CCNA
200-301 v1.1

Developed By: Waleed Hashim Ali Adlan
BSc&MSc in Telecommunication
CCNA/CCNP/CCNP-SPCOR/CCNP-SCOR/CCNP-DCCOR/CCIE#41999
HCIA/HCIP/HCIE#14518
Microsoft AZure Certified Associate
Comptia Security+
Linux Professional Institute LPIC-1
Certified Trainer - Huawei / Microsoft/ Cisco Academy/ Comptia

Course Instructor

- **Name**: Waleed Hashim Ali Adlan
- **Academic Qualifications and Achievements:**

1. MSc of Telecommunication – Leeds University, UK – Distinction(Top of the class)
2. BSc of Electrical Engineering-Khartoum University

Research Publications:

1. Anycast Routing in OBS Grid Networks, 2009
2. Storage Area Networks Extensions in WDM Architecture, 2009

- **Technical Certifications:**

1. HCIE#14518
2. CCIE # 41999
3. CCNP
4. CCNP Security
5. CCNP Service Provider
6. CCNA
7. HCIP Datacom
8. HCIA Datacom
9. Microsoft Certified Azure Administrator
10. Comptia Security+
11. LPI Linux Essentials
12. LPI LPIC-1 Linux Administrator
13. Gold IPv6 Certified Engineer
14. Certified Trainer - Comptia/Huawei/Microsoft/Cisco Academy

Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

Work History

1. Part-timer Teaching Assistant, Khartoum University
2. Network Engineer, Khartoum University – Information Network
3. Routing & Switching Engineer, AZ
4. Base Station Network Engineer, MTN
5. Network Engineer, Excell Group, London
6. Senior Network Architect, Neom, Saudi Arabia
7. Instructor at Fibercli – Spain
8. Senior Network Security Architect Network Plus for Technology & Consultancy Services
9. Instructor Network Plus Training Center

Course Contents

- Introduction to Data Networks
- Network Devices
- OSI Model
- Types of Network Media
- TCP/IP Model
- TCP/IP Math
- Router Internal Components
- Basic Router Configuration
- Routing principles

- Static Routing
- Default Routing
- Floating Static / Default Routes
- Dynamic Routing Categories
- Open Shortest Path First (OSPF)
- Policy Based Routing Description
- Switching Basics
- Basic Switch Configuration
- Spanning Tree Protocol (STP)
- Spanning Tree Protocol Security Features
- Virtual Local Area Networks (VLANs)
- VLAN Configuration
- Router On Stick Design
- Ether-channel Configuration
- Fundamentals of Network Security
- Securing Network Devices

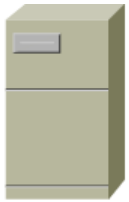
- Port Security Configuration
- Access Control Lists (ACLs)
- Dynamic Host Configuration Protocol (DHCP)
- DHCP Snooping, Dynamic Arp Inspection
- Network Address Translation (NAT)
- IPv6
- SOHO Design
- CDP & LLDP Protocols
- VPN Concepts
- Quality of Service
- NTP

- SNMP
- HSRP
- Router's File Backup
- Concepts of Wireless Networks
- Implementation and Configuration of Access Points
- Concepts of Wireless Security Standards, and Configuration.
- Cloud Concepts.
- Software Defined Networks Principles.
- Description of REST API Structure.
- JavaScript Object Notation Interpretation.
- Network Automation Concepts.
- Ansible and Terraform as Automation Tools
- AI & Machine Learning Overview
- AI & ML for Networking

Cisco Icons and Symbols

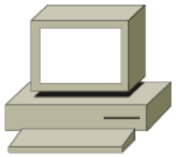
ATM Switch

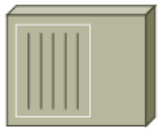
Bridge

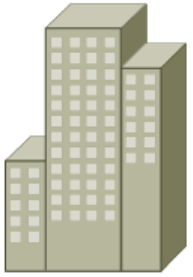

File Server

Network Cloud

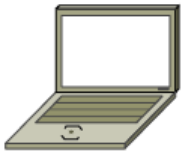
Router

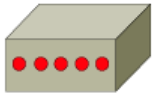

PC


Hub


Building

Switch

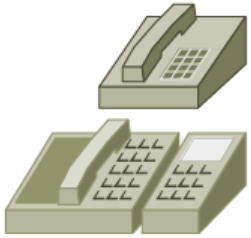

Laptop


Modem

Comm Server

Home Office

ISDN Switch


Phones

Phone Customer

ICND20GR_icons

Data Networks

Sharing data through the use of floppy disks is not an efficient or cost-effective manner.

Businesses needed a solution that would successfully address the following three problems:

- How to avoid duplication of equipment and resources
- How to communicate efficiently
- How to set up and manage a network

Businesses realized that networking technology could increase productivity while saving money.

Networking Devices

Equipment that connects directly to a network segment is referred to as a device.

These devices are broken up into two classifications.

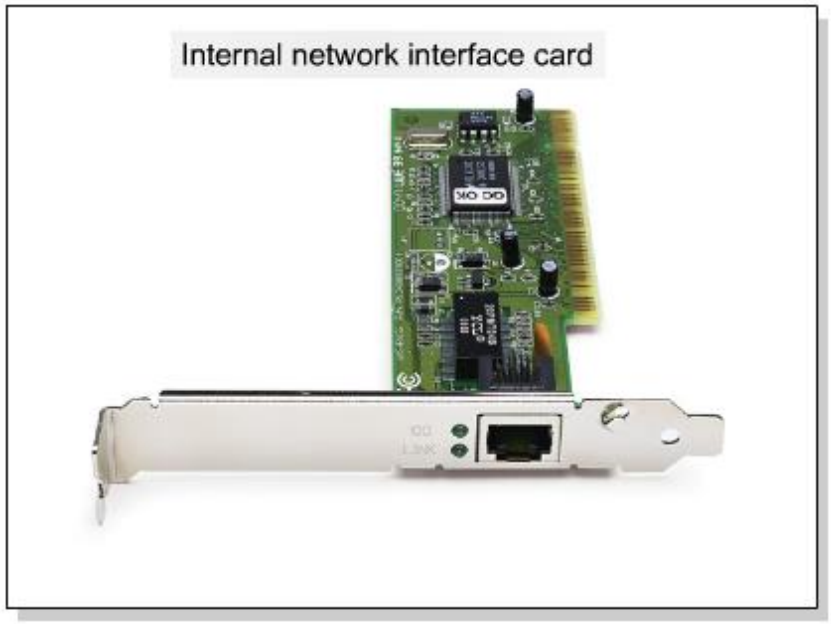
- End-user devices
- Network devices

End-user devices include computers, printers, scanners, and other devices that provide services directly to the user.

Network devices include all the devices that connect the end-user devices together to allow them to communicate.

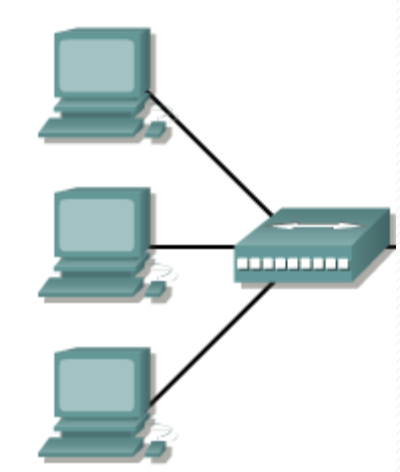
Network Interface Card

A network interface card (NIC) is a printed circuit board that provides network communication capabilities to and from a personal computer. Also called a LAN adapter.



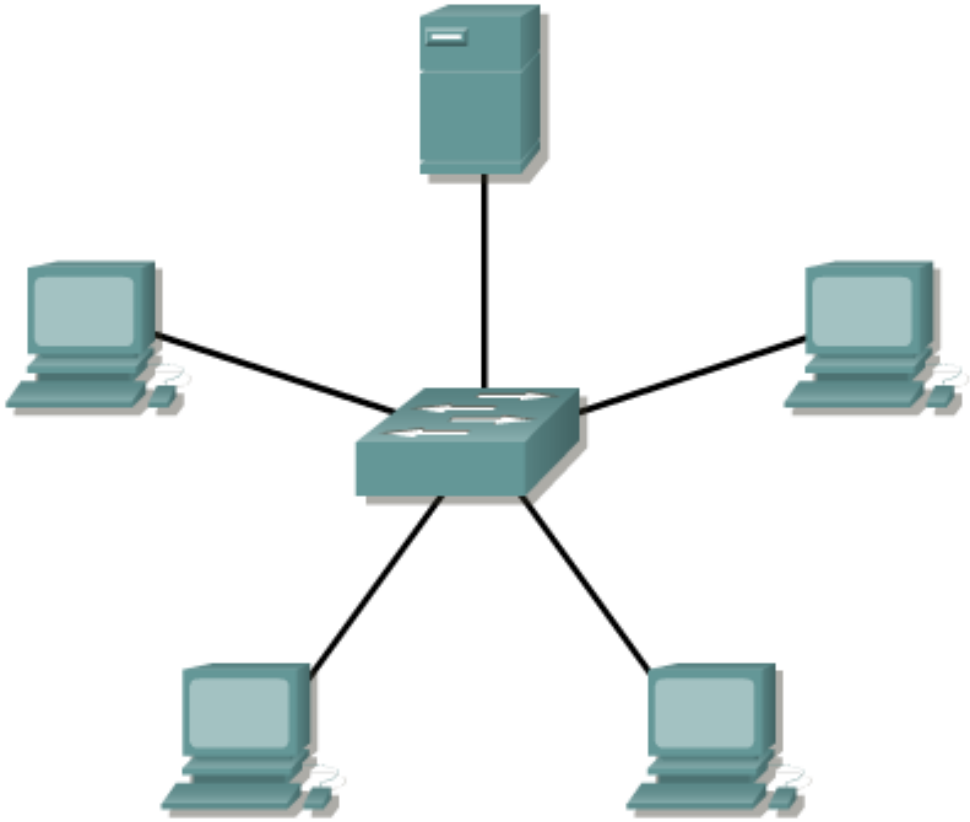
Hub

Connects a group of Hosts



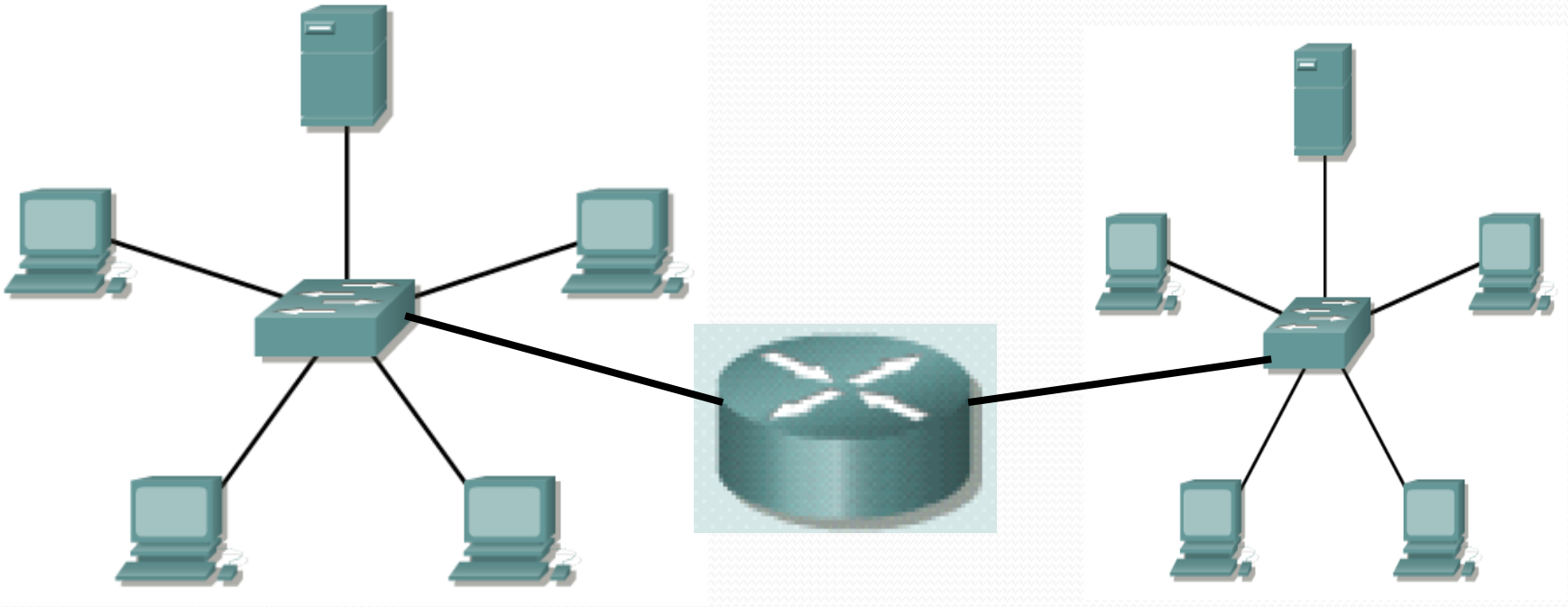
Switch

Switches add more intelligence to data transfer management.



Router

- Routers are used to connect networks together
- Route packets of data from one network to another
- Cisco became the de facto standard of routers because of their high-quality router products
- Routers, by default, break up a *broadcast domain*



Network Addressing Mechanism

- **IP Address:** Is the logical hierarchical address that is used mainly in computer networks addressing, and It is used by Layer3 devices to determine the exit interface.
- **MAC Address:** Is the physical flat address that is used mainly by Switches to determine the exit interface.
- **Name:** Is the address that mainly used for human being to easily remember the websites, however the PCs use the DNS server to translate the name into IP address.

Internetworking Basics

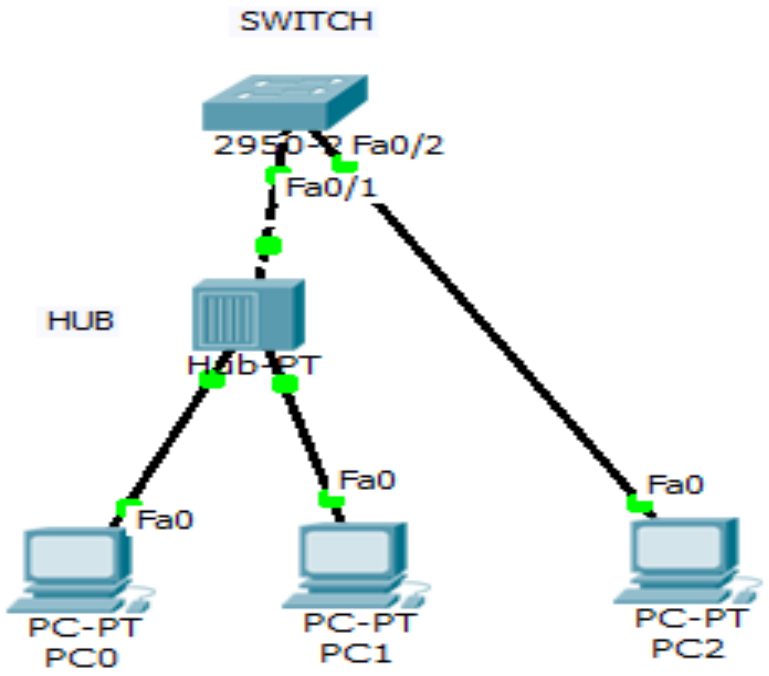
Two Domains:

Collision Domain

- Every Switch port
- The Whole Hub

Broadcast Domain

- Every Router port
- The Whole Switch



Switches can replace the hub, breaking up collision domains.

Switch : Intelligent, Expensive, Configurable, Commonly used
Hub: Dump, Cheap, Dummy, Not used nowadays .

The OSI Model

Why do we need the OSI Model?

- To address the problem of networks increasing in size and in number, the International Organization for Standardization (ISO) researched many network schemes and recognized that there was a need to create a network model

- This would help network builders implement networks that could communicate and work together

- ISO therefore, released the OSI reference model in 1984.

Don’t Get Confused.

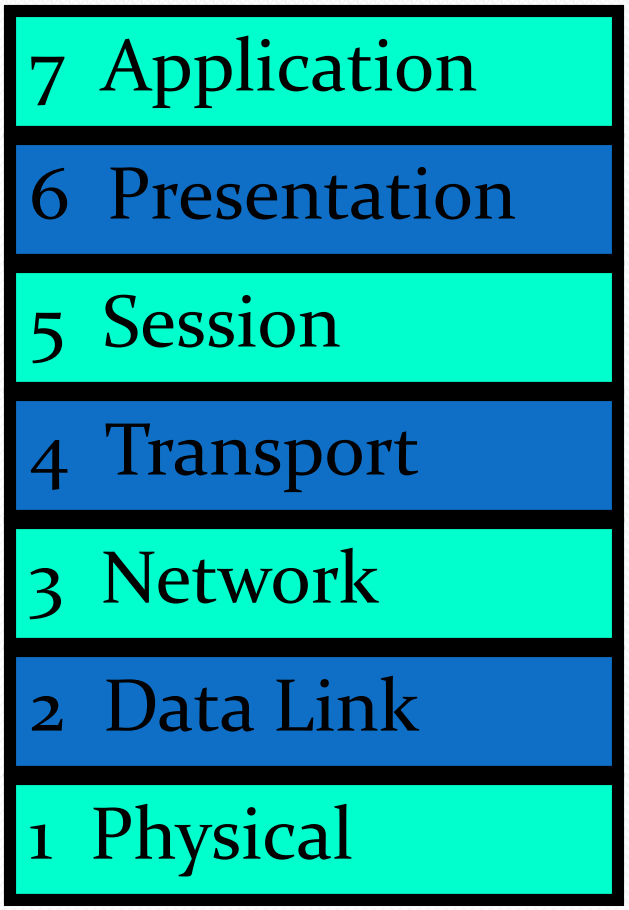
ISO - International Organization for Standardization

OSI - Open System Interconnection

IOS - Internetwork Operating System

To avoid confusion, some people say “International Standard Organization.”

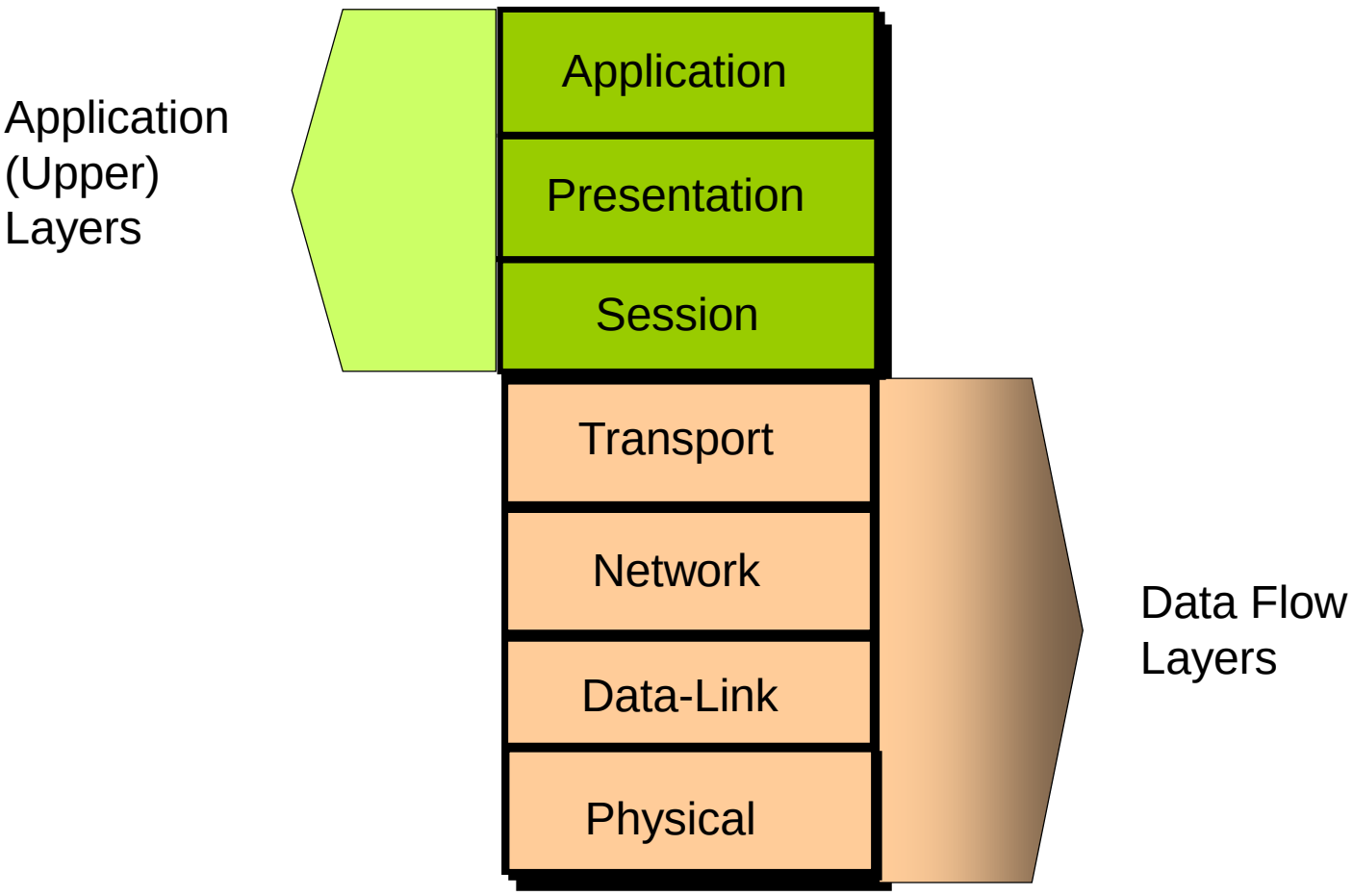
The OSI Reference Model



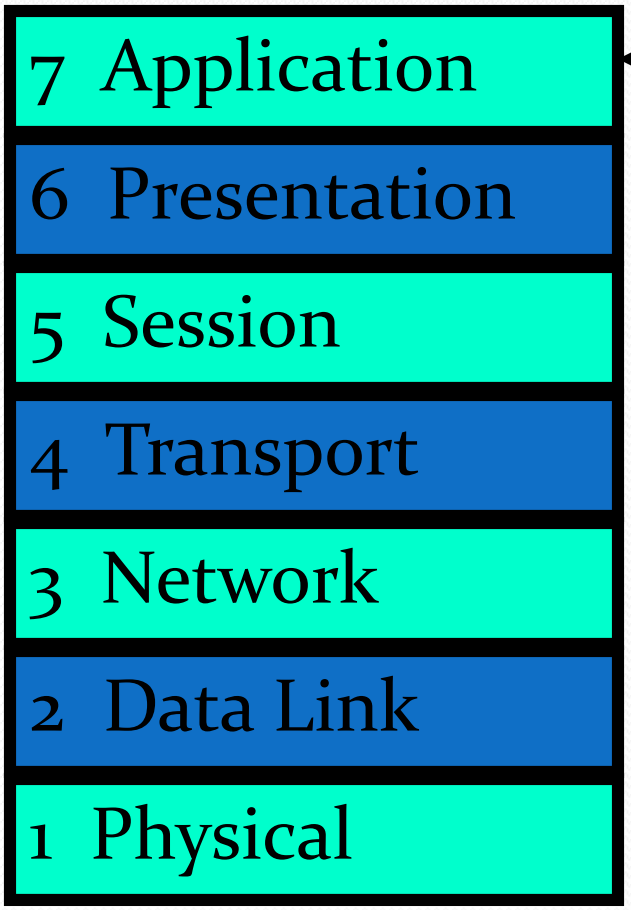
The OSI Model will be used throughout your entire networking career!

Memorize it!

OSI Model


Application
(Upper)
Layers
Application
Presentation
Session
Transport
Network
Data-Link
Physical
Data Flow
Layers

Layer 7 - The Application Layer



This layer deal with networking applications.

