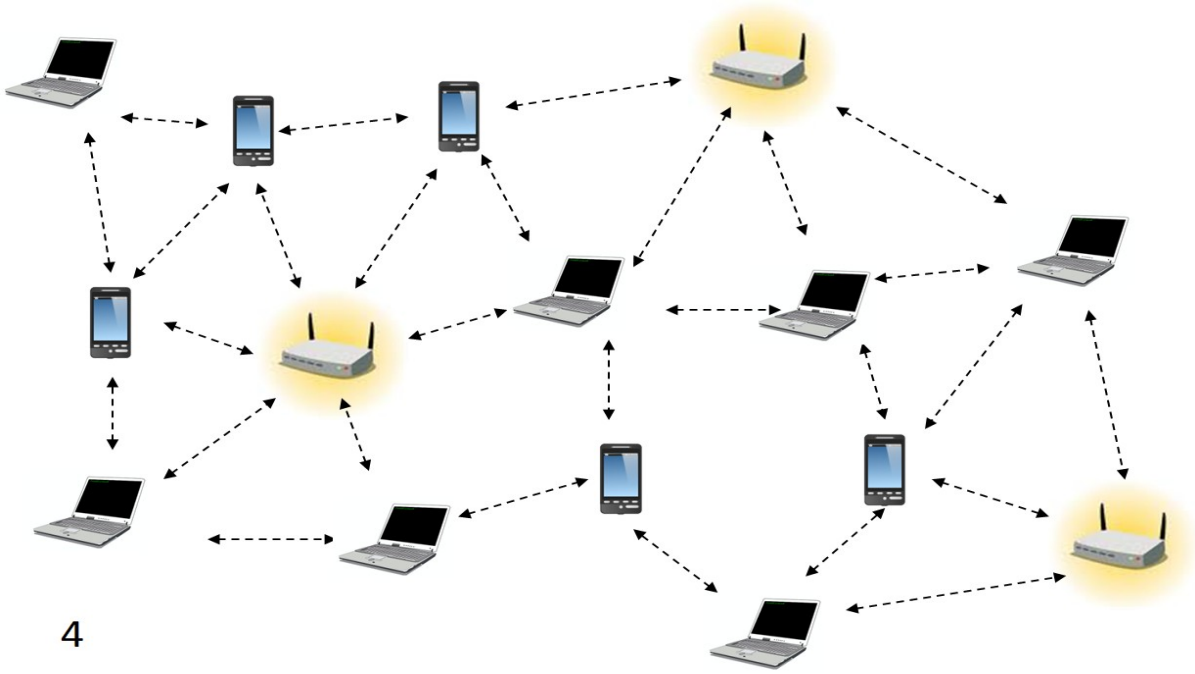
Components

- Station (STA)
  - Mobile terminal
- Access Point (AP)
  - STA connect to access points (infra-structured networks)
- Basic Service Set (BSS)
  - STA and AP with same coverage form a BSS
  - Group of IEEE 802.11 stations associated to an Access Point (AP)
  - Known through the SSID
- Extended Service Set (ESS)
  - Several BSSs interconnected by APs form a ESS



Ad-hoc Networks (IBSS)

- Temporary set of stations
- Forming an ad-hoc network – an independent BSS (IBSS), means that there is no connection to a wired network
- No AP
- No relay function (direct connection)
- Simple setup

