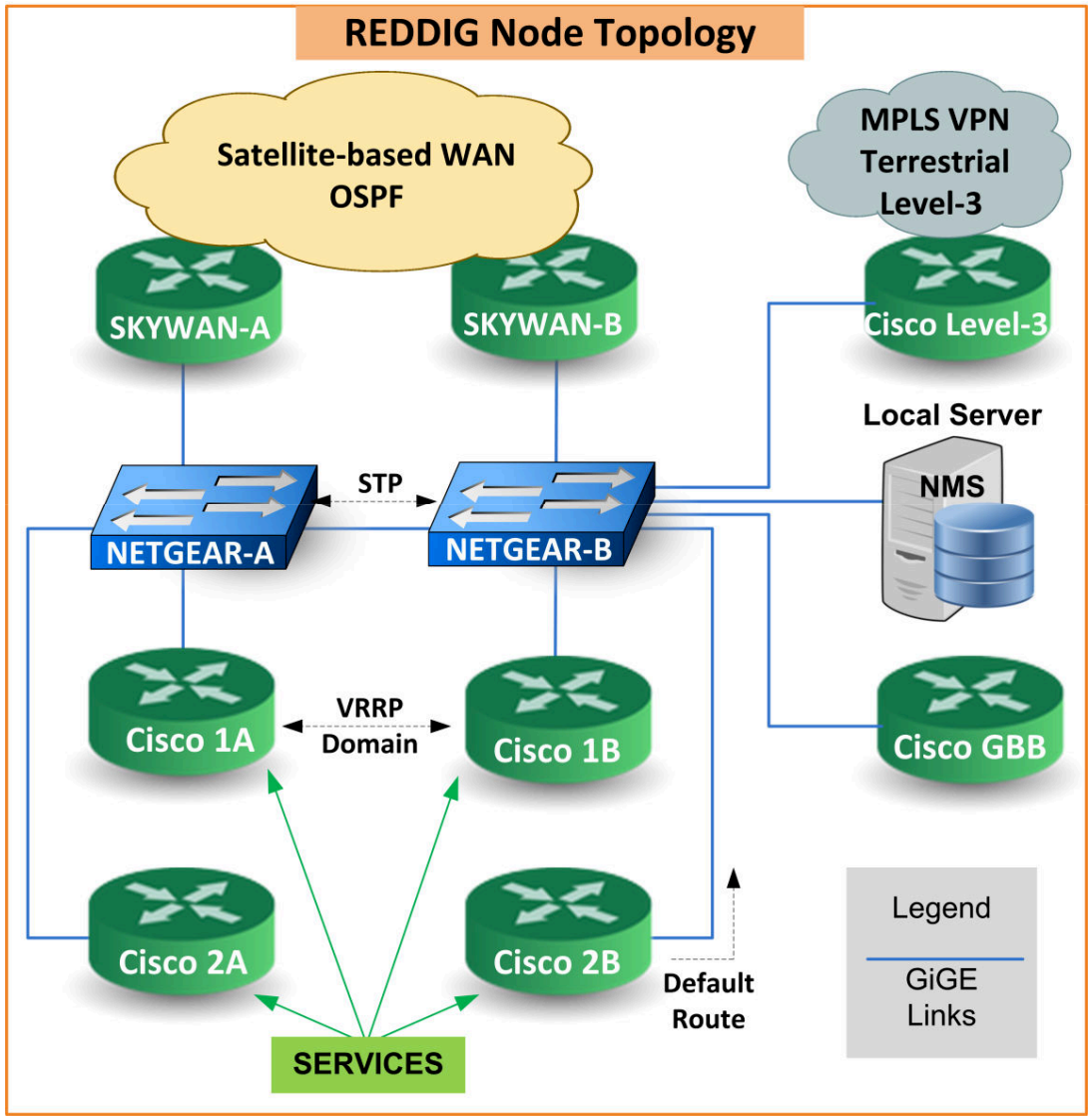
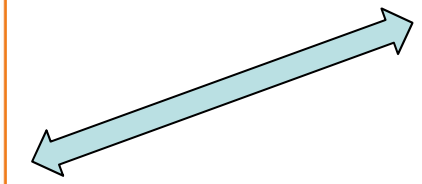
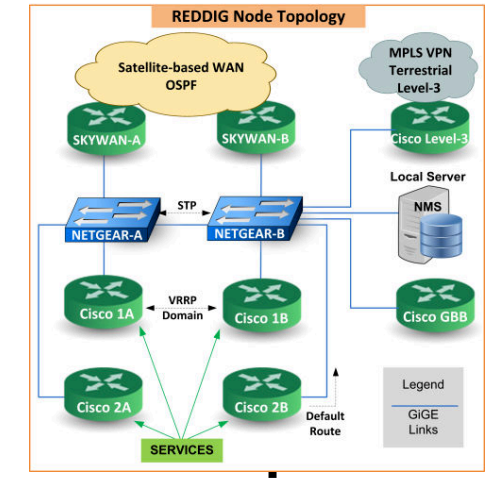
REDDIG II – Computer Networking Training

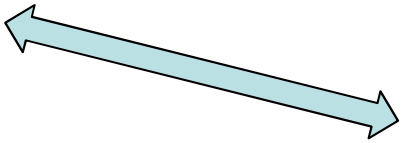
REDDIG2 NETWORK

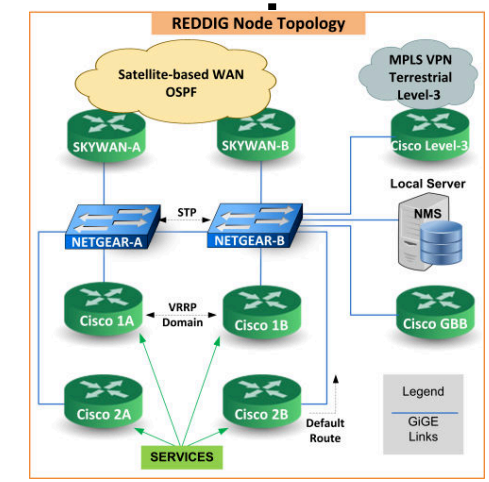






Nodes





INTERNETWORKING

INTERNETWORKING

Characteristics of a Network

- **Speed:** Speed is a measure of how fast data is transmitted over the network.
- **Cost:** Cost indicates the general cost of components, installation, and maintenance of the network.
- **Security:** Security indicates how secure the network is, including the data that is transmitted over the network.
- **Availability:** Availability is a measure of the probability that the network will be available for use when it is required.
- **Scalability:** Scalability indicates how well the network can accommodate more users and data transmission requirements
- **Reliability:** Reliability indicates the dependability of the components (routers, switches, PCs, and so on) that make up the network. This is often measured as a probability of failure, or mean time between failures (MTBF).
- **Topology:** There are two types of topologies: the physical topology, which is the arrangement of the cable, network devices, and end systems (PCs), and the logical topology, which is the path that the data signals take through the physical topology.

INTERNETWORKING

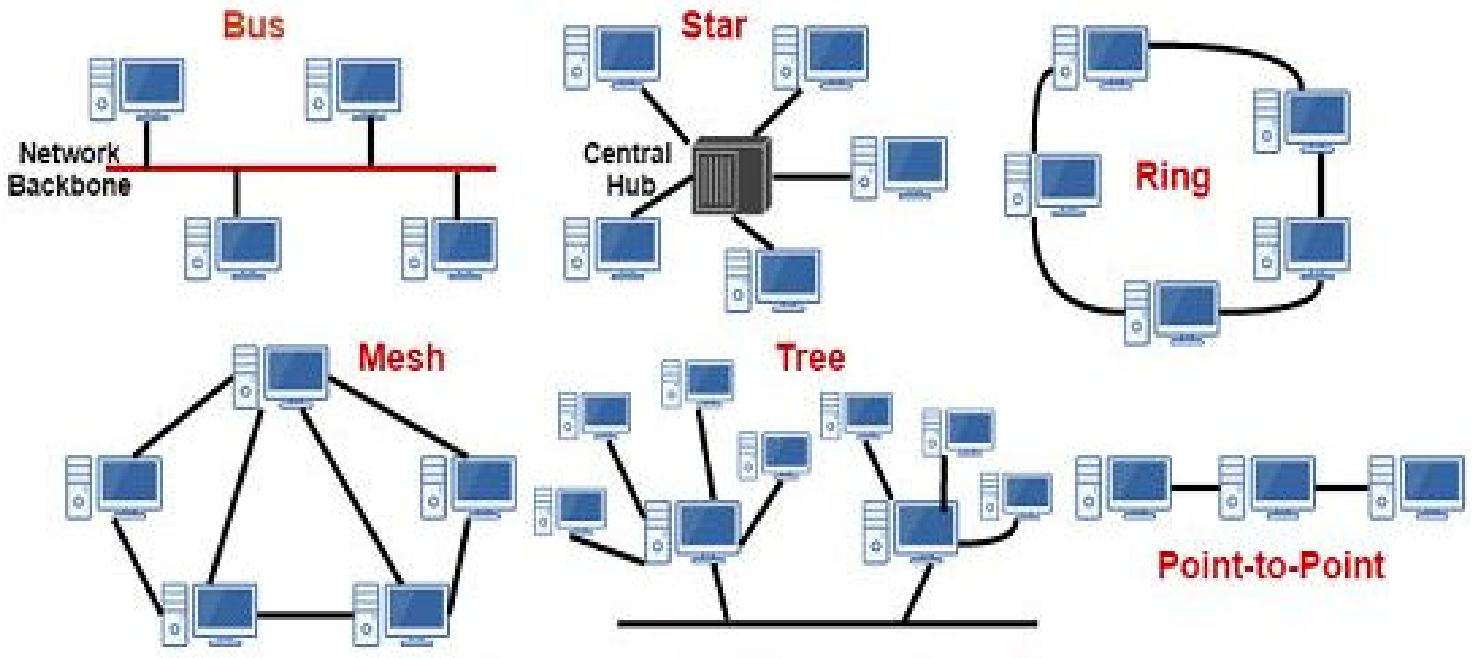
Network topology

• Network topology is the arrangement of various network elements used in data transmission and formation of interconnections like nodes and links with each other. This linking of various elements is known as network topology.

•Network topology is of two types:

- Physical topology
- Logical topology

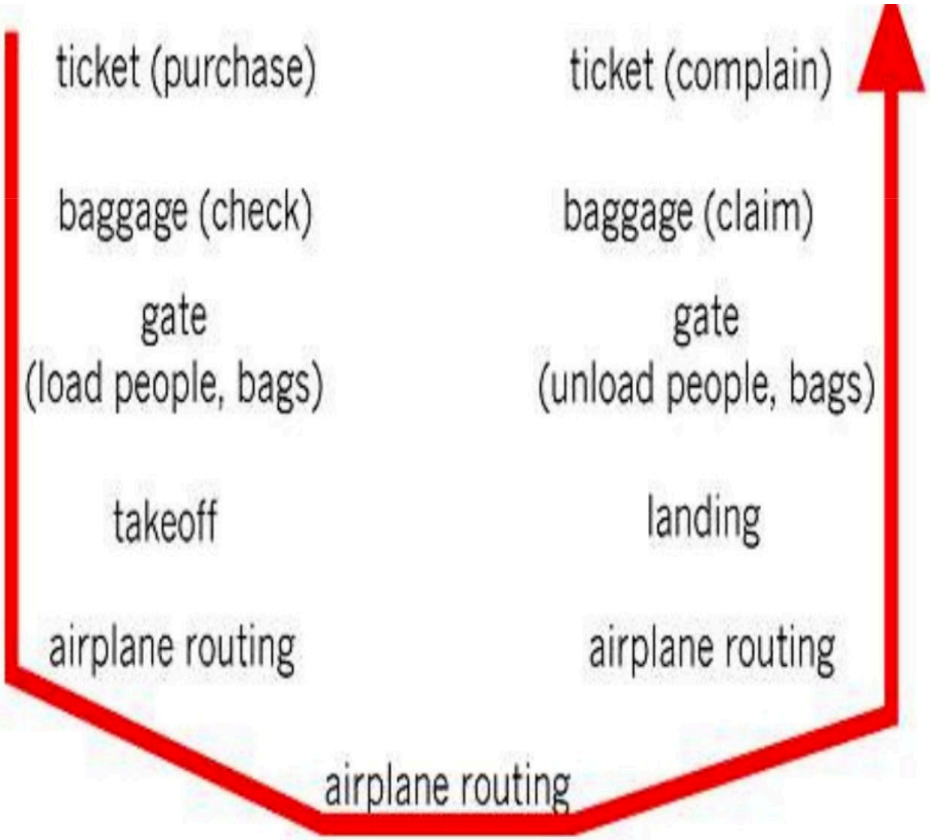
Common topologies:

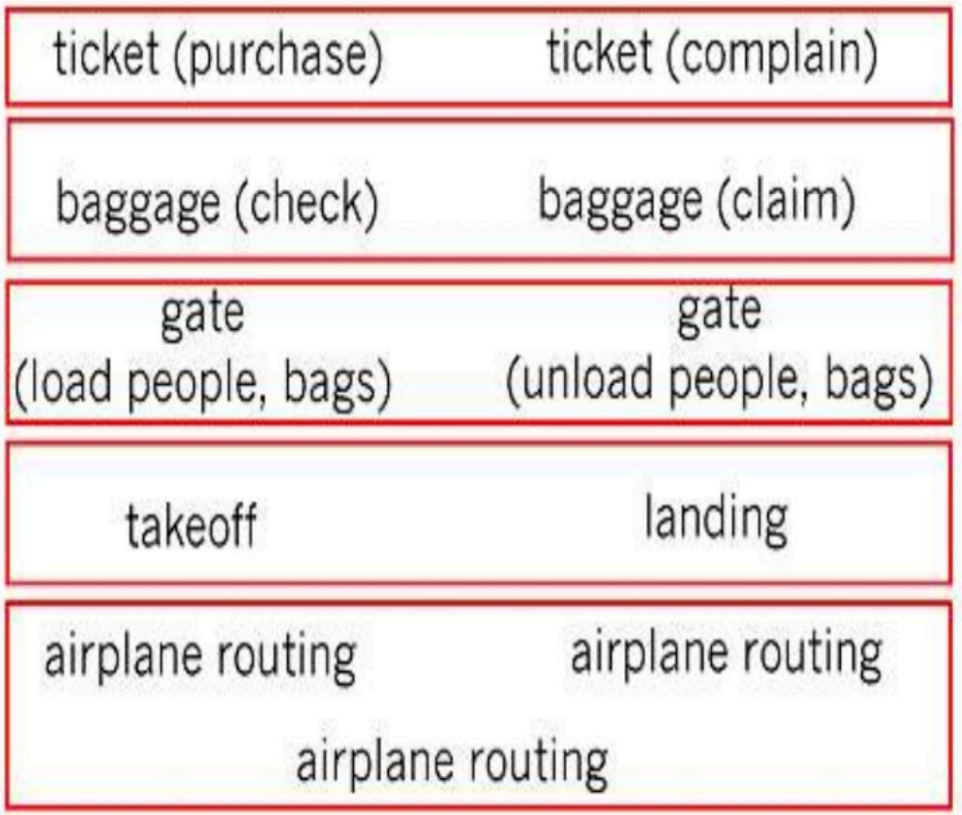


OSI REFERENCE MODEL

OSI Reference Model

- The Layered Approach
- Analogy: Airline System





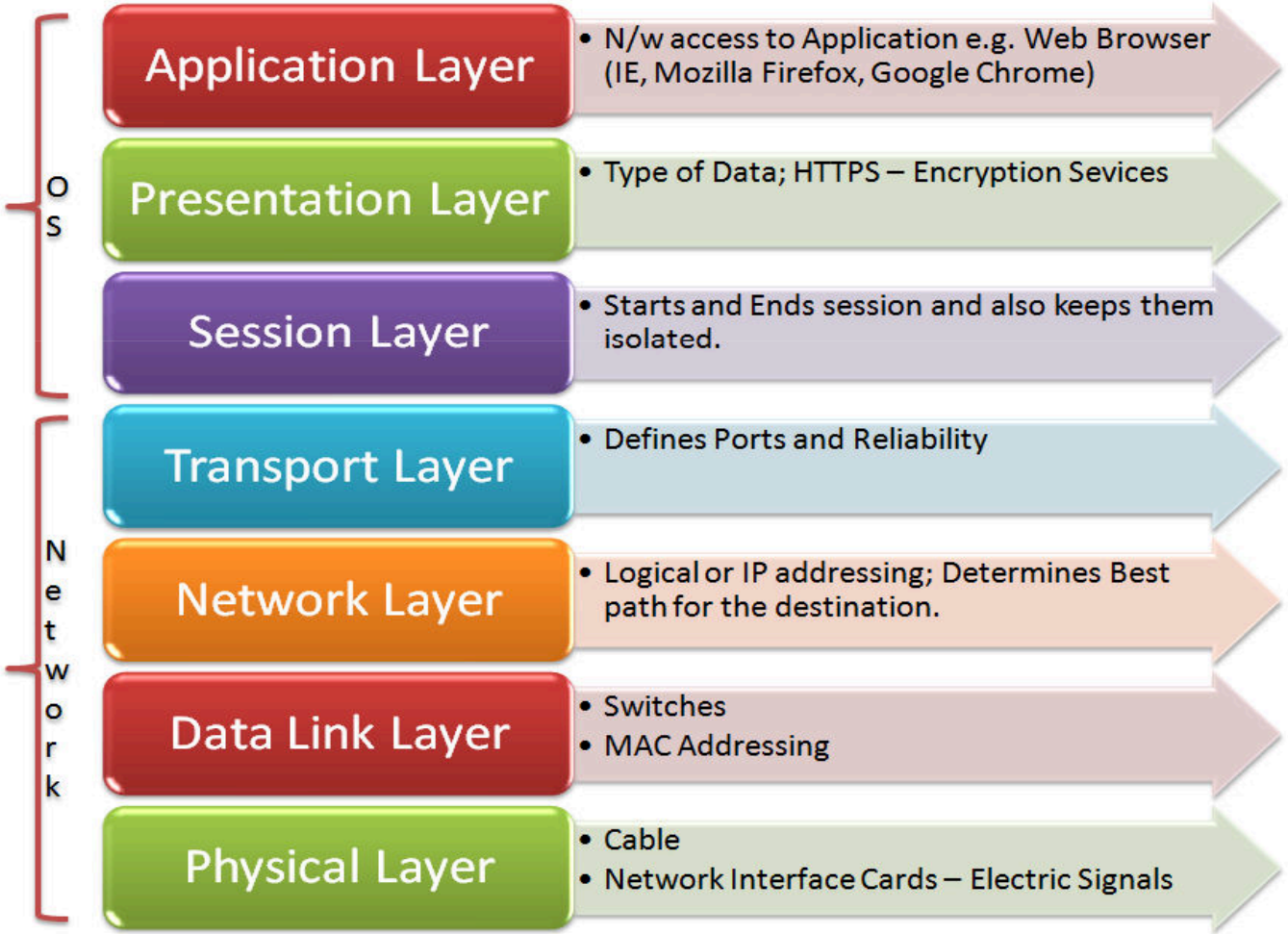
OSI Reference Model Overview

- The Open System Interconnection (OSI) reference model is a framework for defining the conventions and tasks required for network systems to communicate with one another.
- The purpose of the OSI model was to assist vendors and communications software developers to produce interoperable network systems
- The OSI model is based on a widely accepted structuring technique called layering
- The layering approach was developed to address the following goals:
  - Provide a logical decomposition of a complex communications network into smaller, more understandable and manageable parts.
  - Provide standard interfaces between network functions and modules.
  - Provide a standard language for describing network functions, to be used by network designers, managers, vendors, and users

