Local Area Networks (LAN)

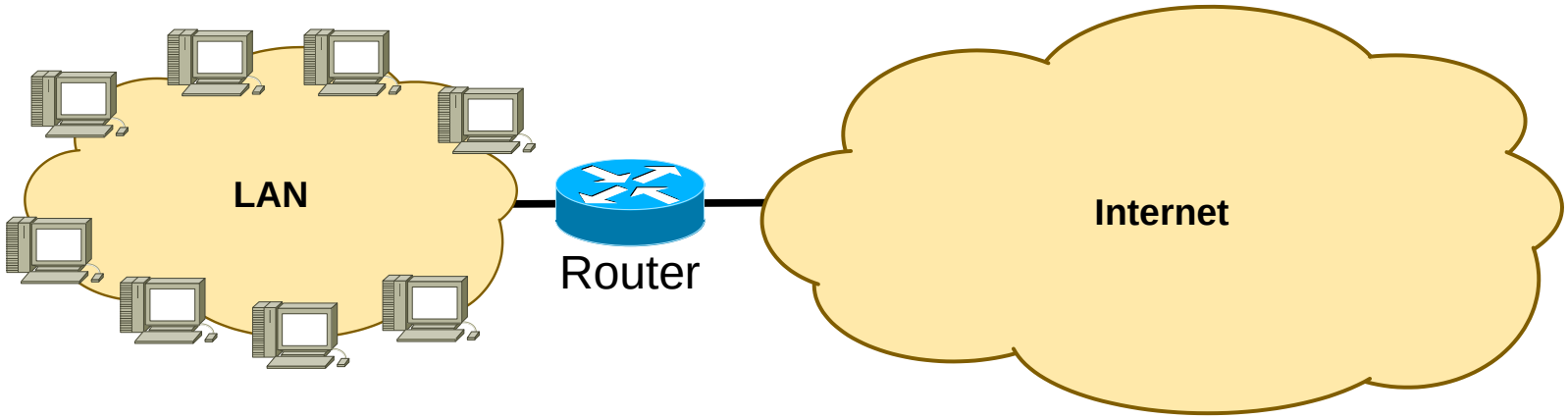
Redes de Comunicações II

Licenciatura em
Engenharia de Computadores e Informática
DETI-UA

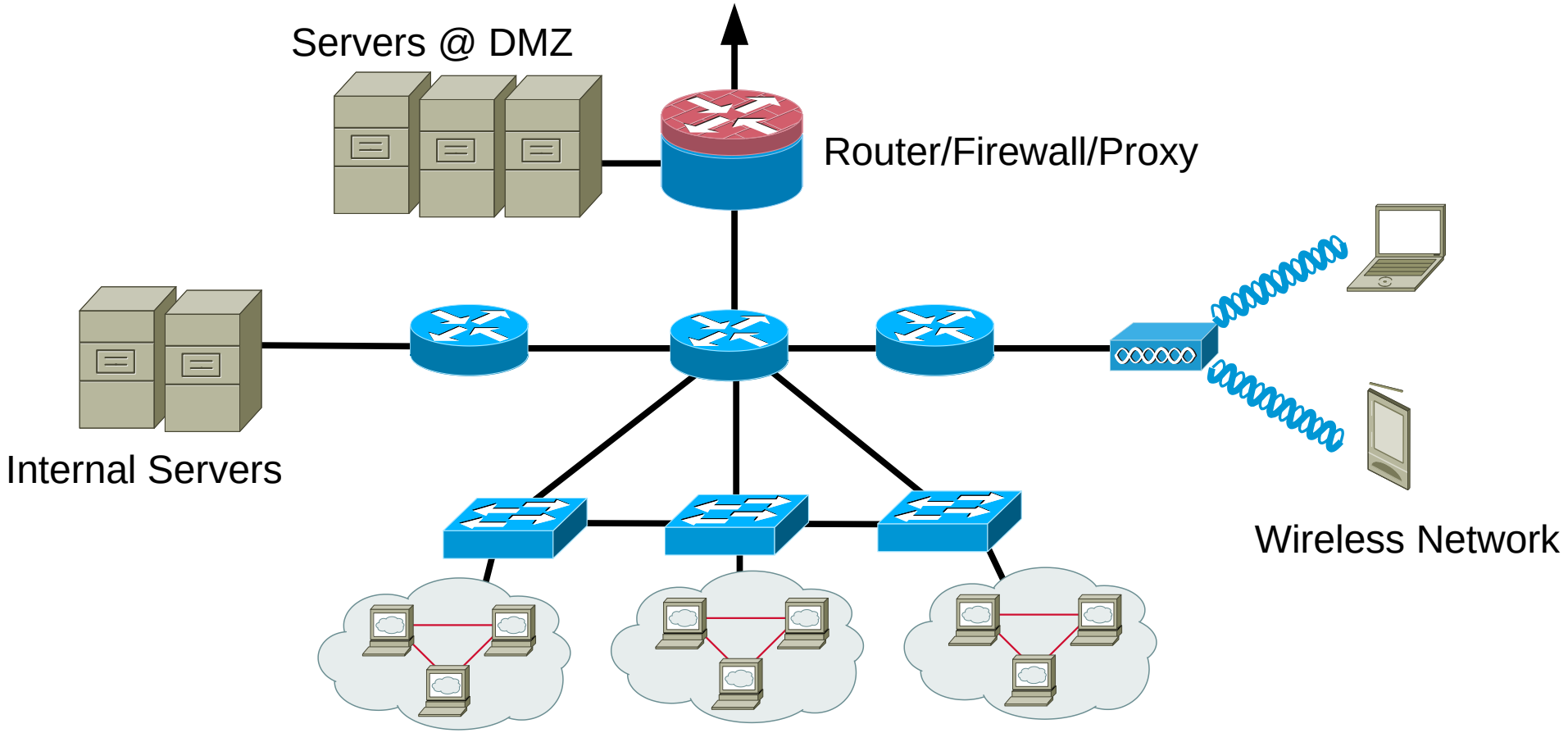
universidade de aveiro
deti.ua.pt

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, …

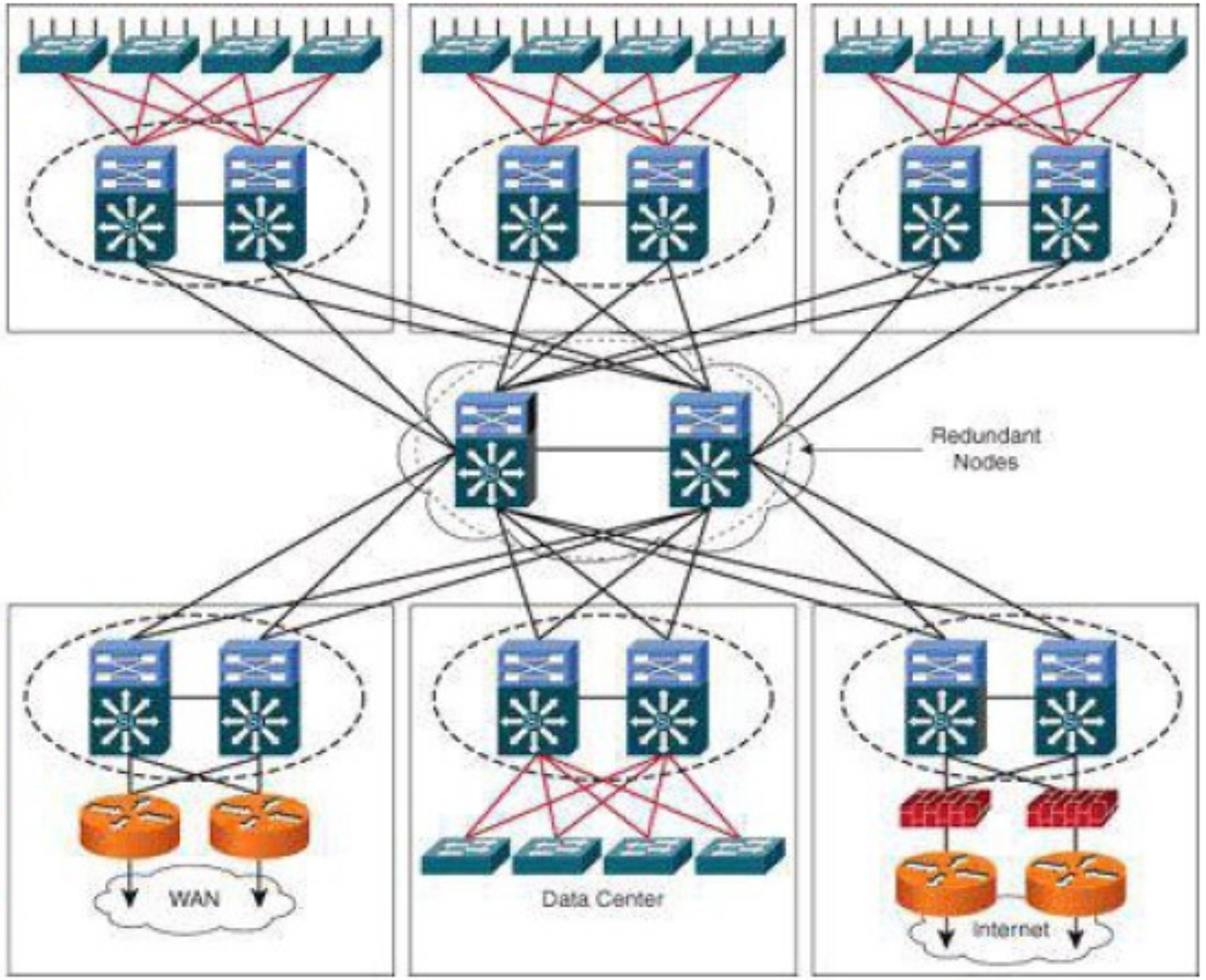


Corporate Access Networks: Small LAN



Corporate Access Networks: Medium/Large LAN

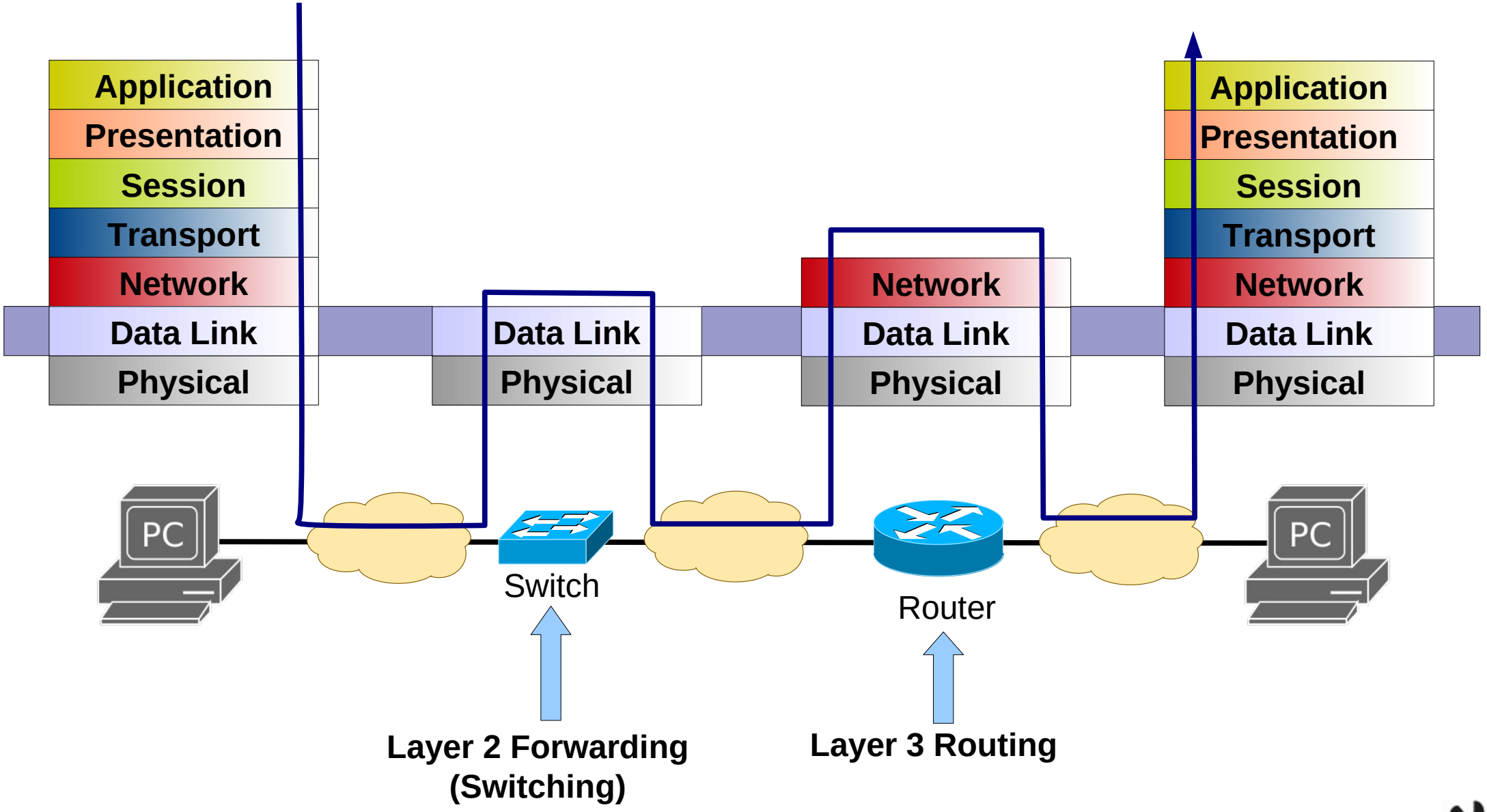
- Hierarchical architecture



Ethernet (802.3)