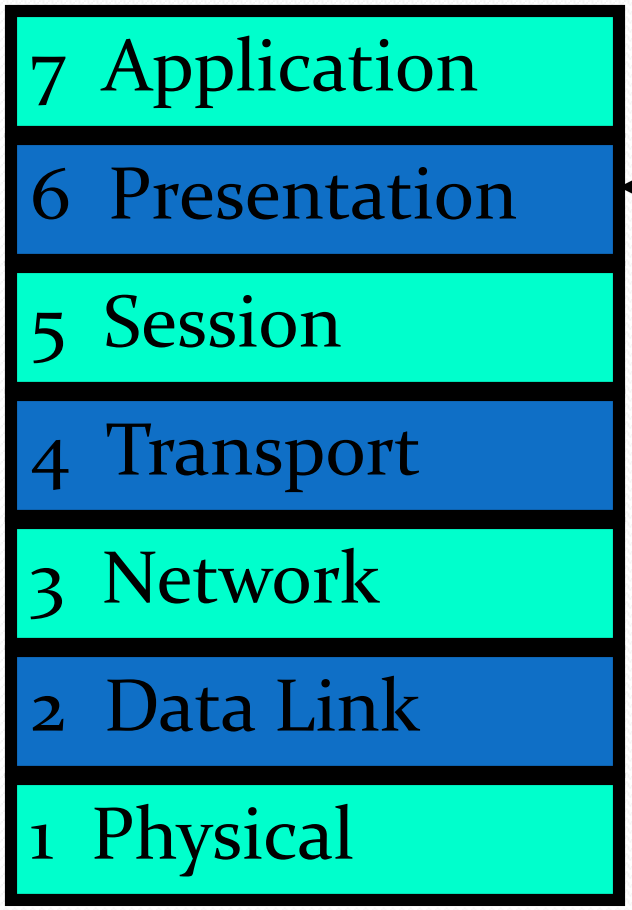
Examples:

- Email
- Web browsers

PDU - User Data

Each of the layers have Protocol Data Unit (PDU)

Layer 6 - The Presentation Layer

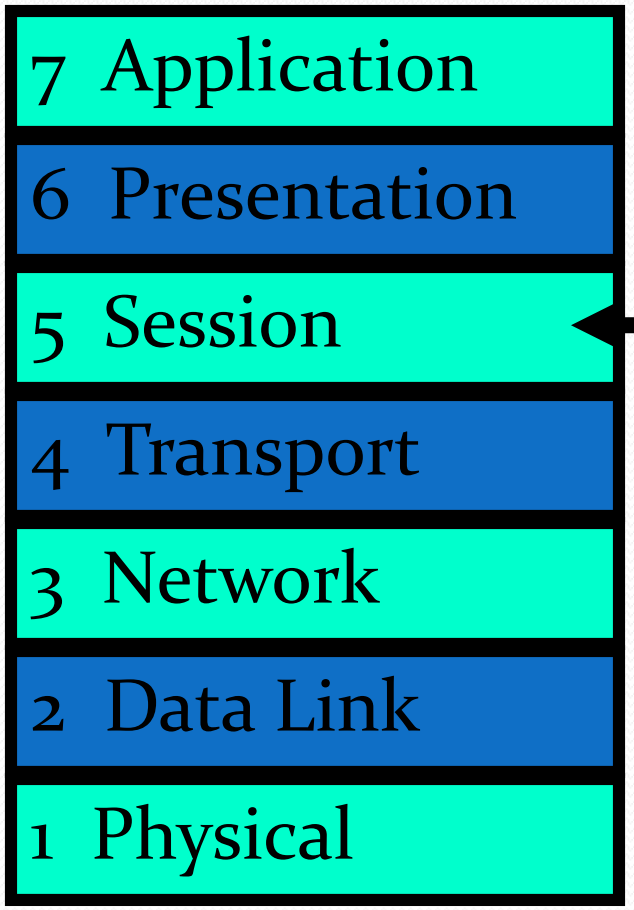


This layer is responsible for presenting the data in the required format which may include:

- Code Formatting
- Encryption
- Compression

PDU - Formatted Data

Layer 5 - The Session Layer



- This layer establishes, manages, and terminates sessions between two communicating hosts.
- Creates Virtual Circuit
- Coordinates communication between systems
- Organize their communication by offering three different modes
  - Simplex
  - Half Duplex
  - Full Duplex

Example:

- Client Software
  (Used for logging in)

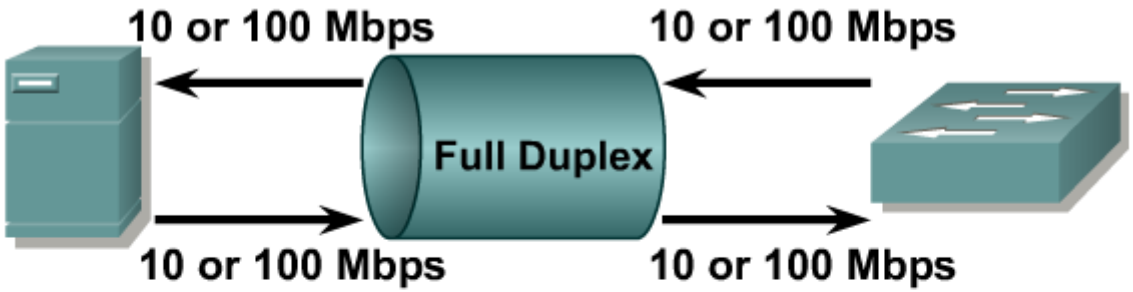
PDU - Formatted Data

Half Duplex

- It uses only one wire pair with a digital signal running in both directions on the wire.
- It also uses the CSMA/CD protocol to help prevent collisions and to permit retransmitting if a collision does occur.
- If a hub is attached to a switch, it must operate in half-duplex mode because the end stations must be able to detect collisions.
- Half-duplex Ethernet—typically 10BaseT—is only about 30 to 40 percent efficient because a large 10BaseT network will usually only give you 3 to 4Mbps—at most.

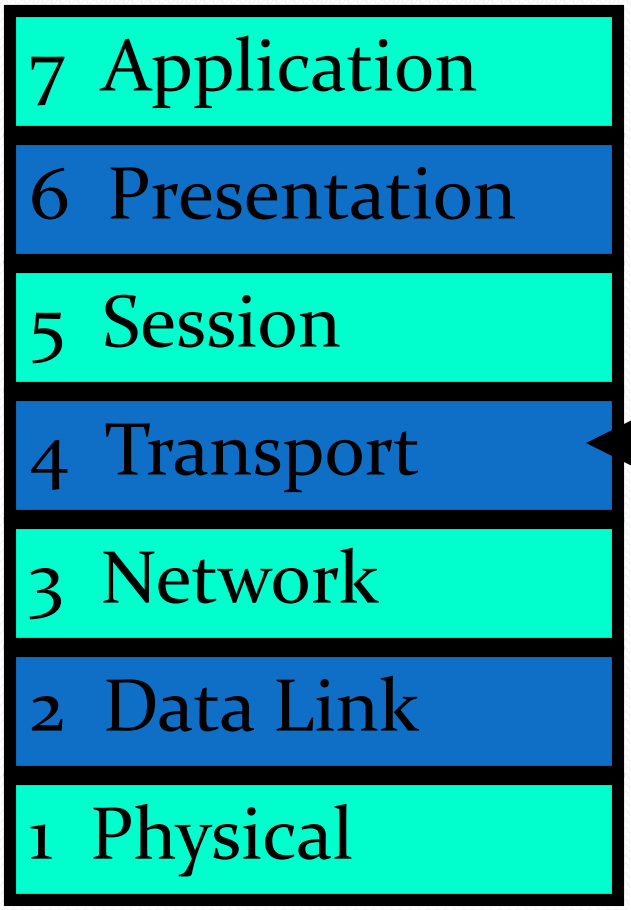
Full Duplex

In a network that uses twisted-pair cabling, one pair is used to carry the transmitted signal from one node to the other node. A separate pair is used for the return or received signal. It is possible for signals to pass through both pairs simultaneously. The capability of communication in both directions at once is known as full duplex.



- Doubles bandwidth between nodes
- Collision-free transmission
- Two 10- or 100- Mbps data paths

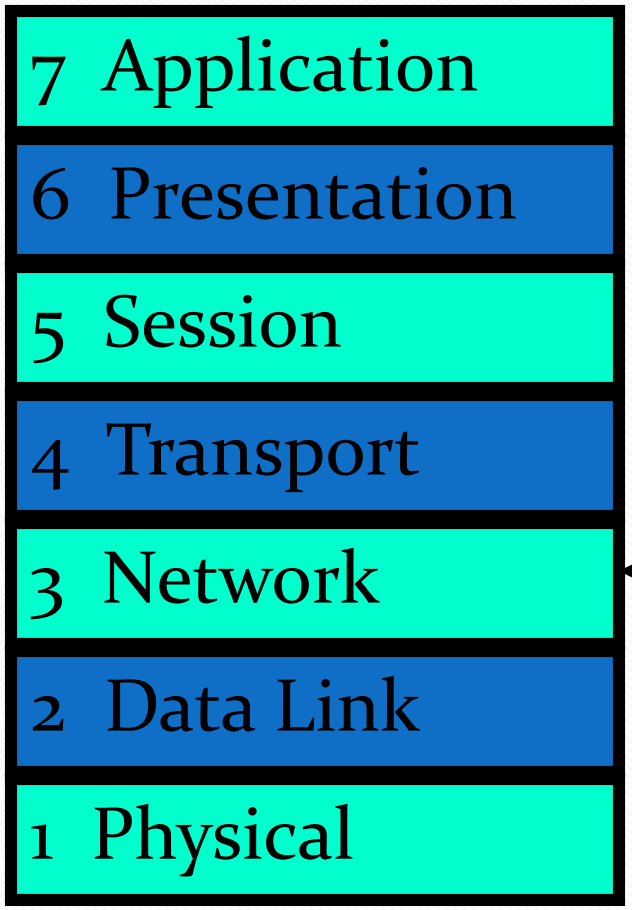
Layer 4 - The Transport Layer



- This layer breaks up the data from the sending host and then reassembles it in the receiver.
- It is also used to ensure reliable data transport across the network.
- Can be reliable or unreliable
- Sequencing
- Acknowledgment
- Retransmission
- Flow Control

PDU - Segments

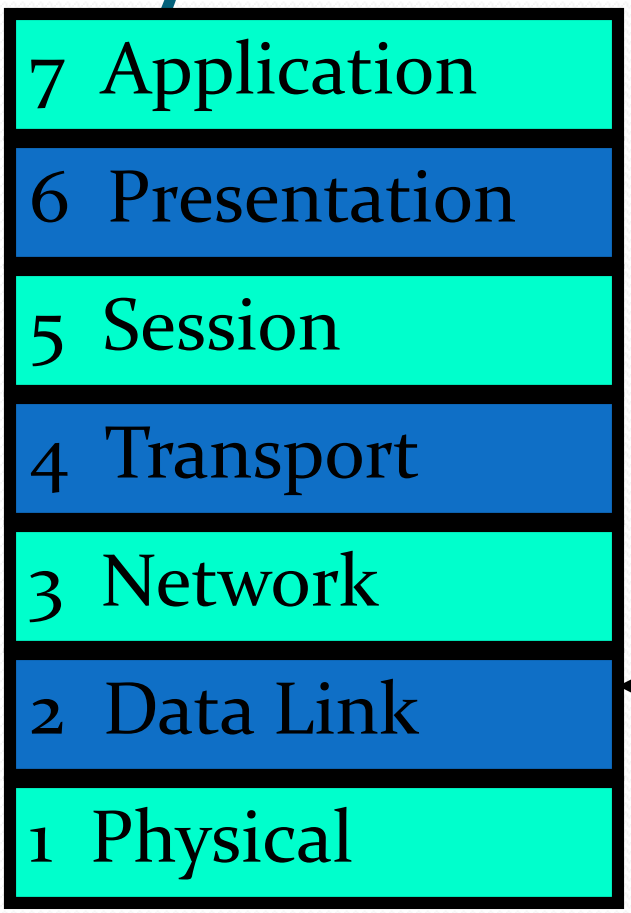
Layer 3 - The Network Layer



- Sometimes referred to as the "Cisco Layer".
- End to End Delivery
- Provide logical addressing that routers use for path determination
- Segments are encapsulated
- Internetwork Communication
- Packet forwarding
- Packet Filtering
- Makes "Best Path Determination"
- Fragmentation

PDU – Packets – IP/IPX

Layer 2 - The Data Link Layer

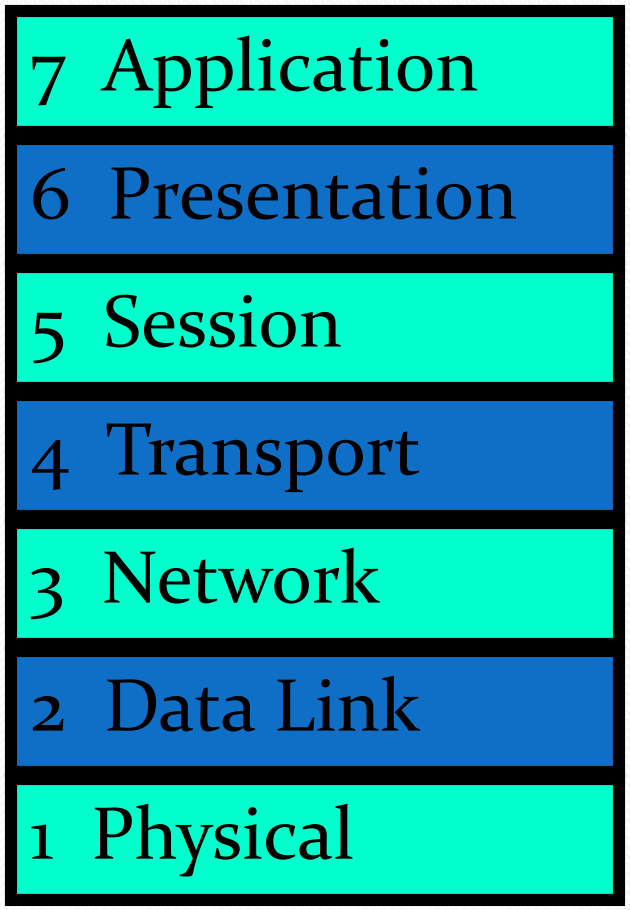


- Performs Physical Addressing
- This layer provides reliable transit of data across a physical link.
- Combines bits into bytes and bytes into frames
- Access to media using MAC address
- Error detection, not correction
- LLC and MAC
- Logical Link Control performs Link establishment
- MAC Performs Access method

PDU - Frames

Preamble	DMAC	SMAC	Data length	DATA	FCS

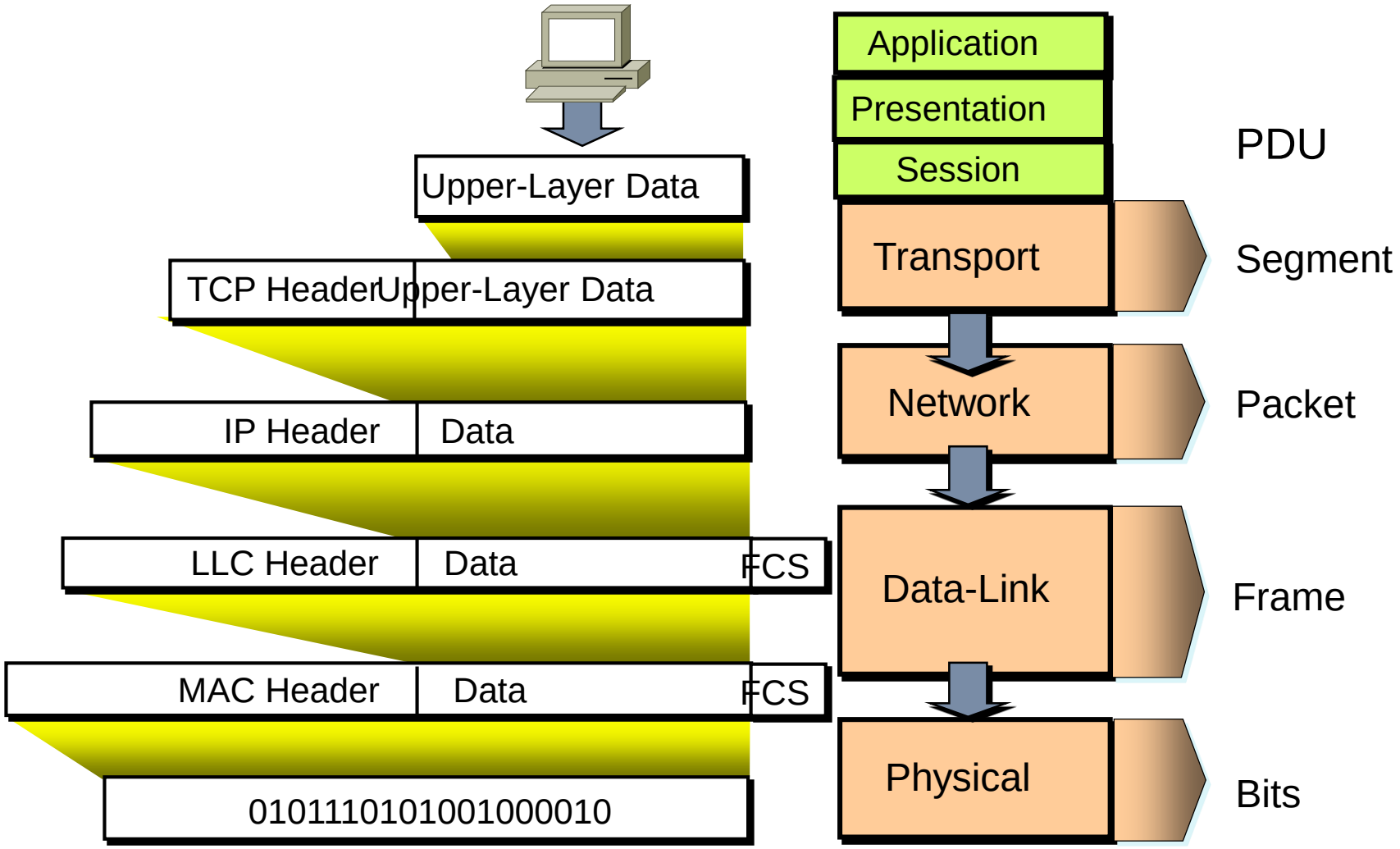
Layer 1 - The Physical Layer



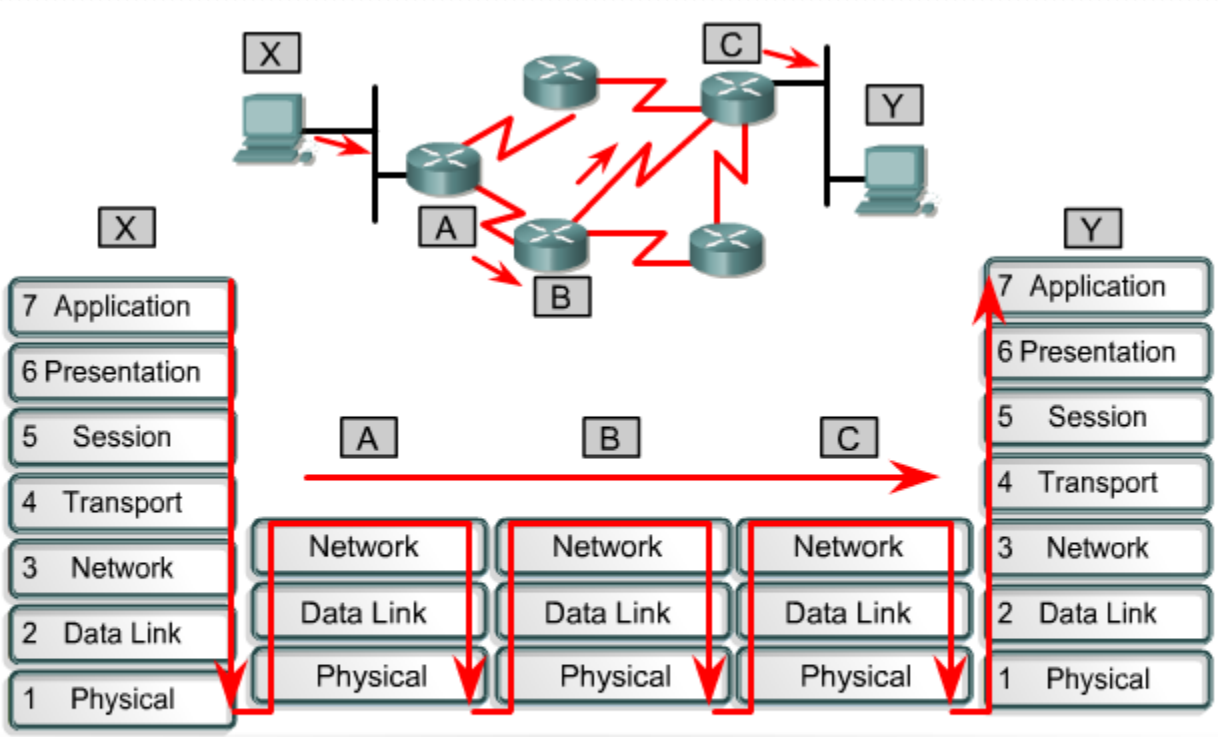
- This is the physical media through which the data, represented as electronic signals, is sent from the source host to the destination host.
- Move bits between devices
- Encoding

PDU - Bits

Data Encapsulation

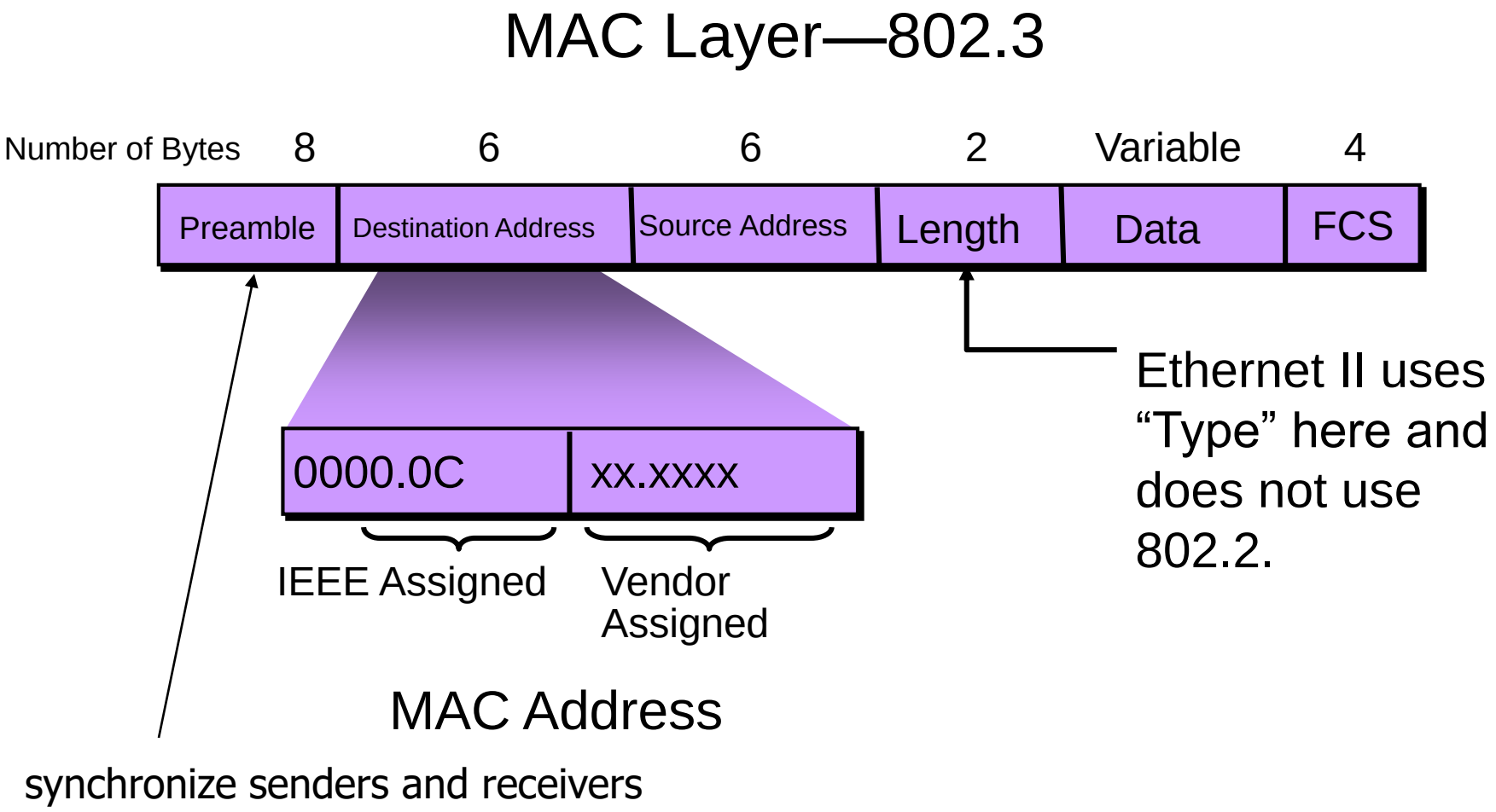


Data Flow Through a Network



Data flow in a network focuses on layers one, two and three of the OSI model. This is after being transmitted by the sending host and before arriving at the receiving host.