INTERNETWORKING

OSI Reference Model - Layers

- 7 layers
- Each layer communicates with its peer layer, and with layer above and below it.
- Different protocols at each layer
- Upper layer deal with application issues, and are implemented in software
- Lower layers handle data transport issues, and are implemented in software and hardware

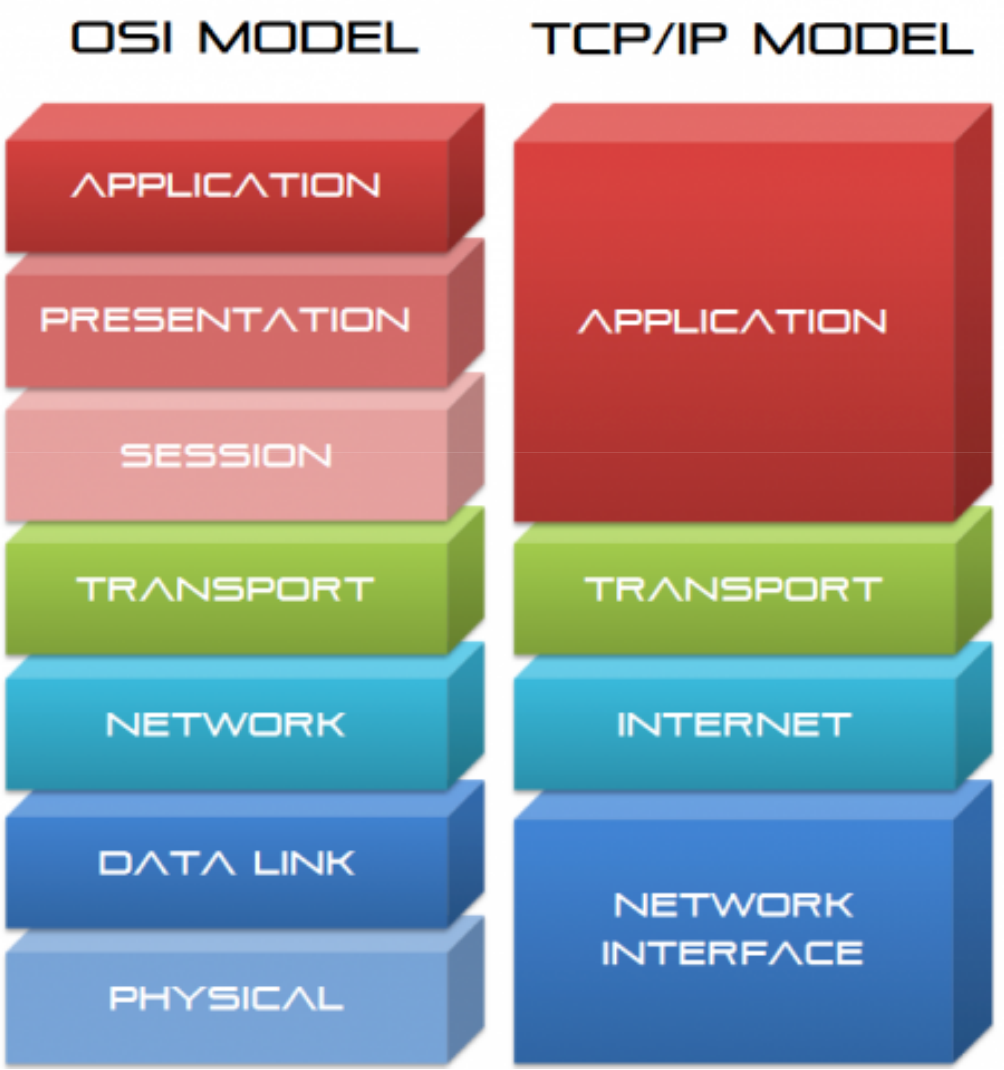


INTERNETWORKING

OSI model Vs TCP/IP model

- TCP/IP is a standard protocol used for every network including the Internet, whereas, OSI is not a protocol but a reference model used for understanding and designing the system architecture.

- TCP/IP is a four layered model, whereas, OSI has seven layers.



INTERNETWORKING

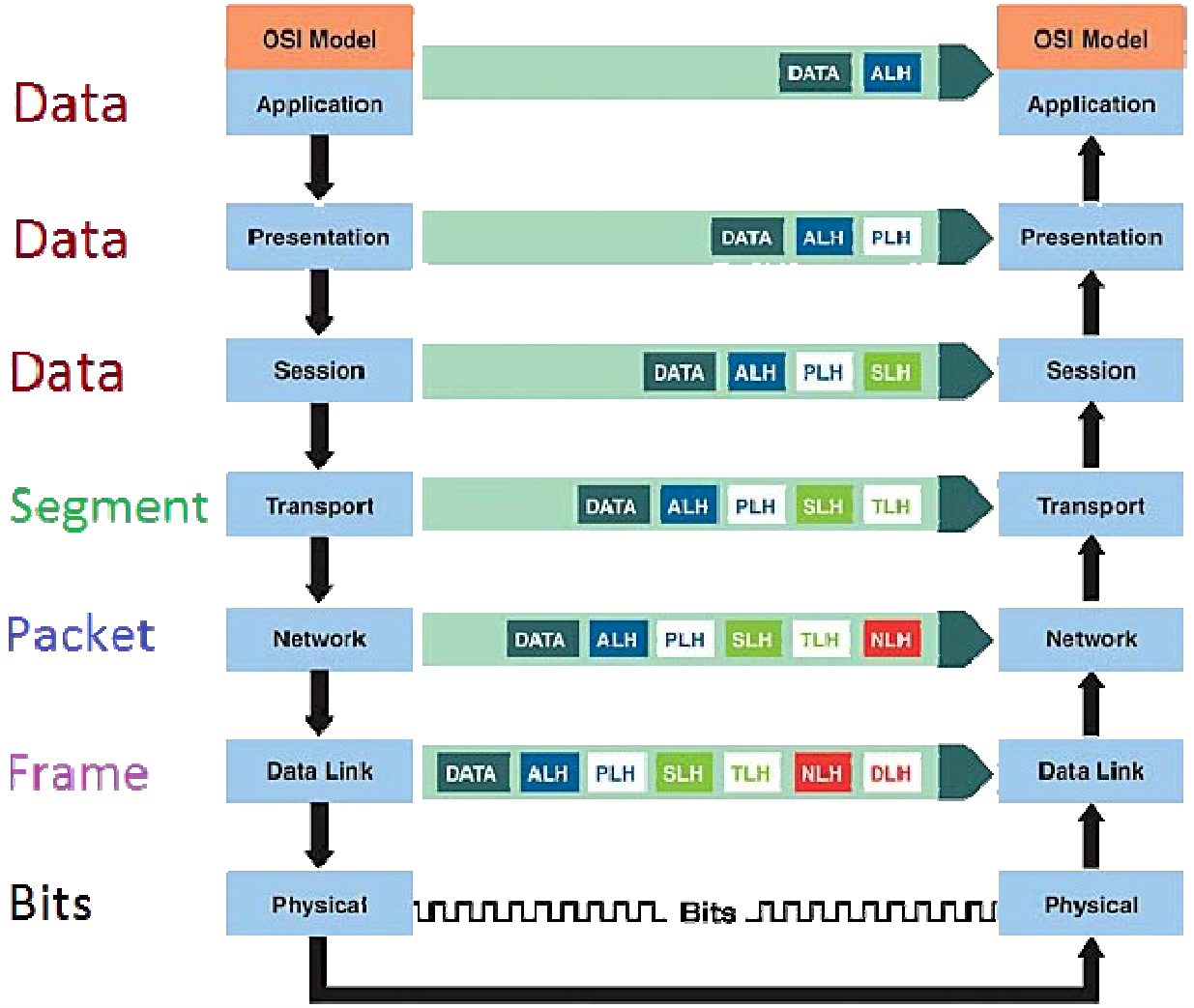
• OSI Model - Encapsulation and PDU (Protocol Data Unit)

• Encapsulation describes the process of putting headers (and sometimes trailers) around some data.

• A PDU represent a unit of data with headers and trailers for the particular layer.

• PDU names:

Transport Layer—Segments
Network Layer—Packets
Data Link Layer—Frames
Physical Layer— Bits



OSI LAYER 4 – TRANSPORT

- Transport layer communication falls under two categories:
  - Connection-oriented – requires that a connection with specific agreed-upon parameters be established before data is sent.
  - Connectionless – requires no connection before data is sent.
- Connection-oriented protocols provide several important services:
  - Segmentation and sequencing – data is segmented into smaller pieces for transport. Each segment is assigned a sequence number.
  - Connection establishment – connections are established, maintained, and ultimately terminated between devices.
  - Acknowledgments – receipt of data is confirmed through the use of acknowledgments. Otherwise, data is retransmitted, guaranteeing delivery.
  - Flow control (or windowing) – data transfer rate is negotiated to prevent congestion.
- The TCP/IP protocol suite incorporates two Transport layer protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)

INTERNETWORKING

OSI LAYER 3 – NETWORK

- The Network layer (Layer-3) controls internetwork communication, and has two key responsibilities:
  - Logical addressing – provides a unique address that identifies both the host, and the network that host exists on.
  - Routing – determines the best path to a particular destination network, and then routes data accordingly.

- Two of the most common Network layer protocols are:
  - Internet Protocol (IP)
  - Novell's Internetwork Packet Exchange (IPX).

OSI REFERENCE MODEL

OSI LAYER 2 – DATA LINK

- While the Network layer is concerned with transporting data between networks, the Data-Link layer (Layer-2) is responsible for transporting data within a network.
- The Data-Link layer consists of two sublayers:
  - Logical Link Control (LLC) sublayer
  - Media Access Control (MAC) sublayer
- The data-link frame contains the source and destination hardware (or physical) address. Hardware addresses uniquely identify a host within a network, and are often hardcoded onto physical network interfaces.
- The most common hardware address is the Ethernet MAC address.

OSI REFERENCE MODEL

OSI LAYER 1 – PHYSICAL

•The Physical layer (Layer-1) controls the signaling and transferring of raw bits onto the physical medium.
•The Physical layer is closely related to the Data-link layer, as many technologies (such as Ethernet) contain both datalink and physical functions.

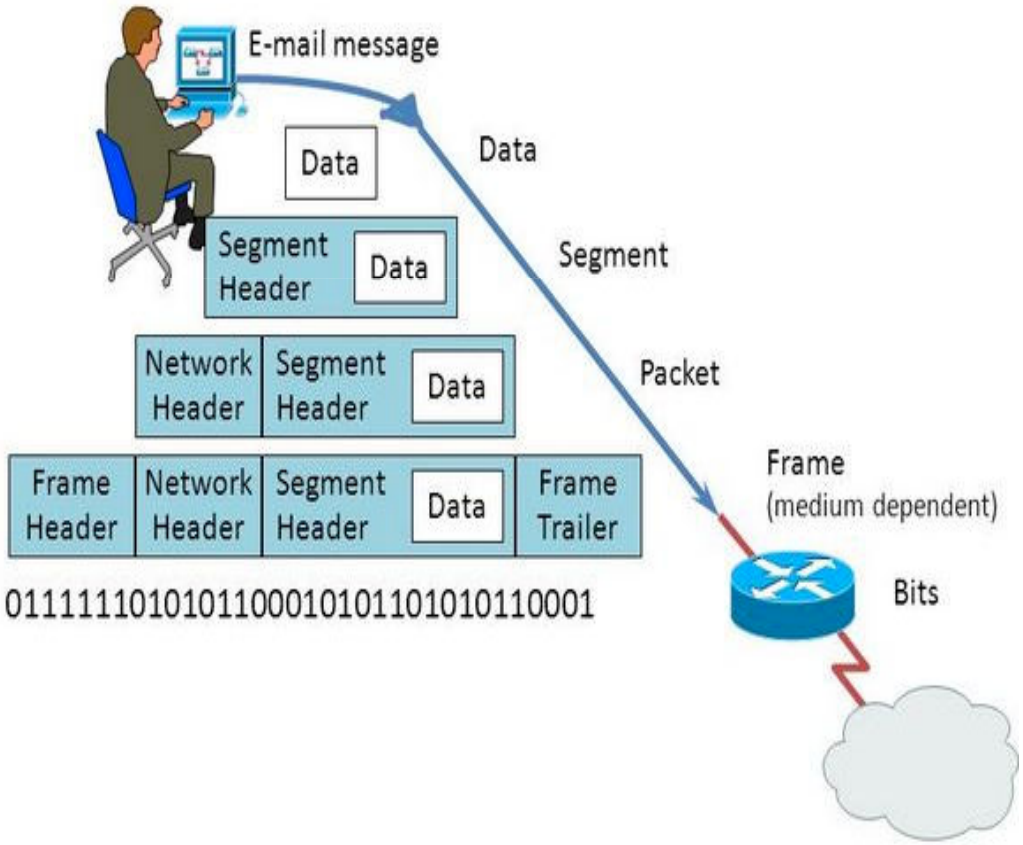
The Physical layer provides specifications for a variety of hardware:

- Cabling
- Connectors and transceivers
- Network interface cards (NICs)
- Wireless radios
- Hub
- Physical connector types and pinouts

OSI REFERENCE MODEL

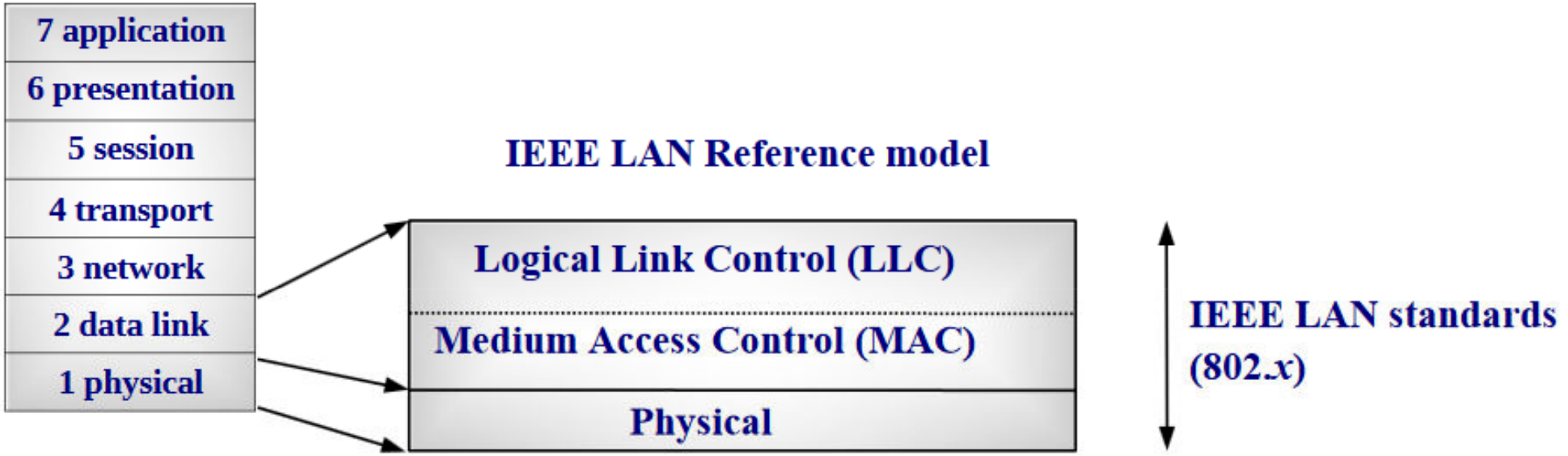
OSI Layers Key Concepts

- The transport layer is responsible for the delivery of a message from one process to another. Uses segments.
- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- The data link layer is responsible for moving frames from one hop (node) to the next.
- The physical layer is responsible for movements of individual bits from one hop (node) to the next.