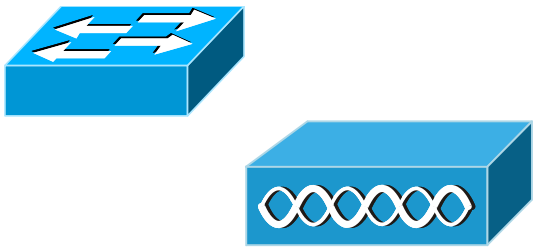
- Most successful LAN technology.
- Invented at Xerox Palo Alto Research Center (PARC).
- Xerox, DEC and Intel defined in 1978 the standard for Ethernet 10Mbps.
- Uses “Carrier Sense/Multiple Access” with “Collision Detect” (CSMA/CD)
  - Carrier Sense: hosts can perceive is the communication channel 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.

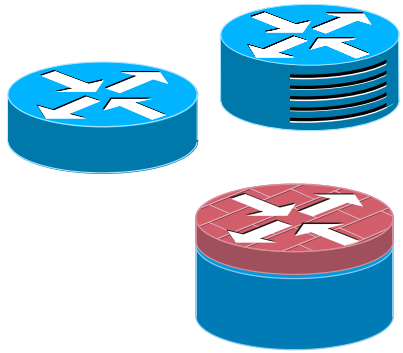
Ethernet based LAN

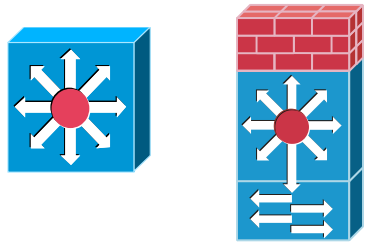


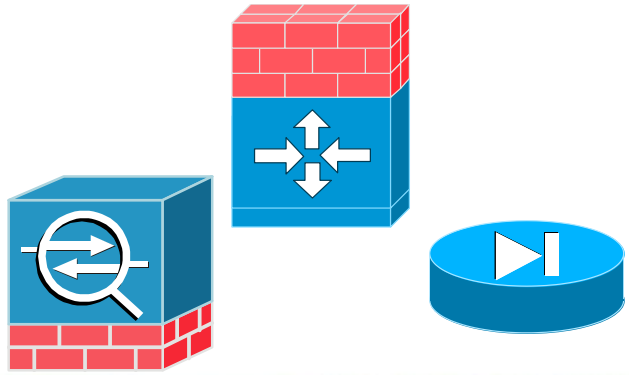
Network Devices

- Switch
  - OSI Layer 2 inter-connection
  - Implements VLAN
  - Spanning-tree based routing
    - STP, RSTP, MSTP
  - Wireless Access Points
- Router
  - OSI Layer 3 inter-connection
  - Have extra functionalities like QoS, Security, VPN gateway, network monitoring, etc...
- L3 Switch
  - Switch+Router
  - Low-end and mid-end range routing functionalities are limited
  - High-end have full routing functionalities
  - Many have dedicated L2 routing hardware
- Router with switching modules
  - L3 Switch with full routing capabilities
- Load-Balancer
- Firewall
- IDS/IPS (Intrusion Detection/Prevention System)
- VPN Gateway/Server
- Services proxy



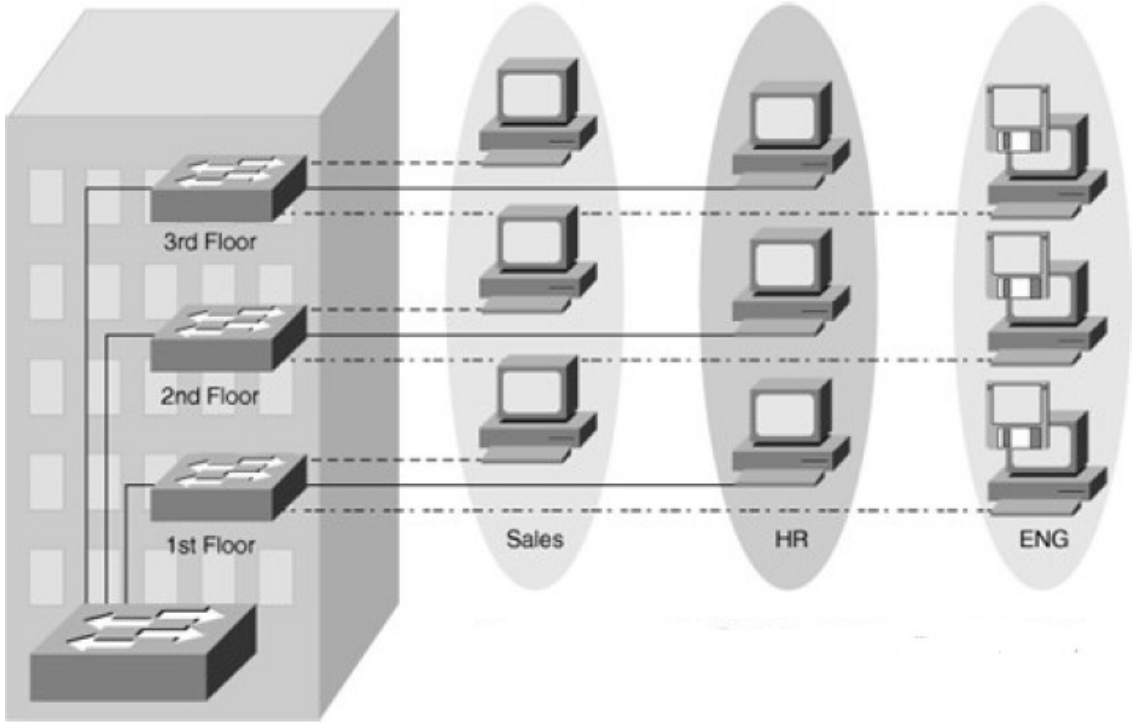






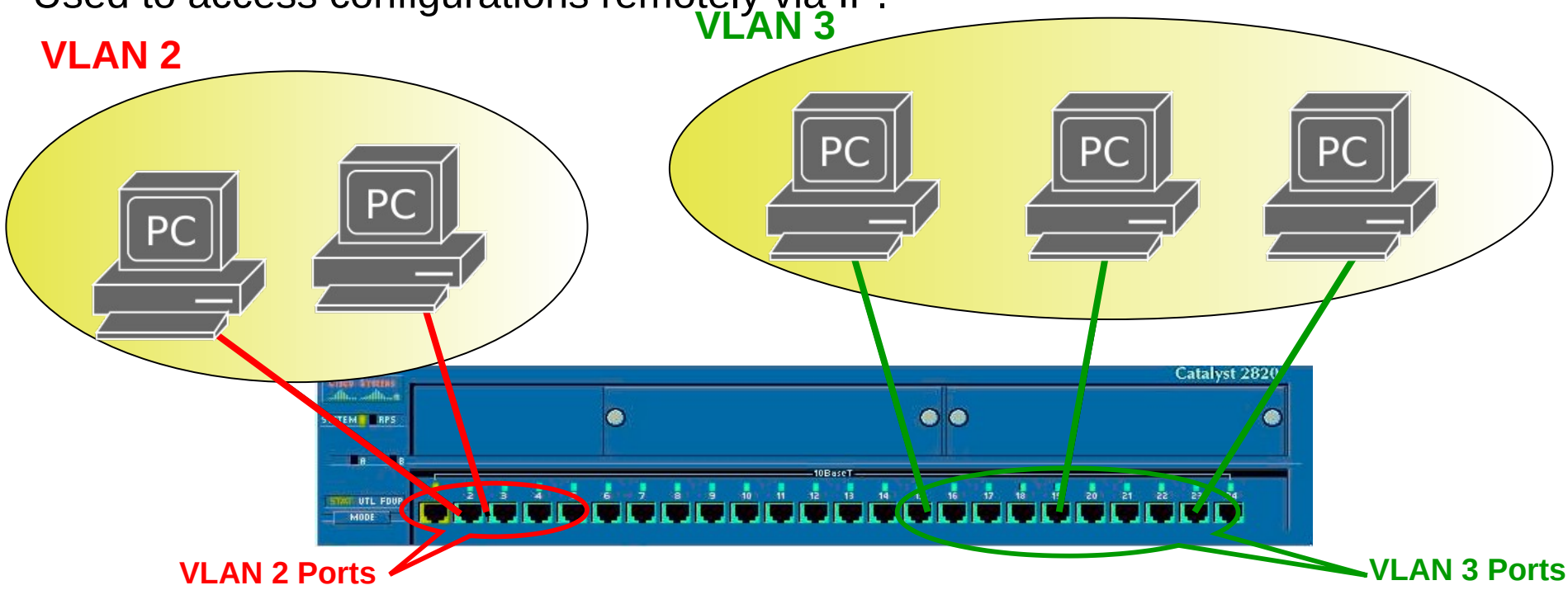
Virtual LAN (VLAN)

- 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).