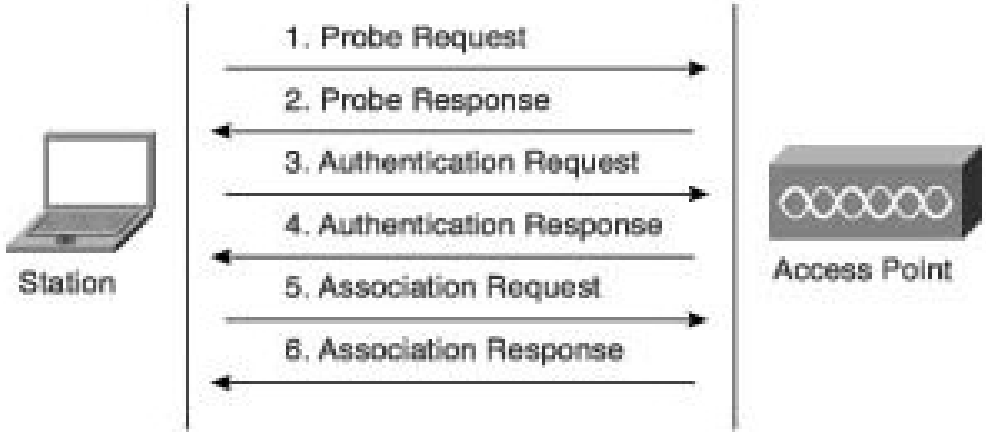


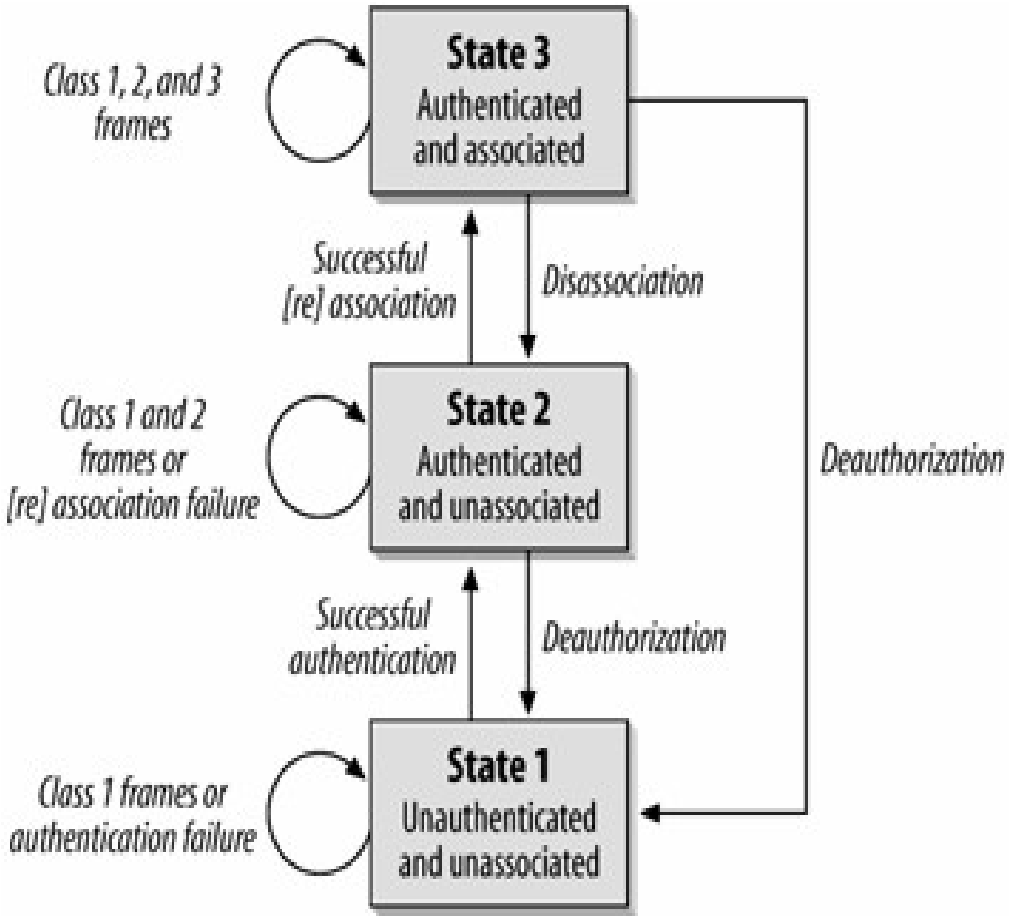
IEEE 802.11 services

- Station services (similar to wired network)
  - Authentication (login)
  - De-authentication (logout)
  - Privacy
  - Data delivery
- Distribution services
  - Association
    - Make logical connection between the AP and the station – the AP will not receive any data from a station before association
  - Re-association (similar to association)
    - Send repeatedly to the AP.
    - Help the AP to know if the station has moved from/to another BSS.
    - After Power Save
  - Disassociation
    - Manually disconnect (PC is shutdown or adapter is ejected)