LANs and VLANs

LAN Reference Model

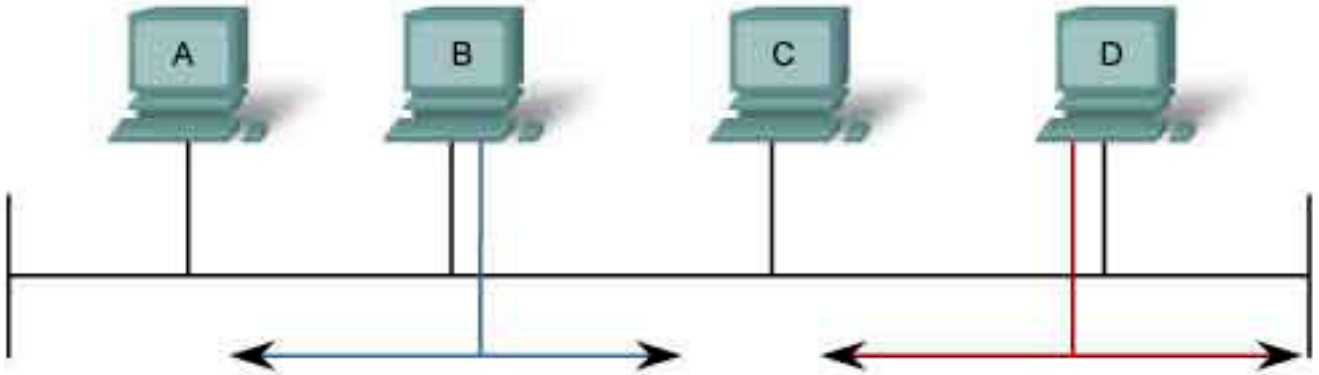


- LLC sublayer (802.2): Common to all 802.x MAC standards. Define the interface with the upper layer and the LLC sublayer takes the network protocol data, which is typically an IPv4 packet.
- MAC sublayer: Data Encapsulation and Media Access Control in order to avoid collisions

Collision Domain

Media Access Control in Ethernet

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)



CSMA/CD controls access to the shared media. If there is a collision, it is detected and frames are retransmitted.

- **Ethernet is a multi-access network!**

Ethernet – Different Ethernet Standards

Commercial name	bps	Standard	year	Name	Cabling	UTP/OF Pairs	Connector	Codification	segment distance*	
									Half duplex	Full duplex
Ethernet	10Mbps	802.3	1983	10Base5	Coax-thick	-	AUI	Manchester	500m	n/a
		802.3a	1985	10Base2	Coax-thin	-	BNC	Manchester	185m	n/a
		802.3i	1990	10BaseT	UTP-cat.3	2	RJ45	Manchester	100m	100m
		802.3j	1993	10BASE-FL	FO	2	SC	on/off Manchester	2000m	>2000m
Fast Ethernet	100Mbps	802.3u	1995	100BaseTX	UTP-cat.5	2	RJ45	4B/5B	100m	100m
		802.3u	1995	100BaseFX	FO	2	SC	4B/5B	412m	2000m
		TIA/EIA-785	1999	100BaseSX	FO/led	2	SC	4B/5B	300m	300m
Gigabit-Eth.	1Gbps	802.3z	1998	1000BaseSX	FO	2	SC	8B/10B	275-316m	275-550m
		802.3z	1998	1000BaseLX	FO	2	SC	8B/10B	316m	550-10000m
		802.3z	1998	1000BaseLH	FO	2	SC	8B/10B	n/a	100km
		802.3ab	1999	1000BaseT	UTP-cat. 5e	4	RJ45	PAM5	100m	100m
10Gigabit-Eth.	10Gbps	802.3ae	2002	10GBASE-CX4	InfiniBand	4	CX4	8B/10B	n/a	15m
		802.3ae	2002	10GBASE-SR	FO	2	SC	64B/66B	n/a	26-300m
		802.3ae	2002	10GBASE-LR	FO	2	SC	64B/66B	n/a	10km
		802.3ae	2002	...	FO	2	SC	...	n/a	...

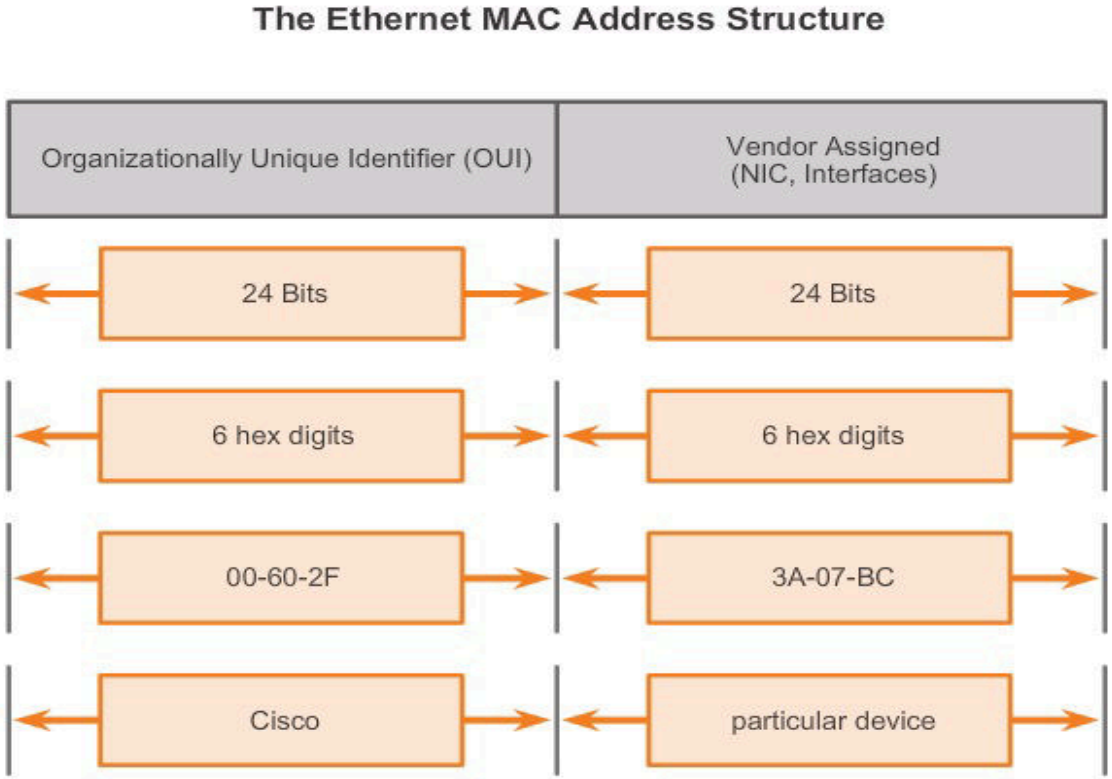
Binary/Decimal/Hexadecimal Conversion

Binary	Decimal	Hexadecimal	Binary	Decimal	Hexadecimal
0000 0000	0	00	0001 0000	16	10
0000 0001	1	01	0001 0001	17	11
0000 0010	2	02	0001 0010	18	12
0000 0011	3	03	0001 0011	19	13
0000 0100	4	04	0001 0100	20	14
0000 0101	5	05	0001 0101	21	15
0000 0110	6	06	0001 0110	22	16
0000 0111	7	07	0001 0111	23	17
0000 1000	8	08	0001 1000	24	18
0000 1001	9	09	0001 1001	25	19
0000 1010	10	0A	0001 1010	26	1A
0000 1011	11	0B	0001 1011	27	1B
0000 1100	12	0C	0001 1100	28	1C
0000 1101	13	0D	0001 1101	29	1D
0000 1110	14	0E	0001 1110	30	1E
0000 1111	15	0F	0001 1111	31	1F

LANs and VLANs

The media access control address (MAC address)

- A MAC address is given to a network adapter when it is manufactured. It is hardwired or hard-coded onto your computer's network interface card (NIC) and is unique to it.
- MAC Address: 48-bits written as 12 hexadecimal digits

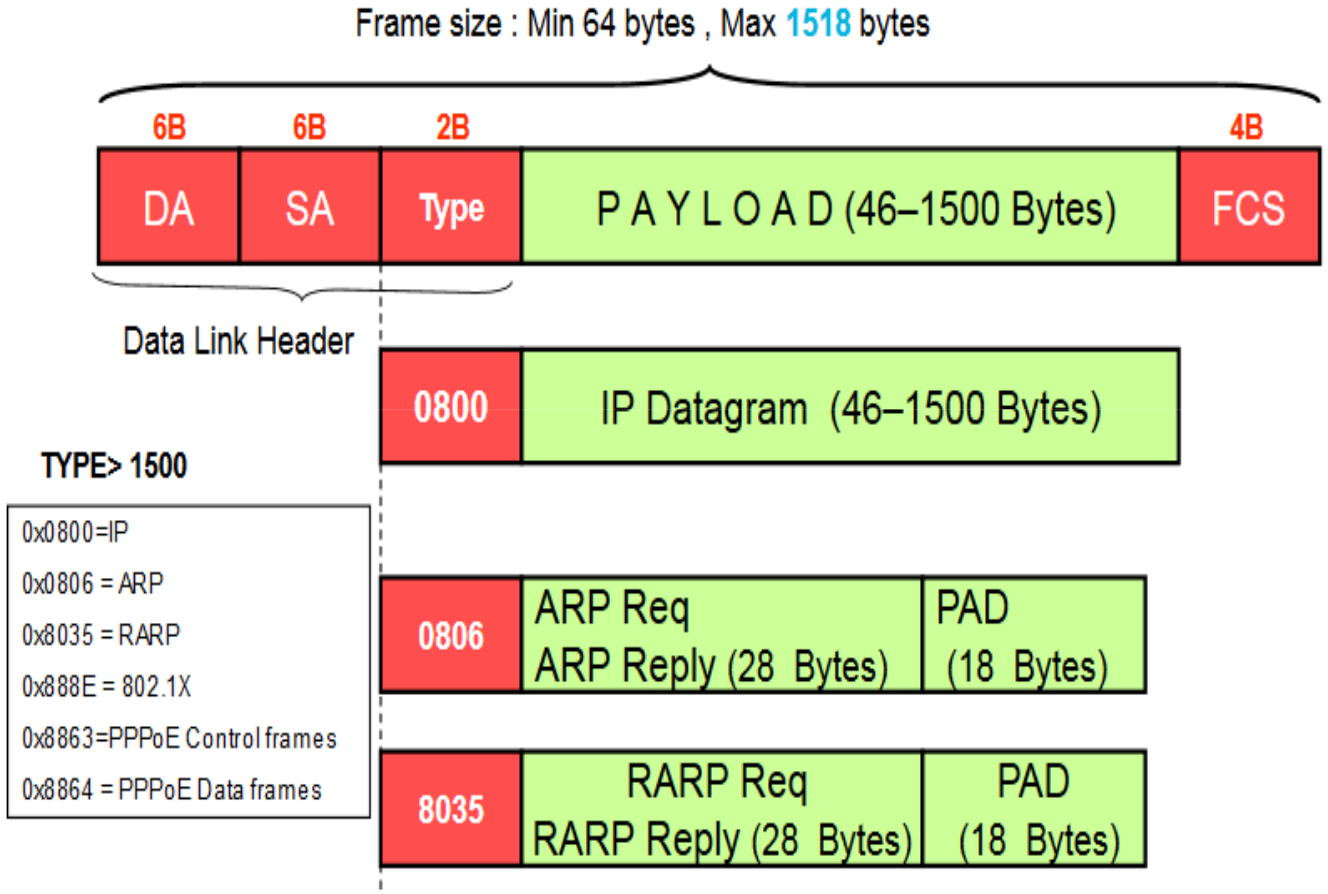


Different display formats:

08:00:69:02:01:FC
08-00-69-02-01-FC
0800.6902.01FC

The Ethernet frame

DA - Destination MAC address
SA - Source MAC address
FCS - Frame check sequence

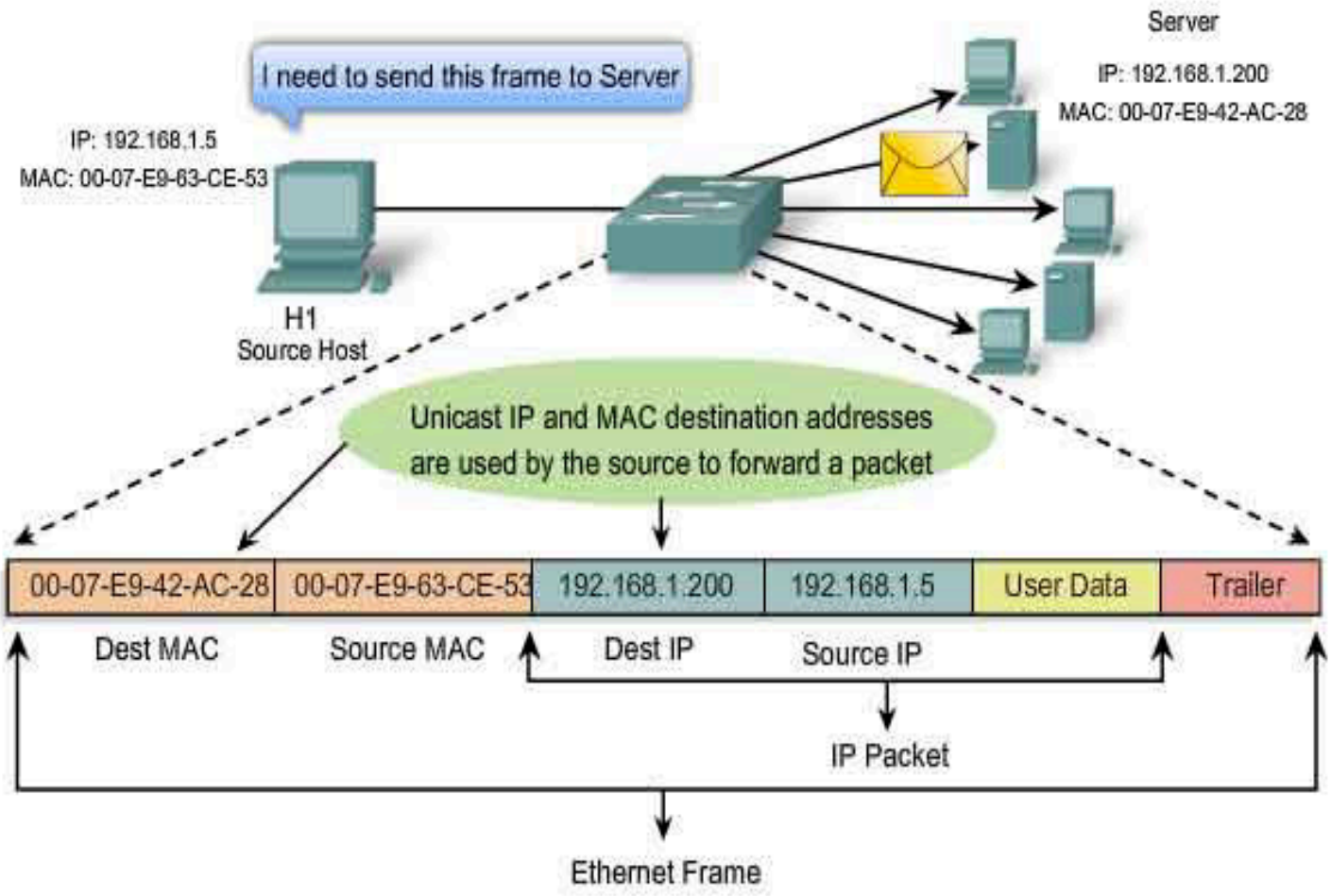


•The minimum size of an Ethernet frame is 64 bytes

LANs and VLANs

Unicast Communication

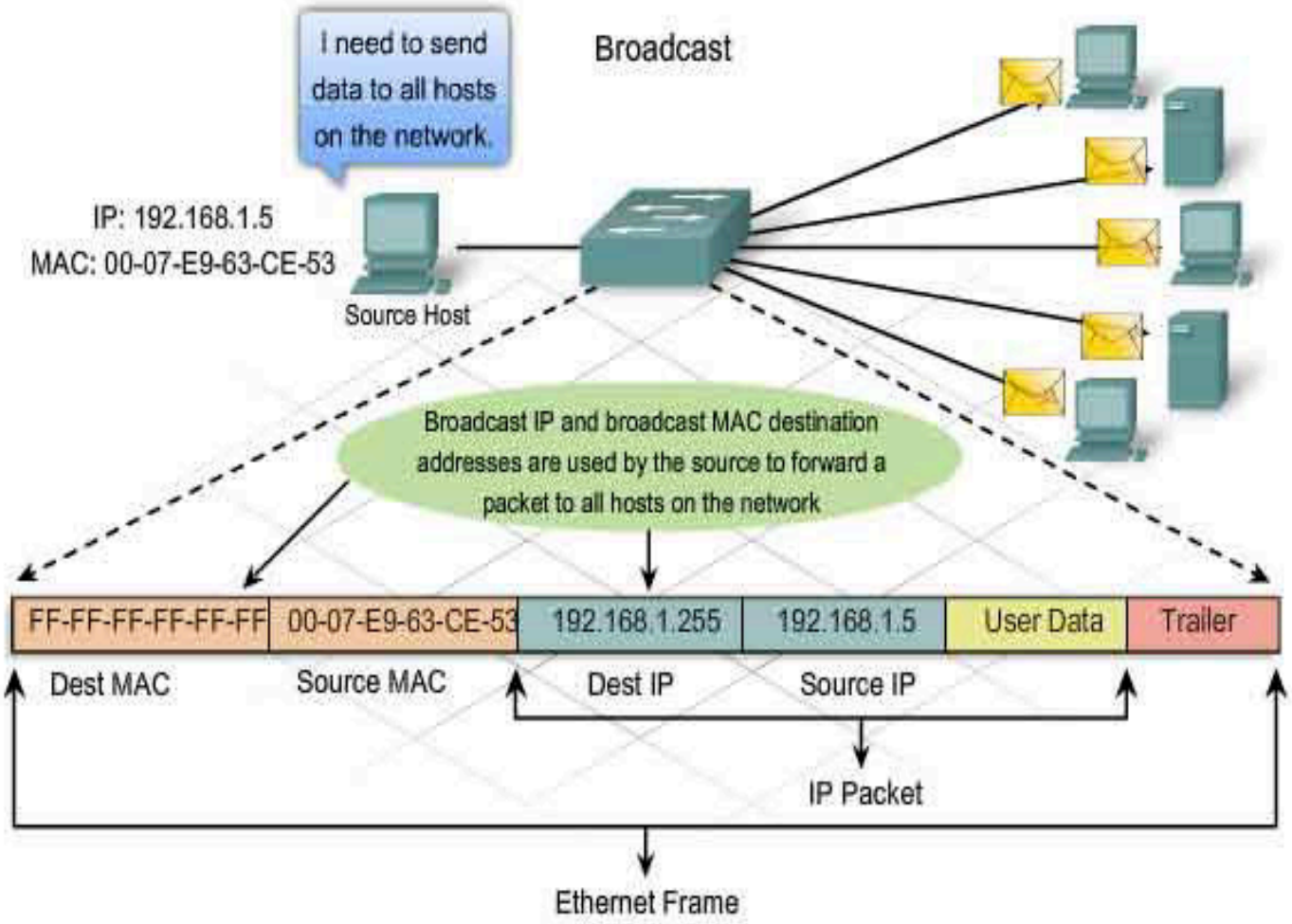
- Unicast is a type of communication where data is sent from one computer to another computer.
- There is only one sender, and one receiver.