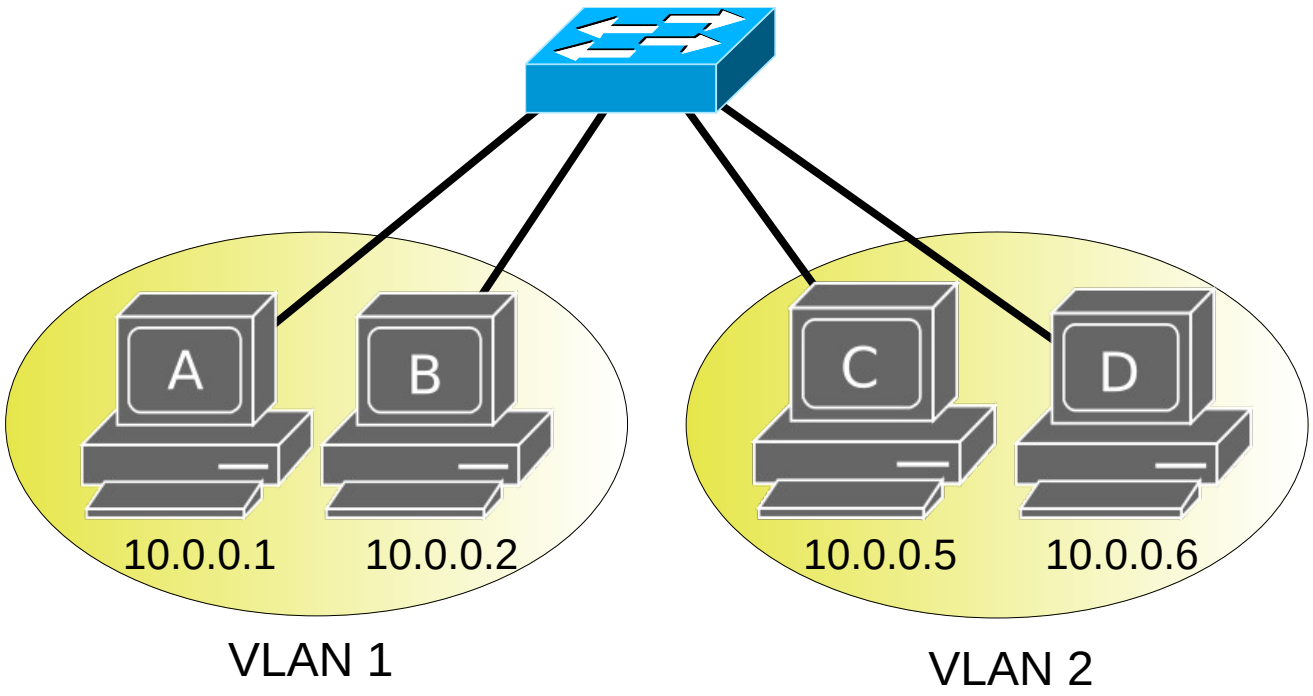
Defining Host VLAN

- 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

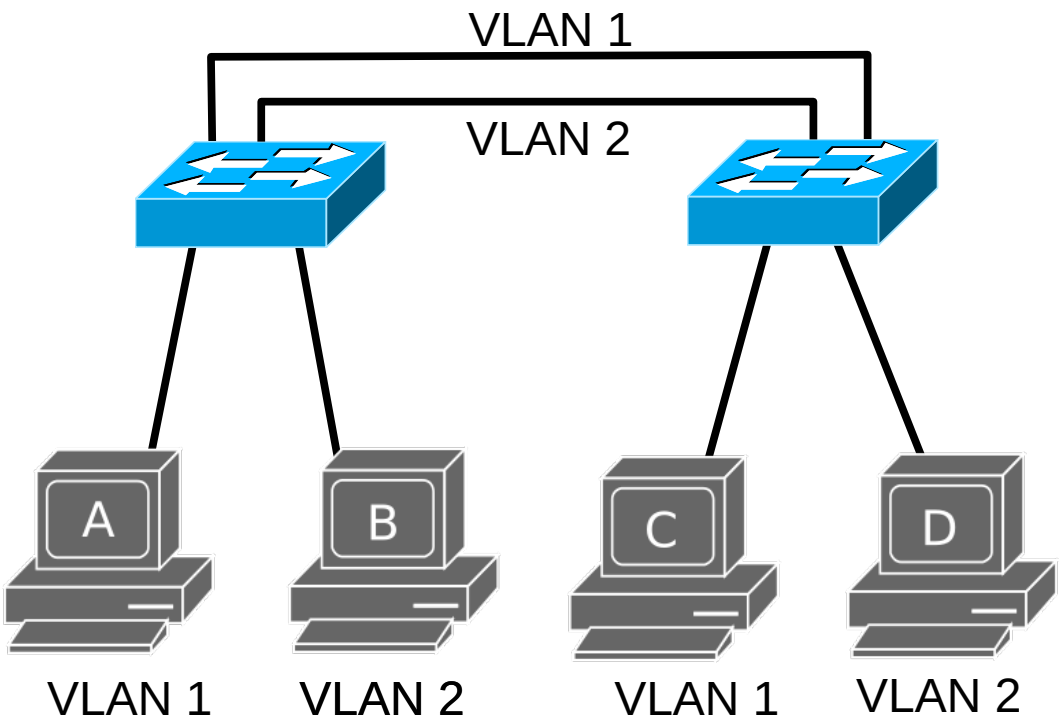
Pings sent by 10.0.0.1



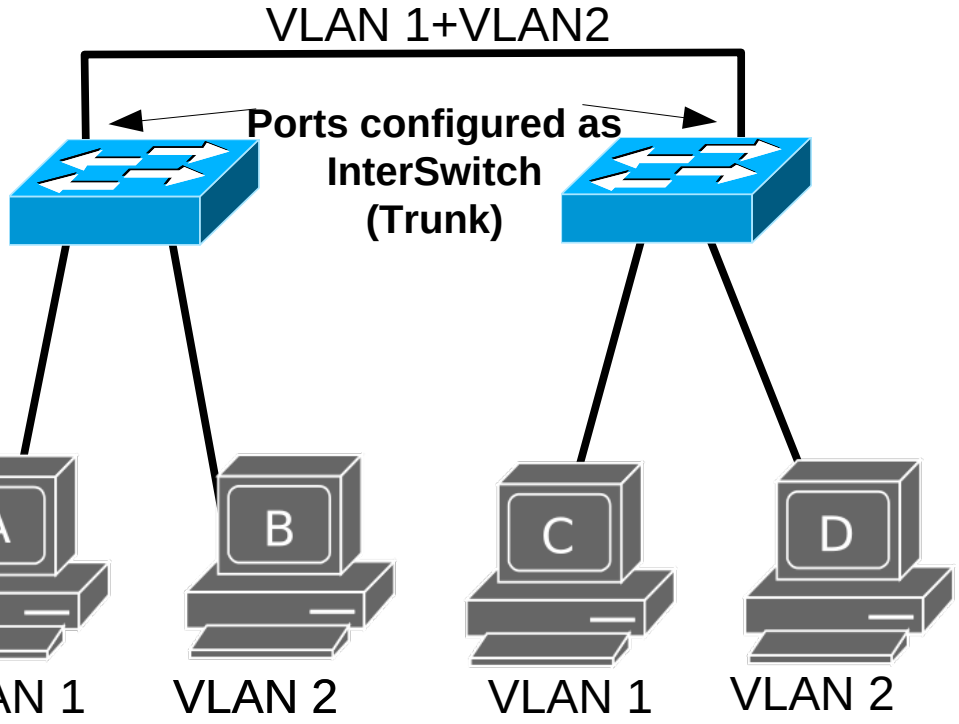

```
# ping 10.0.0.2

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

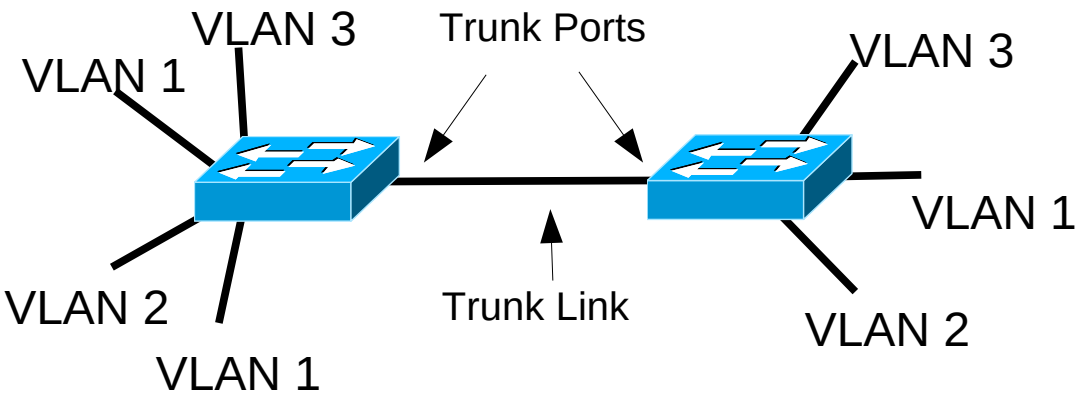


- With a single physical link.
- Using InterSwitch/Trunk port(s).

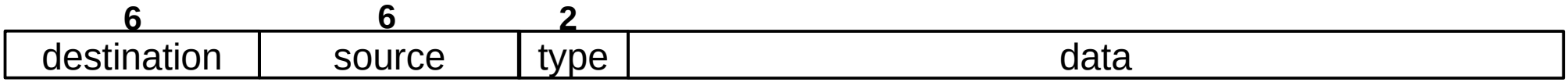


- Using a single physical link requires a mechanism to differentiate frames from different VLAN.
  - Frames must have a tagged
    - Added when forwarding to a trunk port.
    - Read and removed when receiving a frame from a trunk port

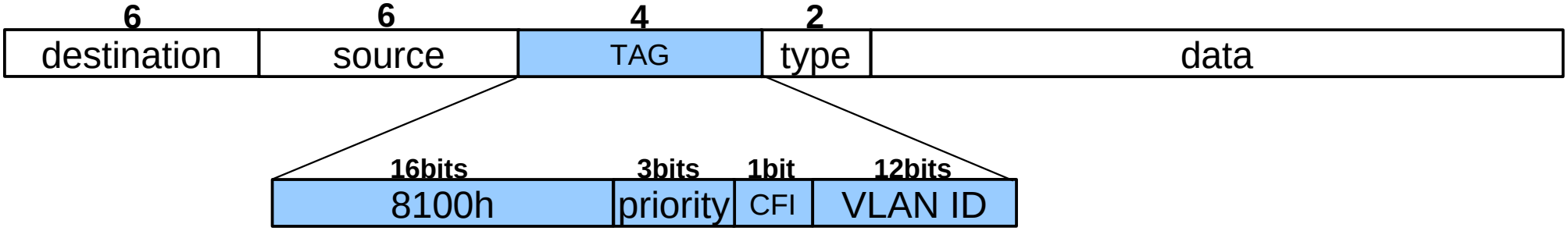
IEEE802.1Q Standard



Ethernet frame without a VLAN tag



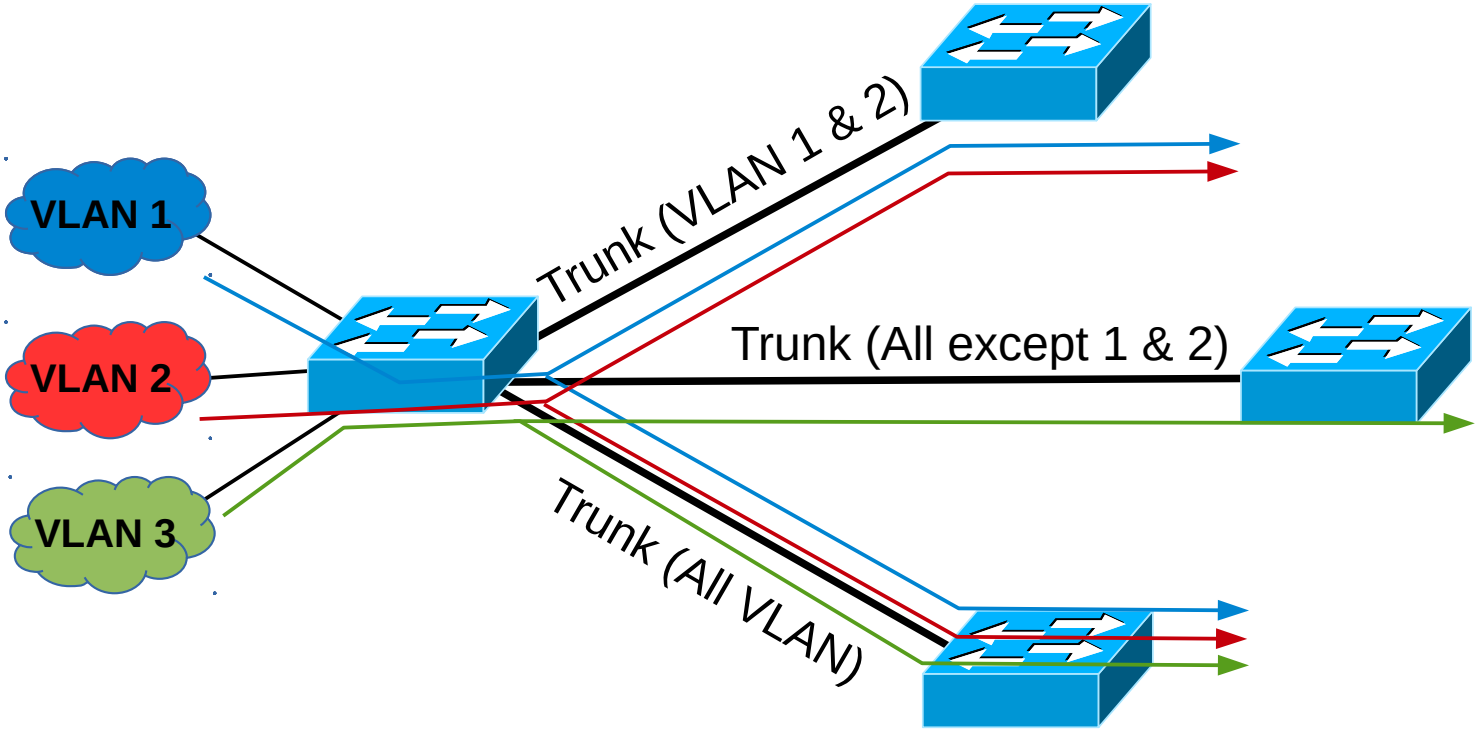
Ethernet frame with a VLAN tag



- 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!



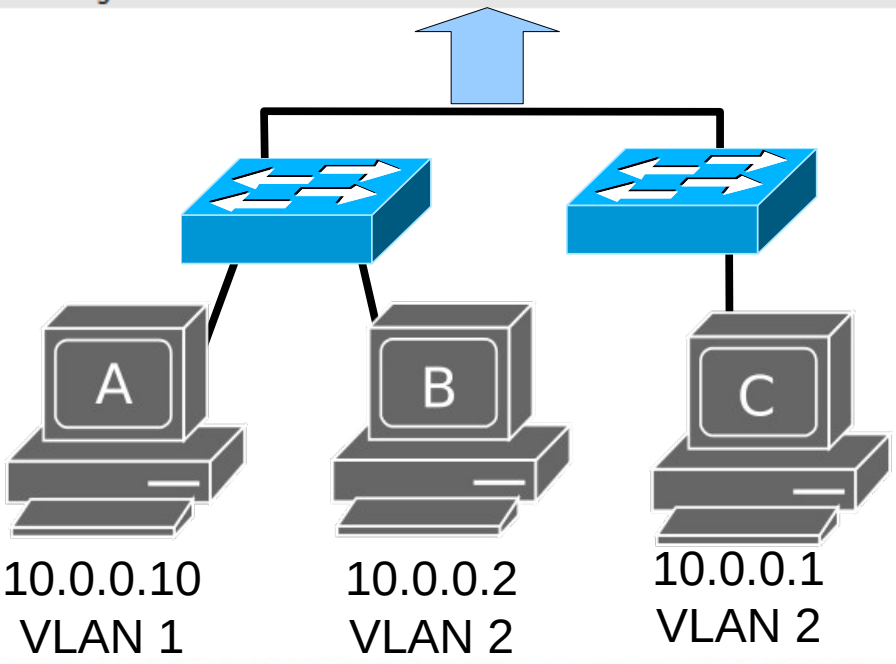
Example – InterSwitch/Trunk Ports

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

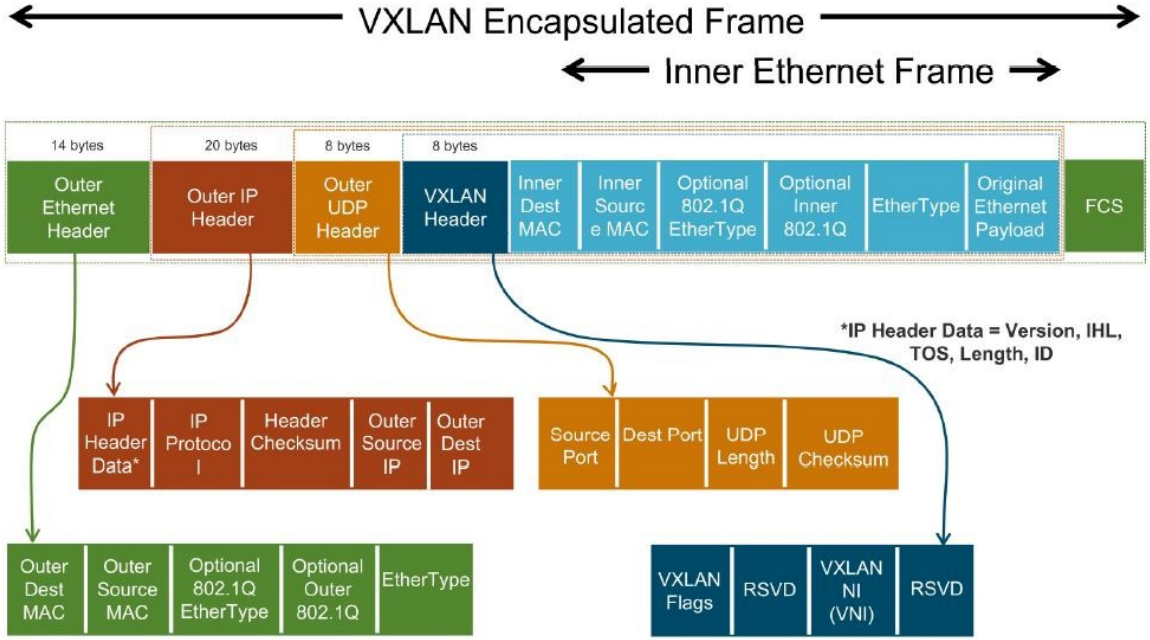
```
▷ Frame 23 (102 bytes on wire, 102 bytes captured)
▷ Ethernet II, Src: 00:aa:00:53:7c:00 (00:aa:00:53:7c:00), Dst: 00:aa:00:fa:67:00 (00:aa:00:fa:67:00)
▽ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 2
    000. .... .... .... = Priority: 0
    ...0 .... .... .... = CFI: 0
    .... 0000 0000 0010 = ID: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