Joining a BSS

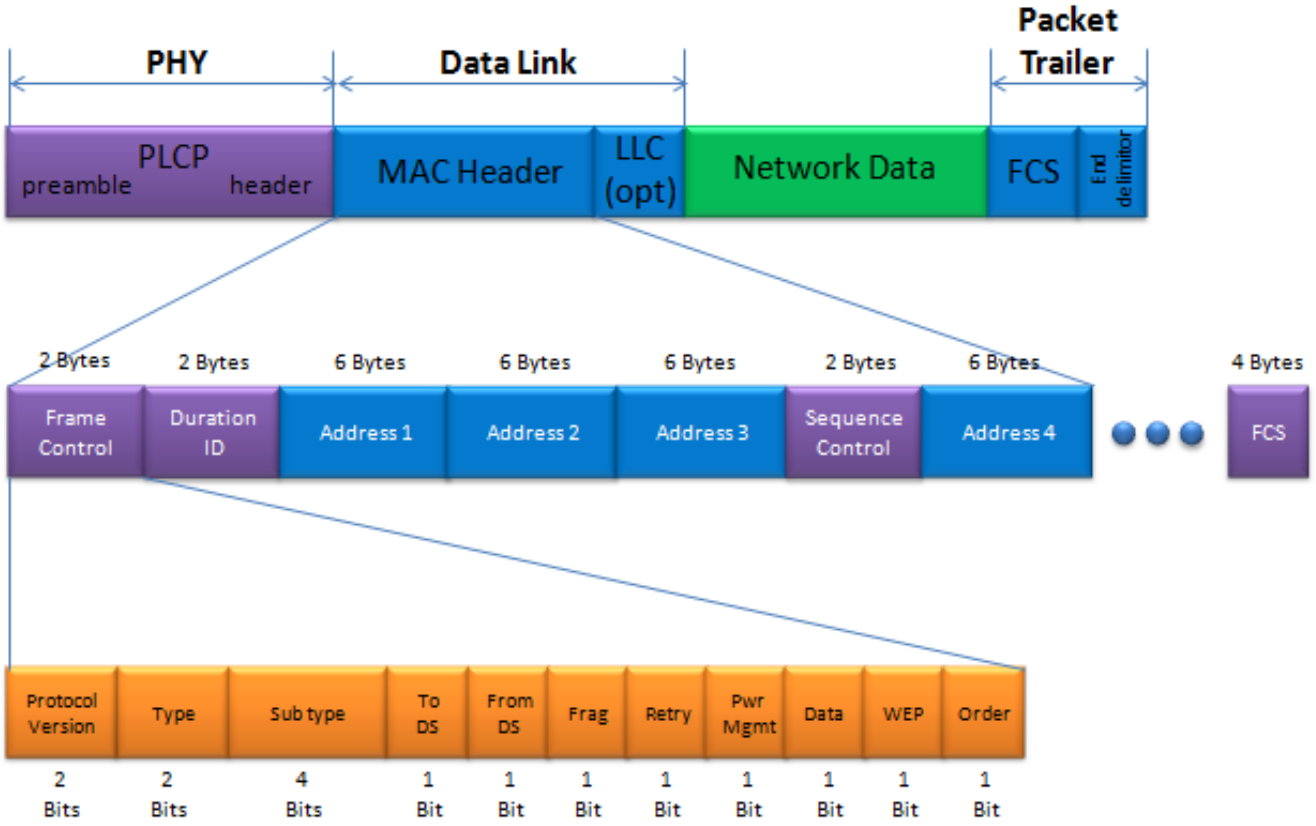
- Station finds BSS/AP by **Scanning/Probing**.
- BSS with AP: both **Authentication** and **Association** are necessary for joining a BSS.





WLAN Frames

- Three types of frames
  - Control: RTS, CTS, ACK
  - Management
  - Data
- Header is different for the different types of frames.



Joining BSS with AP: Scanning

- A station willing to join a BSS must get in contact with the AP. This can happen through:
- 1. Passive scanning
  - The station scans the channels for a Beacon frame that is sent periodically from an AP to announce its presence and provide the SSID, and other parameters for WNICs within range
- 2. Active scanning (the station tries to find an AP)
  - The station sends a Probe Request frame - Sent from a station when it requires information from another station
  - All AP's within reach reply with a Probe Response frame - Sent from an AP containing capability information, supported data rates, etc., after receiving a probe request frame

Beacon Frame

```
▾ IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
  ▸ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1001 1000 1010 .... = Sequence number: 2442
    Frame check sequence: 0x6f0b825c [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 660070796
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0421
  ▾ Tagged parameters (123 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Cisco CCX1 CKIP + Device Name
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Probe Request/Response Frames