Layer 2

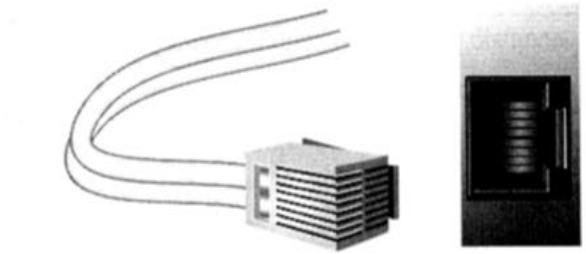

MAC Layer—802.3
Number of Bytes
8
6
6
2
Variable
4
Preamble
Destination Address
Source Address
Length
Data
FCS
0000.0C
xx.xxxx
IEEE Assigned
Vendor Assigned
MAC Address
Ethernet II uses "Type" here and does not use 802.2.
synchronize senders and receivers

The Networking Media

10 Mbps IEEE Standards - 10BaseT

- 10BaseT $\Rightarrow$ 10 Mbps, baseband, over Twisted-pair cable
- Running Ethernet over twisted-pair wiring as specified by IEEE 802.3
- Configure in a star pattern
- Twisting the wires reduces EMI
- Fiber Optic has no EMI

Unshielded twisted-pair



RJ-45 Plug and Socket

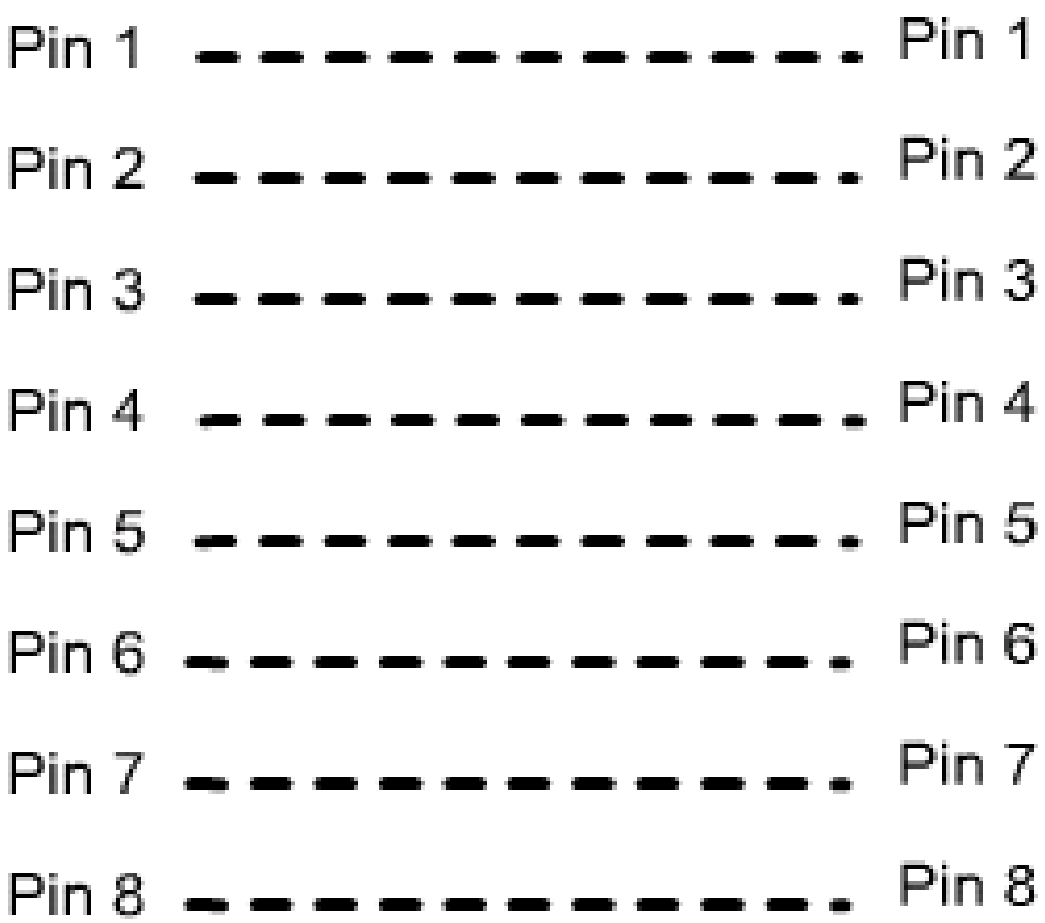
Twisted Pair Cables

- Unshielded Twisted Pair Cable (UTP)
  - most popular
  - maximum length 100 m
  - prone to noise

Category 1	Voice transmission of traditional telephone
Category 2	For data up to 4 Mbps, 4 pairs full-duplex
Category 3	For data up to 10 Mbps, 4 pairs full-duplex
Category 4	For data up to 16 Mbps, 4 pairs full-duplex
Category 5	For data up to 100 Mbps, 4 pairs full-duplex
Category 6	For data up to 1000 Mbps, 4 pairs full-duplex

Straight-through cable

Straight-through cable pinout

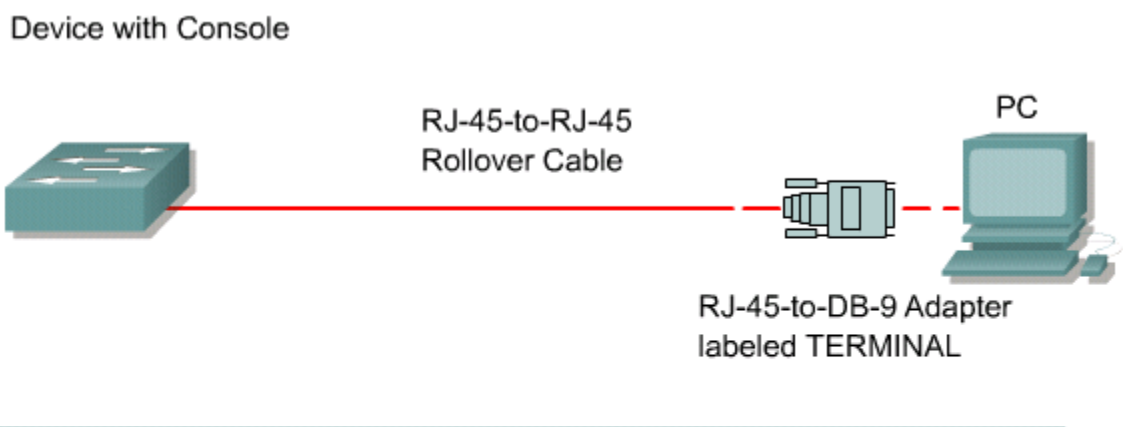


Crossover cable

Crossover cable

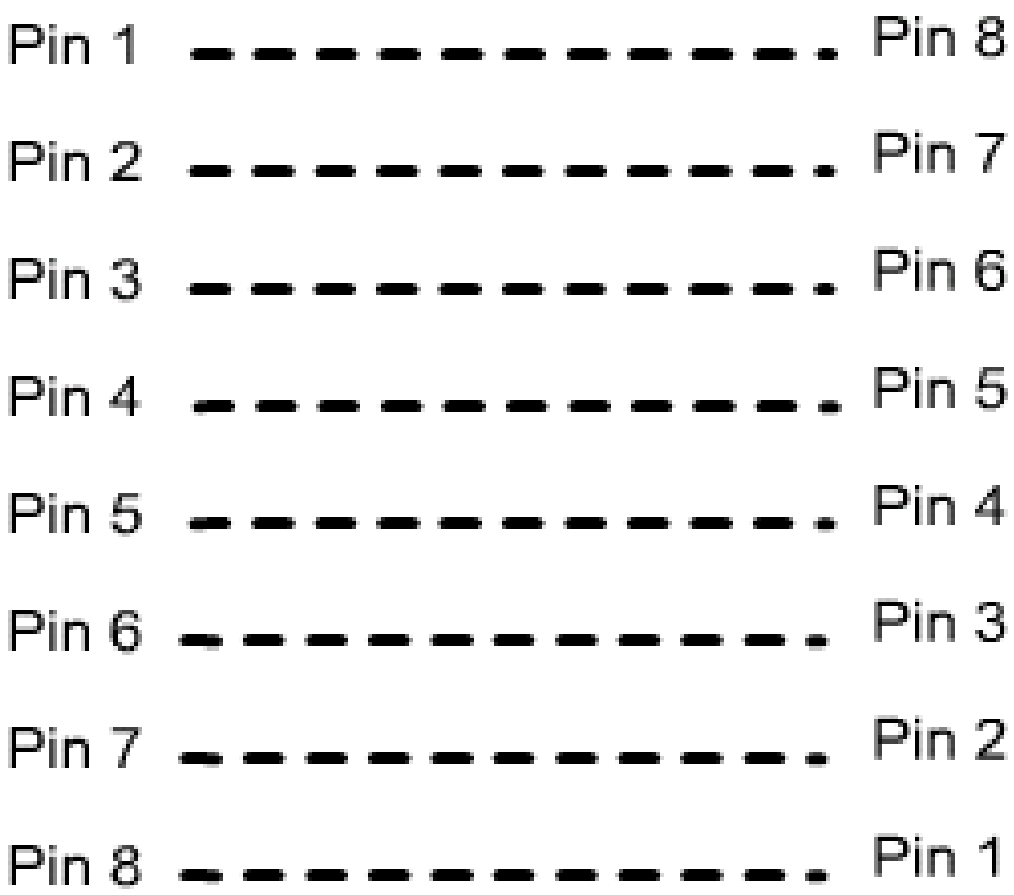
From	To
1	3
2	6
3	1
4	none
5	none
6	2
7	none
8	none

Rollover cable



- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

Rollover cable pinout

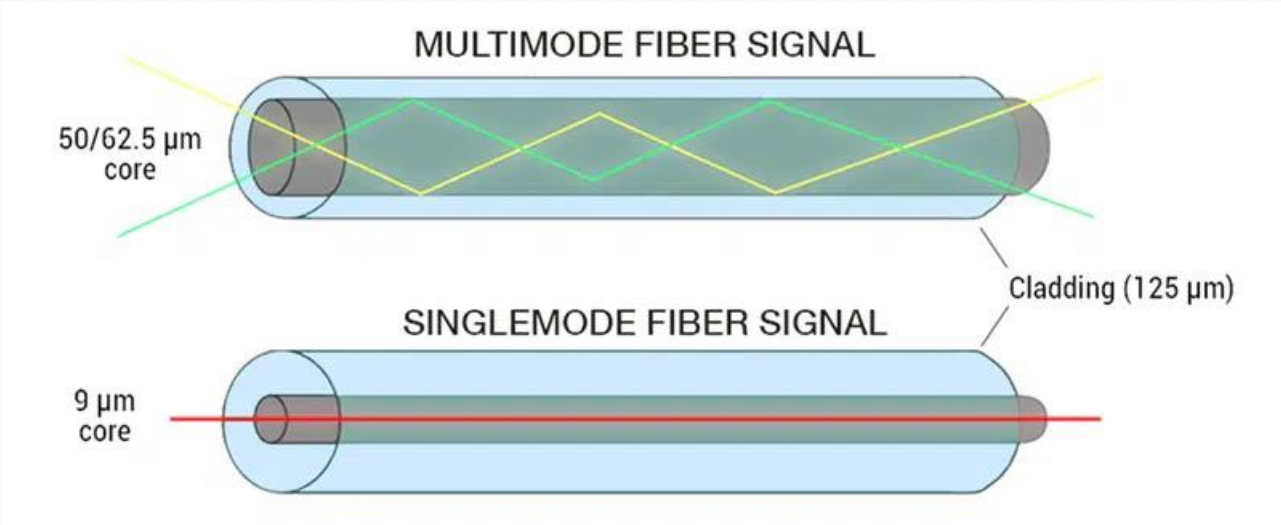


Straight-Thru or Crossover

- Use straight-through cables for the following cabling:
  - Switch to router
  - Switch to PC or server
  - Hub to PC or server
- Use crossover cables for the following cabling:
  - Switch to switch
  - Switch to hub
  - Hub to hub
  - Router to router
  - PC to PC
  - Router to PC

Single and Multimode Fiber

- Single-mode and multimode fiber optic cables are two types of optical fibers used in networking, and they differ in several key aspects, including core size, light propagation, distance, and application



Differences Between Single and Multimode Fiber

1. Core Size
Single-mode Fiber: 8-10 microns
Multimode Fiber: 50 or 62.5 microns

2. Light Propagation
Single-mode Fiber: Light travels in a straight path (single mode).
Multimode Fiber:Light travels in multiple paths (modes).

3. Distance and Bandwidth
Single-mode Fiber: Supports much longer distances (up to 40 km or more with the right equipment).
Higher bandwidth capacity, making it suitable for high-speed applications.

Multimode Fiber: Supports shorter distances (typically up to 500 meters for 10 Gbps).
Lower bandwidth compared to single-mode fiber.

4. Light Source

Single-mode Fiber: Uses a laser as a light source, which is more precise and expensive.

Multimode Fiber:Uses an LED or VCSEL (Vertical Cavity Surface Emitting Laser) as a light source, which is less expensive.

5. Cost

Single-mode Fiber: High Cost

Multimode Fiber: Lower Cost

6. Applications

Single-mode Fiber:

Used in long-distance telecommunication, metropolitan networks, and data centers.

Multimode Fiber:

Used in short-distance communication, such as in LANs, data centers, and campus networks.

Fiber SFP

- In fiber optics, SFP stands for Small Form-factor Pluggable. It is a compact, hot-swappable transceiver used in networking to connect network devices like switches, routers, or servers to a fiber-optic or copper networking cable

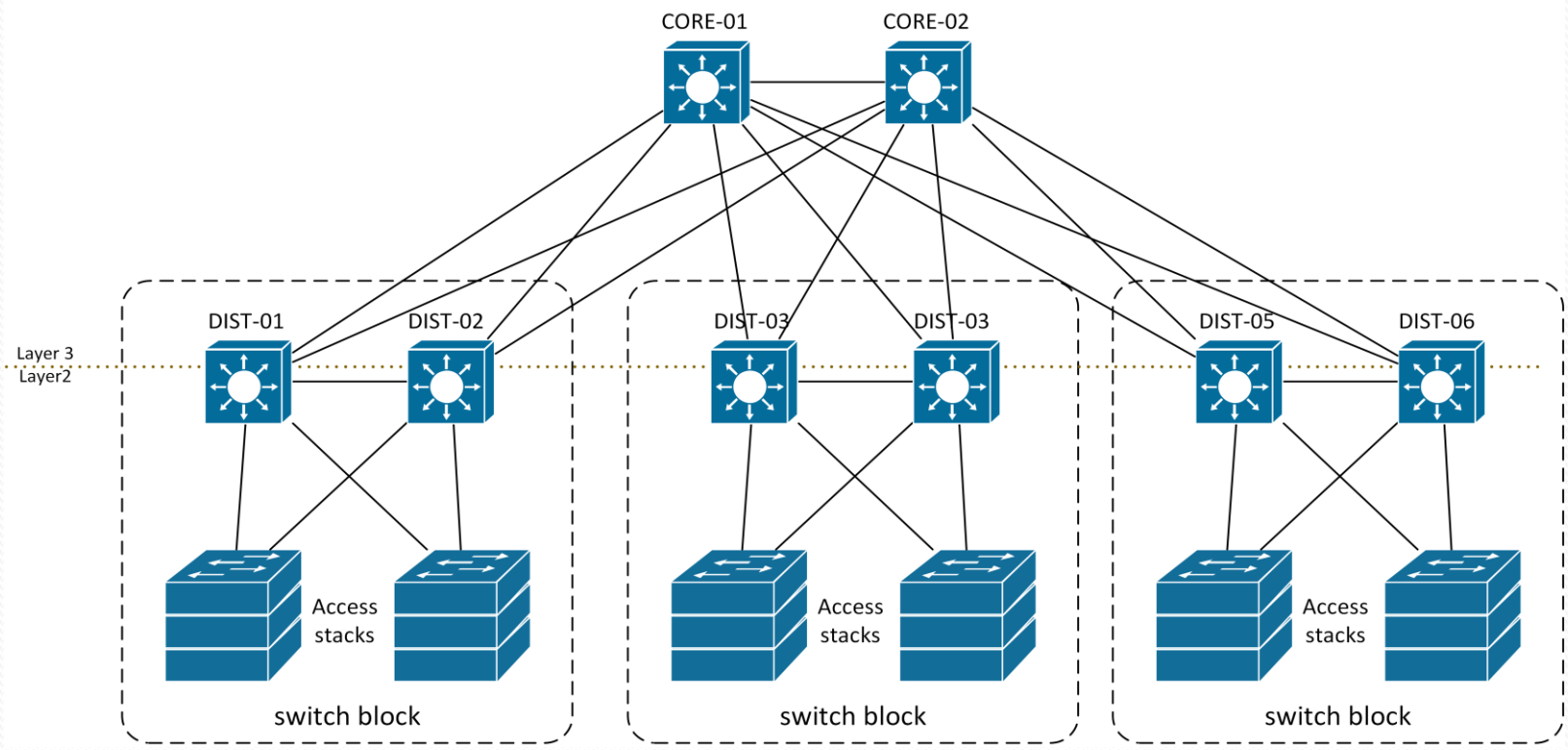
Varinats of SFP Modules

- SFP (Standard): Supports speeds up to 1 Gbps.
- SFP+: Supports speeds up to 10 Gbps.
- SPF28: Supports up to 25 Gbps
- QSFP (Quad SFP): Supports higher speeds like 40 Gbps or 100 Gbps by combining multiple channels.

Traditional Three-Tier Architecture

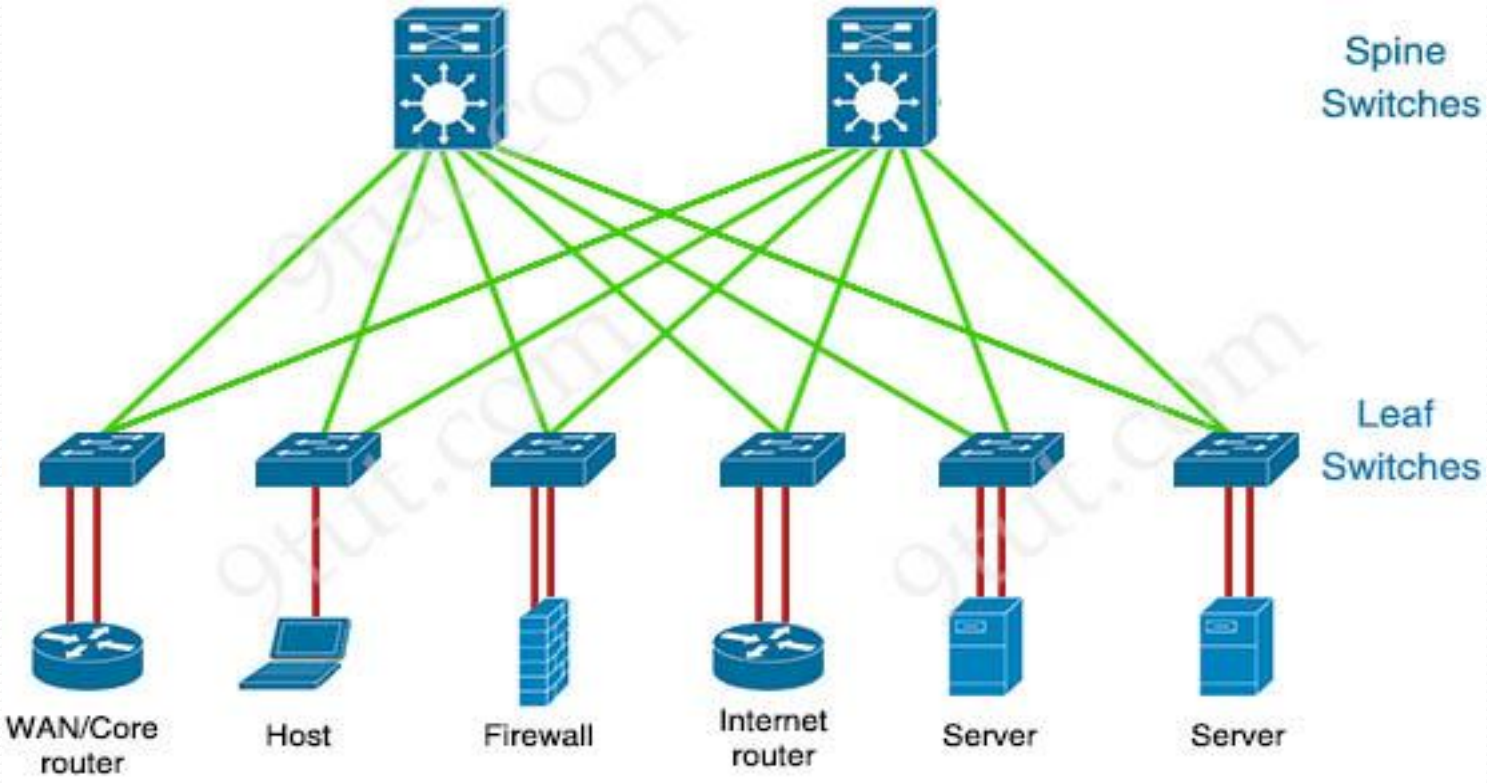
The following are the three layers and their typical functions:

- The core layer: backbone
- The distribution layer: routing
- The access layer: switching



Spine-Leaf Architecture

- Spine-leaf architecture is a modern network topology widely used in data centers and cloud environments



Components of Spine-Leaf Architecture

- **Spine Switches:** These are high-speed switches that form the backbone of the architecture.
- **Leaf Switches**: Leaf switches connect directly to the endpoints (servers, storage devices, routers…) and to every spine switch.

Rules of Spine-Leaf Communication

- Each leaf switch must connect to every spine switch.
- Each spine switch must connect to every leaf switch.
- Leaf switches cannot connect to each other.
- Spine switches cannot connect to each other.
- Endpoints connect only to the leaf switches

Spine-Leaf Traffic Flows

- **East-West Traffic:** When a server connected to one leaf switch needs to communicate with a server connected to another leaf switch, traffic flows up to a spine switch and then down to the destination leaf switch.

- **North-South Traffic:** When a server needs to communicate with an external network (internet or WAN), the traffic typically flows through the leaf switches, which connect to the spine switches, and then to a gateway router.

Key Advantages of Spine-Leaf Design

- **Scalability:** Since each leaf switch connects to every spine switch, adding more leaf switches (and thus more endpoints) doesn't affect the performance. More spine switches can be added to increase bandwidth and support higher loads.

- **Predictable Latency:** The architecture is non-blocking, meaning that every packet between any two endpoints takes the same number of hops (usually two hops: from leaf to spine, and back to leaf), so latency is lower and predictable

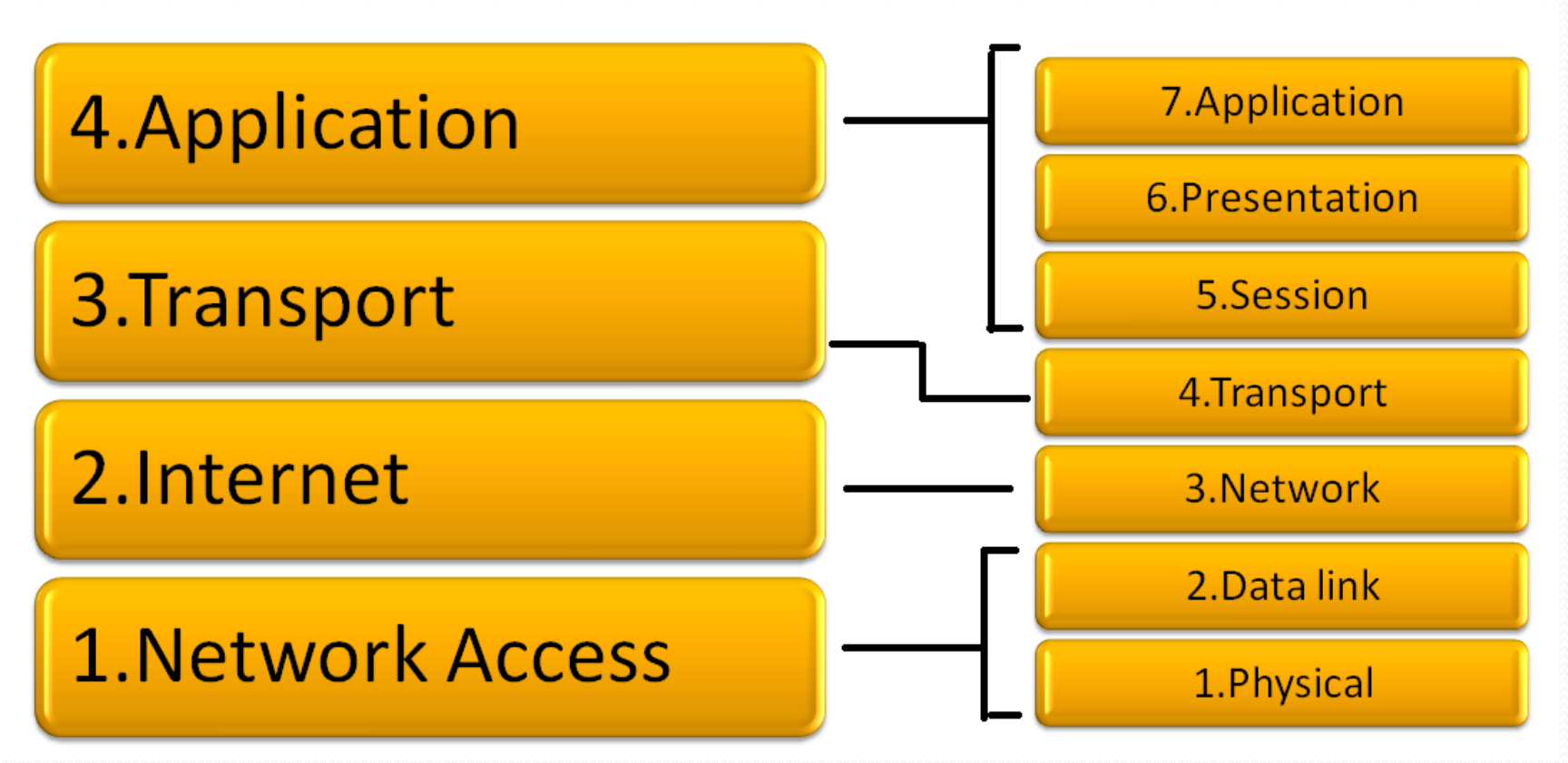
- **High Availability:** The full mesh connectivity between leaf and spine ensures redundancy. If one spine switch fails, traffic can still be routed through other spine switches.

- **Efficient Use of Bandwidth:** The architecture uses Layer 3 routing such as equal-cost multipath (ECMP) routing so STP is no longer required, allowing multiple paths for traffic to be used simultaneously, balancing the load and preventing bottlenecks

Introduction to TCP/IP

TCP/IP and the DoD Model

The figure shows a comparison of the DoD model and the OSI reference model. As you can see, the two are similar in concept, but each has a different number of layers with different names.



Transport Layer

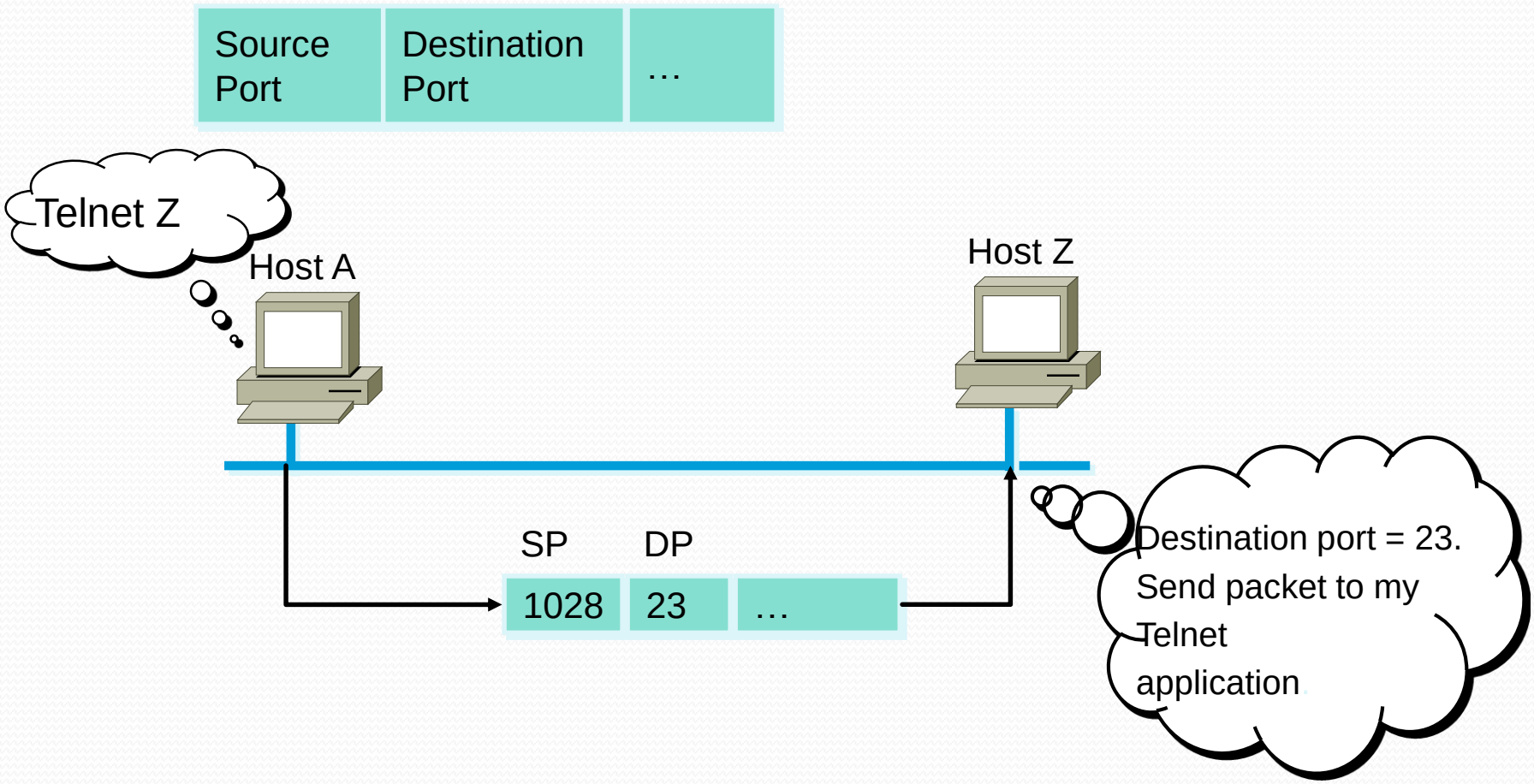
The main purpose of the Host-to-Host layer is to shield the upper layer applications from the complexities of the network.