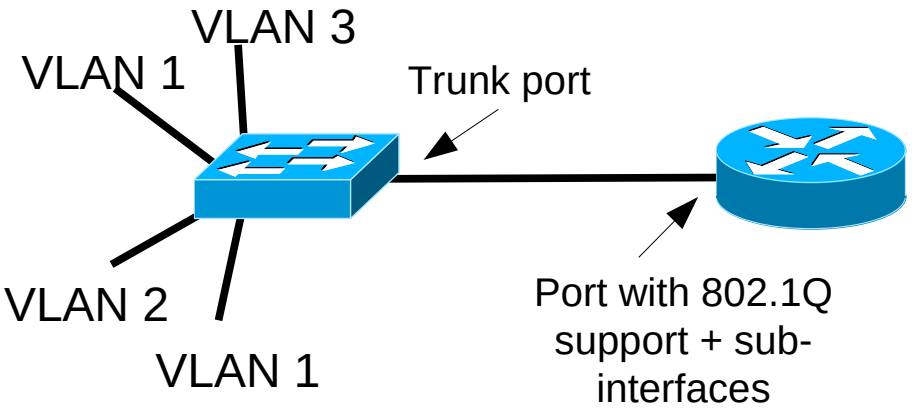
Virtual Extensible LAN (VXLAN)

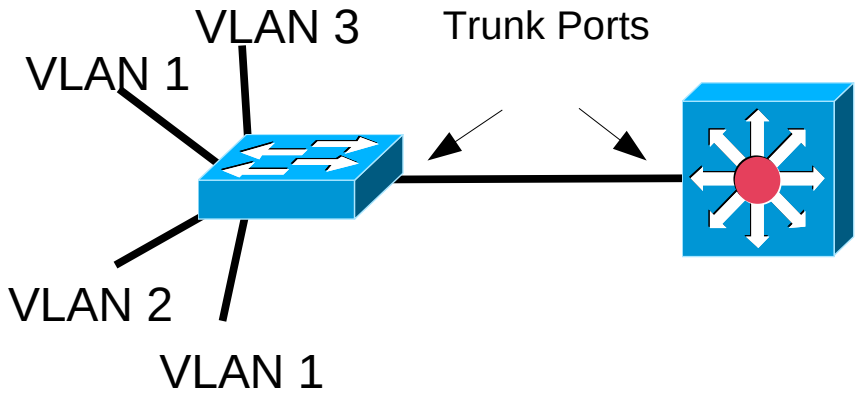
- Alternative/Complement to 802.1Q in Layer3 Switches.
- Encapsulates OSI Layer 2 Ethernet frames within Layer 4 UDP/IP datagrams .
  - Default port 4789.
- VLAN may be additionally identified by a VNI field with 24 bits.
  - 802.1Q tag only as 12 bits.
  - Allows for a very large number of VLAN.
- Usually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



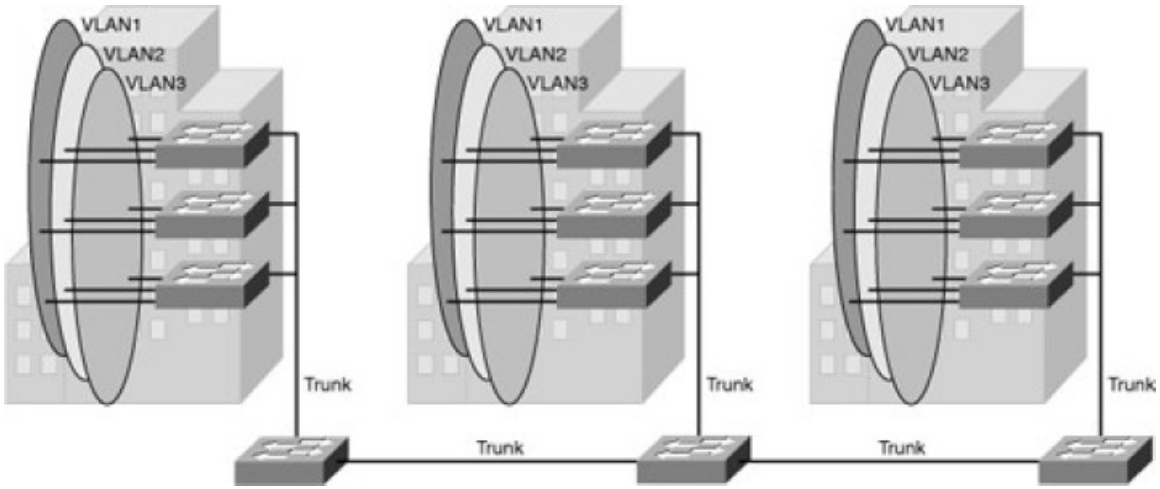
IP Connection between VLANs

- 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.

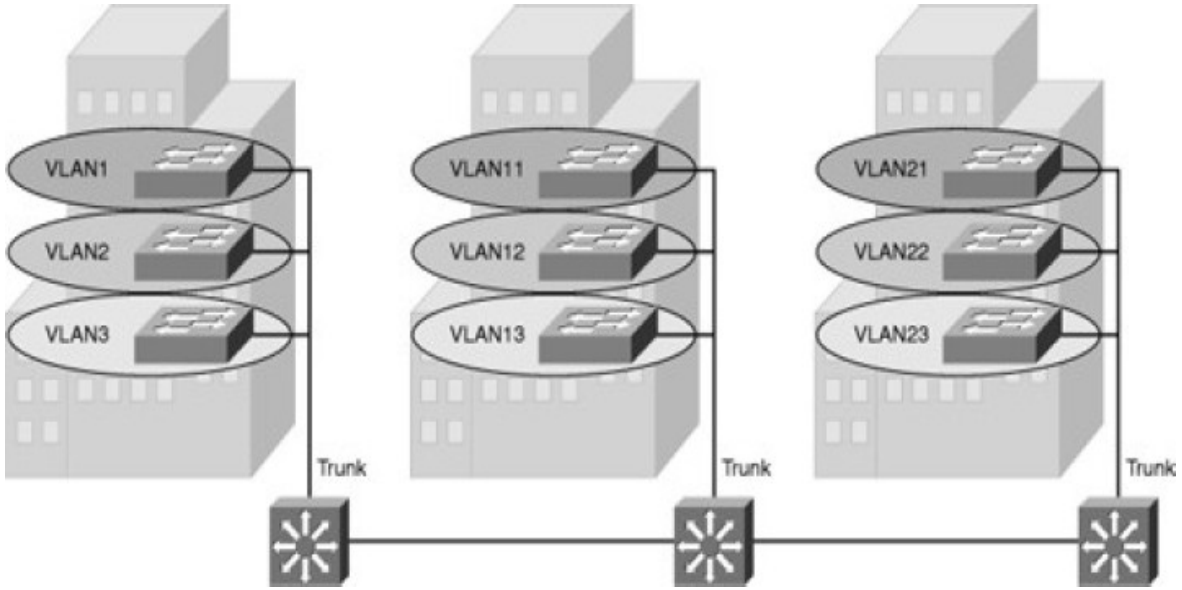




VLAN Segmentation Models



- End-to-End VLAN
  - VLAN are associated with switch ports widely dispersed over the network



- Local VLAN
  - Local VLANs are generally confined to a wiring closet.