```
▾ IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  ▸ Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
    Source address: Microsof_0a:43:e3 (c0:33:5e:0a:43:e3)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    1100 1011 0001 .... = Sequence number: 3249
    Frame check sequence: 0xc7056d0a [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Tagged parameters (62 bytes)
    ▸ Tag: SSID parameter set: TD_WIFI_GUEST
    ▸ Tag: Supported Rates 1, 2, 5.5, 6, 9, 11, 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: HT Capabilities (802.11n D1.10)
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```

```
▾ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▸ Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
    Destination address: IntelCor_d2:98:58 (28:b2:bd:d2:98:58)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1010 0010 1001 .... = Sequence number: 2601
    Frame check sequence: 0x80831320 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (12 bytes)
      Timestamp: 664064263
      Beacon Interval: 0.102400 [Seconds]
    ▸ Capabilities Information: 0x0421
  ▾ Tagged parameters (117 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 13
    ▸ Tag: ERP Information
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Cisco CCX1 CKIP + Device Name
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (1) (1)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCX version = 5
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
    ▸ Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
```

Joining BSS with AP: Authentication

- Once an AP is found/selected, a station goes through authentication
- Open system authentication (default, 2-step process)
  - Station sends authentication frame with its identity
  - AP sends frame as an Ack / NAck
- Shared key authentication
  - Stations receive shared secret key through secure channel independent of 802.11
  - After the WNIC sends its initial authentication request, it will receive an authentication frame from the AP containing a challenge text
  - The WNIC sends an authentication frame containing the encrypted version of the challenge text to the AP.
  - The AP ensures the text was encrypted with the correct key by decrypting it with its own key.
  - The result of this process determines the WNIC's authentication status.

Authentication Frames

- Nowadays, WPA* secure networks use “Open System”.
- Non-”Open System” authentication was used for WEP protected networks (unsecured and functionally deprecated).

```
IEEE 802.11 Authentication, Flags: ........
  Type/Subtype: Authentication (0x000b)
  Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  0001 0100 1011 .... = Sequence number: 331
IEEE 802.11 wireless LAN
  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
```

← From Station

From AP →

```
IEEE 802.11 Authentication, Flags: ........C
  Type/Subtype: Authentication (0x000b)
  Frame Control Field: 0xb000
  .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
  Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
  .... .... .... 0000 = Fragment number: 0
  1010 1001 0000 .... = Sequence number: 2704
  Frame check sequence: 0x9f8350e1 [unverified]
  [FCS Status: Unverified]
IEEE 802.11 wireless LAN
  Fixed parameters (6 bytes)
    Authentication Algorithm: Open System (0)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
```

Joining BSS with AP: Association

- Once a station is authenticated, it starts the association process, i.e., information exchange about the AP/station capabilities and roaming
  - STA → AP: Associate Request frame
    - Enables the AP to allocate resources and synchronize. The frame carries information about the WNIC, including supported data rates and the SSID of the network the station wishes to associate with.
  - AP → STA: Association Response frame
    - Acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such as association ID and supported data rates.
  - New AP informs old AP (if it is a handover).
- Only after association is completed, a station can transmit and receive data frames.

Association Request/Response Frames

← From Station

```
▾ IEEE 802.11 Association Request, Flags: ........
    Type/Subtype: Association Request (0x0000)
  ▸ Frame Control Field: 0x0000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Destination address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Transmitter address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Source address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    0001 0100 1100 .... = Sequence number: 332
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (4 bytes)
    ▸ Capabilities Information: 0x0421
      Listen Interval: 0x000a
  ▾ Tagged parameters (43 bytes)
    ▸ Tag: SSID parameter set: LABCOM
    ▸ Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Extended Capabilities (8 octets)
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information E
```

From AP →

```
▾ IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x0001)
  ▸ Frame Control Field: 0x1000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Transmitter address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    Source address: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    BSS Id: Cisco_61:ee:d0 (00:1c:f6:61:ee:d0)
    .... .... .... 0000 = Fragment number: 0
    1010 1001 0001 .... = Sequence number: 2705
    Frame check sequence: 0xe7103b15 [unverified]
    [FCS Status: Unverified]
▾ IEEE 802.11 wireless LAN
  ▾ Fixed parameters (6 bytes)
    ▸ Capabilities Information: 0x0421
      Status code: Successful (0x0000)
      ..00 0000 0000 0001 = Association ID: 0x0001
  ▾ Tagged parameters (42 bytes)
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Data Frame