"Just give me your data stream, with any instructions, and I'll begin the process of getting your information ready to send."

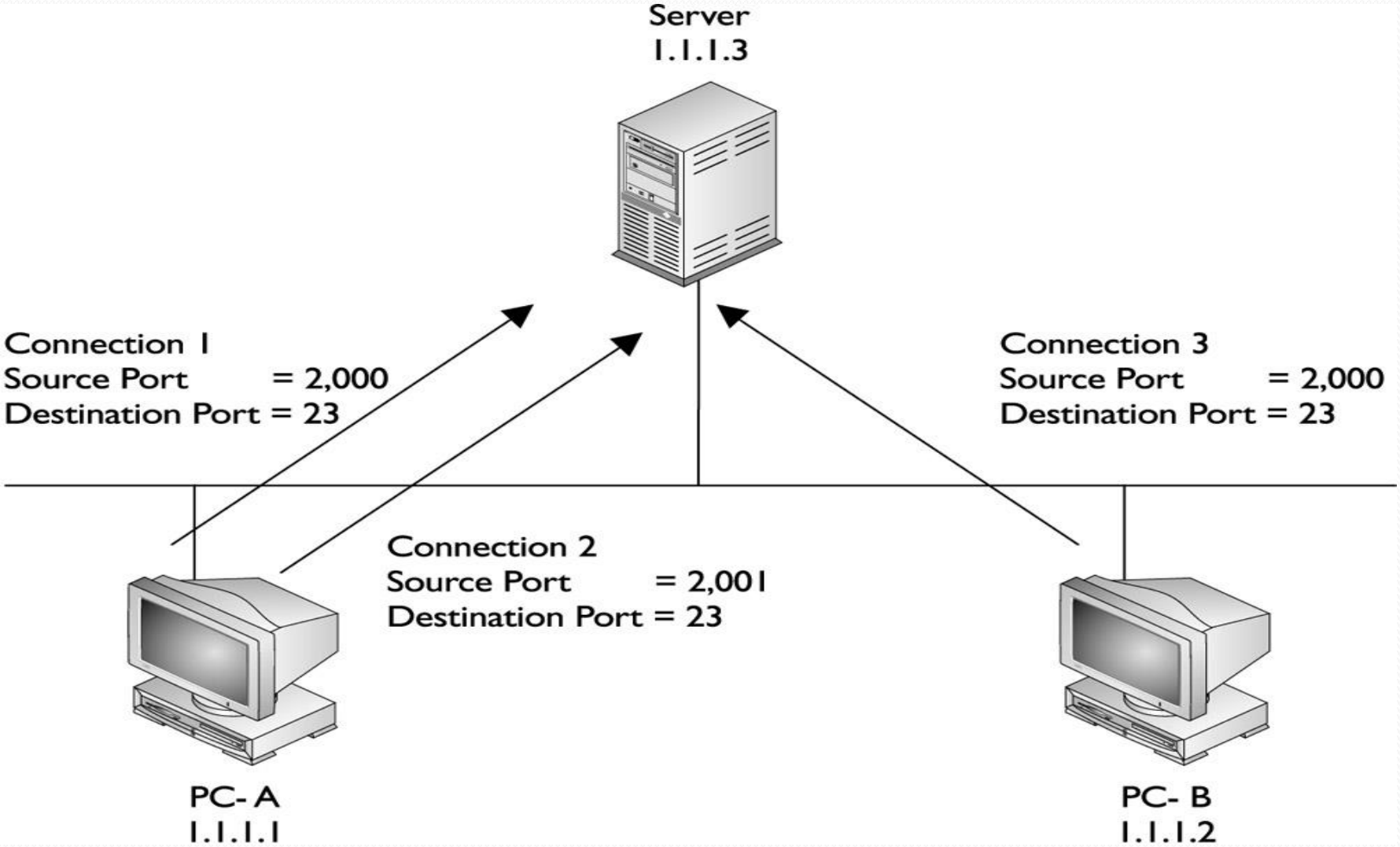
Two protocols at this layer:

- **Transmission Control Protocol (TCP)**
- **User Datagram Protocol (UDP)**

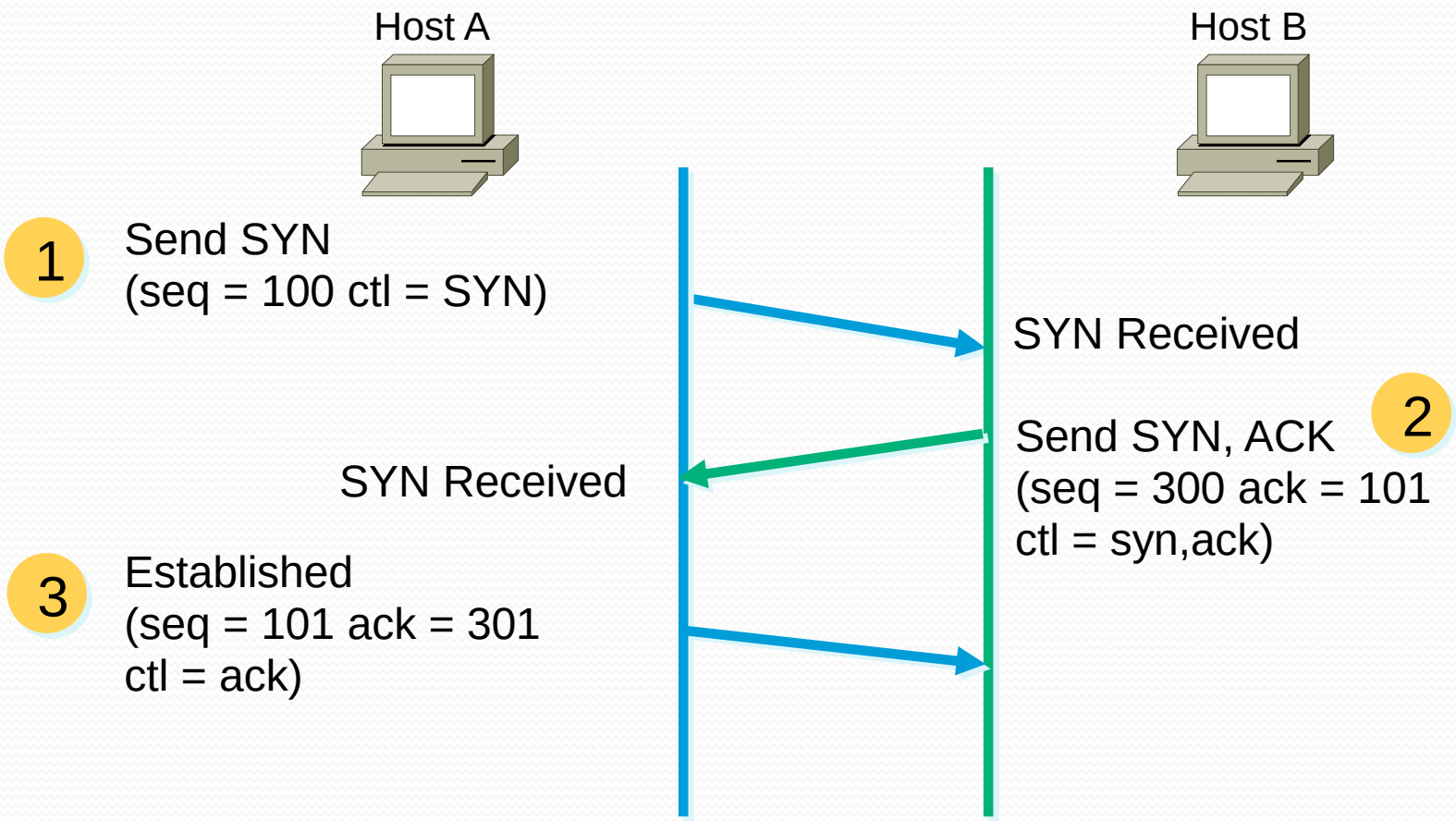
TCP Port Numbers



TCP Port Numbers



TCP Three-Way Handshake/Open Connection



User Datagram Protocol (UDP)

User Datagram Protocol (UDP) is the connectionless transport protocol in the TCP/IP protocol stack.

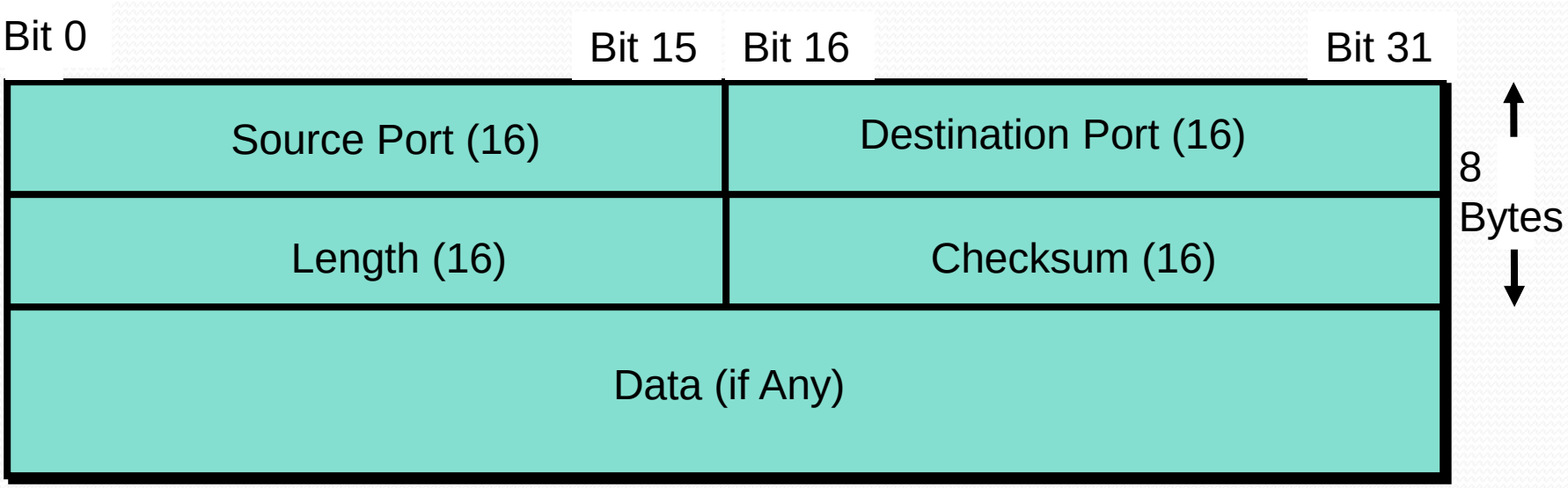
UDP is a simple protocol that exchanges datagrams, without acknowledgments or guaranteed delivery. Error processing and retransmission must be handled by higher layer protocols.

UDP is designed for applications that do not need to put sequences of segments together.

The protocols that use UDP include:

- TFTP (Trivial File Transfer Protocol)
- SNMP (Simple Network Management Protocol)
- DHCP (Dynamic Host Control Protocol)
- DNS (Domain Name System)

UDP Segment Format

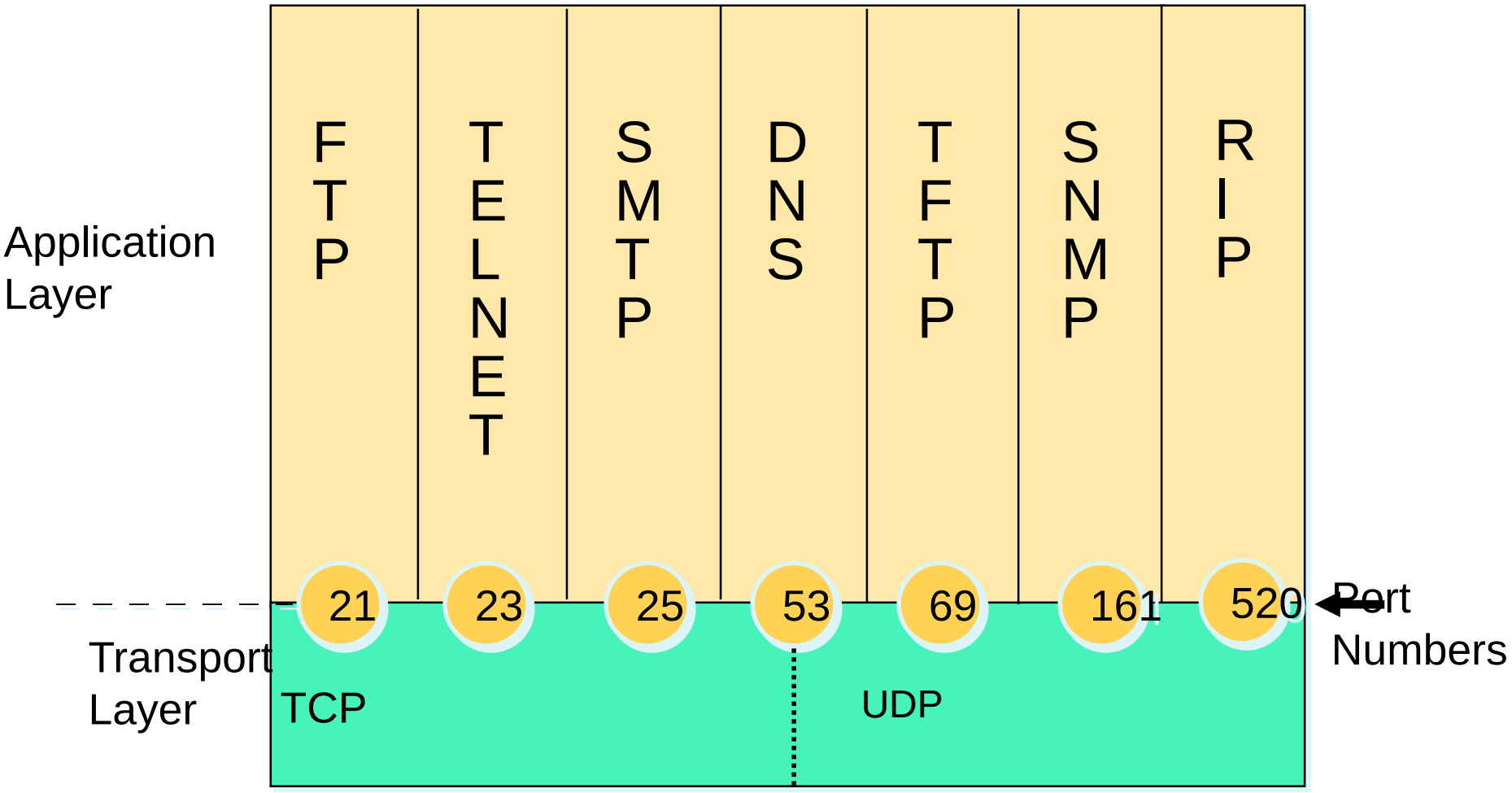


- No sequence or acknowledgment fields

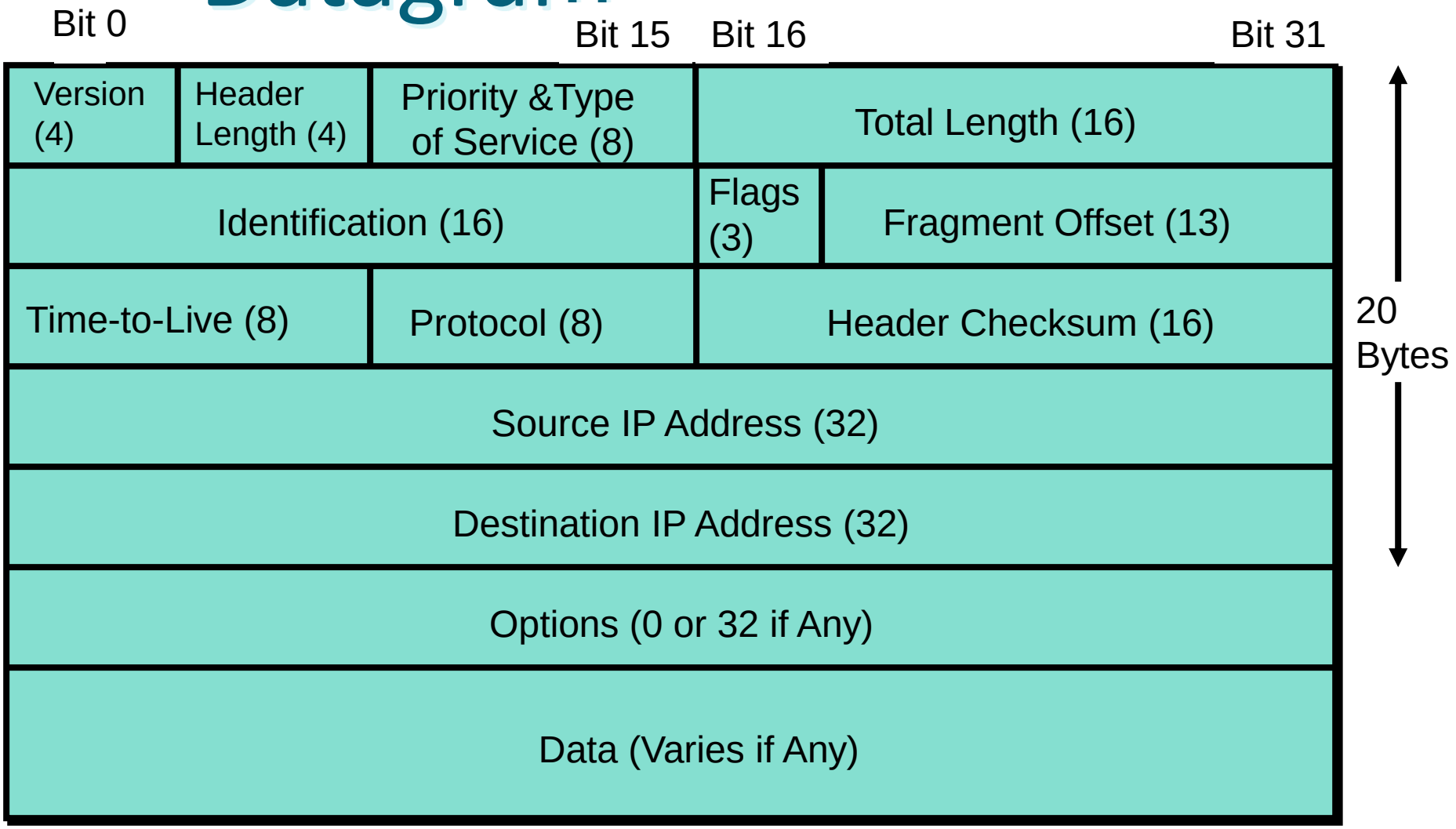
TCP VS UDP

TCP	UDP
Sequenced	Un sequenced
Reliable	Unreliable
Connection-Oriented	Connectionless
Virtual Circuit	Low Overhead
Acknowledgement	No Acknowledgement
Windowing Flow Control	No Windowing or Flow Control

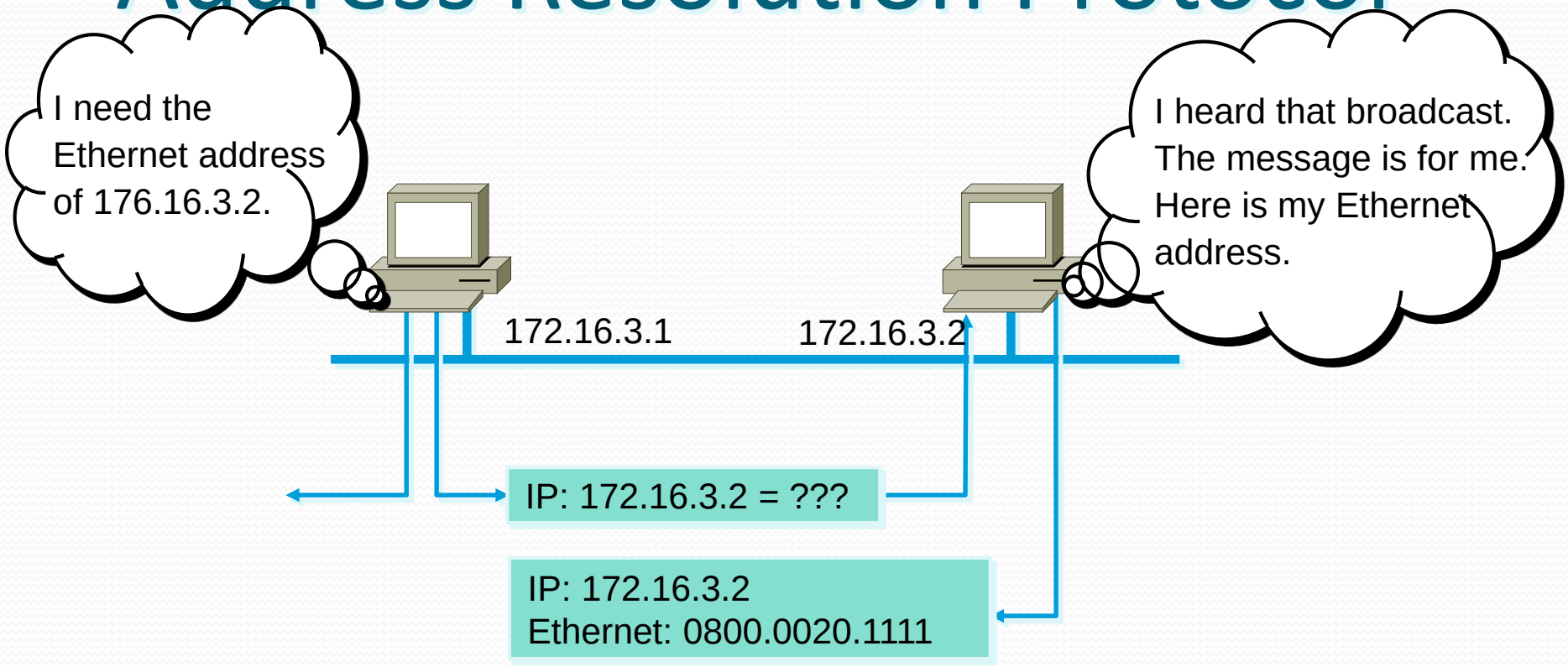
Port Numbers



IP Datagram

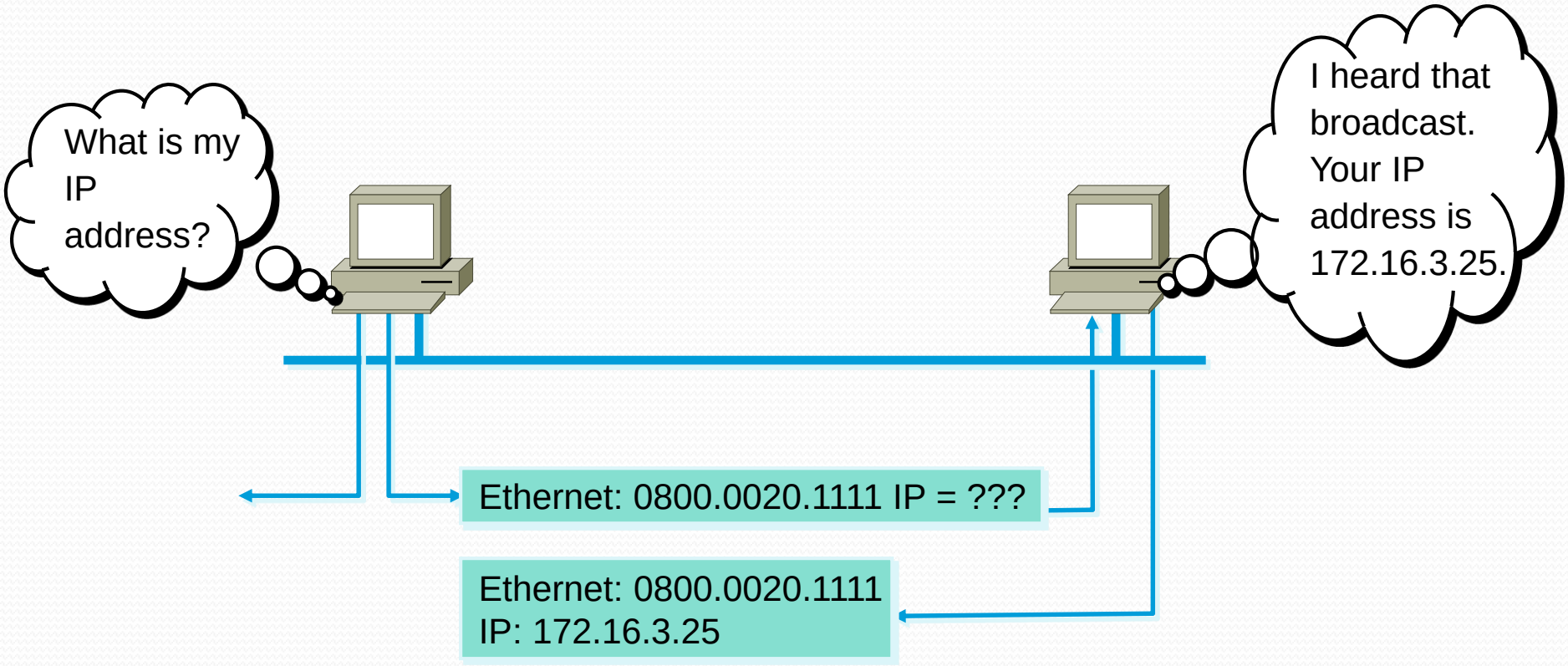

Bit 0
Bit 15
Bit 16
Bit 31
Version (4)
Header Length (4)
Priority &Type of Service (8)
Total Length (16)
Identification (16)
Flags (3)
Fragment Offset (13)
Time-to-Live (8)
Protocol (8)
Header Checksum (16)
Source IP Address (32)
Destination IP Address (32)
Options (0 or 32 if Any)
Data (Varies if Any)
20 Bytes