LANs and VLANs

Broadcast Communication

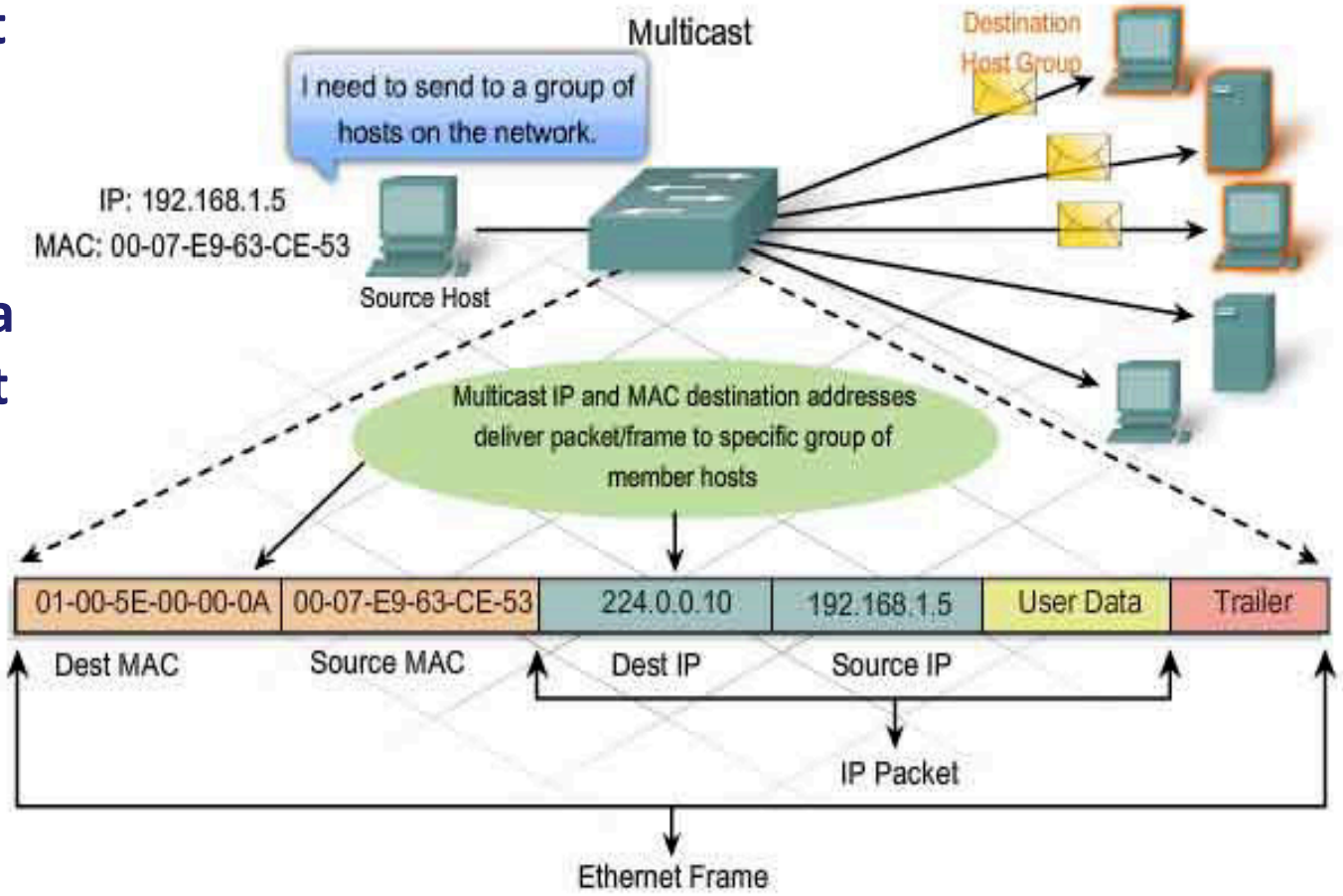
- **Broadcast is a type of communication where data is sent from one computer once and a copy of that data will be forwarded to all the devices.**



Multicast Communication

- Multicast is a type of communication where multicast traffic addressed for a group of devices on the network.

- IP multicast traffic are sent to a group and only members of that group receive and/or process the Multicast traffic.



LANs and VLANs

Collision and Broadcast domains

This device:
- **Continues Collision Domains**
- **Continues Broadcast Domains**

Ethernet Hub

This device:
- **Ends Collision Domains**
- **Continues Broadcast Domains**

Ethernet Switch

These devices:
- **End Collision Domains**
- **End Broadcast Domains**

Router

Firewall

LANs and VLANs

Switch Ethernet Operations

- Switch filters packets :
  - Frame only forwarded to the necessary segments
  - Segments become separate collision domains

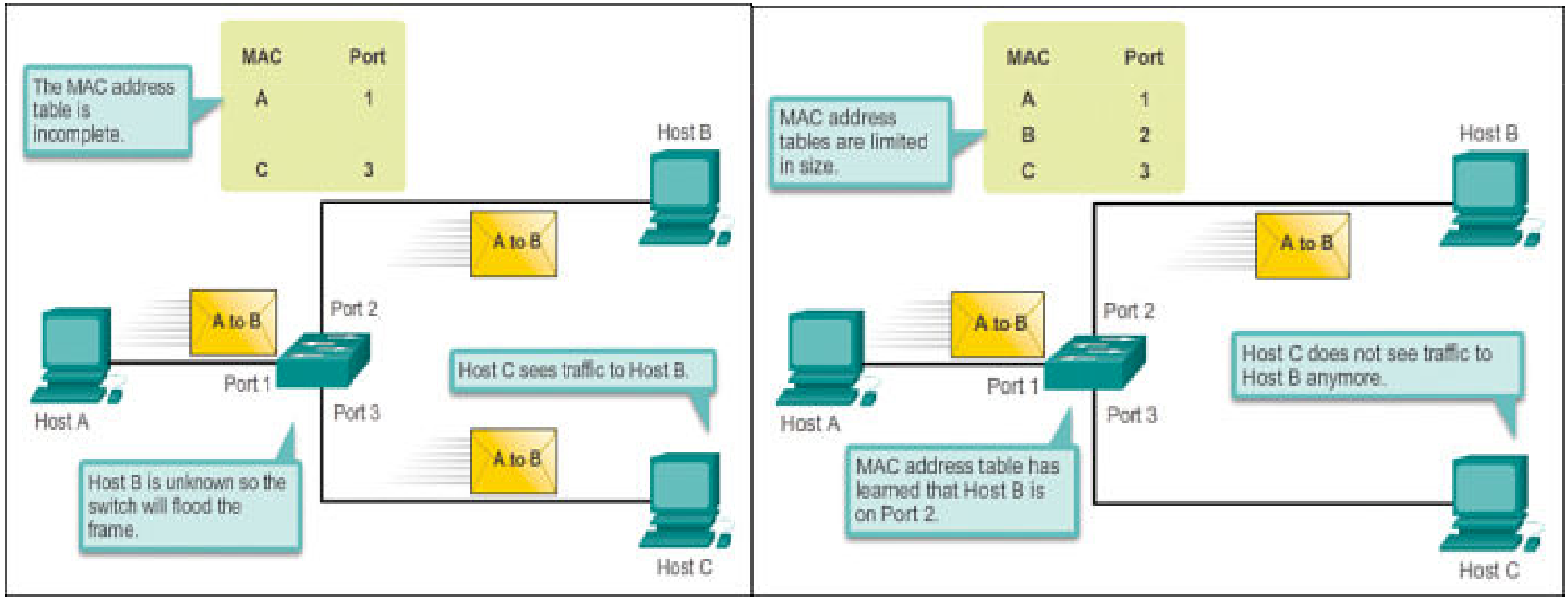
- Switches forward frames selectively :
  - Forward frames only on segments that need them

- Switch mac-address table :
  - Maps destination MAC address to outgoing interface

- When a frame arrives :
  - Inspect the sourceMAC address
  - Associate the address with the incoming interface
  - Store the mapping in the switch table (time-to-live field to forget)

Switch Ethernet Operations

- When frame arrives with unfamiliar destination:
  - Forward the frame out all of the interfaces
  - ... except for the one where the frame arrived



LANs and VLANs

Switch Port Settings

- Auto (default for UTP) - Method to automatically select 'best' transmission method between link partners. Negotiates half/full duplex with connected device.
- Full – sets full-duplex mode
- Half - sets half-duplex mode
- Auto is fine if both devices are using it.

- Potential problem if switch uses it and other device does not. Switch defaults to Half:
  - Full one end and half the other – errors (late collisions).
  - Full-duplex Ethernet supports simultaneously communication by providing separate transmit and receive paths

Ethernet - Interface Performance Problems

- Duplex mismatch: one side of a network link operating in full-duplex and the other side operating in half-duplex

	NIC Settings	Switch Settings	Comments
Setting:	10/Half	10/Half	Yes. This works because both sides of the link are set manually.
Result:	10/Half	10/Half	
Setting:	10/Full	10/Full	No. Although this should work, few manufacturers have implemented full duplex correctly.
Result:	10/Full	10/Full	
Setting:	All other combinations		No. While autonegotiation results in both sides of the link set to full duplex, the "auto" side of the link is likely to reset and renegotiate periodically, causing performance problems.
Result:	Duplex mismatch or NIC/switch resets		

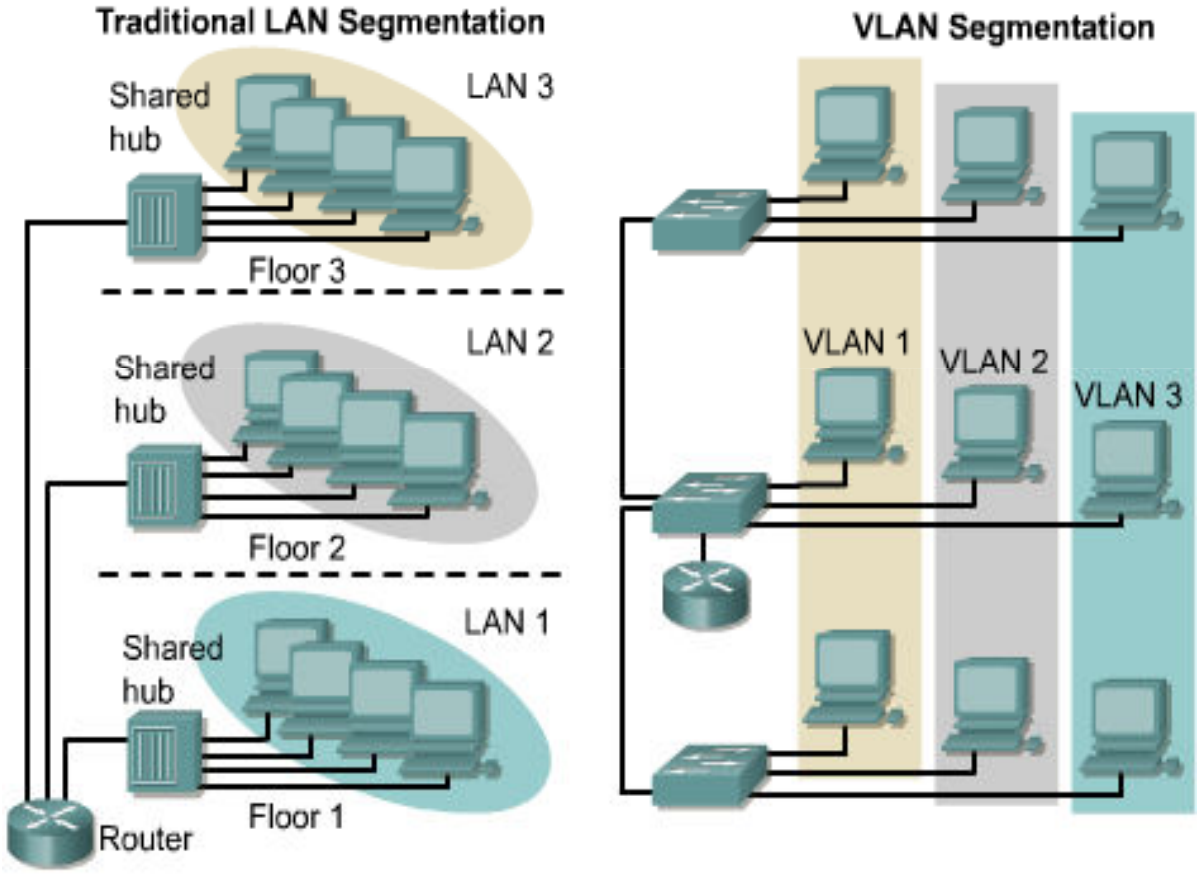
Switch Ethernet - Interface Status Codes

Line Status	Protocol Status	Interface Status	Typical Root Cause
Administratively Down	Down	disabled	The interface is configured with the **shutdown** command.
Down	Down	notconnect	No cable; bad cable; wrong cable pinouts; the speeds are mismatched on the two connected devices; the device on the other end of the cable is (a) powered off, (b) **shutdown**, or (c) error disabled.
Up	Down	notconnect	An interface up/down state is not expected on LAN switch physical interfaces.
Down	Down (err-disabled)	err-disabled	Port security has disabled the interface.
Up	Up	connected	The interface is working.

LANs and VLANs

VLAN Overview

- Created by software running on Layer 2 switches
- Switches maintain a bridging table (broadcast domain) for each VLAN
- Switches can support multiple VLANs
- Switches perform filtering and forwarding based on VLAN ID



LANs and VLANs

Benefits of VLANs

- **Security**

  Groups that have sensitive data are separated from the rest of the network.

- **Cost reduction**

  Cost savings result from less need for expensive network upgrades and more efficient use of existing bandwidth and uplinks.

- **Higher performance**

  Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces unnecessary traffic on the network.

- **Broadcast storm mitigation**

  Dividing a network into VLANs reduces the number of devices that may participate in a broadcast storm.