```
▾ IEEE 802.11 QoS Data, Flags: .p.....TC
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8841
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    Transmitter address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Destination address: D-LinkIn_6a:cc:6e (84:c9:b2:6a:cc:6e)
    Source address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0011 .... = Sequence number: 3
    Frame check sequence: 0xc72771e8 [unverified]
    [FCS Status: Unverified]
  ▸ Qos Control: 0x0000
  ▸ CCMP parameters
▾ Data (1244 bytes)
    Data: f8002648417037bc923106ead1717d4821fde0989beb08b1…
    [Length: 1244]
```

← Node that will receive frame (AP)
← Node that send frame
← Station to receive data
← Station who sent data

- Station “IntelCor*” sending data to station “D-LinkIn*” (via AP).
- Frame captured between station “IntelCor*” and AP (“Cisco*”).

Authentication and authorization mechanisms

- Changing according to the organization and the security level
  - Open network
  - Open network + MAC authentication
  - Open network + VPN-gateway
  - Open network + web-gateway
  - SSID
  - Shared key: WEP
  - Wi-Fi Protected Access (WPA)
  - IEEE 802.11i (WPA2)
  - IEEE 802.1X
  - Virtual Private Networks (VPNs)

Open Network(s)

- Open network
  - Network is open, providing IP addresses with DHCP
  - There is no authentication and access is free
  - Does not require specific software
  - Access control is complicated
  - It is possible to ‘see’ all traffic in the network (sniffing)
- Open network + MAC authentication
  - The control of the station MAC address is added
  - Larger management load
    - ... But MAC addresses can be falsified
    - ... Difficult to support guests
    - ... Impossible to use in public environments

Open Network + Gateways

- Open Network + VPN gateway.
  - Open network, with the client being authenticated in an IP VPN (L3) in order to be able to access its network from outside.
    - Requires VPN client software.
    - Difficult to use by guests.
    - Scalability is being enhanced.
    - VPN controllers can be expensive.
- Open network + web gateway.
  - Open network, with the client being authenticated in web server (L3), providing “credentials”.
    - Easy to use by guests.
    - Standardization is being enhanced.
    - Scalability is being enhanced.
    - A browser needs to be working during the session.

Service Set ID (SSID)

- **SSID – name of the network.**
- Identifies the BSS, emitted in the beacon.
- Networks can block beacon and force the AP to be directly specified by its name.
- This is not very efficient.
  - Operating systems are smarter.
  - The change of SSID requires a new advertisement to all stations.
  - With the increasing number of stations, security will decrease.
  - SSID is only useful to the self-organization of the stations, not to security.

WEP Protocol

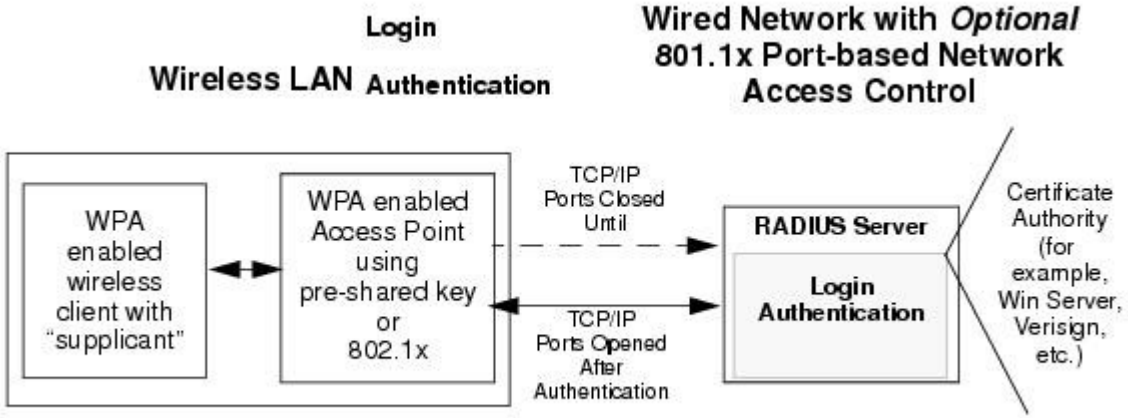
- Wired Equivalent Privacy → shared key scheme.
- Part of basic 802.11 standard.
- Security protocol at link layer (L2).
- Designed to be computationally efficient and self-synchronized.
- The station has to know the key (like a password) to access the AP.
- With passive monitoring, it can be broken (in seconds)
  - Header is not ciphered, all destinations and origins are visible.
  - Control frames are not ciphered, and then they can be changed.
  - AP is not authenticated and can be falsified.
  - **Should not be implemented!**

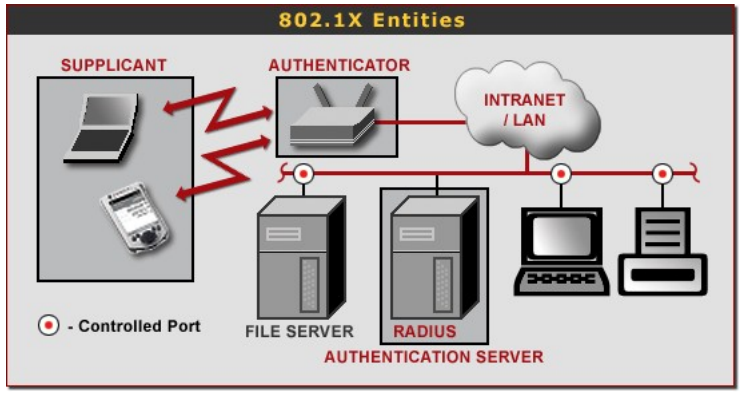
WPA and 802.11i (WPA2)

- **IEEE 802.11i - IEEE 802.11 task group “MAC enhancement for wireless security”.**
- **Wi-Fi Protected Access (WiFi Alliance), WPA, is a subset internal in 802.11i.**
  - Compatible with work developed in 802.11i.
  - Only supports BSS.
  - Defined to work in actual equipment.
    - Firmware update only.
  - Pass-phrase constant and shared, but keys are generated per session.
  - Used in the AP and station.
  - Uses “Open System” during authentication phase.
- WPA has two distinct components.
  - Authentication, based on 802.1X.
  - Ciphering based on TKIP (Temporal Key Integrity Protocol).

IEEE 802.1X

- Layer 2 solution between station and AP.
  - Available in many equipments (e.g. IEEE 802.xx).
  - Web systems frequently use 802.1X.
- Several authentication-mechanisms available (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP)
- Multiple standard ciphering algorithms .
- Can cipher data with dynamic keys.
- Resorts to RADIUS servers.





WPA* Key Exchange

- Done during the Association process.
  - After Association Request/response frames.