Address Resolution Protocol



- Map IP ⟶ MAC
- Local ARP

Reverse ARP

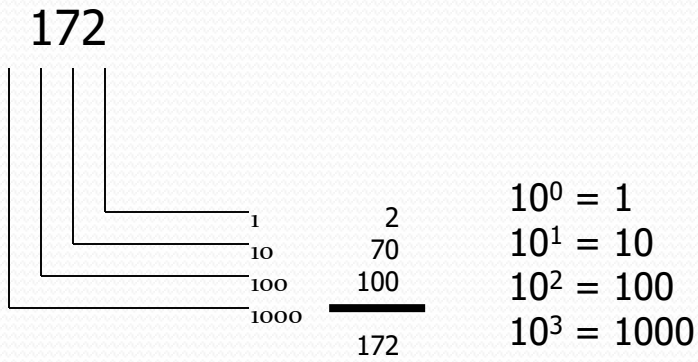


- Map MAC → IP

TCP/IP Math

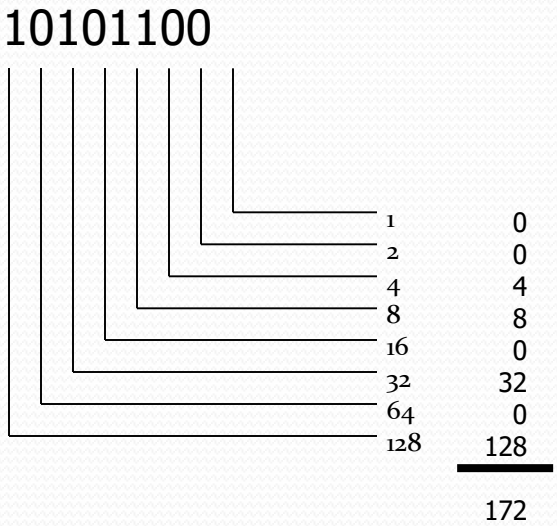
Decimal to Binary

172 – Base 10



$10^0 = 1$
$10^1 = 10$
$10^2 = 100$
$10^3 = 1000$

10101100– Base 2



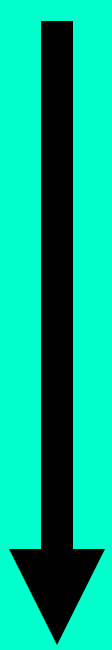
$2^0 = 1$
$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$

Base 2 Number System

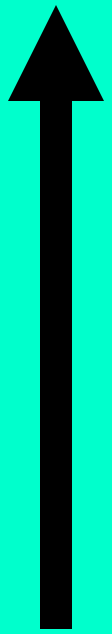
$$10110_2 = (1 \times 2^4 = 16) + (0 \times 2^3 = 0) + (1 \times 2^2 = 4) + (1 \times 2^1 = 2) + (0 \times 2^0 = 0) = 22$$

Converting Decimal to Binary

Convert 201_{10} to binary:



201 / 2 = 100 remainder 1
100 / 2 = 50 remainder 0
50 / 2 = 25 remainder 0
25 / 2 = 12 remainder 1
12 / 2 = 6 remainder 0
6 / 2 = 3 remainder 0
3 / 2 = 1 remainder 1
1 / 2 = 0 remainder 1

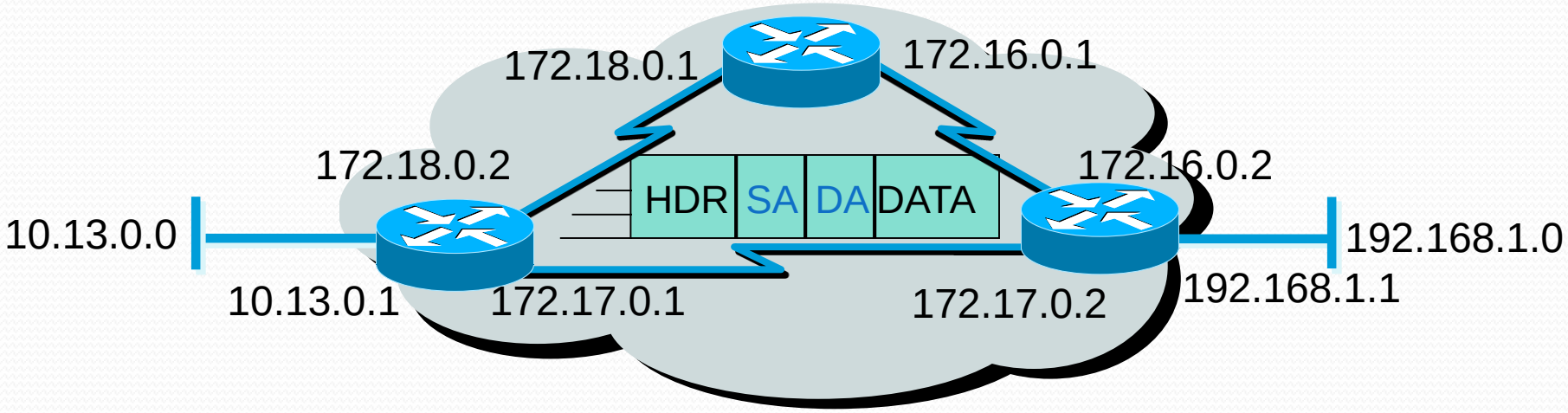


When the quotient is 0, take all the remainders in reverse order for your answer: $201_{10} = 11001001_2$

Binary to Decimal Chart

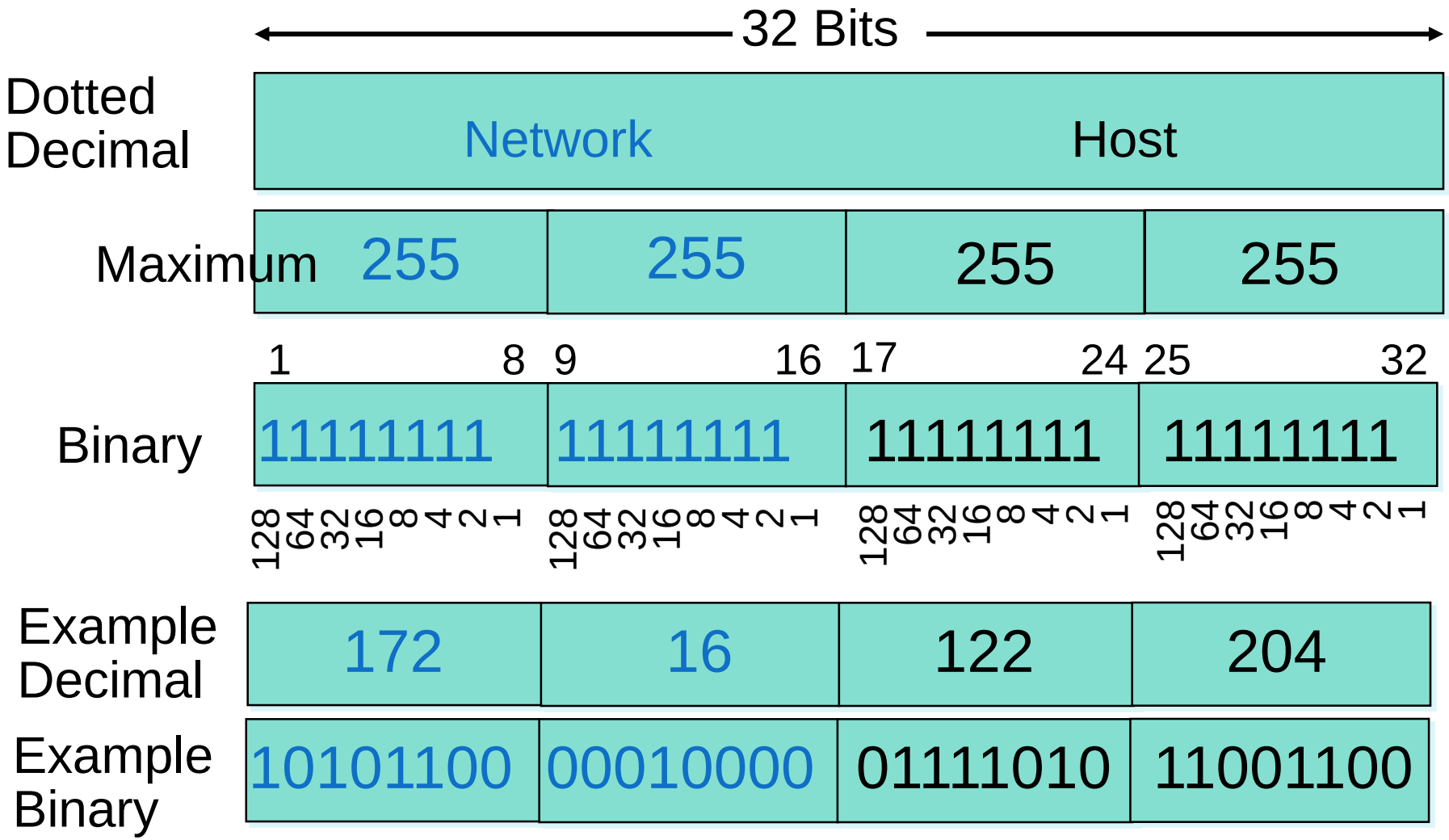
Binary	Decimal
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

Introduction to TCP/IP Addresses



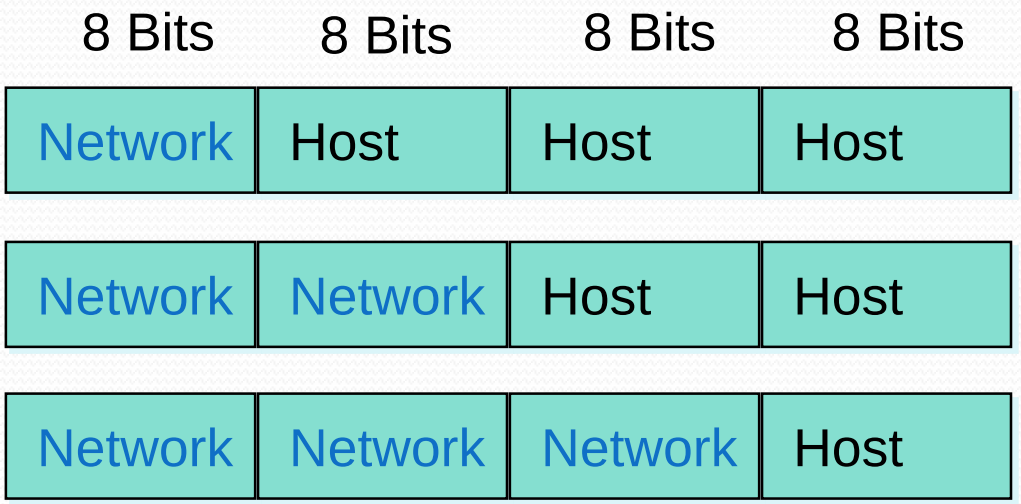
- Unique addressing allows communication between end stations.
- Path choice is based on destination address.

IP Addressing

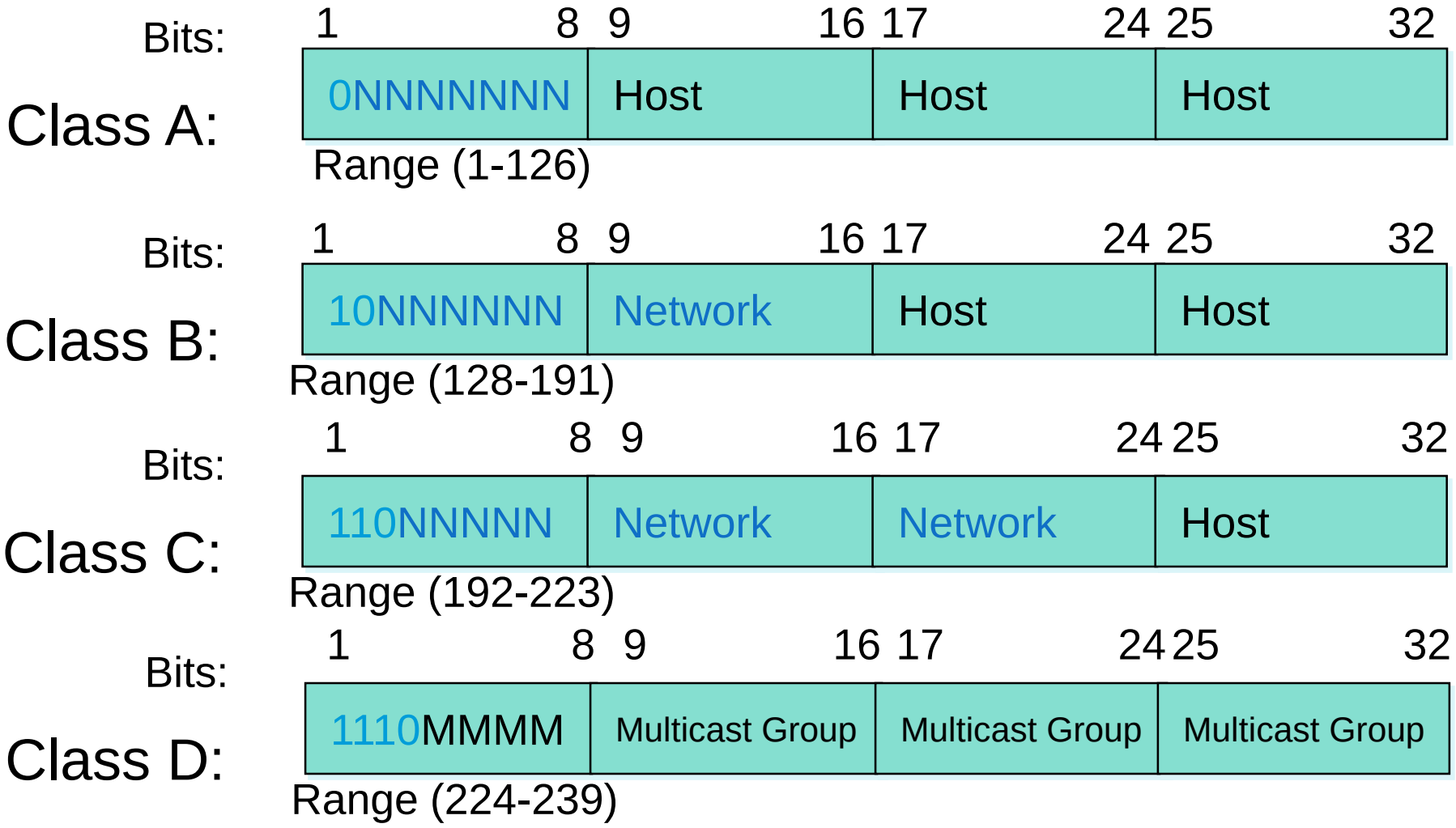


IP Address Classes

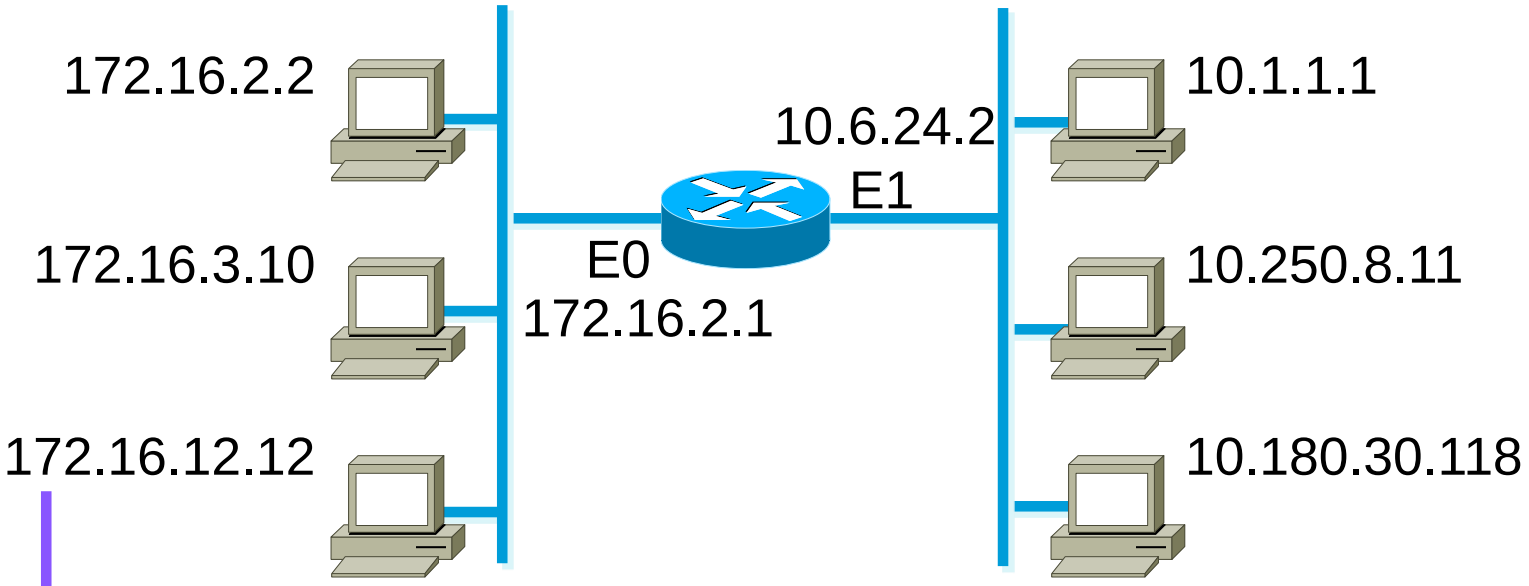
- Class A:
- Class B:
- Class C:
- Class D: Multicast
- Class E: Research



IP Address Classes



Host Addresses



172.16 . 12 . 12

Network Host

Routing Table	
Network	Interface
172.16.0.0	E0
10.0.0.0	E1

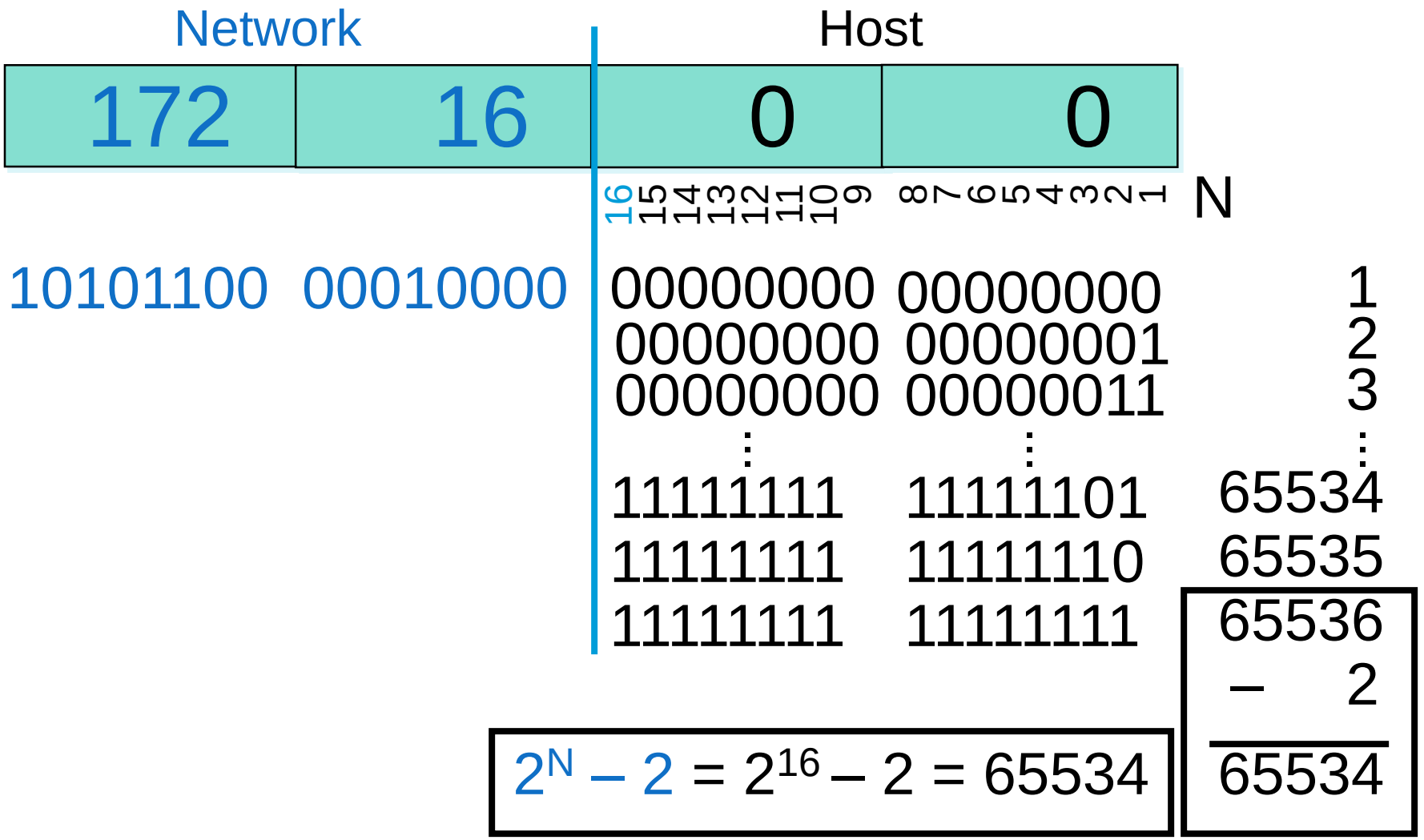
Classless Inter-Domain Routing (CIDR)

- Basically the method that ISPs (Internet Service Providers) use to allocate an amount of addresses to a company, a home
- Ex : 192.168.10.32/28
- The slash notation (/) means how many bits are turned on (1s)

CIDR Values

CIDR Value	Subnet Mask
/8	255.0.0.0
/9	255.128.0.0
/10	255.192.0.0
/11	255.224.0.0
/12	255.240.0.0

Determining Available Host Addresses



IP Address Classes Exercise

Address	Class	Network	Host
10.2.1.1			
128.63.2.100			
201.222.5.64			
192.6.141.2			
130.113.64.16			
256.241.201.10			

IP Address Classes Exercise Answers

Address	Class	Network	Host
10.2.1.1	A	10.0.0.0	0.2.1.1
128.63.2.100	B	128.63.0.0	0.0.2.100
201.222.5.64	C	201.222.5.0	0.0.0.64
192.6.141.2	C	192.6.141.0	0.0.0.2
130.113.64.16	B	130.113.0.0	0.0.64.16
256.241.201.10	Nonexistent		

Subnetting

- Subnetting is logically dividing the network by extending the 1's used in SNM
- Advantage
  - Can divide network in smaller parts
  - Restrict Broadcast traffic
  - Security
  - Simplified Administration