- **VLANs make it easier to manage the network.**

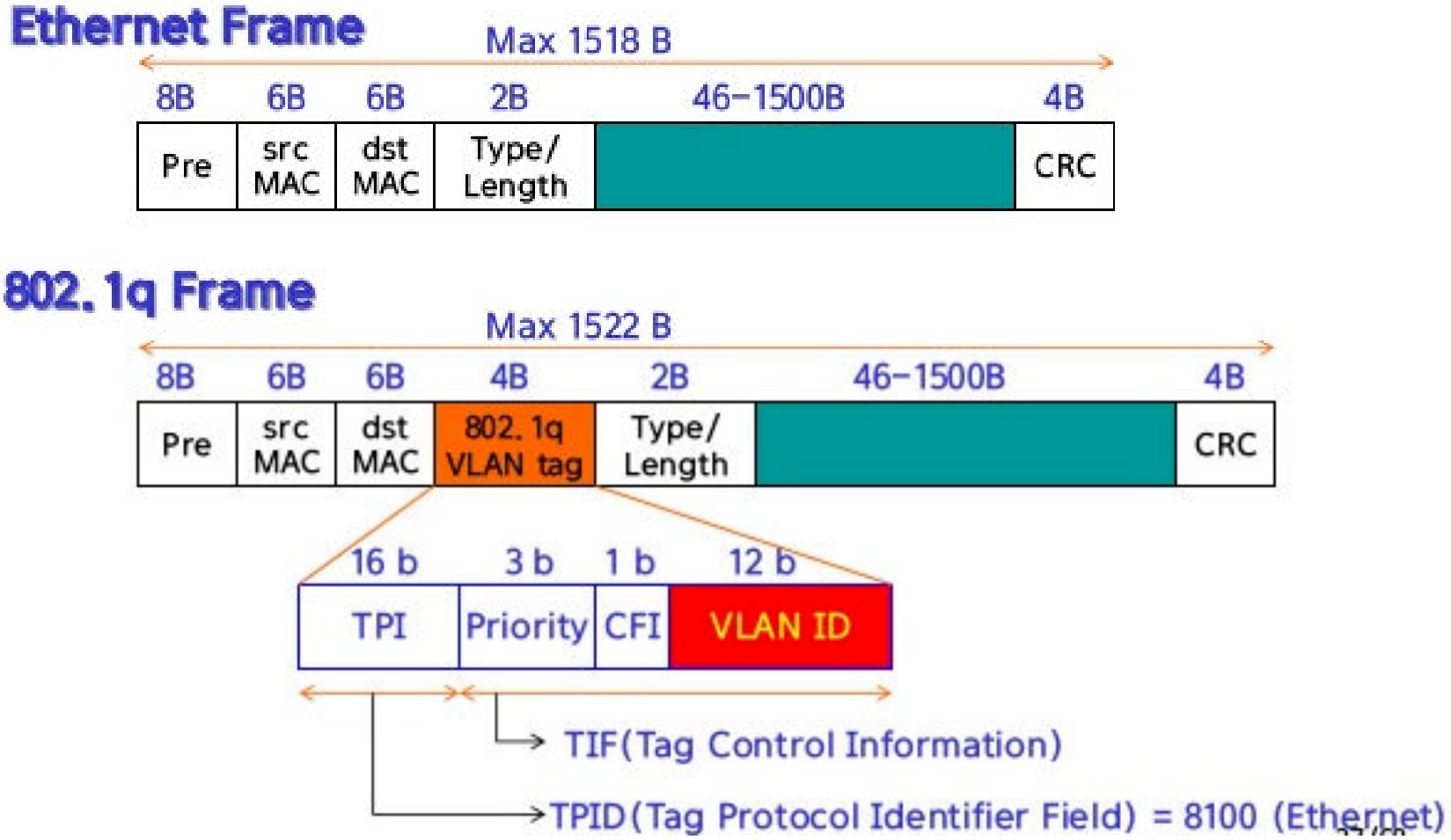
LANs and VLANs

Switch Port Tagged vs. Untagged

- Edge ports are not tagged, they are just “members” of a VLAN
- You only need to tag frames in switch-to-switch links (trunks), when transporting multiple VLANs
- A trunk can transport both tagged and untagged VLANs

- Port Untagged (other vendors) = Interface Access (Cisco)
- Port Tagged (other vendors) = Interface Trunk (Cisco)

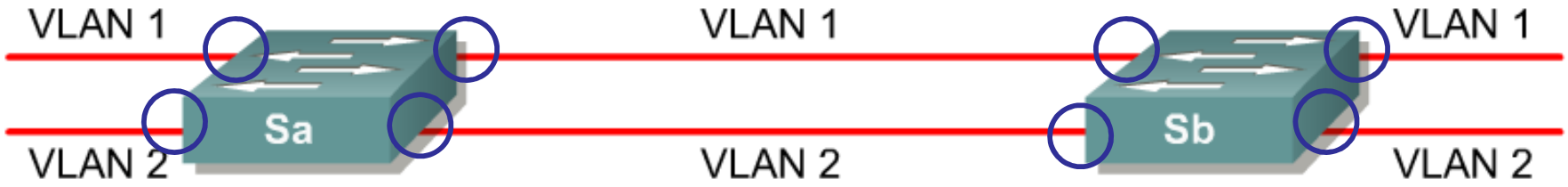
IEEE 802.1Q VLAN Frame



- VLAN ID is a 12–bit field and can have a value between 0 and 4095.

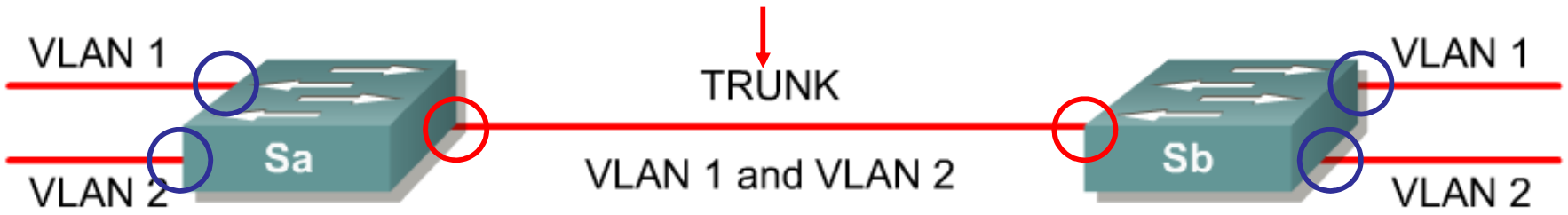
Switch Interface Configuration

No VLAN Tagging




```
Switch(config-if)switchport mode access
```

VLAN Tagging

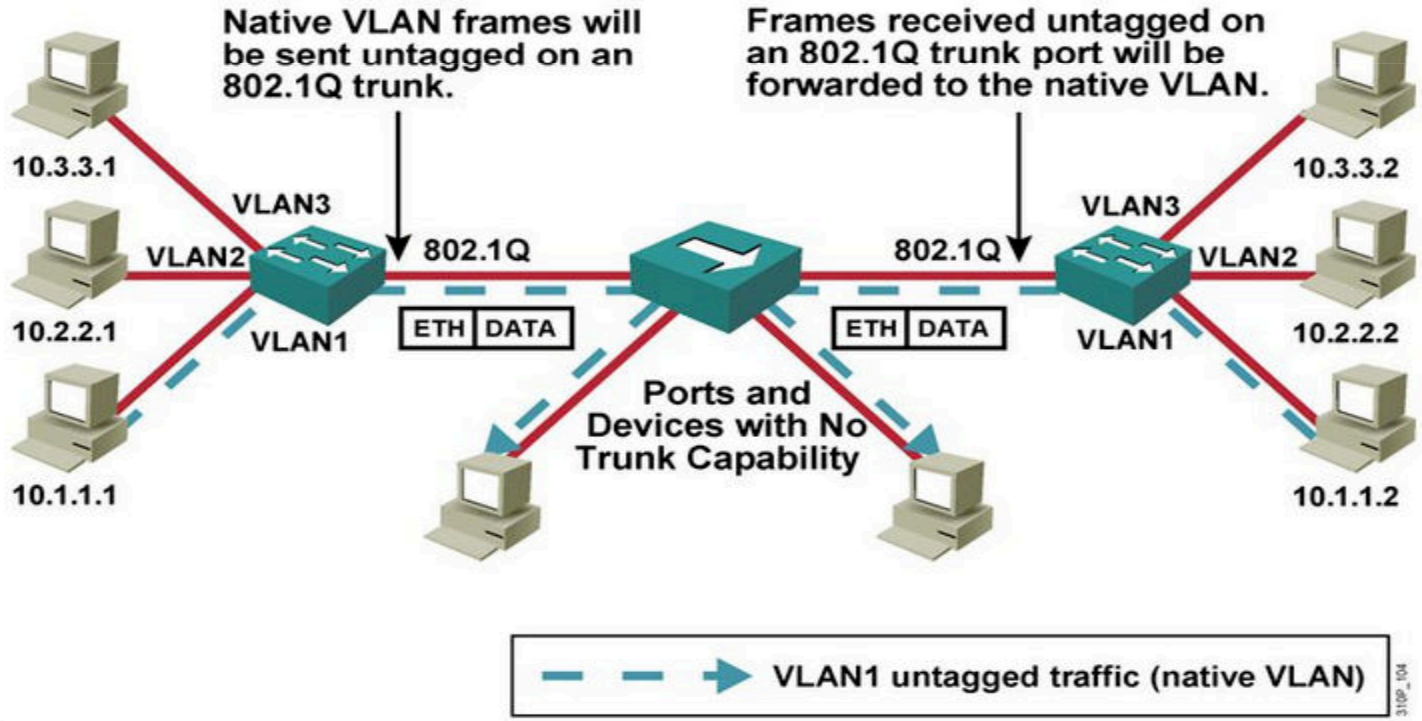



```
Switch(config-if)switchport mode trunk
```

LANs and VLANs

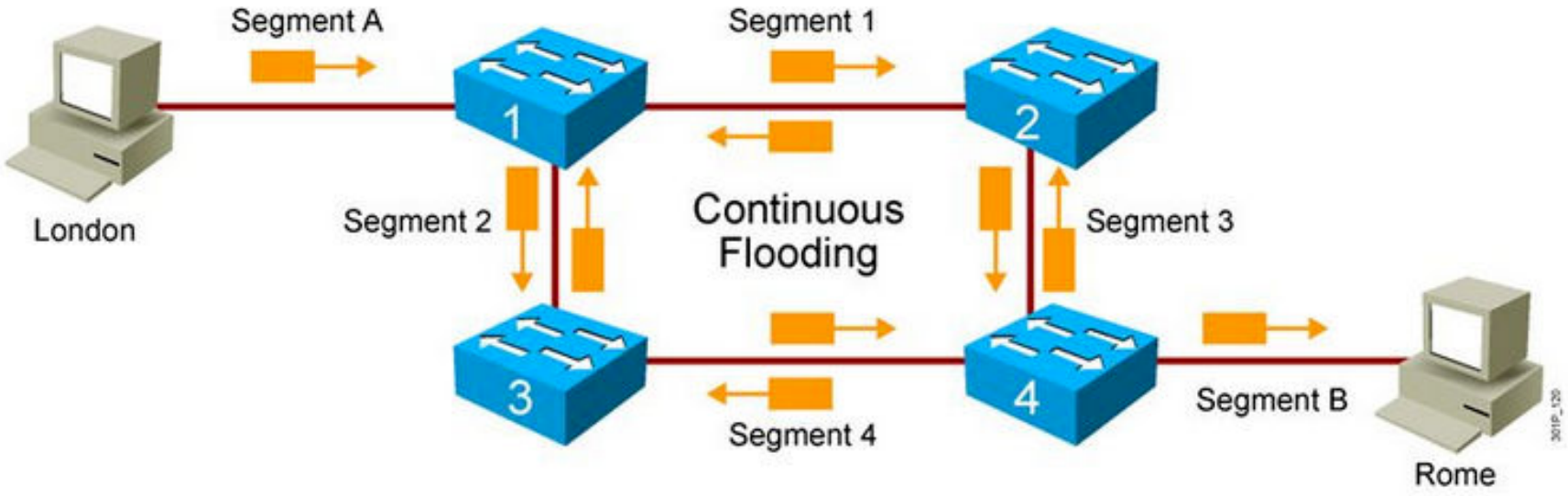
Native VLAN

- An 802.1Q trunk port supports traffic coming from many VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic).
- The 802.1Q trunk port places untagged traffic on the native VLAN.
- Native Vlan (Cisco) = PVID – Port VLAN ID (non-Cisco switches)



Ethernet Loops

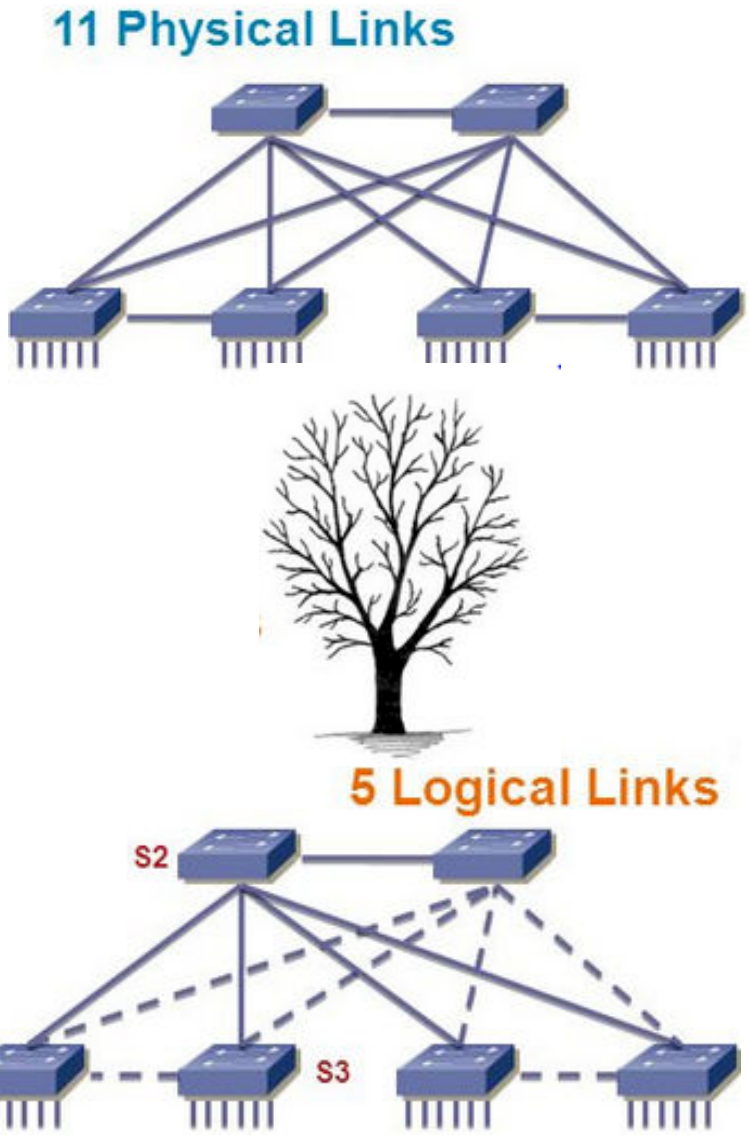
- Broadcasts and Layer 2 loops can be a dangerous combination.
- Ethernet frames have no TTL field
- After an Ethernet frame starts to loop, it will probably continue until someone shuts off one of the switches or breaks a link.
- Physical loops without STP can be disastrous



LANs and VLANs

Spanning Tree Protocol (STP)

- The algorithm used to create this loop free logical topology is the spanning-tree algorithm.
- Allows redundancy without loops
- The loop free logical topology created is called a tree.
- It is a spanning tree because all devices in the network are reachable or spanned.
- Slow to converge, so now there is Rapid Spanning Tree



LANs and VLANs

Spanning tree algorithm

- STP uses the Spanning Tree Algorithm (STA) to determine which switch ports on a network need to be configured for blocking to prevent.

- STA designates a single switch as the root bridge and uses it as the reference point for all calculations. This is done using messages called BPDUs (Bridge Protocol Data Units).

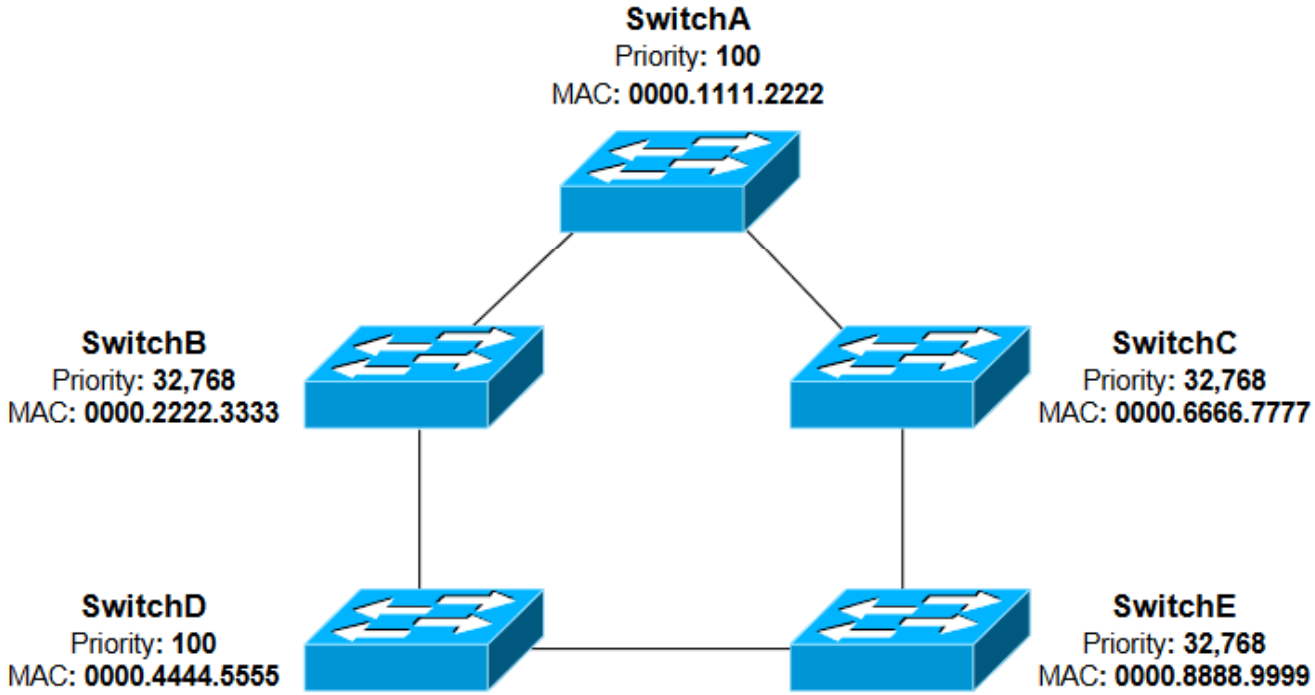
- The switch with the lowest BID becomes the Root Bridge.
  Bridge ID – bridge priority (0-65,535) + MAC Address

- When STA has determined which paths are to be left available, it configures the ports into distinct port roles.