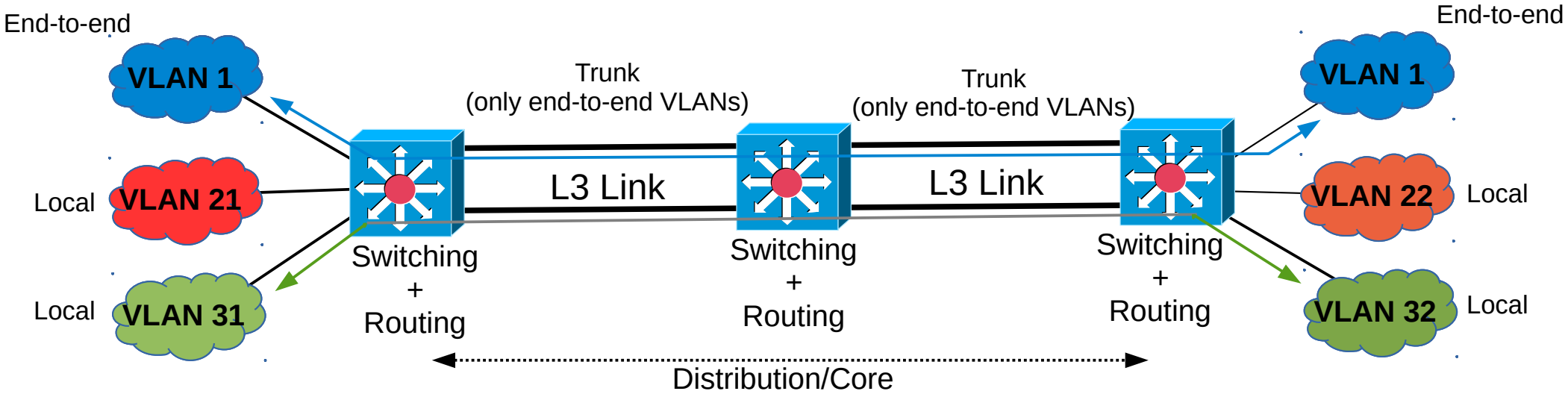
VLAN Segmentation Purpose

- Joint in the same logical network services/terminals/users with same traffic/security/QoS policies.
  - Each VLAN must have an unique IP (sub-)network.
  - May have more than one IP (sub-)network.
    - Including IPv4 public and IPv4 private networks.
    - And, IPv6 networks.
- Neighbor (local) VLANs with similar traffic/security/QoS policies should have IP (sub-)networks that can be summarized/aggregated.
  - E.g.: VLAN of VoIP phones in Building 1 (VLAN 21: 200.0.0.0/24)
  - VLAN of VoIP phones in Building 2 (VLAN 22: 200.0.1.0/24)
  - Summarized/aggregated address of VLAN21+VLAN22: 200.0.0.0/23.

VLAN Segmentation (examples)

- Local VLANs
  - Per service/function
    - VoIP phones, Video conference, printers, cameras, PCs, servers, …
  - Per user role
    - Engineers I, engineers II, technicians, administrators, …
  - Per location
    - Building I, floor 4, right wing, etc...
  - Mixture of service/function, role, location
    - e.g.: VLAN of VoIP phones, of the Engineers in Building I.
- End-to-end VLANs
  - Services/roles that have a global scope within the network.
  - Wireless network
    - Same IP network (same IP address) independently of location.
    - To avoid IP changes when moving from location to location.
  - Administration VLAN (optional)
    - VLAN used by the network administrator to remotely access network equipments.
    - Same administrator of (all) equipments independent of location.

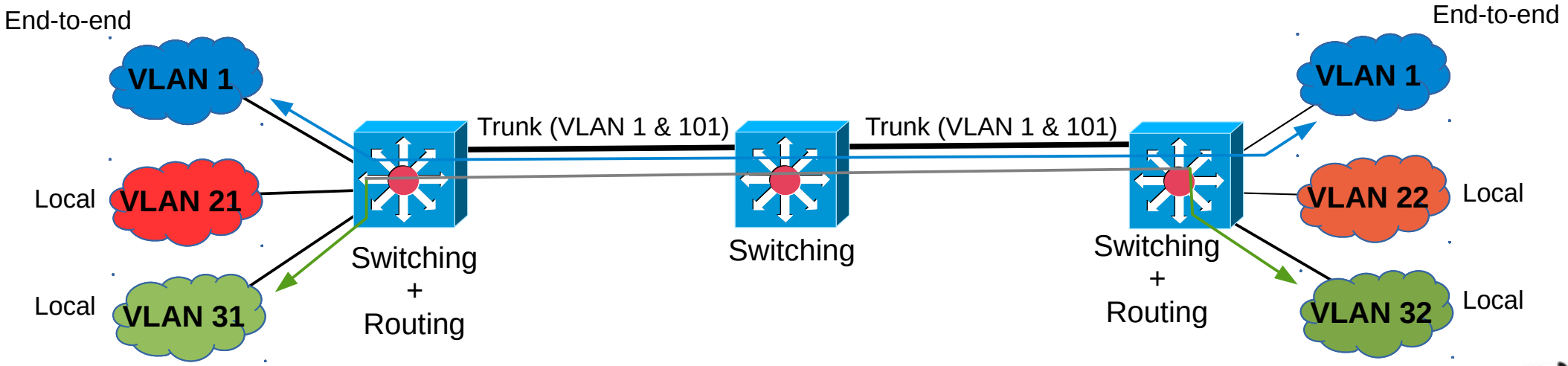
Inter-(V)LAN Traffic



- End-to-end VLANs traffic **should be switched** over the Distribution/Core layers
  - Using a trunk (for end-to-end VLANs only).
- Local VLANs traffic **should be routed** over the Distribution/Core layers
  - Using standard layer 3 Links.
  - Using IP routing.
    - Exchange the routing information only through the L3 links
    - End-to-end VLAN should be passive interfaces for the routing processes.
      - Routes are not exchanged → Traffic is not routed!

Inter-(V)LAN Traffic (2)

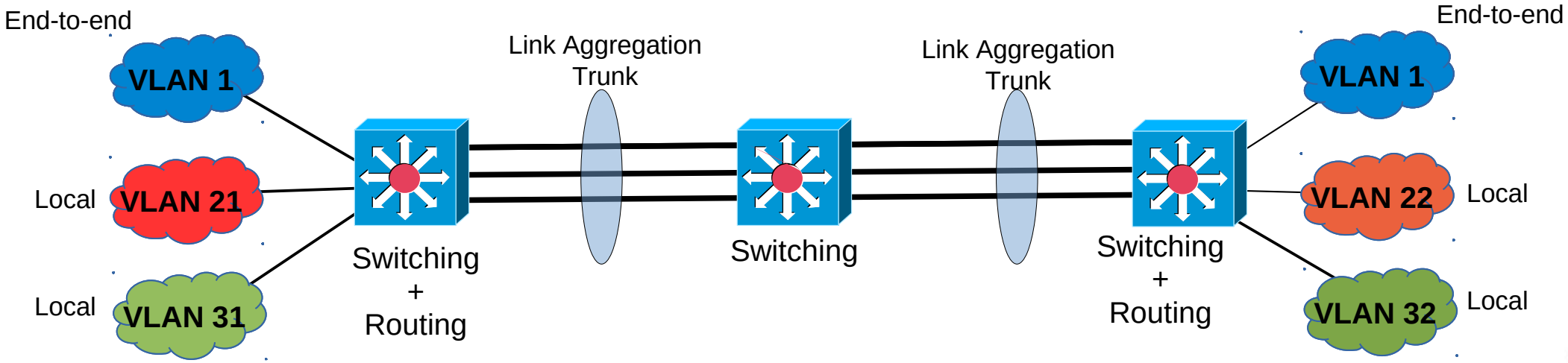
- Layer 2 and Layer 3 traffic should share the same physical link!
  - The layer 3 link is replaced by an Interconnection/Core VLAN.
- Interconnection/Core VLANs
  - VLAN used only for interconnection between local-VLANs.
  - Allows the mixture of VLAN segmentation models.
- Interconnection trunks should allow ONLY:
  - Ends-to-end VLANS
  - Interconnection/Core VLANs (also end-to-end VLANS).
- Exchange of routing information **should** only be done through the interconnection VLAN.
  - Other VLAN should be *passive-interfaces* for the routing processes.



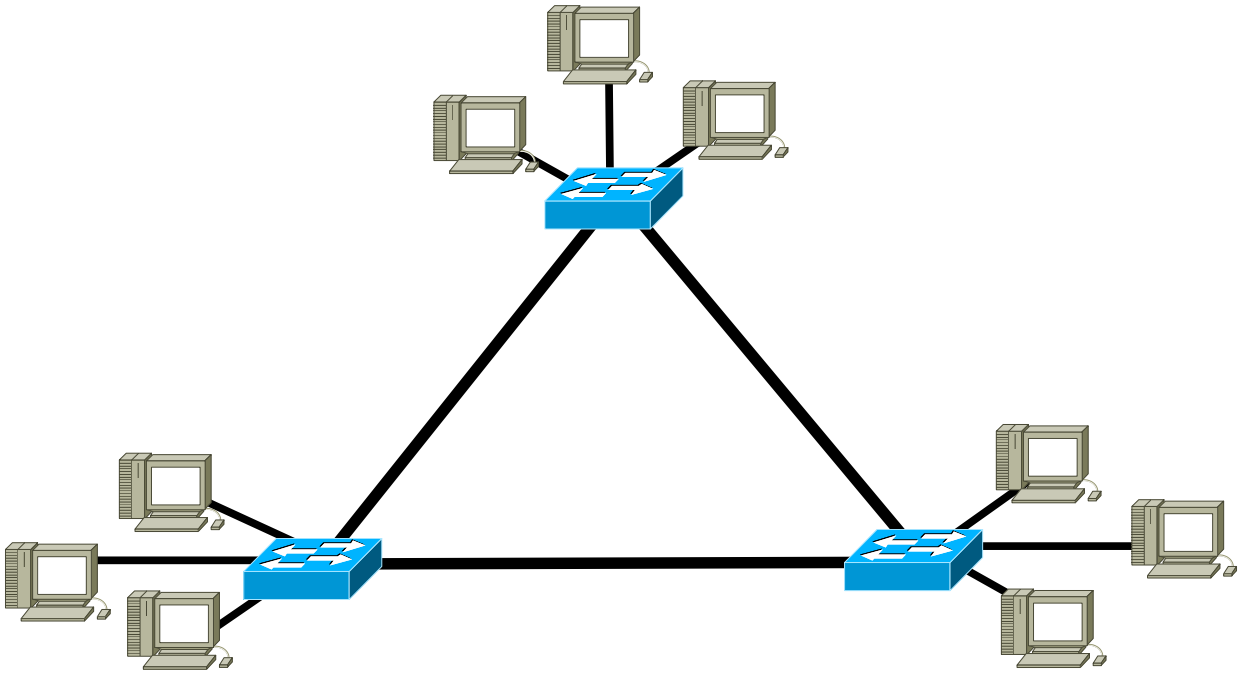
VLAN 101 is the interconnection VLAN.

Ethernet Link Aggregation

- The throughput/speed of one connection link may not be enough to fulfill the requirements.
- Multiple Ethernet links may aggregated, provide a seamless trunk connection with N times the single throughput/speed of one link.
- Ethernet frames are “load-balanced” between all available physical links.