Formula

- Number of subnets – 2^x-2

  Where X = number of bits borrowed

- Number of Hosts – 2^y-2

  Where y = number of 0's

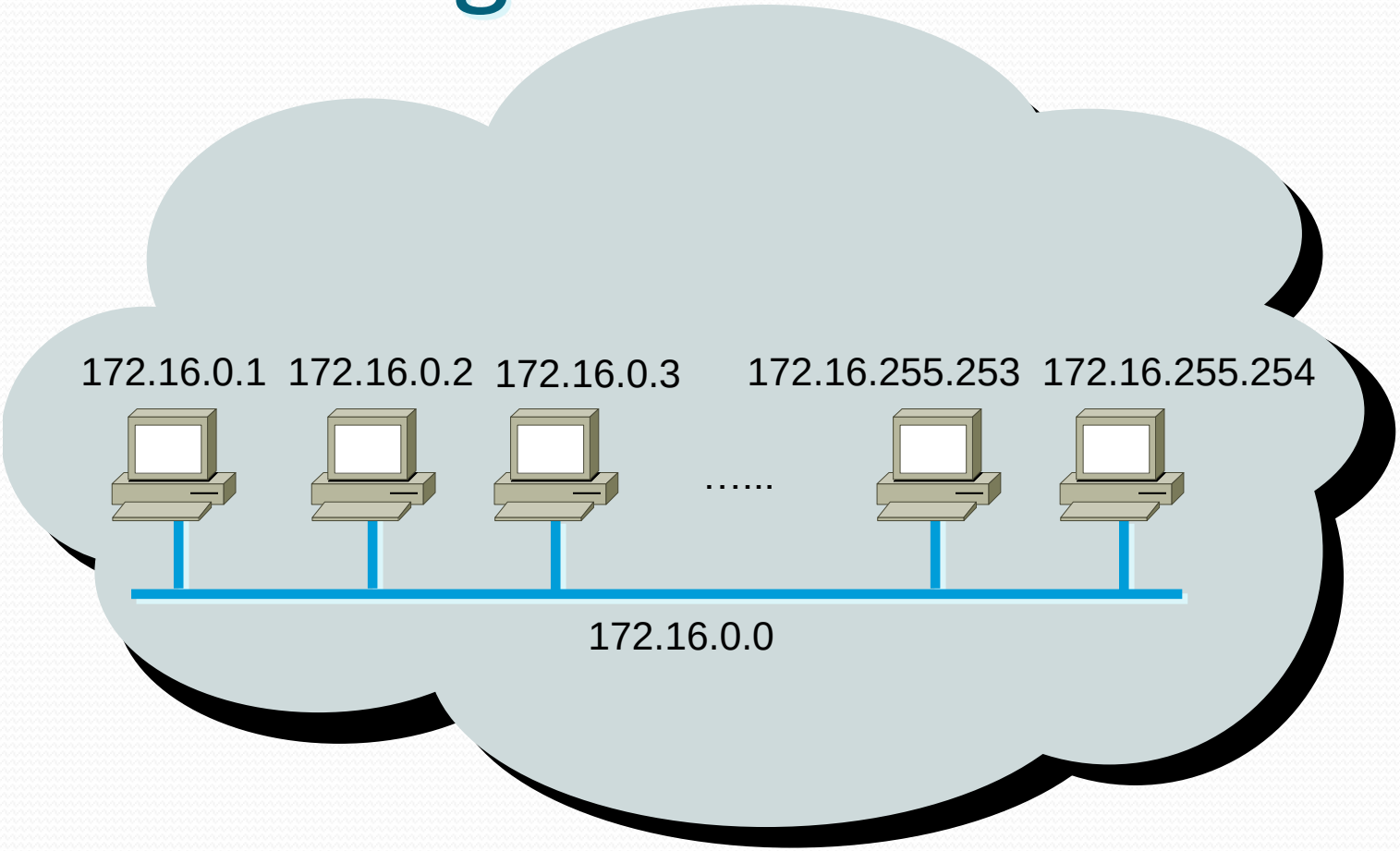
- Block Size = Total number of Address

  Block Size = 256-Mask

Subnetting

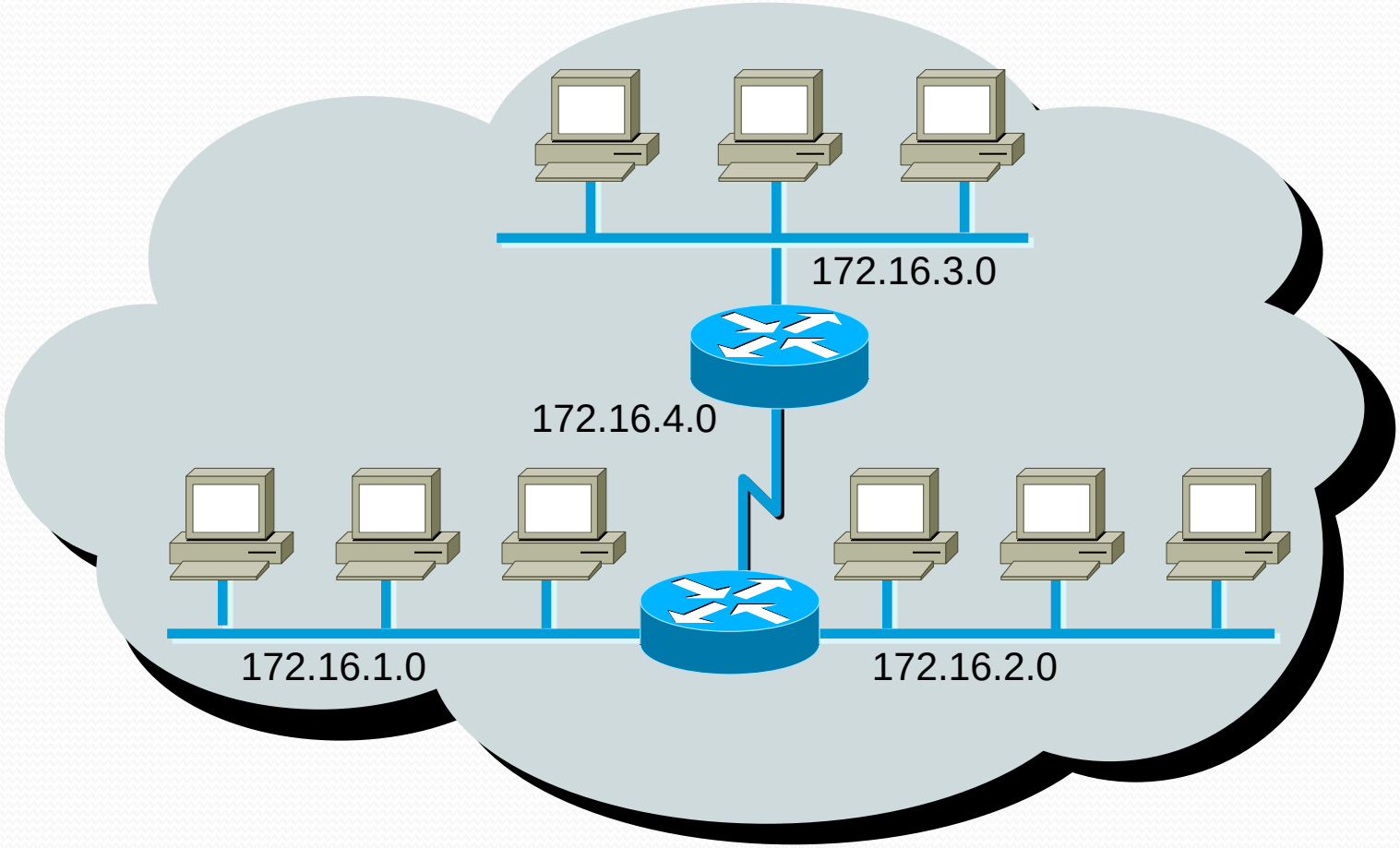
- Classful IP Addressing SNM are a set of 255's and 0's.
- In Binary it's contiguous 1's and 0's.
- SNM cannot be any value as it won't follow the rule of contiguous 1's and 0's.
- Possible subnet mask values
  - **0**
  - **128**
  - **192**
  - **224**
  - **240**
  - **248**
  - **252**
  - **254**
  - **255**

Addressing Without Subnets



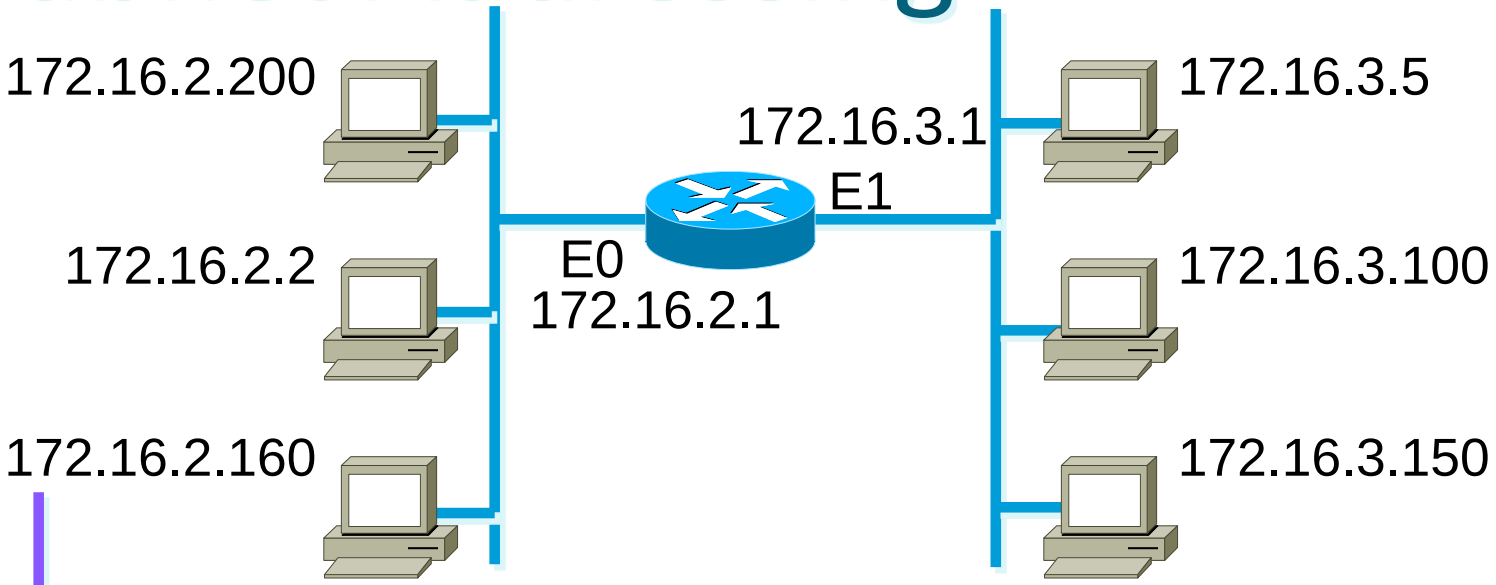
- Network 172.16.0.0

Addressing with Subnets



- Network 172.16.0.0

Subnet Addressing



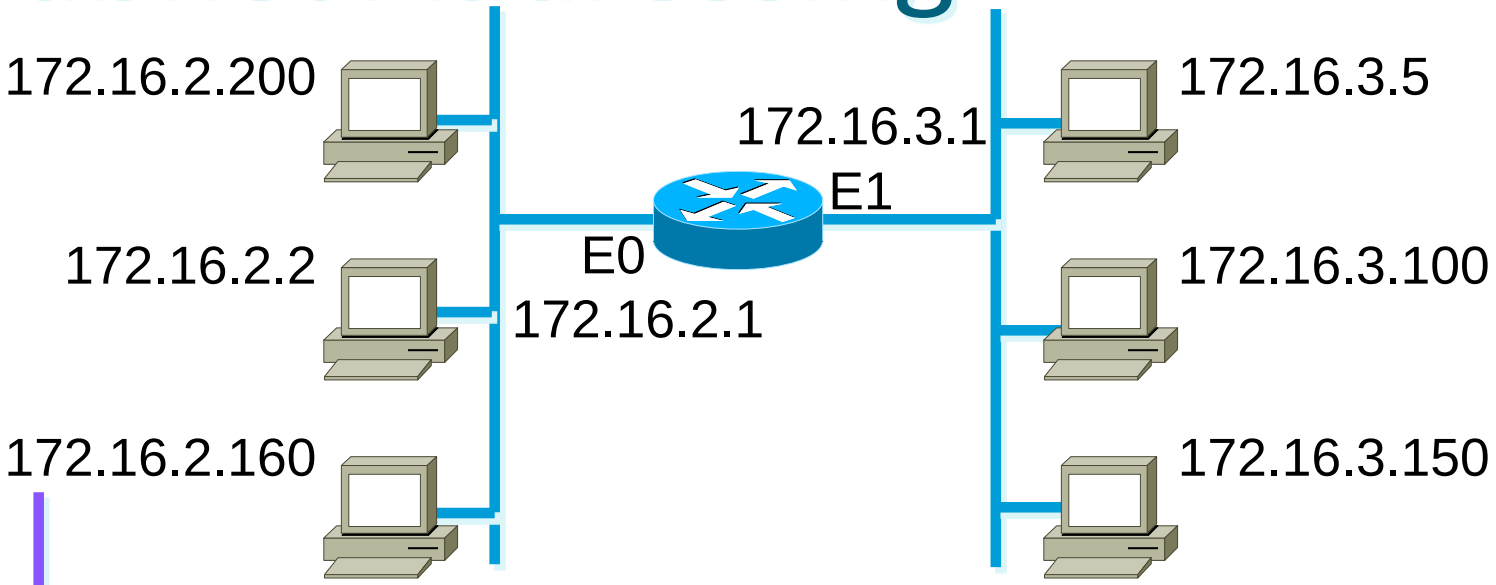
172.16 . 2 . 160

Network Host

New Routing Table

Network	Interface
172.16.0.0	E0
172.16.0.0	E1

Subnet Addressing



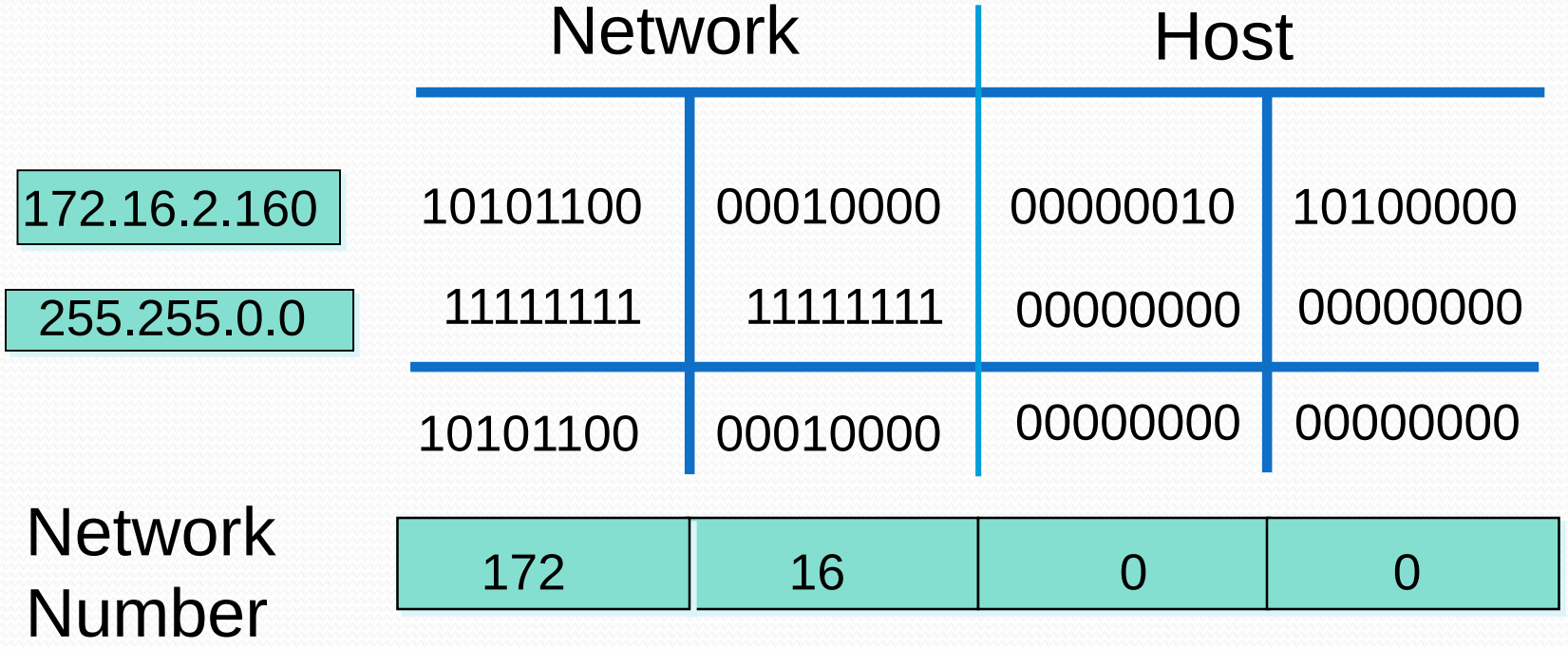
172.16 . 2 . 160

Network Subnet Host

New Routing Table

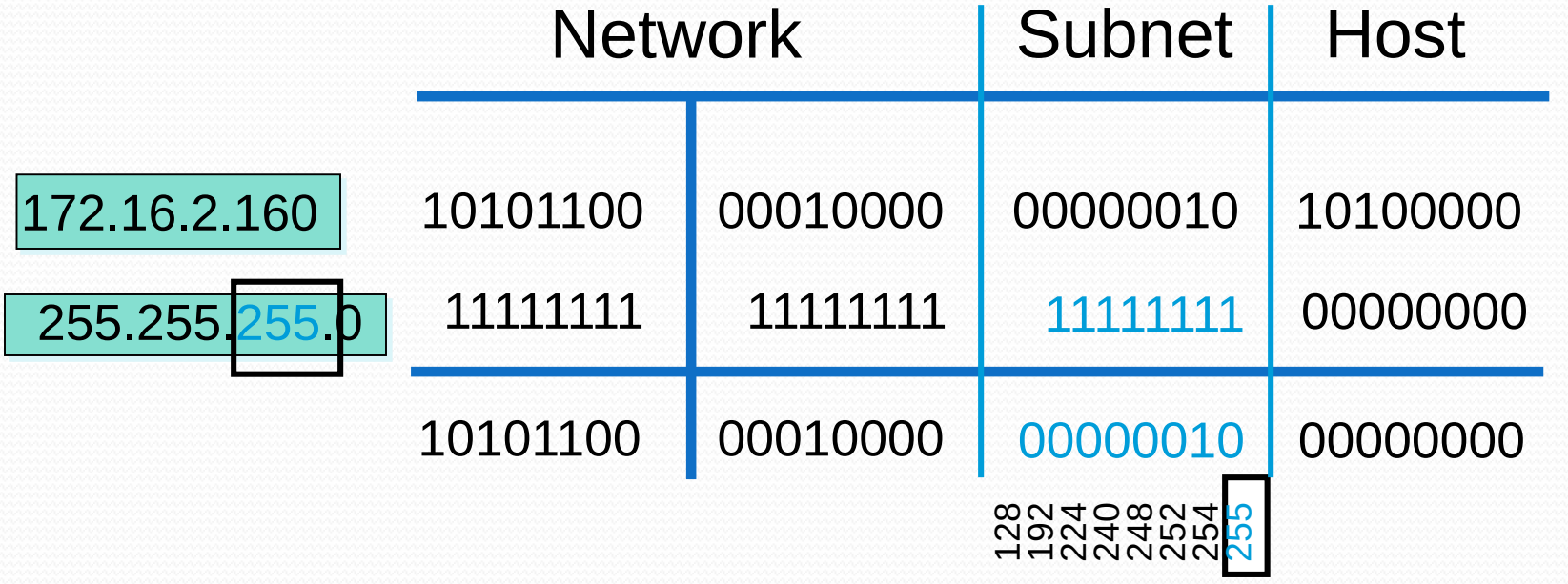
Network	Interface
172.16.2.0	E0
172.16.3.0	E1

Subnet Mask Without Subnets



- Subnets not in use—the default

Subnet Mask with Subnets

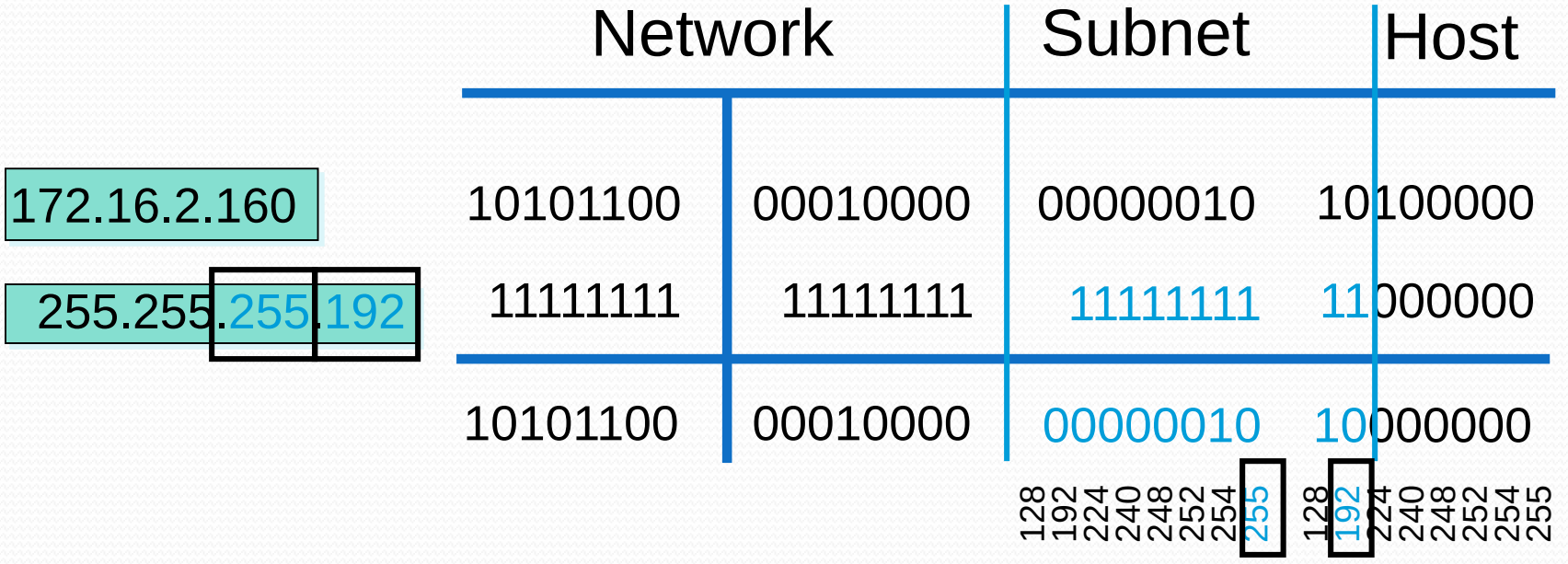


Network Number

172	16	2	0

- Network number extended by eight bits

Subnet Mask with Subnets (cont.)



Network Number

172	16	2	128

- Network number extended by ten bits

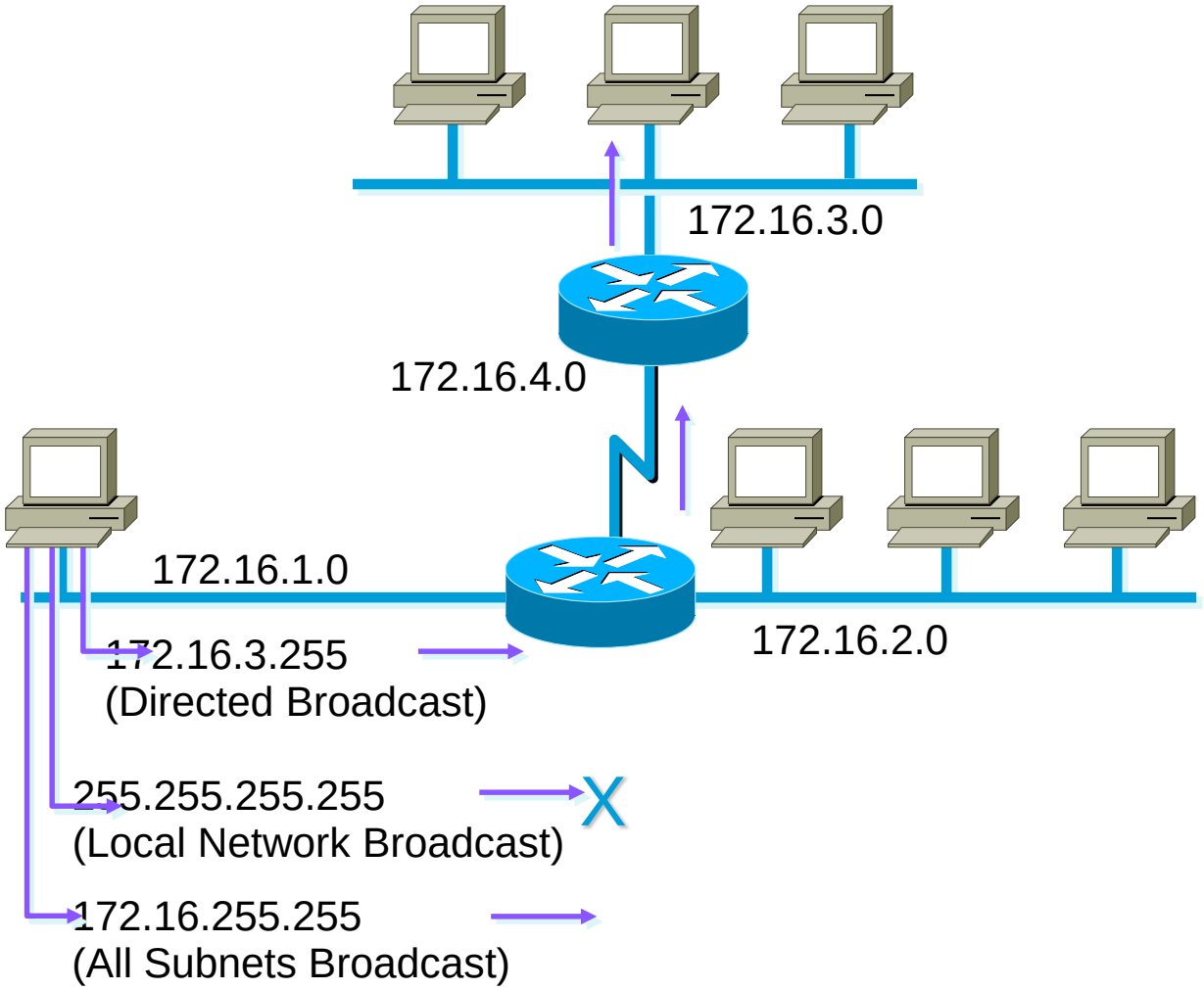
Subnet Mask Exercise

Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0		
10.6.24.20	255.255.240.0		
10.30.36.12	255.255.255.0		

Subnet Mask Exercise Answers

Address	Subnet Mask	Class	Subnet
172.16.2.10	255.255.255.0	B	172.16.2.0
10.6.24.20	255.255.240.0	A	10.6.16.0
10.30.36.12	255.255.255.0	A	10.30.36.0