Root Bridge Election

Switches exchange BPDU's to perform the election process, and the lowest Bridge ID determines the Root Bridge:

- **SwitchB, SwitchC, and SwitchE have the default priority of 32,768.**
- **SwitchA and SwitchD are tied with a lower priority of 100.**
- **SwitchA has the lowest MAC address, and will be elected the Root Bridge.**

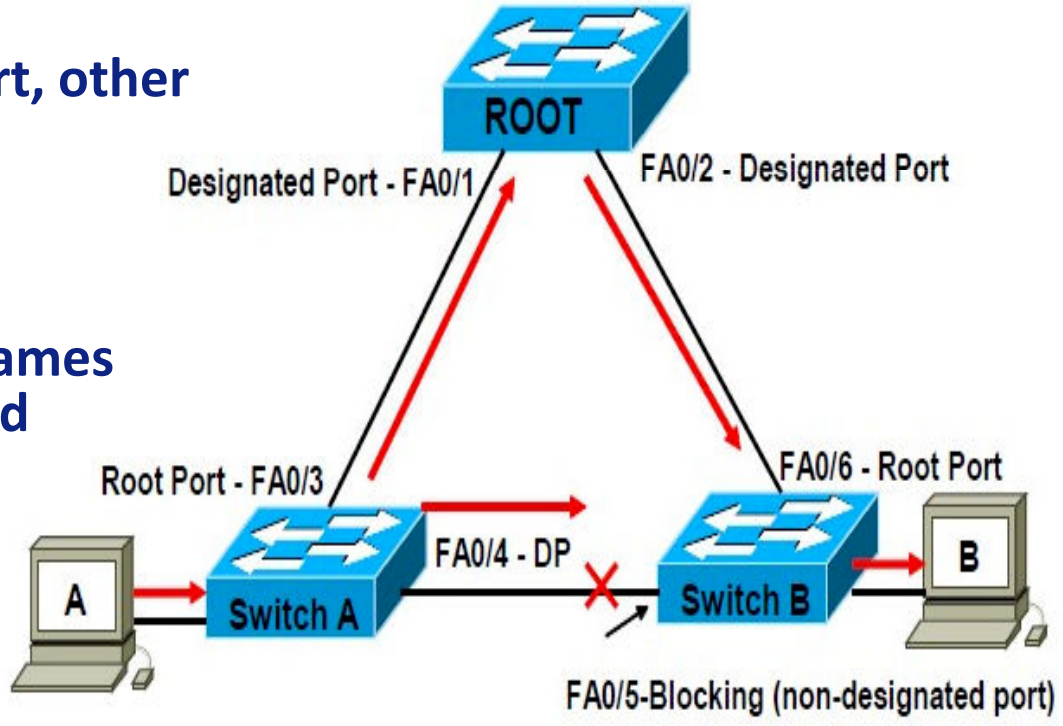


Spanning tree Port Roles

- **Root port:**
  - -Switch ports closest to the root bridge.
    If there two equal cost paths from switch to root bridge:
    - -Which port has lowest port priority? 128 is the default
    - -Which port has lowest interface ID?
    - -Port with lowest value becomes root port, other becomes alternate port and is blocked

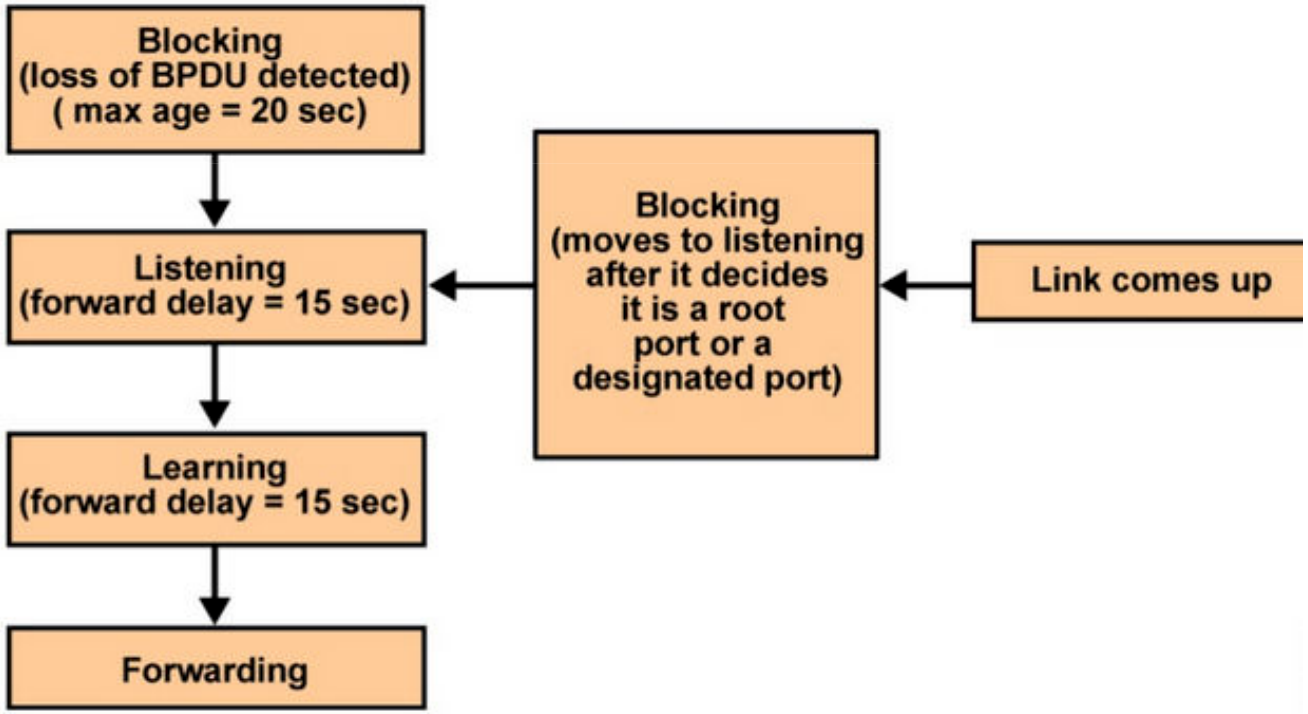
- **Designated port:**
  - -One designated port per segment
  - -Designated port receives and forwards frames
  - -All ports on the root bridge are designated

- **Non-designated port (alternate port):**
  - -Is blocked to prevent loops
  - -Does not forward frames or populate its MAC address table
  - -Does continue to receive BPDUs



Spanning tree Port States

- When a bridge is first attached to a network segment, and before it can start forwarding data, it goes through a series of states while it processes BPDUs and learns the topology of the network

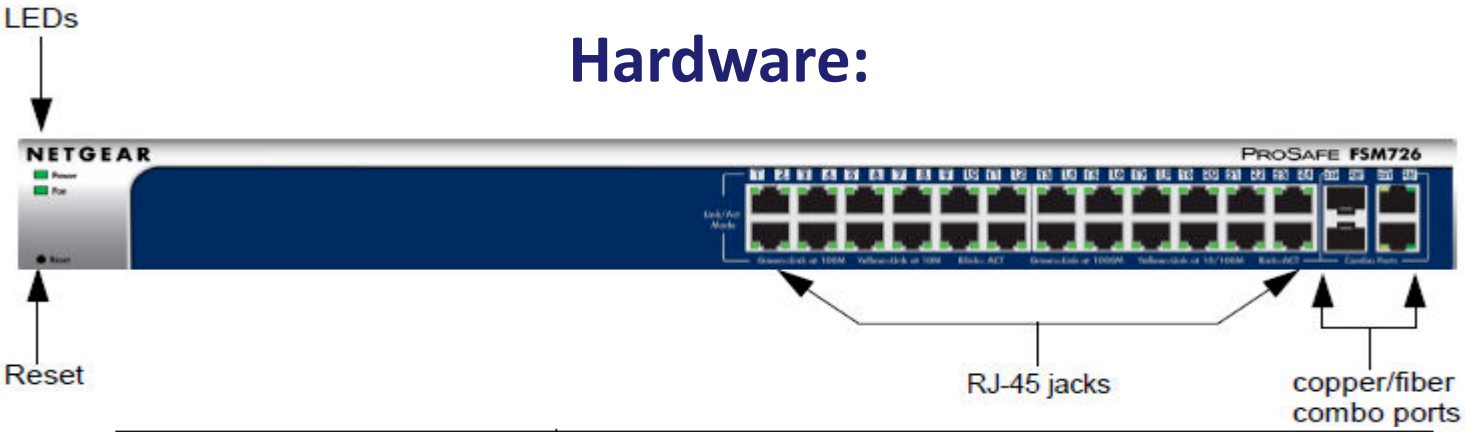


- Port Fast feature allows the port to go directly from blocking to forwarding

LANs and VLANs

Netgear Switch

Hardware:



Commands:

telnet 10.100.xx.51 or 52

(M4100-26G) #show version
(M4100-26G) #show run
(M4100-26G) #show mac-addr-table
(M4100-26G) #show vlan
(M4100-26G) #show port status all
(M4100-26G) #show interface counters

LED	Description
PWR (Power)	• **Solid green**. Power is supplied and the switch is working. • **Blinking green**. Power-on self-test (POST) in progress. • **Solid yellow**. System is booting up. • **Blinking yellow**. POST, CPU, or power supply has failed • **Off**. Power is disconnected.
FAN	• **Yellow**. The fan has failed. • **Green**. The fan is operating normally.
10/100 (port 1 to 24) (1 LED per port)	**Link/ACT LED** • **Off**. No link is established on the port. • **Solid green**. A valid 100 Mbps link is established on the port. • **Blinking green**. The port is sending or receiving packets at 100M. • **Solid yellow**. A valid 10Mbps link is established on the port. • **Blinking yellow**. The port is sending or receiving packets at 10 Mbps.

LANs and VLANs

VLANs REDDIG2

- Vlan 1 – Local network for Intra-Network Elements Communication

  Subnet – 10.100.XX.0/24
- Vlan 100 – AMHS

  Subnet – 10.0.AA.0/24
- Vlan 101 – RADAR

  Subnet – 10.0.BB.0/24
- Vlan 102 – AIDC

  Subnet – 10.0.CC.0/24
- Vlan 120 - NATIVE SERVICES

  Subnet – 10.120.XX.0/24

Operating Cisco IOS Software

Operating Cisco IOS Software

Introduction to Cisco IOS

- Cisco Internetwork Operating System (IOS) is an operating system used on Cisco devices, such as routers and switches. It is a multitasking operating system that implements and controls logic and functions of a Cisco device.
- The user can interact with the system using a command line interface (CLI) or a graphical user interface (GUI).
- Command Line Interface (CLI):
  - User interacts directly with the system in a text-based environment by entering commands on the keyboard at a command prompt.
  - The system executes the command, often providing textual output.
  - CLI requires very little overhead to operate. However, it does require that the user have knowledge of the underlying structure that controls the system.

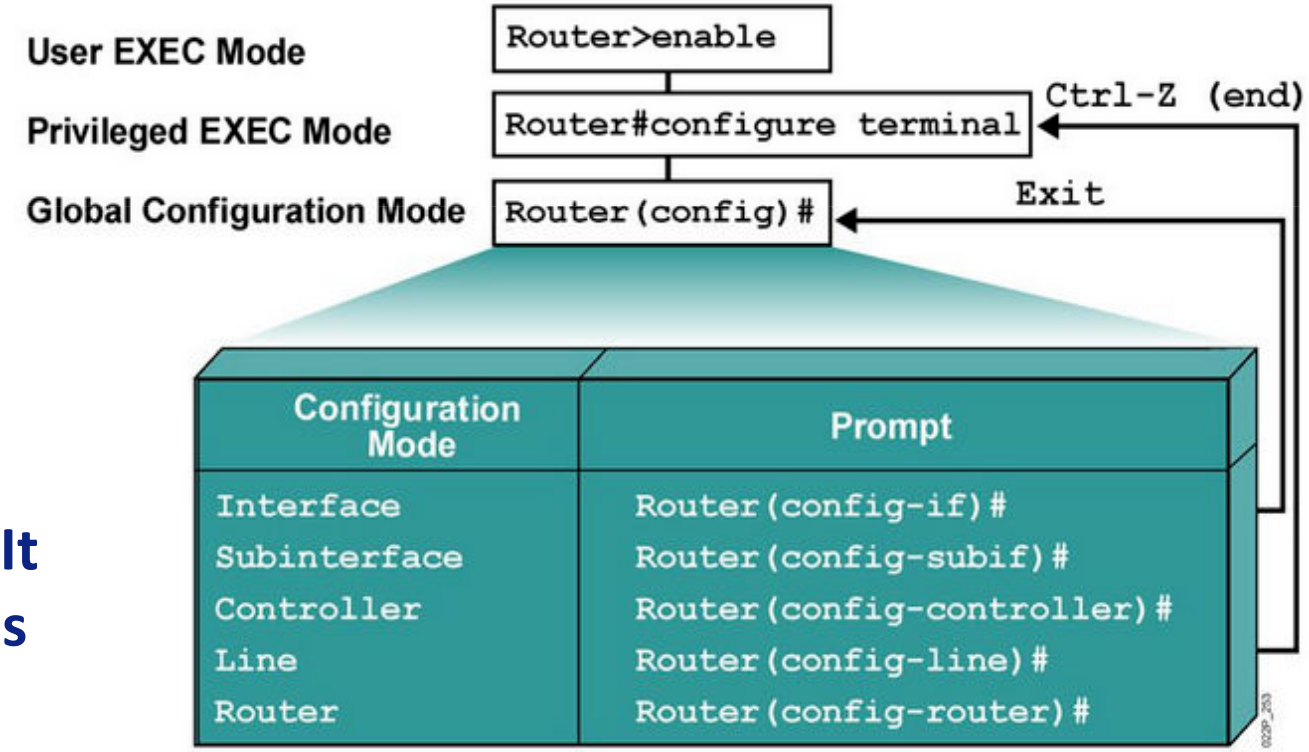
Operating Cisco IOS Software

Cisco IOS CLI Command Modes

- User EXEC Mode: It is mostly used to view statistics and run commands like ping or telnet

- Privileged EXEC Mode: It is called privileged because it allows you to execute more powerful commands, such as reload.

- Global Configuration Mode: It is used to make global changes to the device and change its configuration

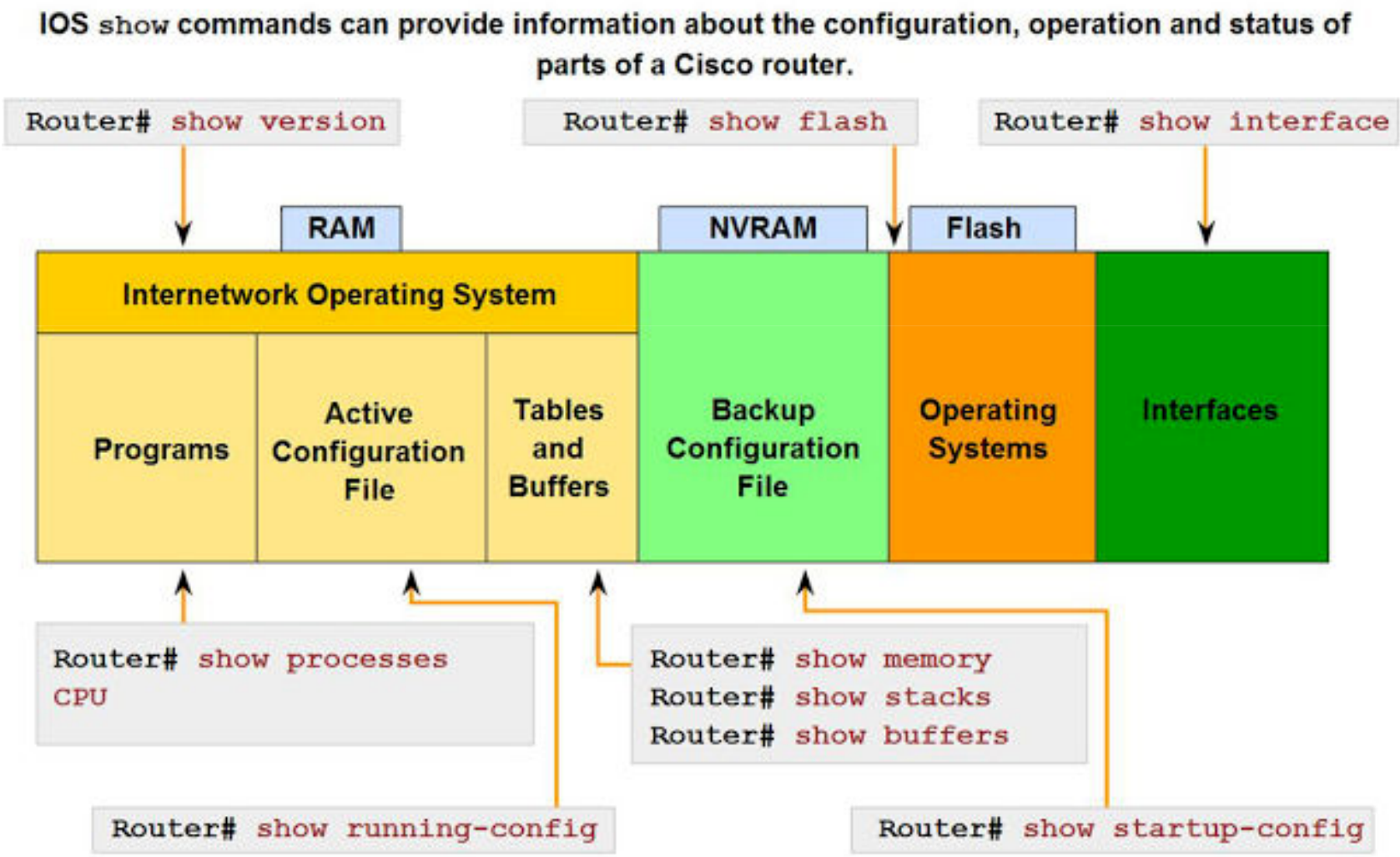


Cisco – Types of Memory

- ***ROM:*** **The Read-Only Memory (ROM) on a Cisco device is like the ROM on a computer in the sense that it stores the POST and the boot loader program. The boot loader program is responsible for locating the IOS.**
- ***Flash:*** **The flash memory is used to store the Cisco IOS. Can be expanded using PCMCIA (removable) cards.**
- ***RAM:*** **RAM is used to store things like the routing table on a router, or the MAC address table on a switch. It is also used to store the running-config. RAM is also known as volatile RAM, or VRAM.**
- ***NVRAM:*** **Non-volatile RAM (NVRAM) is used to store the startup-config, which is copied to the running-config on bootup after the IOS is loaded.**