Redundant Layer 2 Network

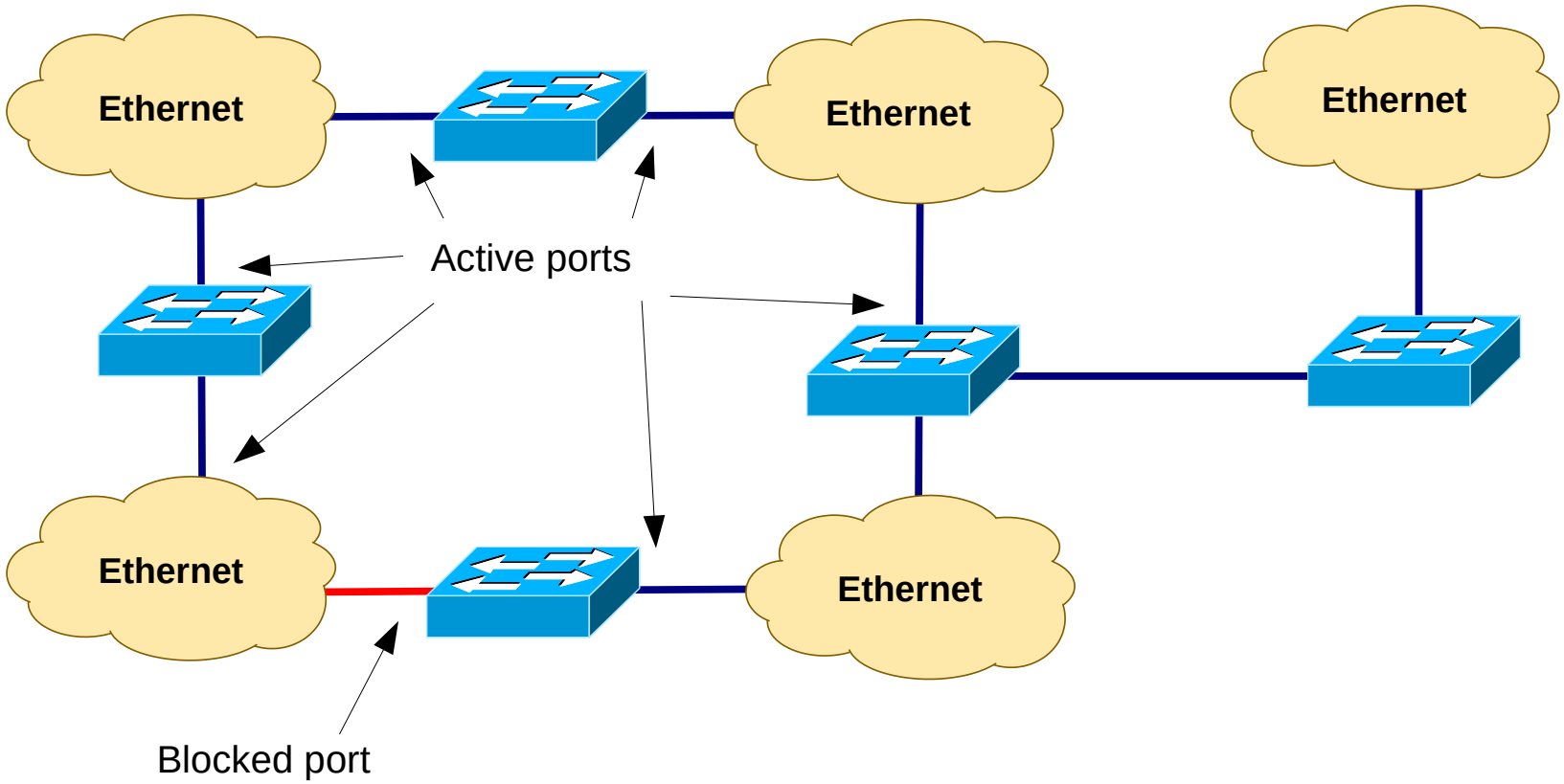


- Objective: Allow the network for dynamically recover from network failures.
- Problem: Link redundancy creates Layer 2 loops. Causes the collapse of communications when MAC frames with broadcast address are sent by any host due to infinite frame flooding.

Spanning Tree Protocol (SPT)

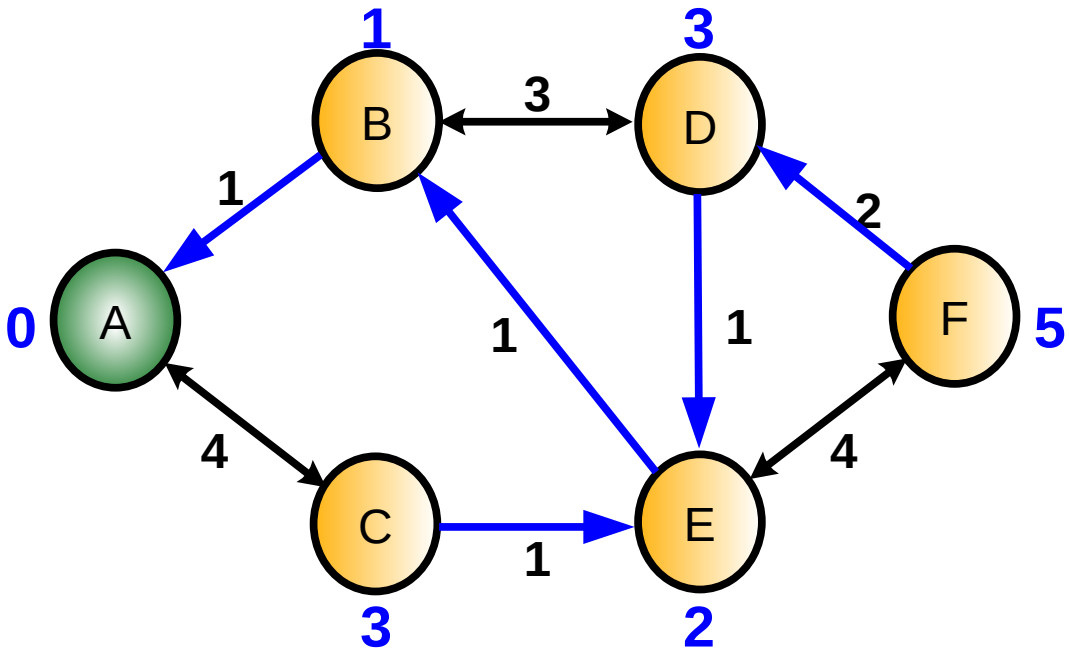
- STP enables the network to deterministically block ports and provide a loop-free topology in a network with redundant links.
- There are several STP Standards and Features:
  - STP is the original IEEE 802.1D version (802.1D-1998) that provides a loop-free topology in a network with redundant links.
  - 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

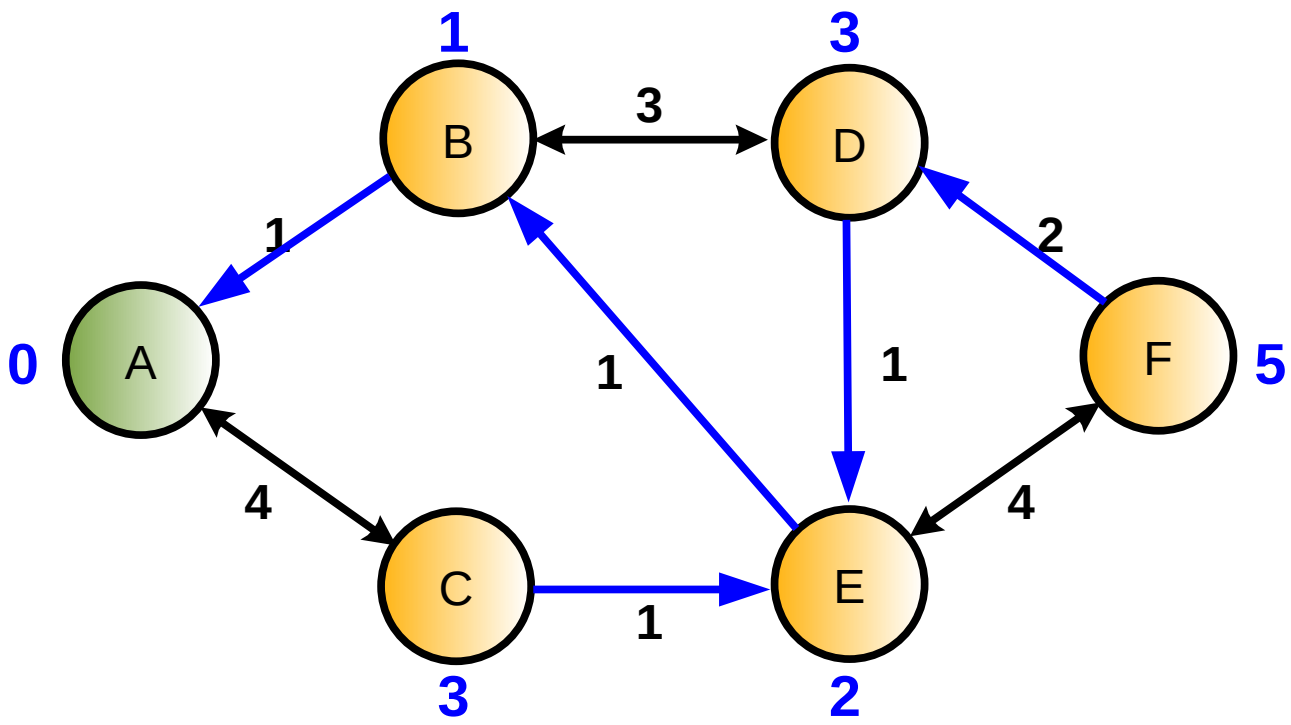


Routing based on Spanning Trees

- 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.



Bellman Equations



- When link cost are not negative, then:

Shortest path from one node X to node A

=

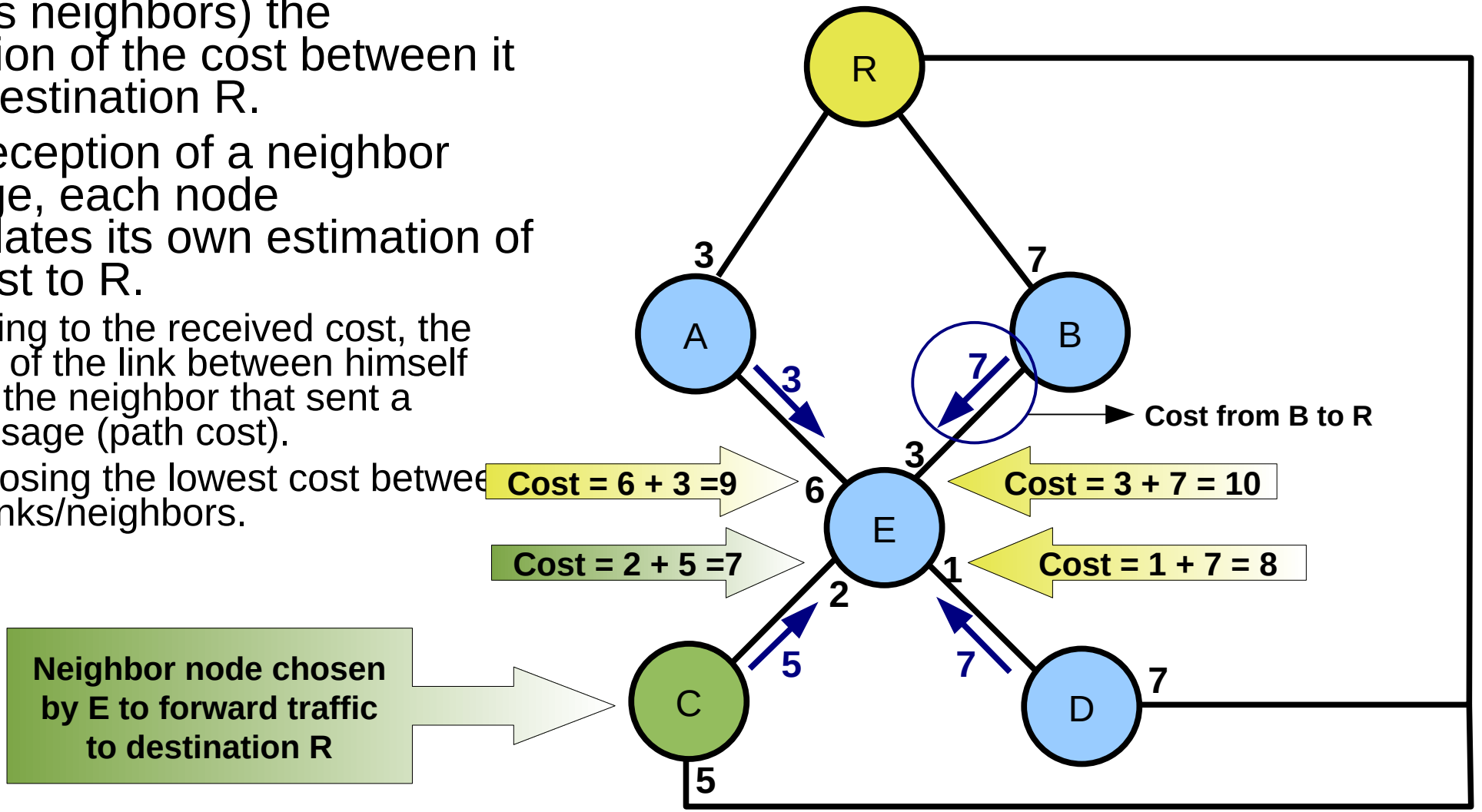
Cost of the link from that node X to the node that follows it in the shortest path to A