Broadcast Addresses



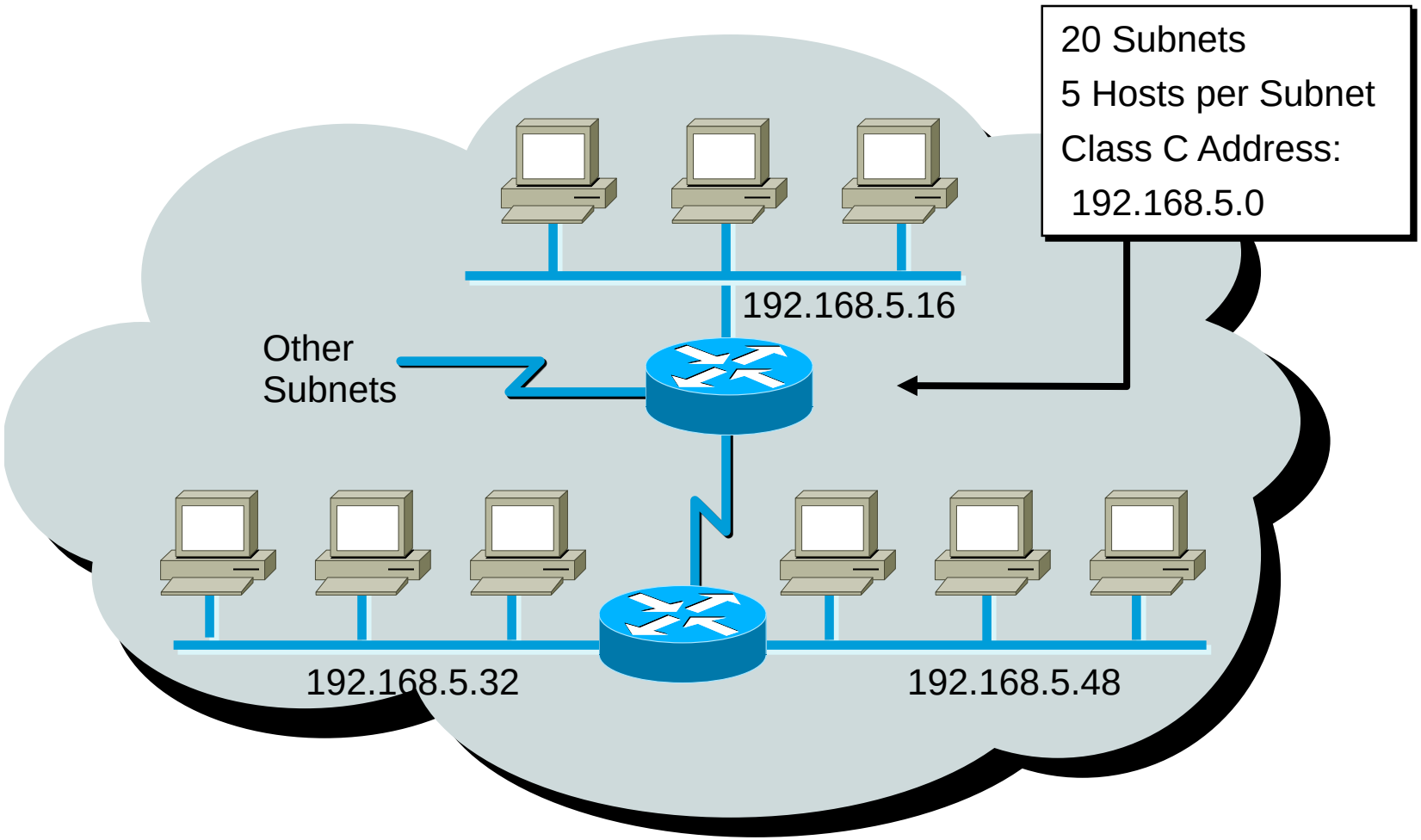
Class B Subnet Example

IP Host Address: 172.16.2.121
Subnet Mask: 255.255.255.0

	Network	Network	Subnet	Host
172.16.2.121:	10101100	00010000	00000010	01111001
255.255.255.0:	11111111	11111111	11111111	00000000
Subnet:	10101100	00010000	00000010	00000000
Broadcast:	10101100	00010000	00000010	11111111

- Subnet Address = 172.16.2.0
- Host Addresses = 172.16.2.1–172.16.2.254
- Broadcast Address = 172.16.2.255
- Eight Bits of Subnetting

Subnet Planning



Class C Subnet Planning Example

IP Host Address: 192.168.5.121
Subnet Mask: 255.255.255.248

	Network	Network	Network	Subnet	Host
192.168.5.121:	11000000	10101000	00000101	01111	001
255.255.255.248:	11111111	11111111	11111111	11111	000
Subnet:	11000000	10101000	00000101	01111	000
Broadcast:	11000000	10101000	00000101	01111	111

- Subnet Address = 192.168.5.120
- Host Addresses = 192.168.5.121–192.168.5.126
- Broadcast Address = 192.168.5.127
- Five Bits of Subnetting

Exercise

- **192.168.10.0**
- **/27**

? – SNM

? – Block Size

?- Subnets

Exercise

- **/27**

? – SNM – 224

? – Block Size = 256-224 = 32

?- Subnets

Subnets	10.0	10.32	10.64
FHID	10.1	10.33	
LHID	10.30	10.62	
Broadcast	10.31	10.63	

Exercise

- **192.168.10.0**
- **/30**

? – SNM

? – Block Size

?- Subnets

Exercise

- **/30**

? – SNM – 252

? – Block Size = 256-252 = 4

?- Subnets

Subnets	10.0	10.4	10.8
FHID	10.1	10.5	
LHID	10.2	10.6	
Broadcast	10.3	10.7	

Exercise

	Mask	Subnets	Host
/26	?	?	?
/27	?	?	?
/28	?	?	?
/29	?	?	?
/30	?	?	?

Exercise

	Mask	**Subnets**	**Host**
/26	192	4	62
/27	224	8	30
/28	240	16	14
/29	248	32	6
/30	252	64	2

Exam Question

- Find Subnet and Broadcast address
  - 192.168.0.100/27

Exercise

- 192.168.10.54 /29
- Mask ?
- Subnet ?
- Broadcast ?

Exercise

- 192.168.10.130 /28
- Mask ?
- Subnet ?
- Broadcast ?

Exercise

- 192.168.10.193 /30
- Mask ?
- Subnet ?
- Broadcast ?

Exercise

- 192.168.1.100 /26
- Mask ?
- Subnet ?
- Broadcast ?

Exercise

- 192.168.20.158 /27
- Mask ?
- Subnet ?
- Broadcast ?

Class B

172.16.0.0 /19

Subnets ?

Hosts ?

Block Size ?

Class B

172.16.0.0 /19

Subnets 2^3 -2 = 6

Hosts 2^{13} -2 = 8190

Block Size 256-224 = 32

Subnets	0.0	32.0	64.0	96.0
FHID	0.1	32.1	64.1	96.1
LHID	31.254	63.254	95.254	127.254
Broadcast	31.255	63.255	95.255	127.255

Class B

172.16.0.0 /27

Subnets ?

Hosts ?

Block Size ?

Class B

172.16.0.0 /27

Subnets 2^{11} -2 = 2046

Hosts 2^{5} -2 = 30

Block Size 256-224 = 32

Subnets	0.0	0.32	0.64	0.96
FHID	0.1	0.33	0.65	0.97
LHID	0.30	0.62	0.94	0.126
Broadcast	0.31	0.63	0.95	0.127

Class B

172.16.0.0 /23

Subnets ?

Hosts ?

Block Size ?

Class B

172.16.0.0 /23

Subnets 2^7 -2 = 126

Hosts 2^9 -2 = 510

Block Size 256-254 = 2

Subnets	0.0	2.0	4.0	6.0
FHID	0.1	2.1	4.1	6.1
LHID	1.254	3.254	5.254	7.254
Broadcast	1.255	3.255	5.255	7.255

Class B

172.16.0.0 /24

Subnets ?

Hosts ?

Block Size ?

Class B

172.16.0.0 /24

Subnets 2^8 -2 = 254

Hosts 2^8 -2 = 254

Block Size 256-255 = 1

Subnets	0.0	1.0	2.0	3.0
FHID	0.1	1.1	2.1	3.1
LHID	0.254	1.254	2.254	3.254
Broadcast	0.255	1.255	2.255	3.255

Class B

172.16.0.0 /25

Subnets ?

Hosts ?

Block Size ?

Class B

172.16.0.0 /25

Subnets 2^9 -2 = 510

Hosts 2^7 -2 = 126

Block Size 256-128 = 128

Subnets	0.0	0.128	1.0	1.128	2.0	2.128
FHID	0.1	0.129	1.1	1.129	2.1	2.129
LHID	0.126	0.254	1.126	1.254	2.126	2.254
Broadcast	0.127	0.255	1.127	1.255	2.127	2.255

Find out Subnet and Broadcast Address

- 172.16.85.30/29

Find out Subnet and Broadcast Address

- 172.30.101.62/23

Find out Subnet and Broadcast Address

- 172.20.210.80/24

Exercise

- Find out the mask which gives 100 subnets for class B

Exercise

- Find out the Mask which gives 100 hosts for Class B

Class A

10.0.0.0 /10

Subnets ?

Hosts ?

Block Size ?

Class A

10.0.0.0 /10
Subnets 2^2 -2 = 2
Hosts 2^{22} -2 = 4194302
Block Size 256-192 = 64

Subnets	10.0	10.64	10.128	10.192
FHID	10.0.0.1	10.64.0.1	10.128.0.1	10.192.0.1
LHID	10.63.255.254	10.127.255.254	10.191.255.254	10.254.255.254
Broadcast	10.63.255.255	10.127.255.255	10.191.255.255	10.254.255.255

Class A

10.0.0.0 /18

Subnets ?

Hosts ?

Block Size ?

Class A

10.0.0.0 /18
Subnets 2^{10} -2 = 1022
Hosts 2^{14} -2 = 16382
Block Size 256-192 = 64

Subnets	10.0.0.0	10.0.64.0	10.0.128.0	10.0.192.0
FHID	10.0.0.1	10.0.64.1	10.0.128.1	10.0.192.1
LHID	10.0.63.254	10.0.127.254	10.0.191.254	10.0.254.254
Broadcast	10.0.63.255	10.0.127.255	10.0.191.255	10.0.254.255

Broadcast Addresses Exercise

Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248			
15.16.193.6	255.255.248.0			
128.16.32.13	255.255.255.252			
153.50.6.27	255.255.255.128			

Broadcast Addresses Exercise Answers

Address	Subnet Mask	Class	Subnet	Broadcast
201.222.10.60	255.255.255.248	C	201.222.10.56	201.222.10.63
15.16.193.6	255.255.248.0	A	15.16.192.0	15.16.199.255
128.16.32.13	255.255.255.252	B	128.16.32.12	128.16.32.15
153.50.6.27	255.255.255.128	B	153.50.6.0	153.50.6.127

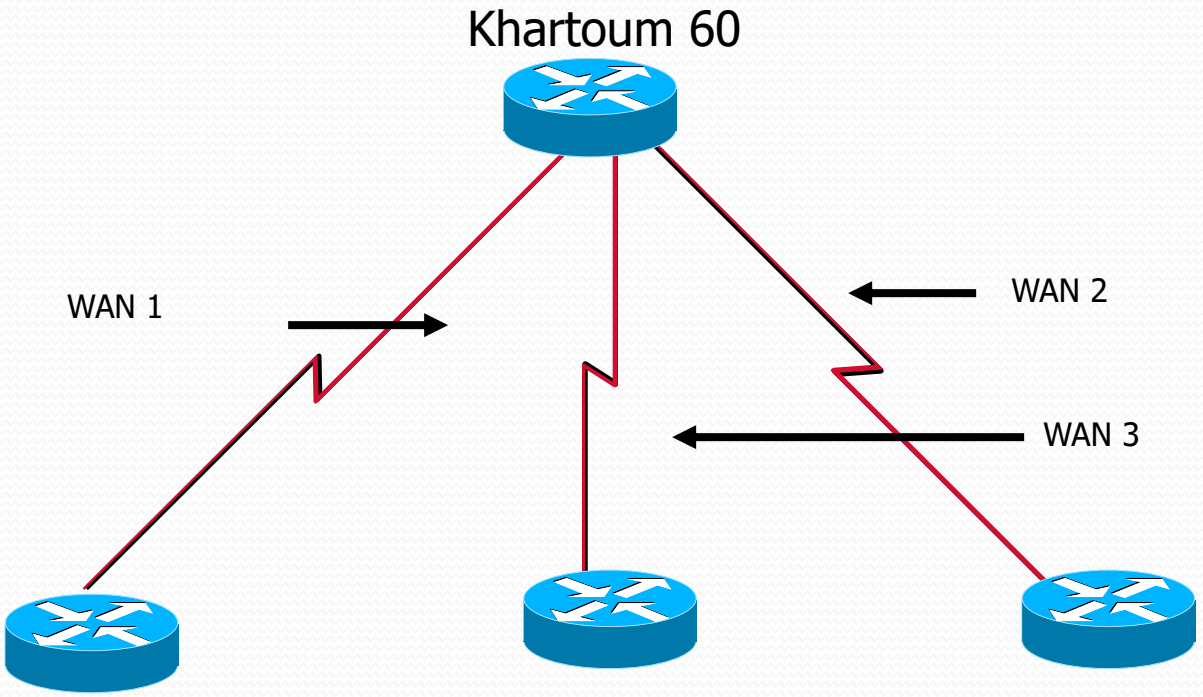
VLSM

- VLSM is a method of designating a different subnet mask for the same network number on different subnets
- Can use a long mask on networks with few hosts and a shorter mask on subnets with many hosts
- With VLSMs we can have different subnet masks for different subnets.

Variable Length Subnetting

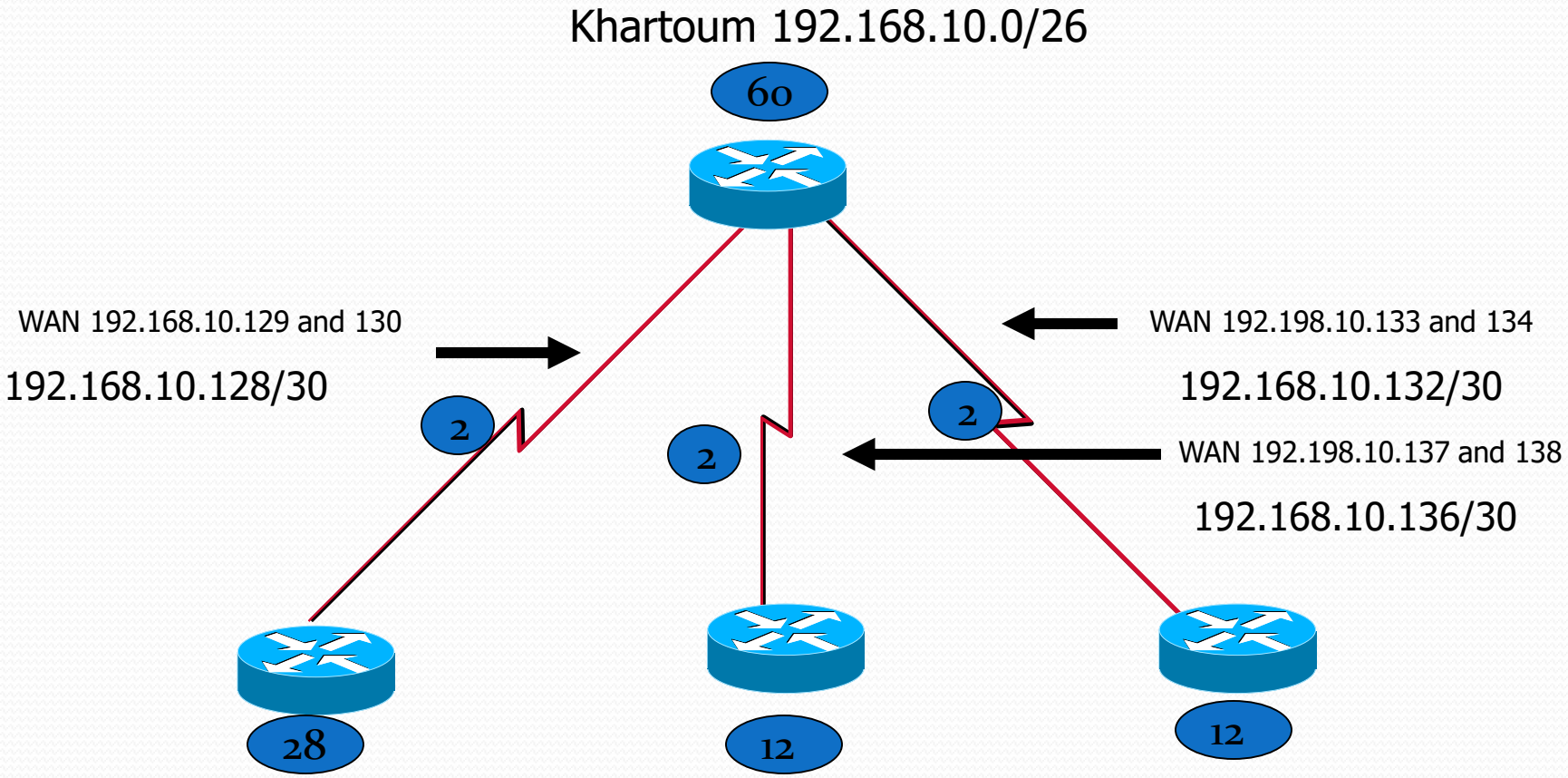
- VLSM allows us to use one class C address to design a networking scheme to meet the following requirements:
  - Khartoum 60 Hosts
  - Medani 28 Hosts
  - PortSudan 12 Hosts
  - Nyala 12 Hosts
  - WAN 1 2 Hosts
  - WAN 2 2 Hosts
  - WAN 3 2 Hosts

Networking Requirements

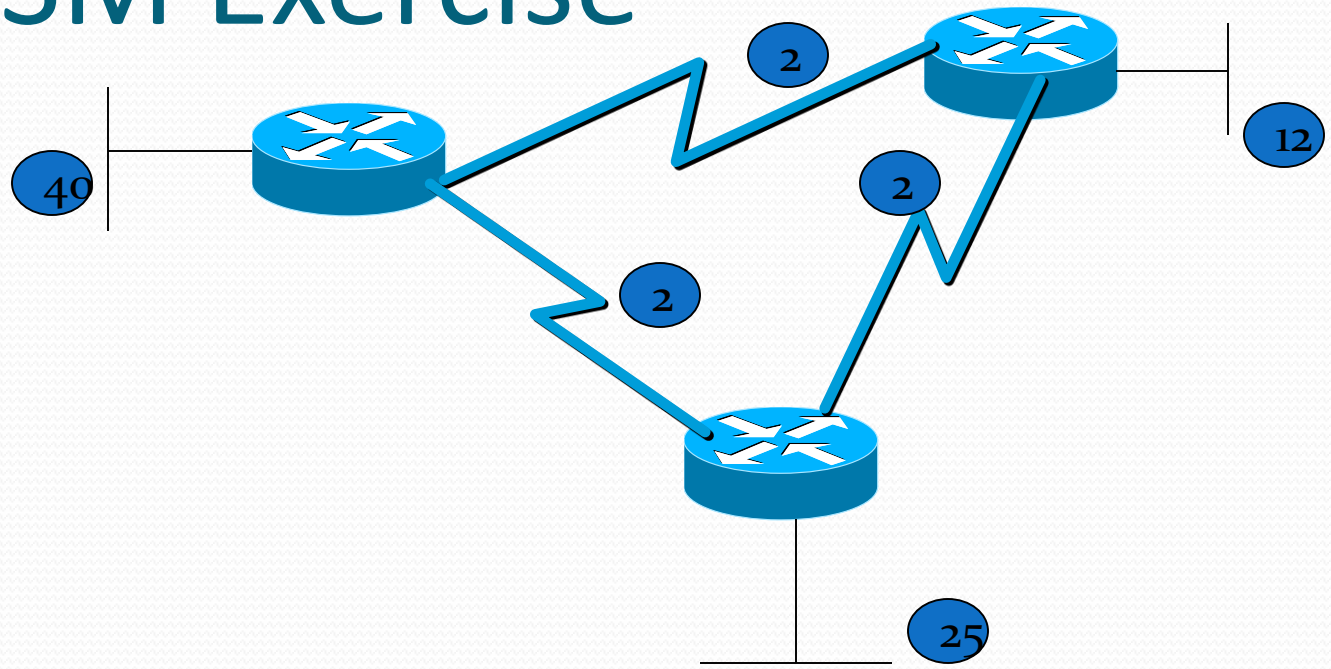


- In the example above, a /26 was used to provide the 60 addresses for Bangalore and the other LANs. There are no addresses left for WAN links

Networking Scheme

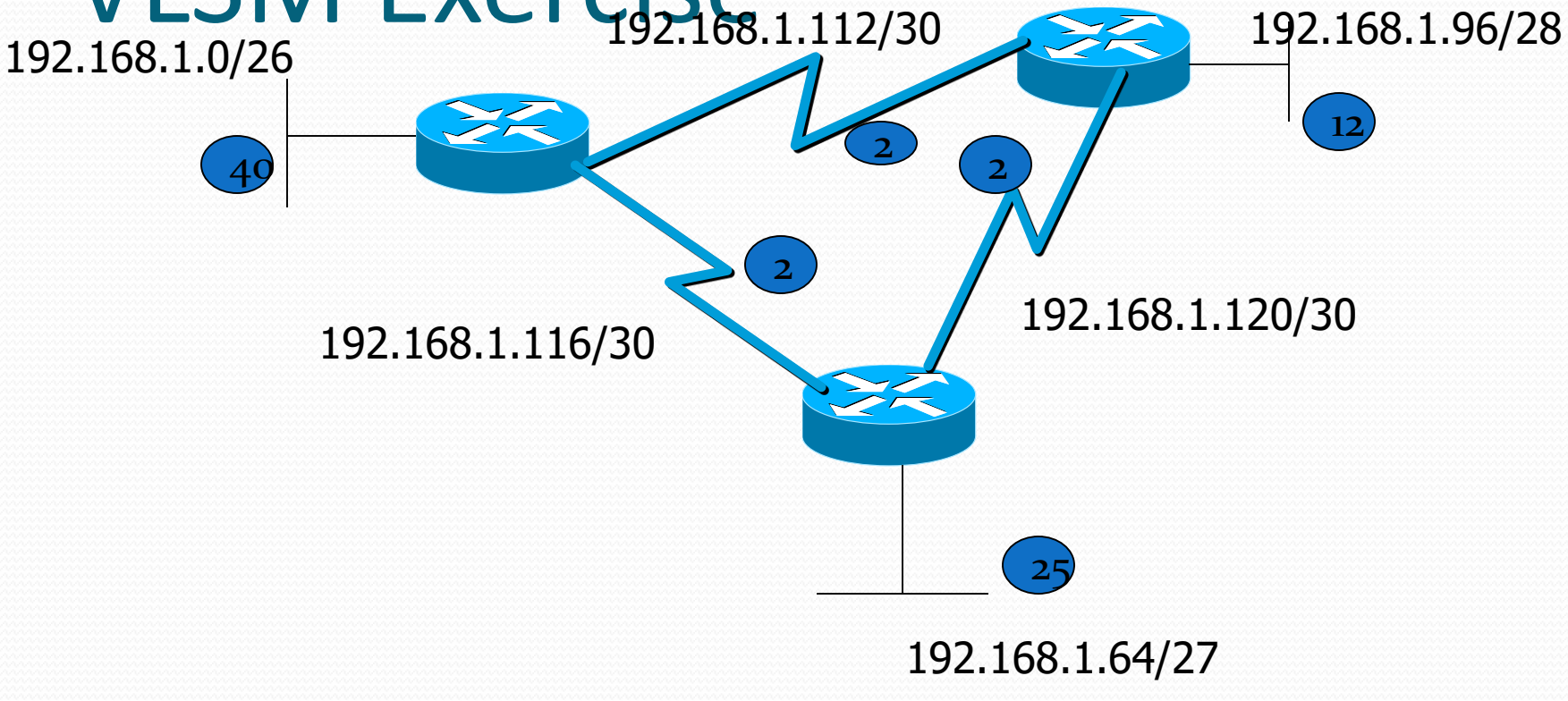


VLSM Exercise

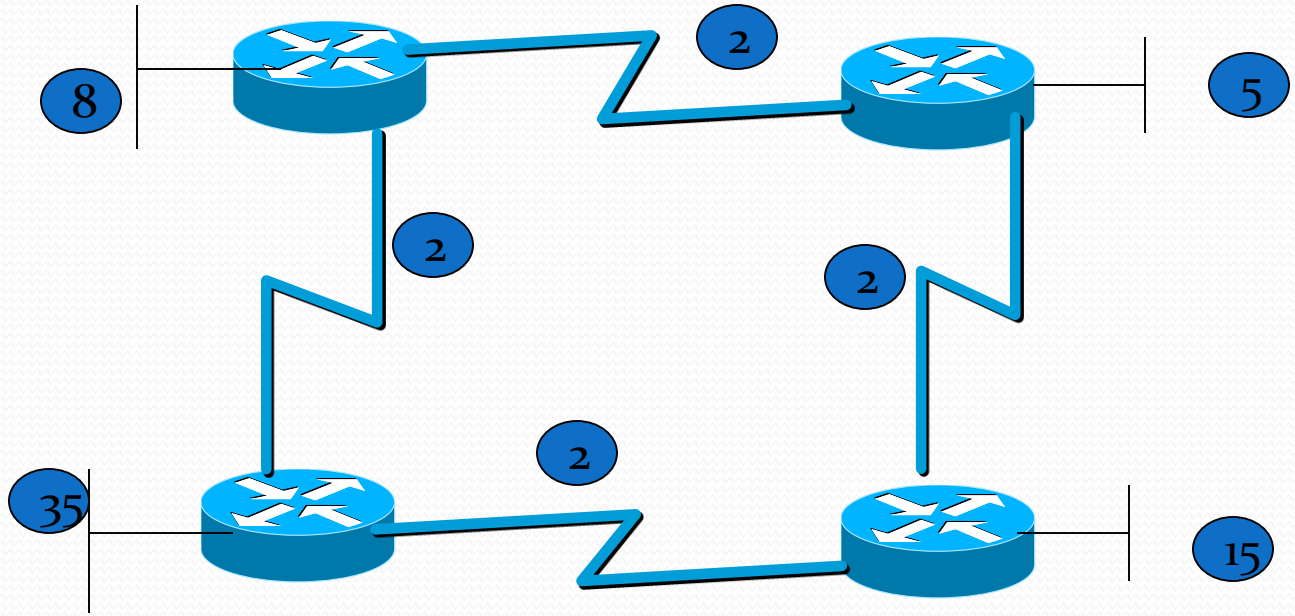


192.168.1.0

VLSM Exercise



VLSM Exercise

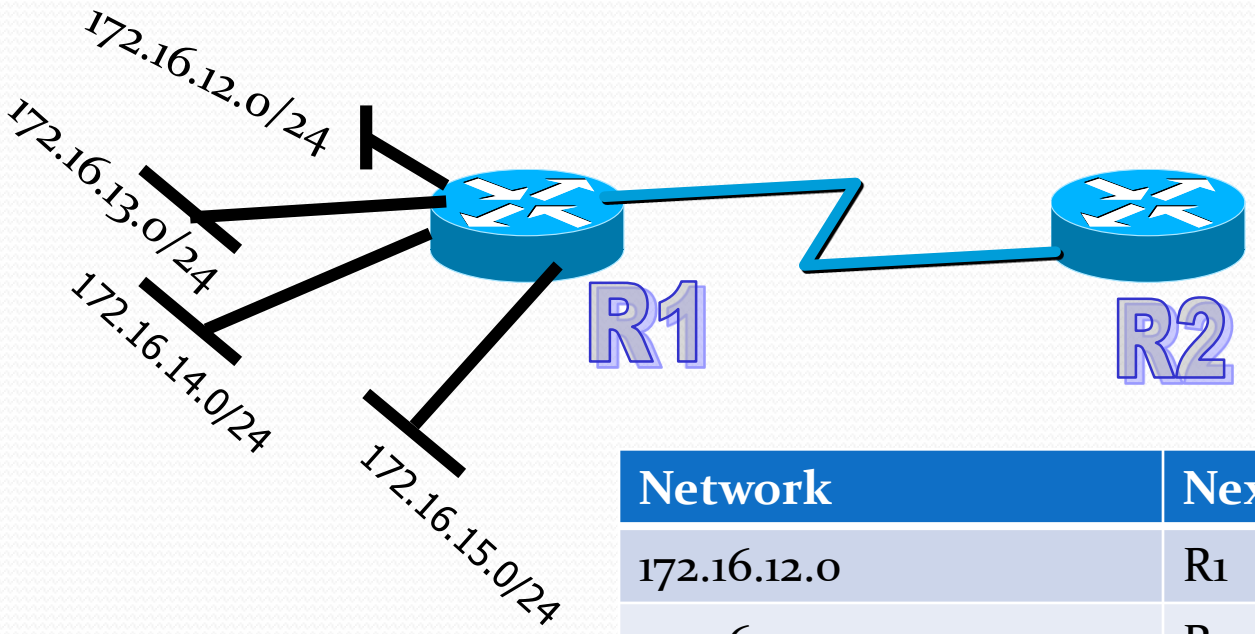


192.168.1.0

Summarization

- Summarization, also called route aggregation, allows routing protocols to advertise many networks as one address.
- The purpose of this is to reduce the size of routing tables on routers to save memory
- Route summarization (also called route aggregation or supernetting) can reduce the number of routes that a router must maintain
- Route summarization is possible only when a proper addressing plan is in place
- Route summarization is most effective within a subnetted environment when the network addresses are in contiguous blocks