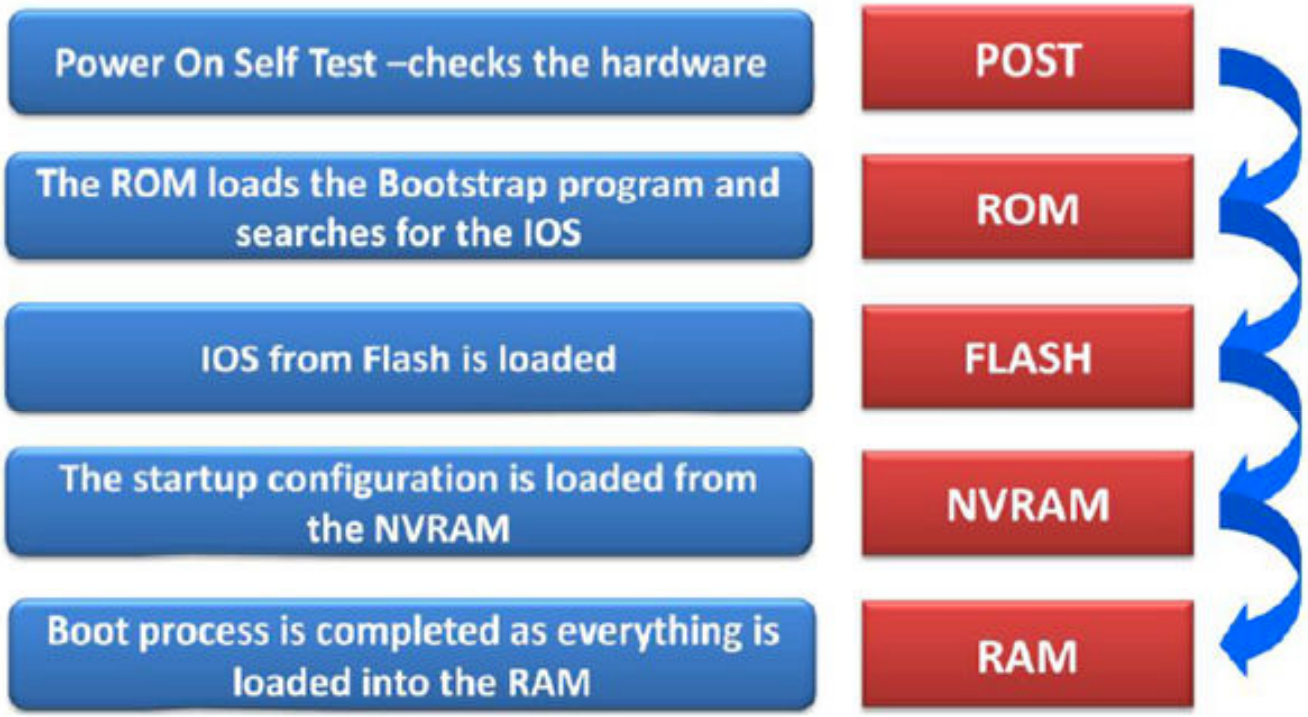
Operating Cisco IOS Software

Cisco – Types of Memory



Operating Cisco IOS Software

Cisco IOS boot sequence



What could be wrong if the Router does not boot:

- Configuration file has missing or incorrect boot system statement
- Incorrect configuration register value
- Corrupted flash image
- Hardware failure

Operating Cisco IOS Software

Configuration Register

- Cisco equipments use a 16-bit software configuration register, with which you can set specific system parameters. Settings for the software configuration register are written into (NVRAM).
- The register can be used to recover a lost password (into the ROM monitor).

- **0x2102**=load IOS from flash and then the configuration from NVRAM. The router looks in NVRAM for the boot sequence
- **0x2100**=Load ROM Monitor Mode
- **0x2101**=load Mini-IOS from ROM
- **0x2142**=Load IOS from Flash and do not load startup-config

Modifying the Configuration-Register

```
Router#config t
Router(config)#config-register 0x2102
```

Operating Cisco IOS Software

Cisco Device – Basic Commands

#1: The "?“

#2: show running-configuration

#3: copy running-configuration startup-configuration

#4: show interface

#5: show ip interface

#6: config terminal, enable, interface, and router

#7: no shutdown

#8: show ip route

#9: show version

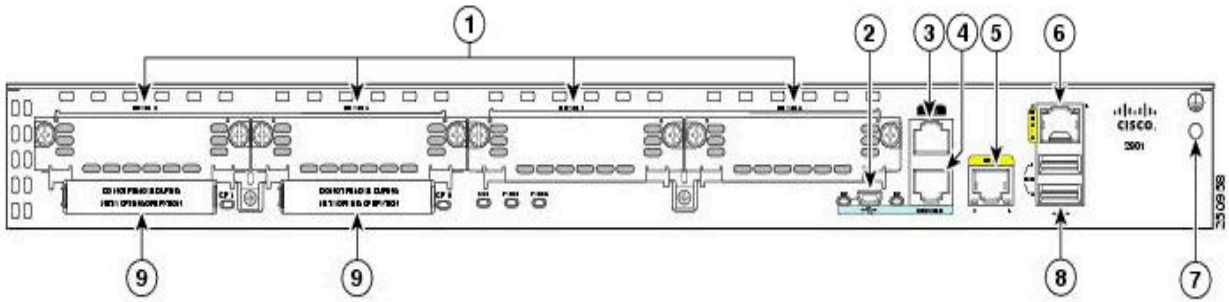
#10: debug

Operating Cisco IOS Software

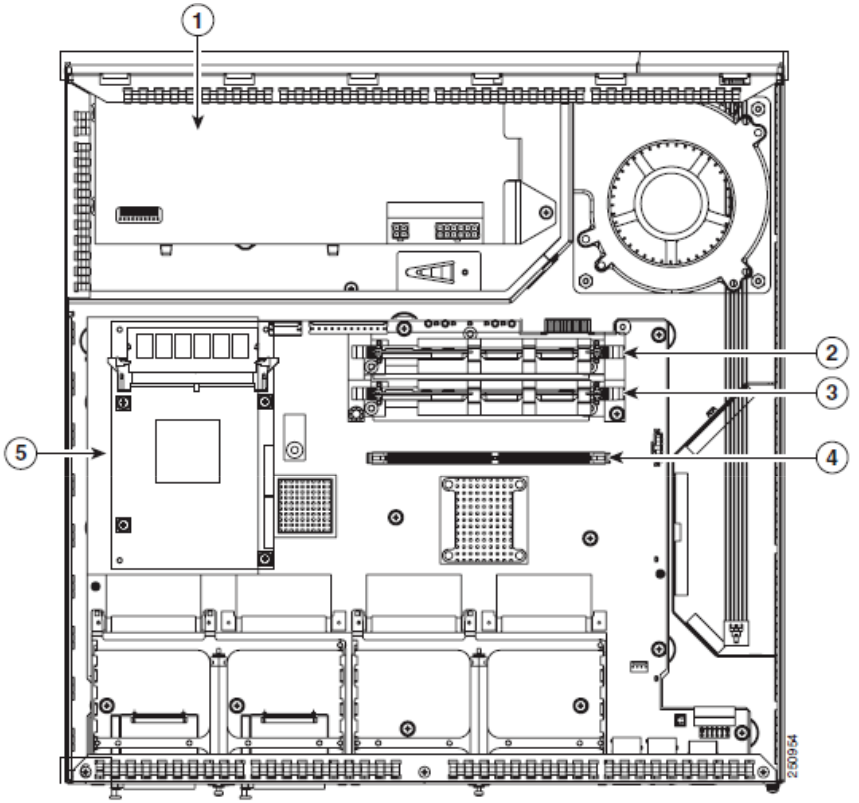
Cisco Hardware

- The routers used in REDDIG are of the 2900 family.

Cisco 2901



1	EHWIC slots [1] 0, 1, 2, and 3 (0, Far right)	2	USB[2] serial port
3	Aux port	4	RJ-45 serial console port
5	10/100/1000 Ethernet ports (GE0/1)	6	10/100/1000 Ethernet port (GE0/0)
7	Ground	8	USB0 and USB1 (1, Top)
9	CompactFlash[3] 0 and 1		

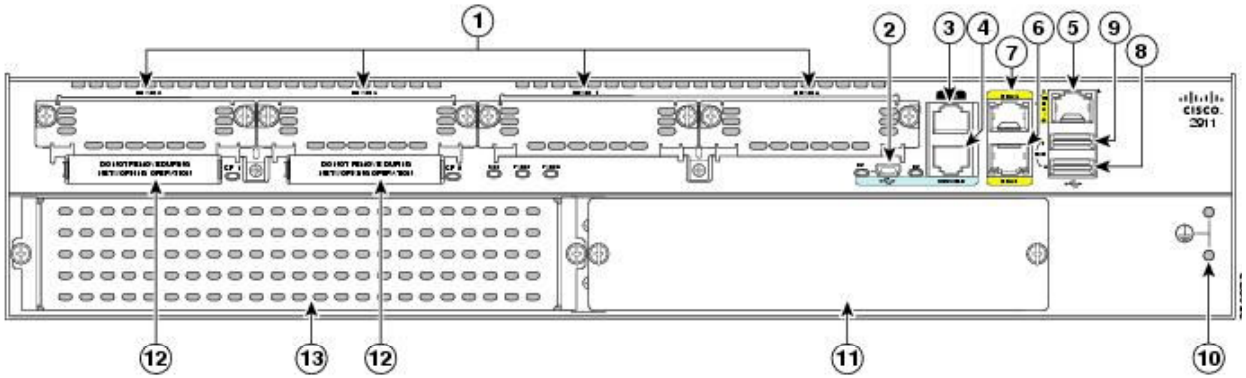


1) Power supply
2) PVDM 3 -1
3) PVDM 3 -0
4) DIMM socket
5) ISM

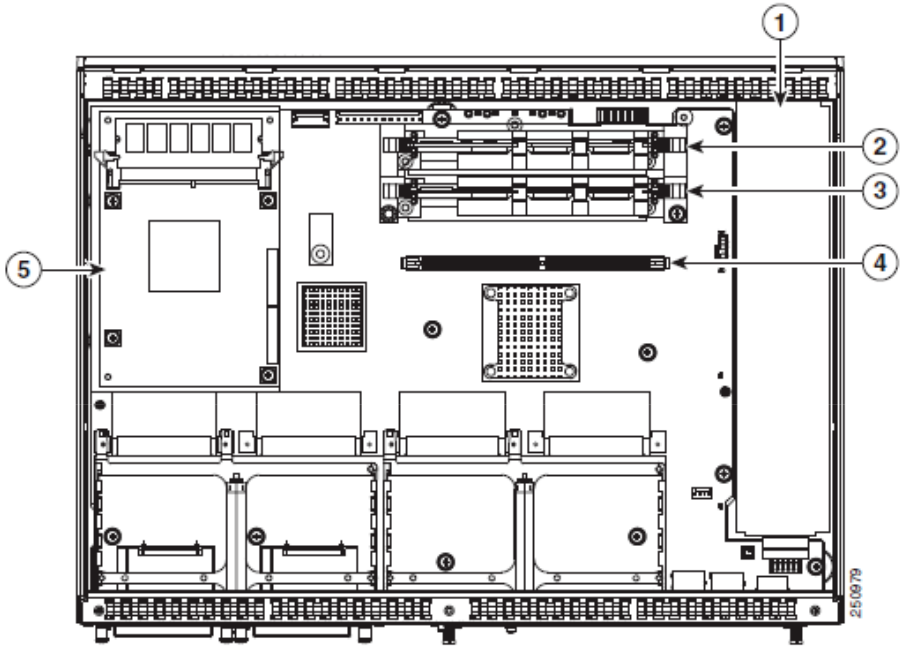
Operating Cisco IOS Software

Cisco Hardware

- **Cisco 2911**



1	EHWIC slots[1] 0, 1, 2, and 3 (0, Far right)	2	USB serial port
3	AUX	4	RJ-45 serial console port
5	10/100/1000 Ethernet port (GE0/0)	6	10/100/1000 Ethernet port (GE0/1)
7	10/100/1000 Ethernet port (GE0/2)	8	USB 0
9	USB 1	10	Ground
11	AC or DC or AC-POE Power Module	12	CompactFlash[2] 0 and 1 (0, Right)
13	Service module[3] slot 1		



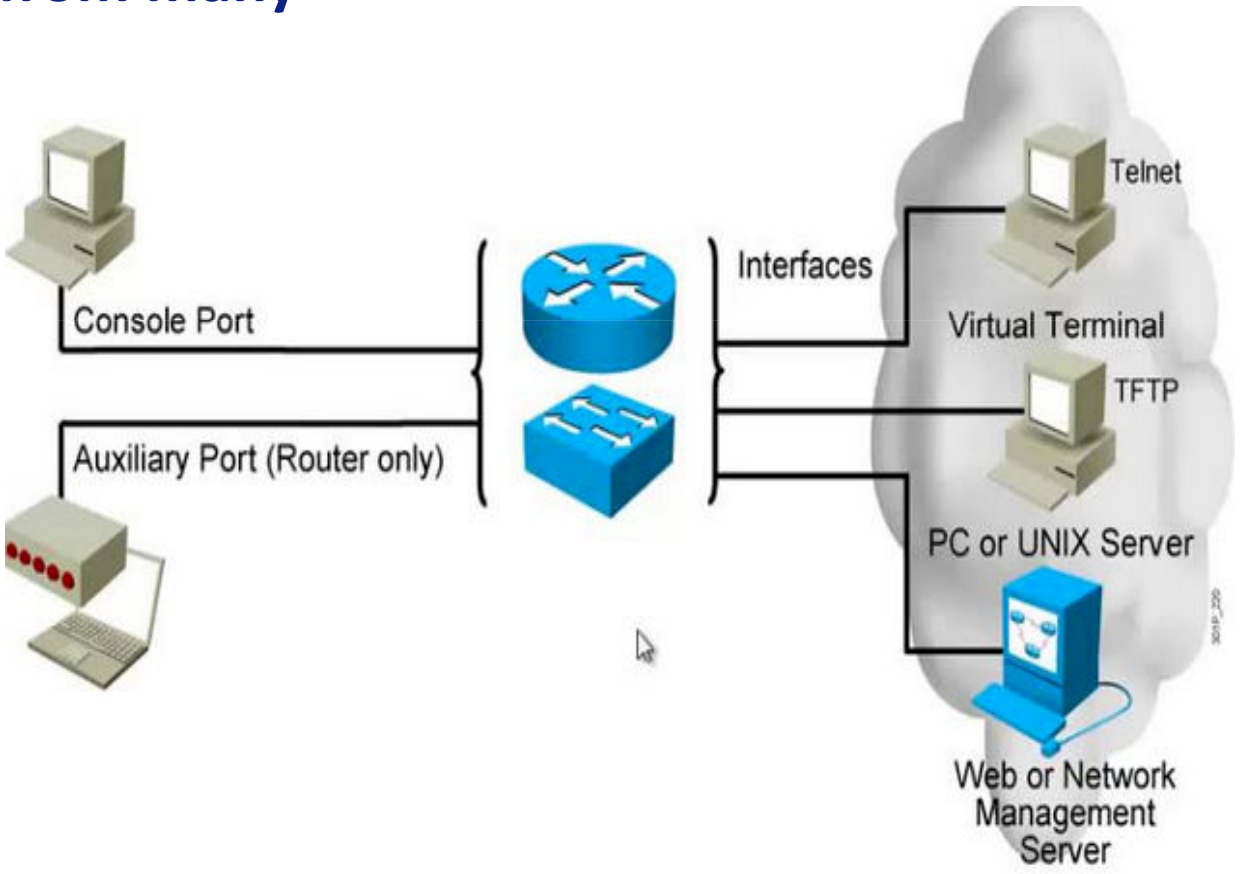
1) Power supply
2) PVDM 3 -1
3) PVDM 3 -0
4) DIMM socket
5) ISM

Operating Cisco IOS Software

External Configuration Sources

Cisco Devices can be configured from many sources:

- Console – direct PC serial access
- Auxilliary port – Modem access
- Virtual terminals – Telnet or SSH access
- TFTP Server – copy configuration file into router RAM
- Network Management Software – Cisco Prime



Operating Cisco IOS Software

Cisco Basic Initial Configuration Steps

1.Configure the host names: Router(config)#hostname R1

2.Disable that name resolution: R1(config)#no ip domain-lookup

3.Protect the 'privileged exec mode' with a password using MD5 encryption algorithm:
R1(config)#enable secret cisco_enable

4.Encrypt the password with 'over-shoulder' algorithm: R1(config)#service password-encryption

5.Protect the access to the console port 0: R1(config-line)#password cisco_console
R1(config-line)#login

6.Configure the console port 0 such, that system messages sent to the screen, do not interfere with what you are typing: R1(config-line)#logging synchronous

7.Configure and enable the router's interface Ethernet: R1(config)#interface f1/0
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#no shutdown

8.Configure and enable the router's interface serial: R1(config-if)#interface s0/1
R1(config-if)#ip address 172.31.1.1 255.255.255.252
R1(config-if)#no shutdown

9.Enable the remote access to your devices via telnet: R1(config-if)#line vty 0 4
R1(config-if)#password cisco_remote
R1(config-if)#login

10. Save the configuration on both switch and the router so it is available after reload/power cycle:
R1#copy running-config startup-config

Operating Cisco IOS Software

Cisco IOS Privilege Levels

Cisco IOS permits to define multiple privilege levels for different accounts. This could be useful when many people work on the same router different roles (operator, tecnhician, network manager)

- **Privilege level 0 - No Access at all**
- **Privilege level 1 - User Mode (also known as "user EXEC" mode)**
- **Privilege level 15 - Privileged mode (enable mode or "privileged EXEC" mode)**
- **Privilege level 2 through 14 are available for customization. For example:**