```
205 595.669409767  IntelCor_e8:14:53   Cisco_61:ee:d1      802.11   110 Association Request, SN=38, FN=0, Flags=........, SSID=LABCOM_SEC
206 595.671214291  Cisco_61:ee:d1      IntelCor_e8:14:53   802.11   128 Association Response, SN=14, FN=0, Flags=........
207 595.673042781  Cisco_61:ee:d1      IntelCor_e8:14:53   EAPOL    211 Key (Message 1 of 4)
208 595.678333124  IntelCor_e8:14:53   Cisco_61:ee:d1      EAPOL    168 Key (Message 2 of 4)
209 595.681795313  Cisco_61:ee:d1      IntelCor_e8:14:53   EAPOL    269 Key (Message 3 of 4)
210 595.683690439  IntelCor_e8:14:53   Cisco_61:ee:d1      EAPOL    146 Key (Message 4 of 4)

▸ Frame 207: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits) on interface 0
▸ Radiotap Header v0, Length 56
▸ 802.11 radio information
▾ IEEE 802.11 QoS Data, Flags: ......F.
    Type/Subtype: QoS Data (0x0028)
  ▸ Frame Control Field: 0x8802
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Transmitter address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    Destination address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    Source address: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    BSS Id: Cisco_61:ee:d1 (00:1c:f6:61:ee:d1)
    STA address: IntelCor_e8:14:53 (b8:8a:60:e8:14:53)
    .... .... .... 0000 = Fragment number: 0
    0000 0001 1100 .... = Sequence number: 28
  ▸ Qos Control: 0x0007
▸ Logical-Link Control
▾ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  ▸ Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 4f65d0b4e9e77b88f2cbb135749eeb105a3aa1ef65de66a8…
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
  ▸ WPA Key Data: dd14000fac046616ebb59b83e8cc1816ced0e542a935
```