+

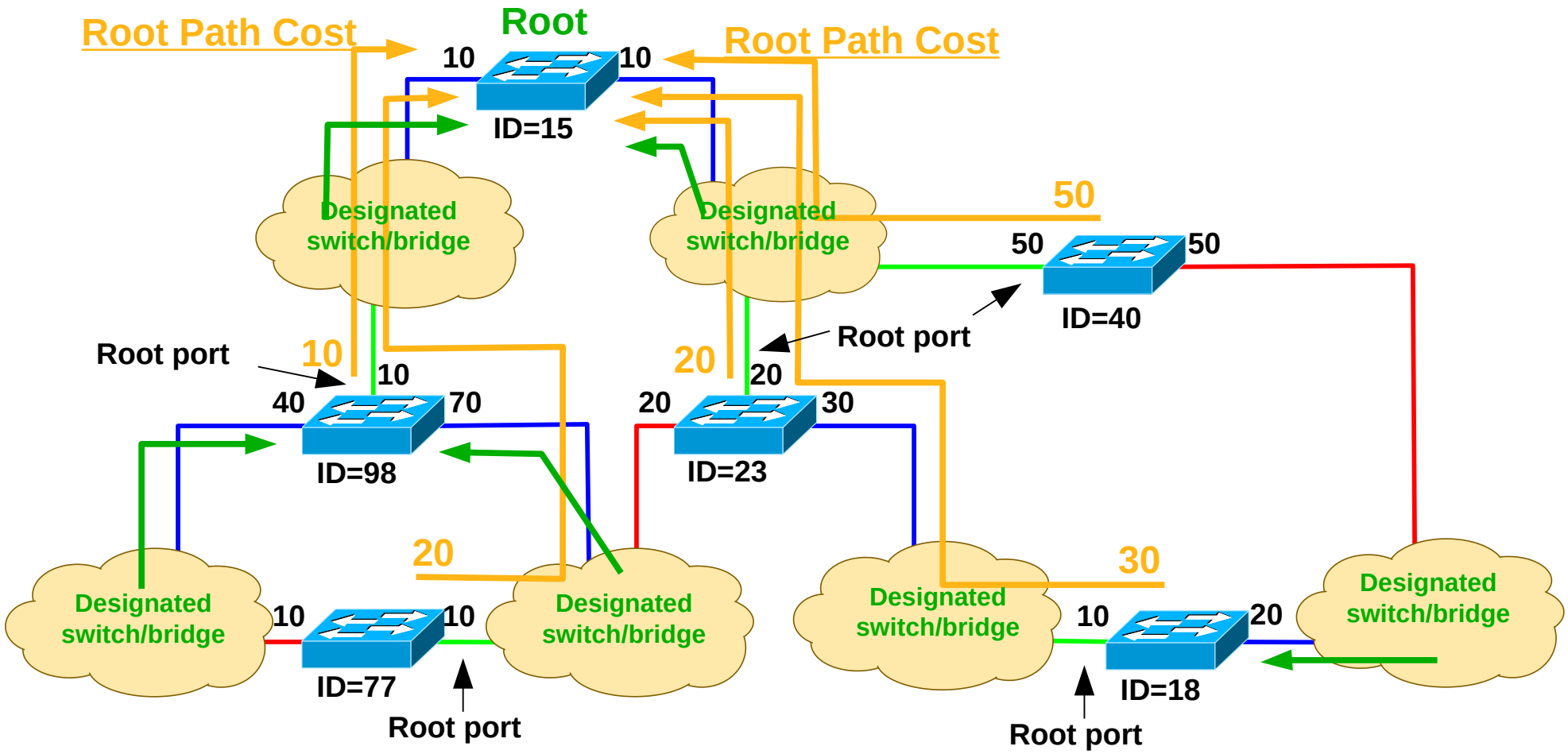
Shortest path from that node to node A

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 betwee all links/neighbors.

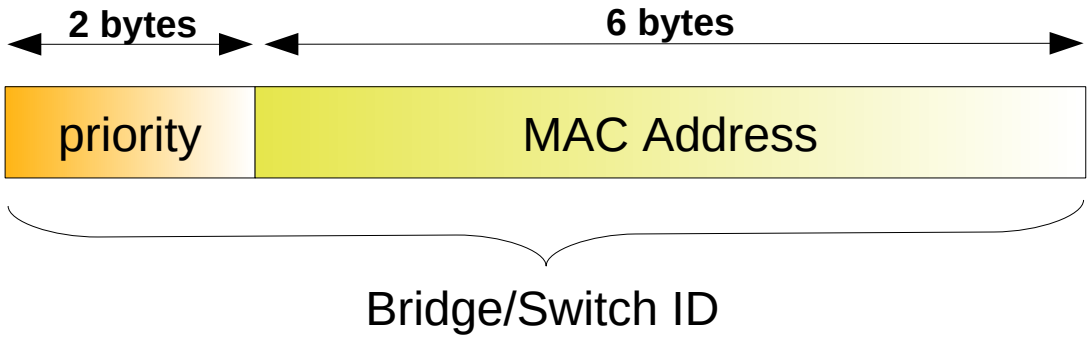


Spanning Tree Basic Concepts (1)



Spanning Tree Basic Concepts (2)

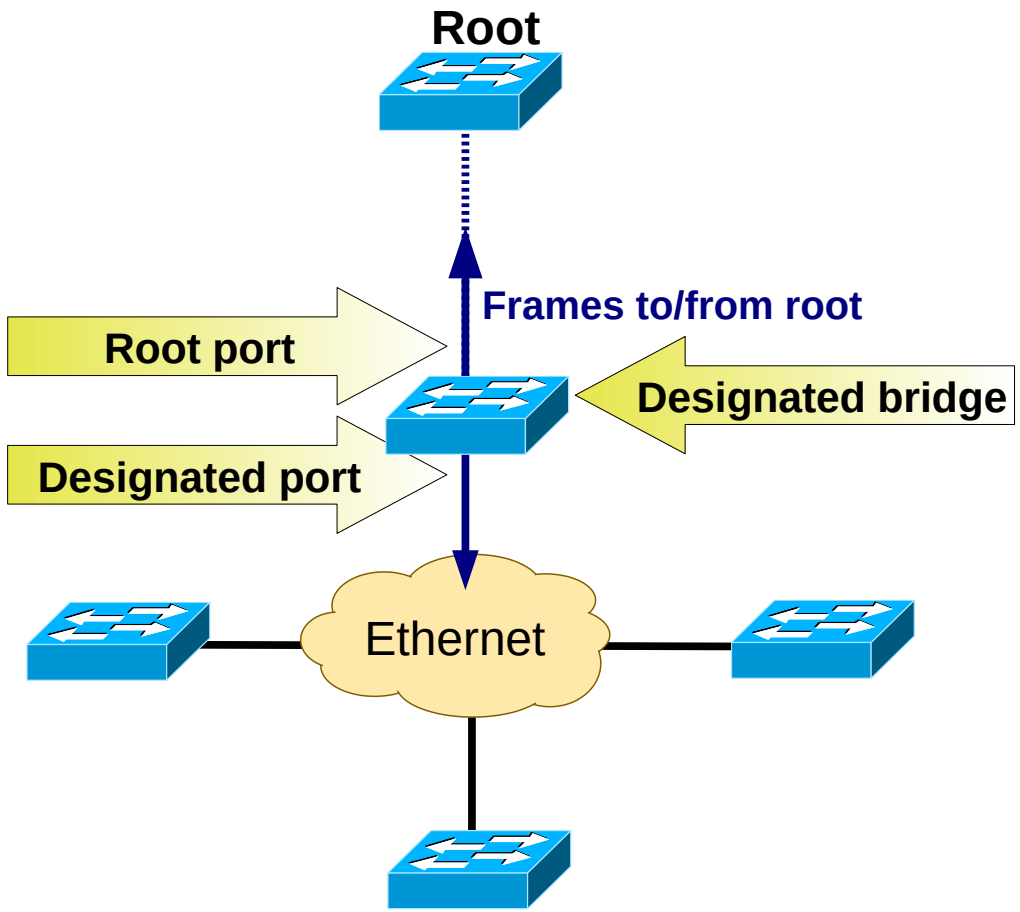
- Bridge/Switch ID – each switch is identified by an 8 bytes identifier based on:
  - 2 **Priority** bytes, defined by configuration.
  - 6 bytes (one of the **MAC Address** of the switch, or any other unique 48 bit sequence).
  - Priority has precedence over the 6 bytes sequence (usually MAC address).



- Root Switch/bridge – Switch chosen as origin/root of the spanning tree.
  - Switch with the **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.



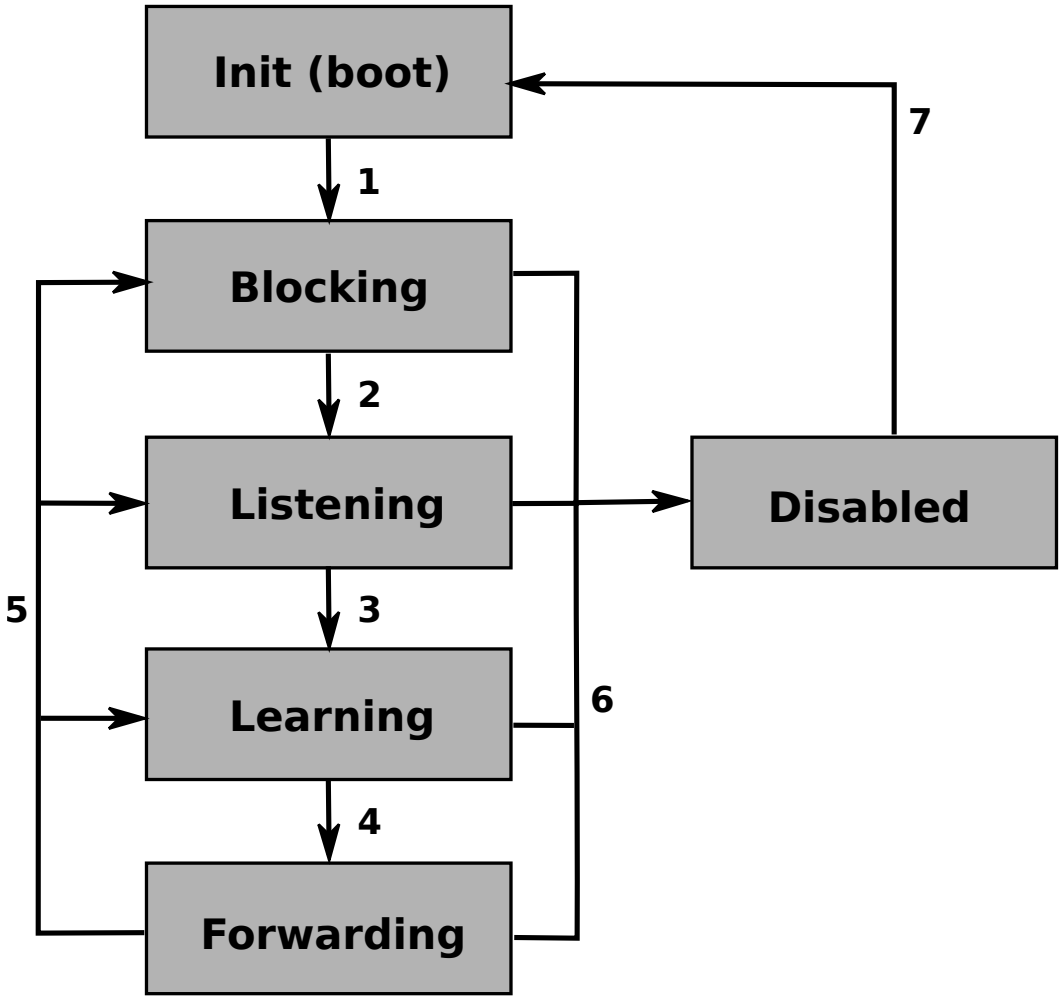
Spanning Tree Basic Concepts (4)

- 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.