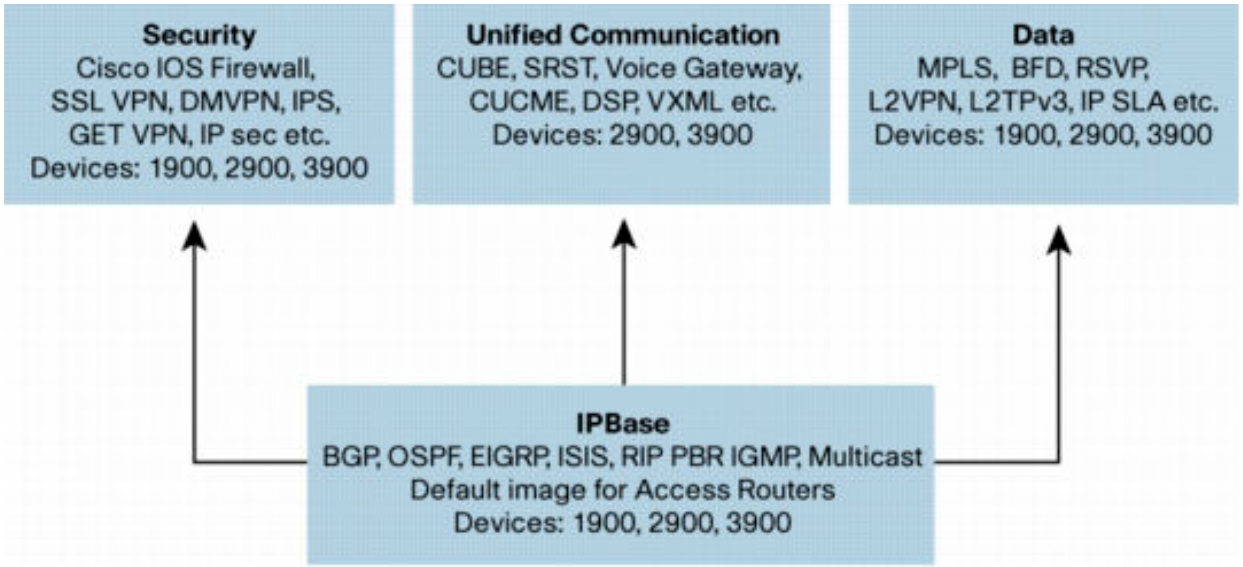
```
Router# username user_6 privilege 6 password pass_6
Router# privilege exec level 6 show running
Router# privilege exec level 8 configure terminal
```

User user_6 is able to Telnet in and execute the show run command, but user cannot configure anything (configure terminal is at level 8)

Operating Cisco IOS Software

Cisco IOS Software Packages and licenses

- After the introduction of Cisco IOS 15.0 and ISR2 (1900, 2900 and 3900) routers, the features available on a router are unlocked with various licenses.
- Specifically, we have four technology package licenses:



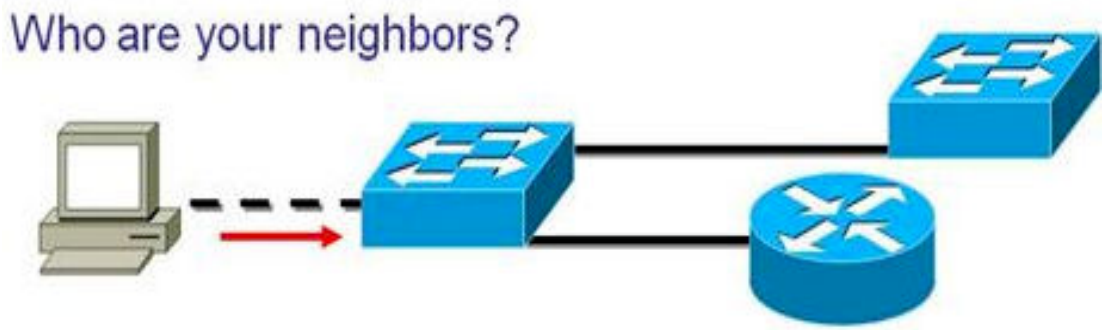
Licenses has two types:

- Evaluation (Temporary) License: which mean will be available with all functionality for trial period would be 60 days
- Permanent License: which mean you must get new license from cisco to run it for ever

Operating Cisco IOS Software

CDP (Cisco Discovery Protocol)

- CDP is a proprietary protocol designed by Cisco System for Cisco devices. CDP helps administrators in collecting information about cisco devices.
- CDP messages are not forwarded. It means you can get CDP information only about the directly connected devices.
- CDP messages contain useful information about cisco device including following:
- IOS version number
- Hardware platform and capabilities
- Layer 3 address (IP address) of device
- Port ID
- Device type
- Name of device configured with hostname



CDP (Cisco proprietary protocol) = LLDP (IEEE standart)

Operating Cisco IOS Software

CDP and LLDP examples in REDDIG Network:

Netgear 4100:

```
(M4100-26G) #show lldp remote-device all

LLDP Remote Device Summary

Local
Interface RemID    Chassis ID            Port ID             System Name
--------- -------  --------------------  ------------------  --------------
0/1         18     C4:04:15:8C:30:20     0/2                 SBMN-SWI-A
0/2         19     C4:04:15:8C:30:20     0/1                 SBMN-SWI-A
0/3
0/4
0/5
0/7
0/8
0/9
0/10
0/11
0/12
0/13
0/14
0/15
0/16
0/17
0/18
--More-- or (q)uit
0/19
0/20
0/21
0/22
0/23
0/24        15     C4:04:15:8C:2F:E0     0/24                SBMN-SWI-B
0/25
0/26
```

Cisco 2911:

```
SBMN-CISCO-VSAT-1-A-V15#sh cdp neighbors detail
-------------------------
Device ID: 39223C5L00368
Entry address(es):
Platform: M4100-26G,  Capabilities: Router
Interface: GigabitEthernet0/1,  Port ID (outgoing port): 0/14
Holdtime : 163 sec

Version :
10.0.1.16

advertisement version: 2
Management address(es):

-------------------------
Device ID: 39223C5L00368
Entry address(es):
Platform: M4100-26G,  Capabilities: Router
Interface: GigabitEthernet0/0,  Port ID (outgoing port): 0/4
Holdtime : 163 sec

Version :
10.0.1.16

advertisement version: 2
Management address(es):
```

Monitoring Cisco Devices

Monitoring Cisco Devices

System Message Logging

- Many network administrators overlook the importance of router logs.
- Logging is critical for fault notification, network forensics, and security auditing.
- By default, the router sends all log messages to its console port.
- Terminal logging is similar to console logging, but it displays log messages to the router's VTY lines instead. You need to need activate it for each required line.
- Buffered logging creates a circular buffer within the router's RAM for storing log messages.
- The router can use syslog to forward log messages to external syslog servers for centralized storage.

Monitoring Cisco Devices

System Message Logging

Cisco log messages are categorized by severity level. Note that the lower the severity level, the more critical the log message is.

	Level	Keyword	Description	Definition
Highest Level	0	emergencies	System is unusable	LOG_EMERG
	1	alerts	Immediate action is needed	LOG_ALERT
	2	critical	Critical conditions exist	LOG_CRIT
	3	errors	Error conditions exist	LOG_ERR
	4	warnings	Warning conditions exist	LOG_WARNING
	5	notifications	Normal but significant condition	LOG_NOTICE
	6	informational	Informational messages only	LOG_INFO
Lowest Level	7	debugging	Debugging messages	LOG_DEBUG

Monitoring Cisco Devices

System Message Format

- The log message is broken into three sections that are delimited by colons.

Router# show log

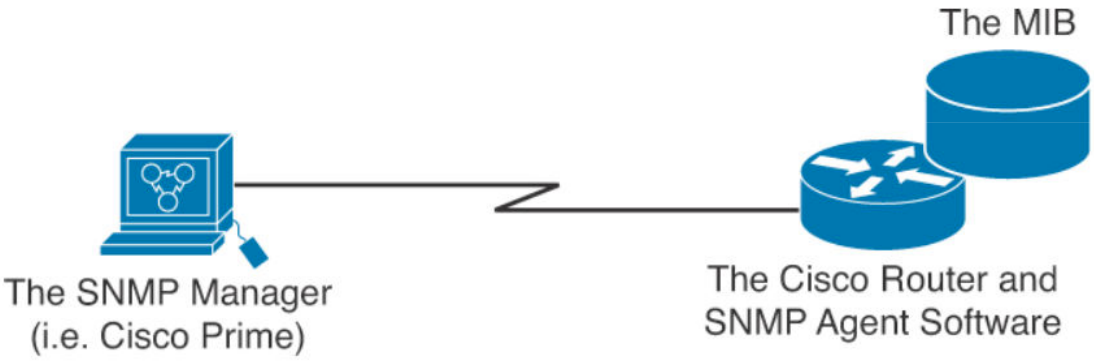
```
*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line
protocol on Interface FastEthernet0/0, changed state
to down
```

- A timestamp: *Dec 18 17:10:15.079
- The facility on the router that generated the message: %LINEPROTO
- The severity level: 5
- A mnemonic for the message: UPDOWN
- The description of the message: Line protocol on Interface FastEthernet0/0, changed state to down

Monitoring Cisco Devices

Simple Network Management Protocol (SNMP)

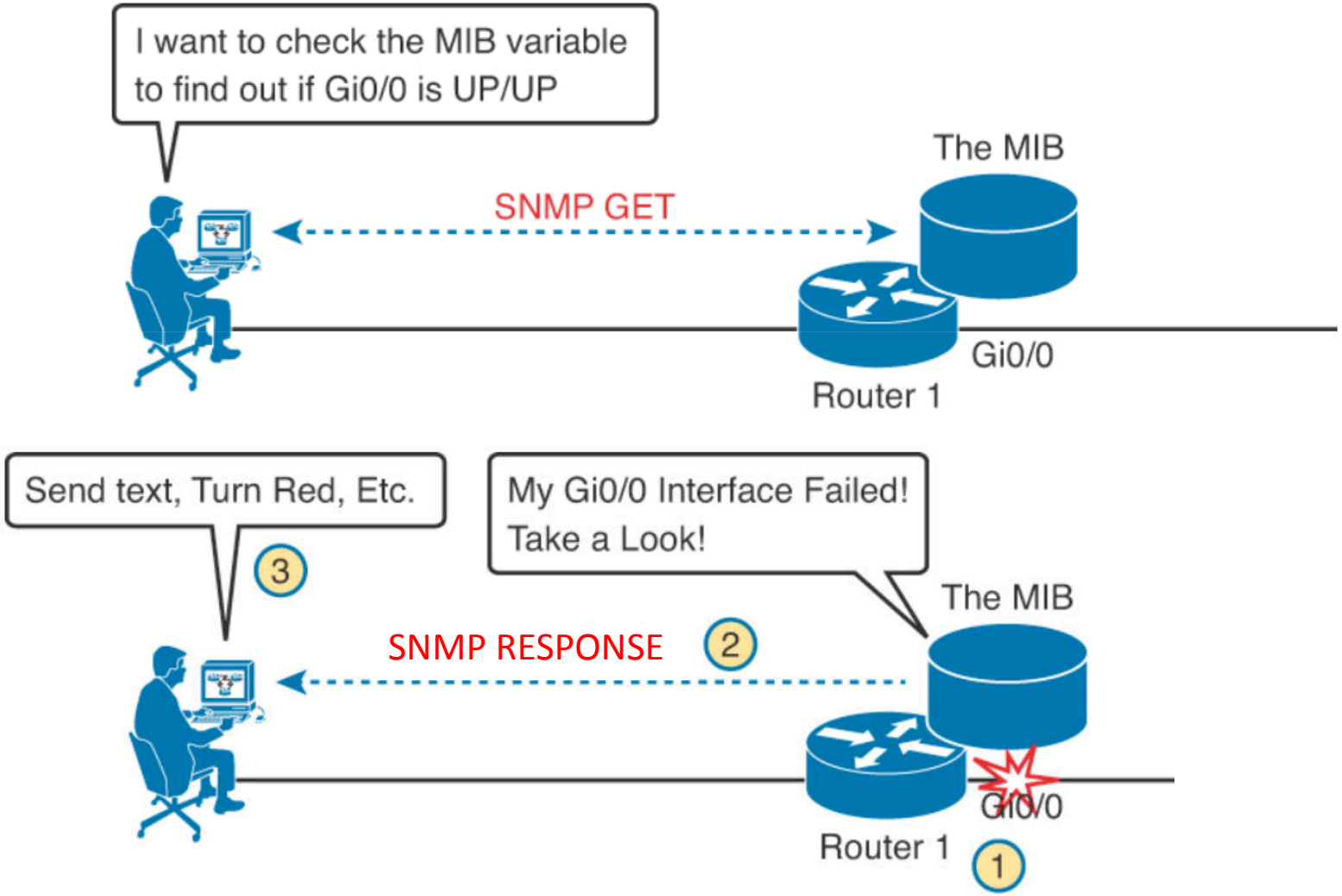
- SNMP is an application layer protocol that provides a message format for communication between what are termed managers and agents
- Supports message exchange using UDP/IP to port 161



- **Components:**
- Manager:
  Polls agents on the network
  Correlates and displays information
- Agent:
  Collects and stores information
  Responds to manager requests for information and generates traps.
- MIB:
  Database of objects (information variables)
  Read and write community strings for controlling acces

Monitoring Cisco Devices

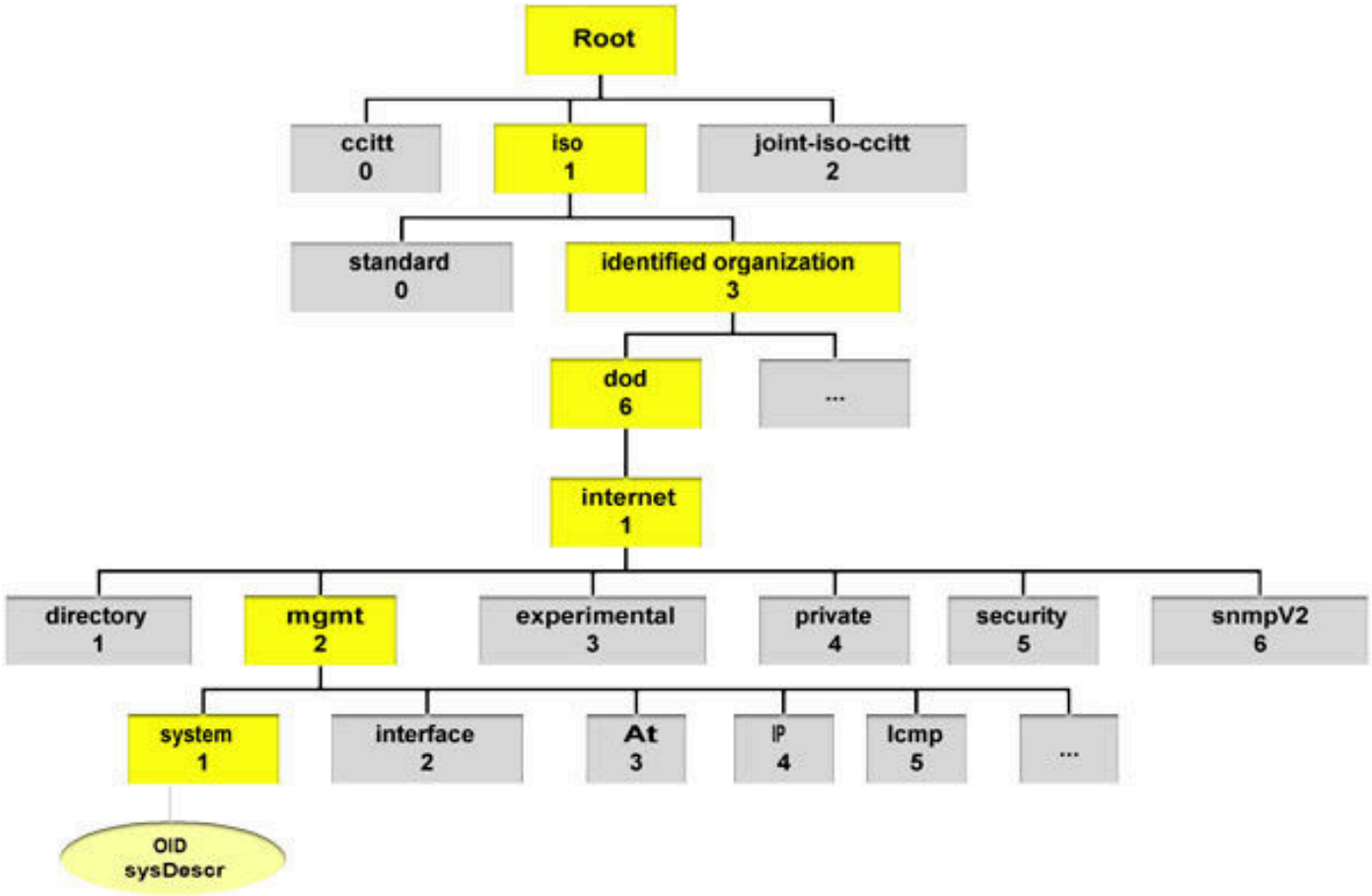
SNMP operations



Monitoring Cisco Devices

The Management Information Base (MIB)

- MIB defines each variable as an object ID (OID)
- Organizes into a hierarchy of OIDs, usually shown as a tree:



OID examples:

1.3.6.1.2.1.1.1 - sysDescr
1.3.6.1.2.1.1.2 - sysObjectID
1.3.6.1.2.1.1.3 - sysUpTime
1.3.6.1.2.1.1.4 - sysContact
1.3.6.1.2.1.1.5 - sysName
1.3.6.1.2.1.1.6 - sysLocation
1.3.6.1.2.1.1.7 - sysServices

Monitoring Cisco Devices

SNMP Community string

- The “SNMP Community string” is like a user id or password that allows access to a router's or other device's statistics.
    - If the community string is correct, the device responds with the requested information.
    - If the community string is incorrect, the device simply discards the request and does not respond.

- There are two types of community strings in SNMP Version 2c:
    - Read-only (RO): Provides access to the MIB variables, but does not allow these variables to changed, only read. Because security is so weak in version 2c, many organizations only use SNMP in this read-only mode.
    - Read-write (RW): Provides read and write access to all objects in the MIB.