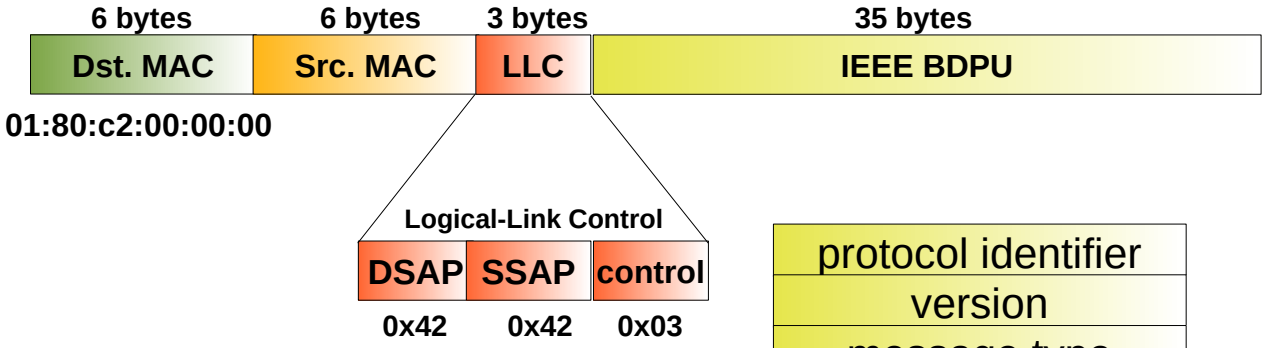
5) After a topology change the port transitions immediately to **Blocking** state.

6) and 7) Administrative actions.

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

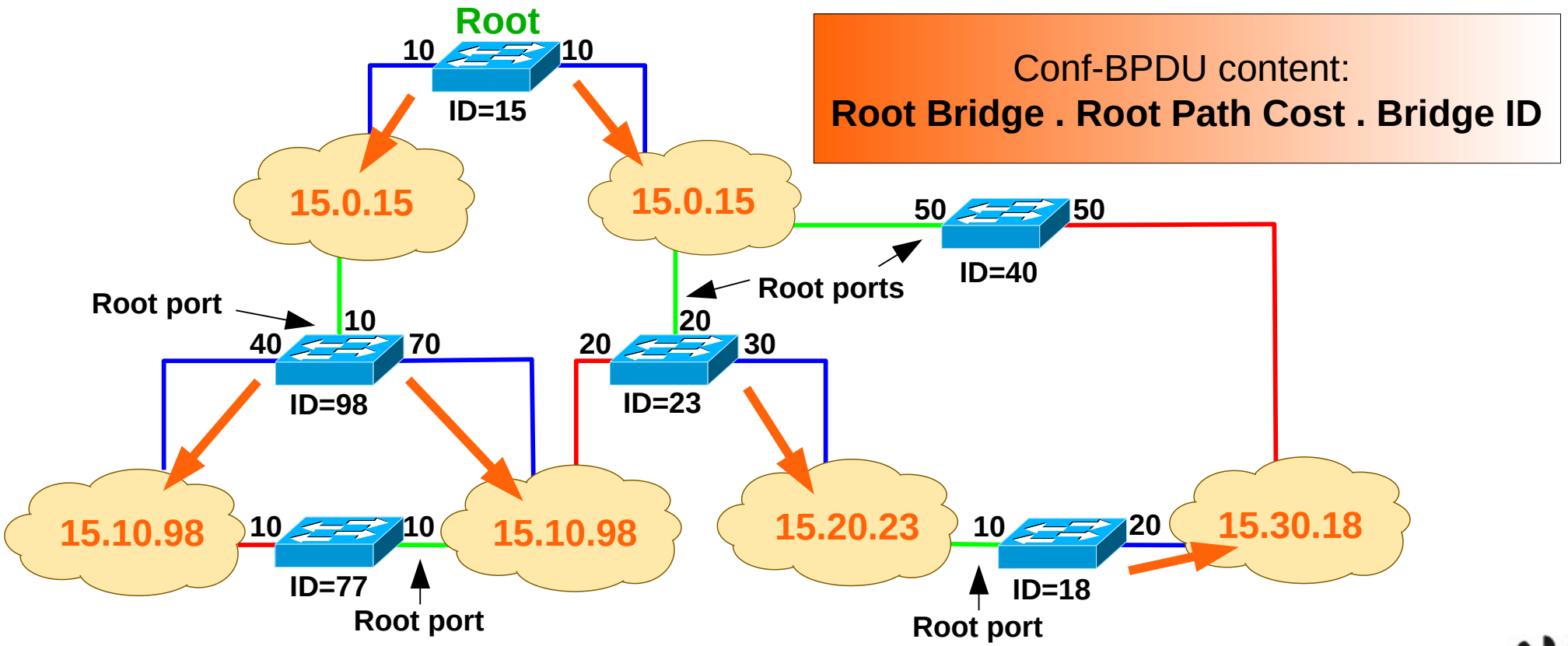
- The setup of the Spanning Tree id dune using Conf - BPDU (configuration messages).

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

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

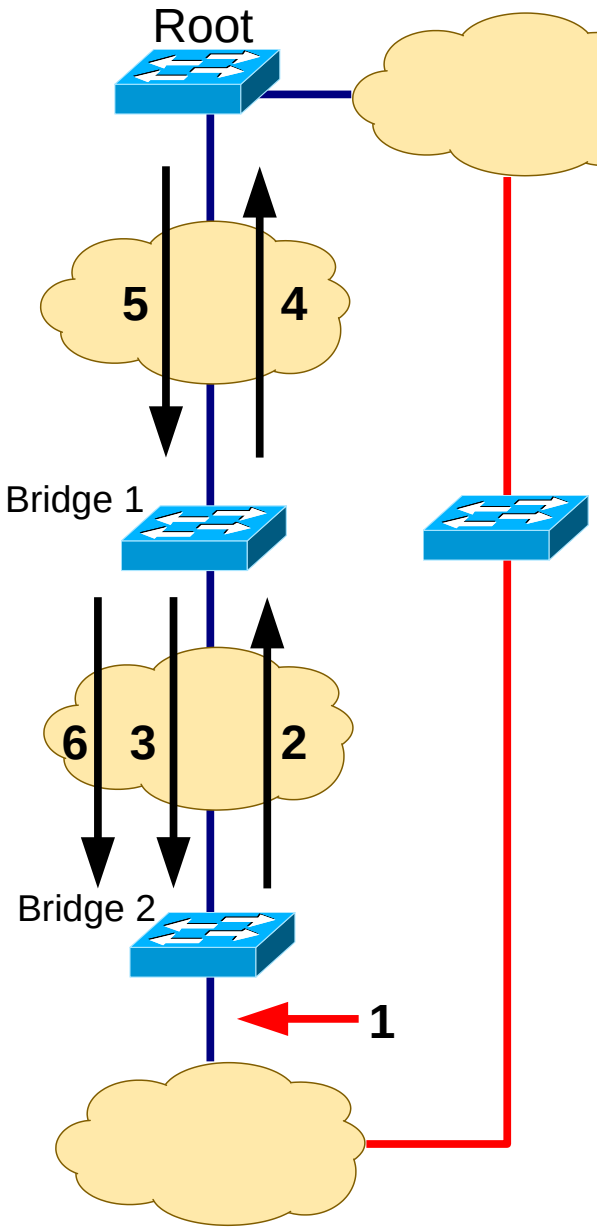
Conf (Configuration) BPDU

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***

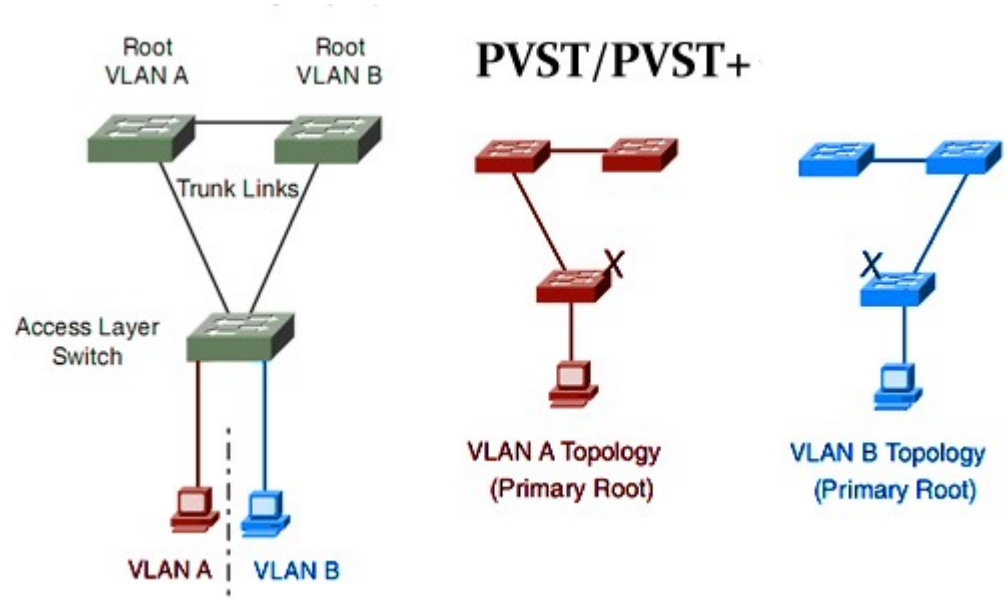
   Root bridge uses the forwarding table short lifetime during this period
6. **Sends Conf-BPDU with TC=1**

   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

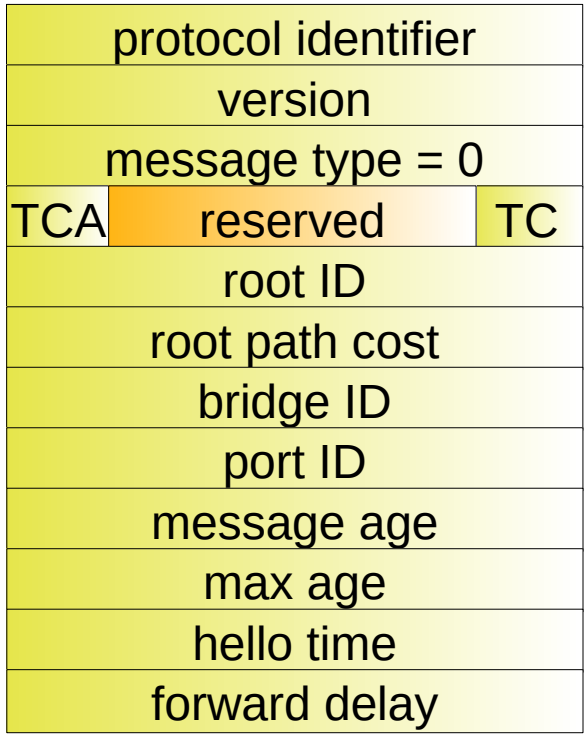
Other Protocols (2)

- 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



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