Summarization



Network	Next Hop
172.16.12.0	R1
172.16.13.0	R1
172.16.14.0	R1
172.16.15.0	R1

Supernetting

	Network	Network	Network	Subnet
			16 8 4 2 1	
172.16.12.0	11000000	10101000	00001100	00000000
172.16.13.0	11000000	10101000	00001101	00000000
172.16.14.0	11000000	10101000	00001110	00000000
172.16.15.0	11000000	10101000	00001111	00000000
255.255.255.0	11111111	11111111	11111111	00000000

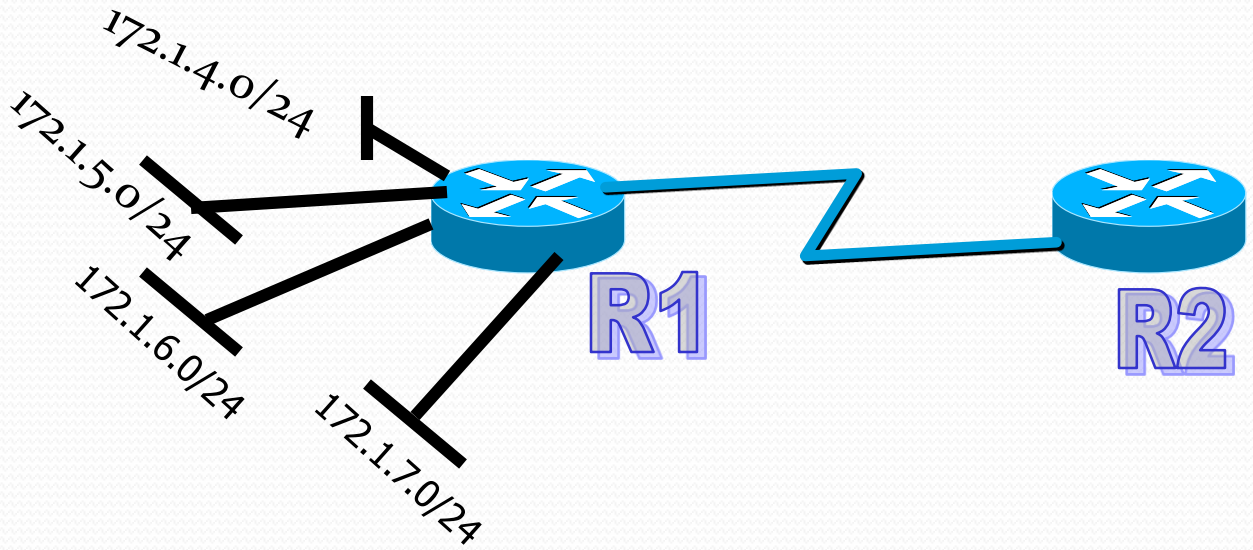
Supernetting

	Network	Network	Network	Subnet
			16 8 4 2 1	
172.16.12.0	11000000	10101000	00001100	00000000
172.16.13.0	11000000	10101000	00001101	00000000
172.16.14.0	11000000	10101000	00001110	00000000
172.16.15.0	11000000	10101000	00001111	00000000
255.255.252.0	11111111	11111111	11111100	00000000

172.16.12.0/24
172.16.13.0/24
172.16.14.0/24
172.16.15.0/24

} 172.16.12.0/22

Supernetting Question



- **What is the most efficient summarization that R1 can use to advertise its networks to R2?**

A. 172.1.4.0/24 172.1.5.0/24 172.1.6.0/24 172.1.7.0/24
B. 172.1.0.0/22
C. 172.1.4.0/25 172.1.4.128/25 172.1.5.0/24 172.1.6.0/24 172.1.7.0/24
D. 172.1.0.0/21
E. 172.1.4.0/22

Routers & Cisco IOS

Cisco IOS

Cisco technology is built around the Cisco Internetwork Operating System (IOS), which is the software that controls the routing and switching functions of internetworking devices.

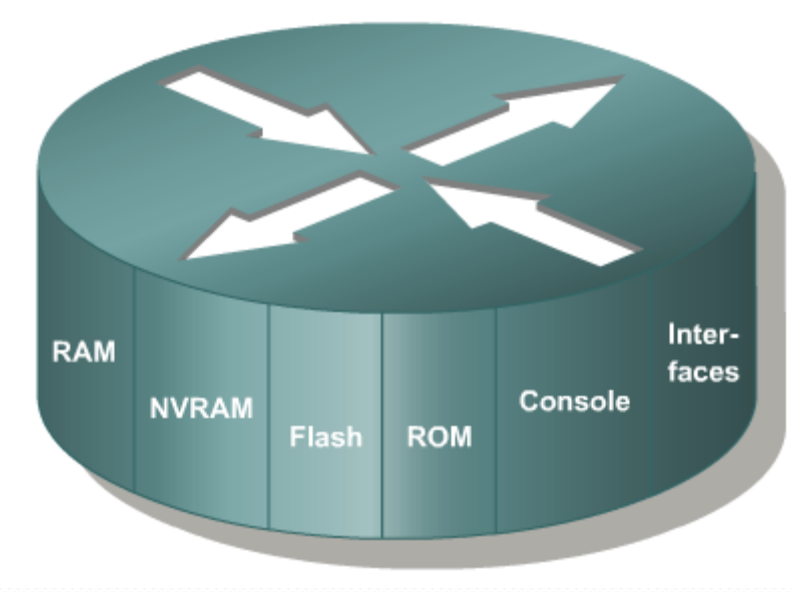
A solid understanding of the IOS is essential for a network administrator.

The Purpose of Cisco IOS

As with a computer, a router or switch cannot function without an operating system. Cisco calls its operating system the Cisco Internetwork Operating System or Cisco IOS.

Introduction to Routers

A router is a special type of computer. It has the same basic components as a standard desktop PC. However, routers are designed to perform some very specific functions. Just as computers need operating systems to run software applications, routers need the Internetwork Operating System software (IOS) to run configuration files. These configuration files contain the instructions and parameters that control the flow of traffic in and out of the routers. The many parts of a router are shown below:



Router Memory Components

ROM - Read Only Memory – Bootstrap/POST

FLASH Memory - IOS Images are kept here
- Erasable reprogrammable ROM
- Contents are kept on Power down or reload

RAM - Random Access memory
- Routing Tables
- Running Configuration
- Contents are lost on reboot

NVRAM - Start up configuration
- Configuration Register
- Contents are kept on reload

ROM

Read-Only Memory

ROM has the following characteristics and functions:

- Maintains instructions for power-on self test (POST) diagnostics
- Stores bootstrap program and basic operating system software
- Mini IOS

RAM

Random Access Memory, also called dynamic RAM (DRAM)

RAM has the following characteristics and functions:

- Stores routing tables
- Holds ARP cache
- Performs packet buffering (shared RAM)
- Provides temporary memory for the configuration file of the router while the router is powered on
- Loses content when router is powered down or restarted

NVRAM

Non-Volatile RAM

NVRAM has the following characteristics and functions:

- Provides storage for the startup configuration file
- Retains content when router is powered down or restarted
- Configuration Register – 16 bit register which decides boot sequence

Flash

Flash memory has the following characteristics and functions:

- Holds the operating system image (IOS)
- Allows software to be updated without removing and replacing chips on the processor
- Retains content when router is powered down or restarted
- Can store multiple versions of IOS software
- Is a type of electronically erasable, programmable ROM (EEPROM)

Interfaces

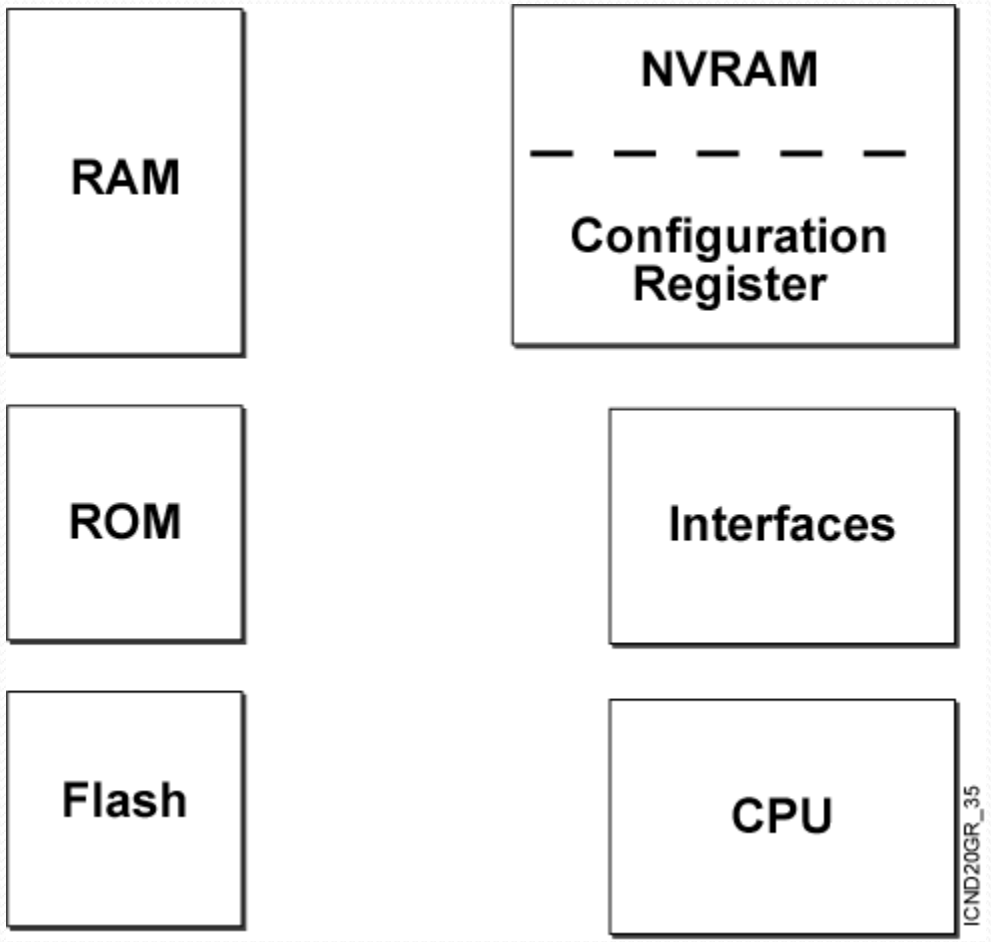
Interfaces have the following characteristics and functions:

Connect router to network for frame entry and exit
Can be on the motherboard or on a separate module

Types of interfaces:

- Ethernet
- Fast Ethernet
- Serial
- ISDN BRI
- Loopback
- Console
- Aux

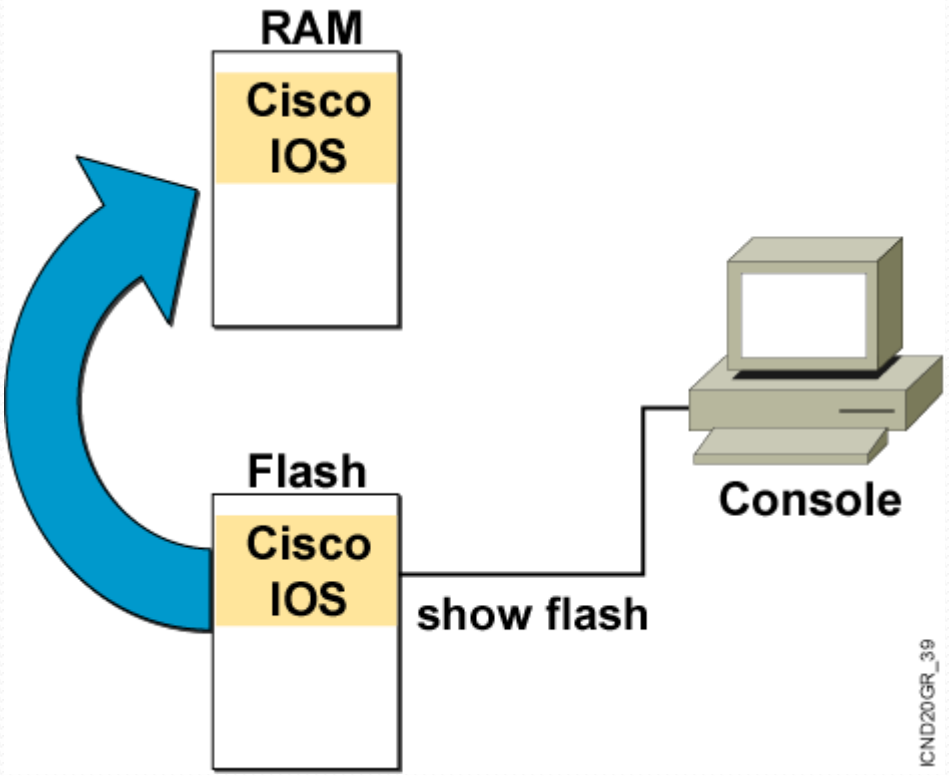
Router Internal Components



Router Power-On/Bootup Sequence

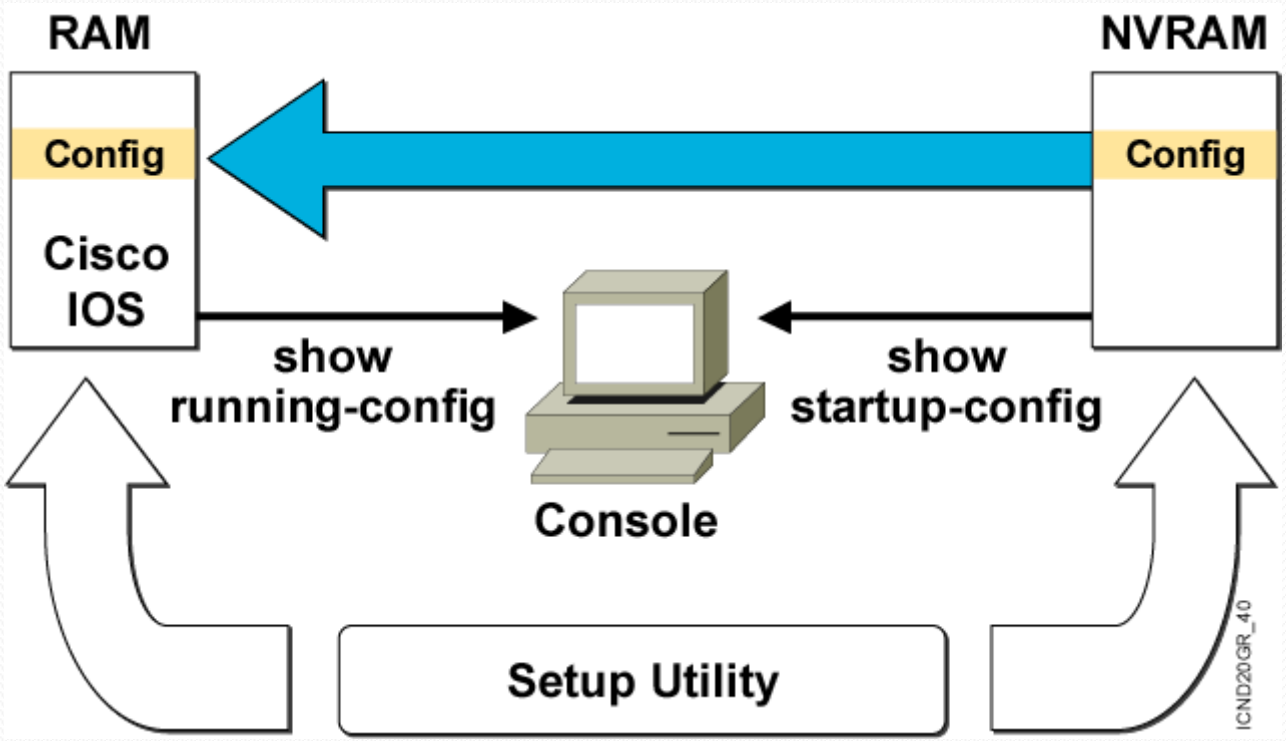
1. Perform power-on self test (POST).
2. Load and run bootstrap code.
3. Find the Cisco IOS software.
4. Load the Cisco IOS software.
5. Find the configuration.
6. Load the configuration.
7. Run the configured Cisco IOS software.

Loading the Cisco IOS Software From Flash Memory



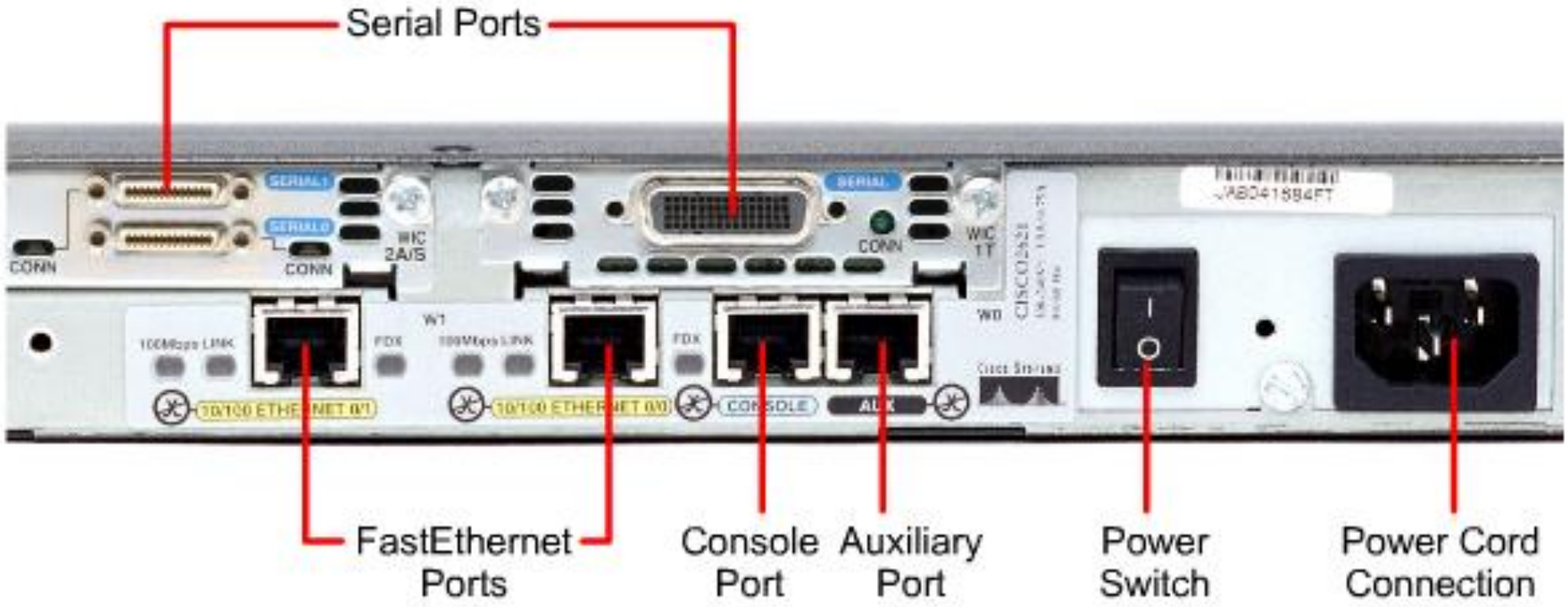
- **The flash memory file is decompressed into RAM.**

Loading the Configuration

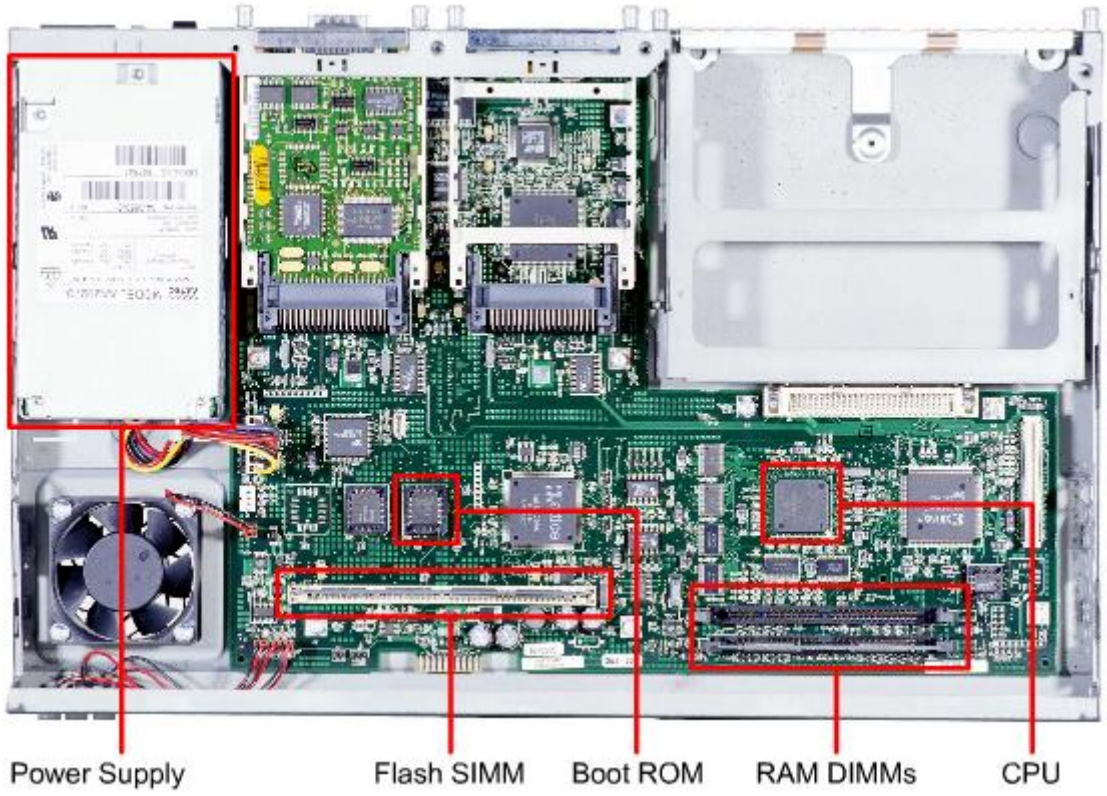


- **Load and execute the configuration from NVRAM.**
- **If no configuration is present in NVRAM, enter setup mode.**

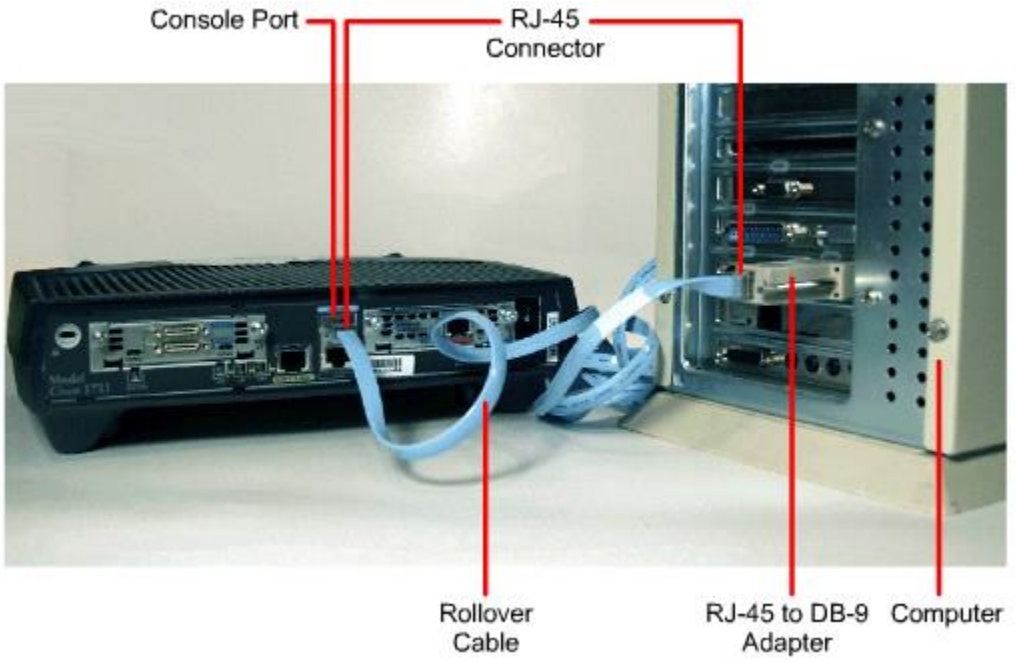
External Components of a 2600 Router



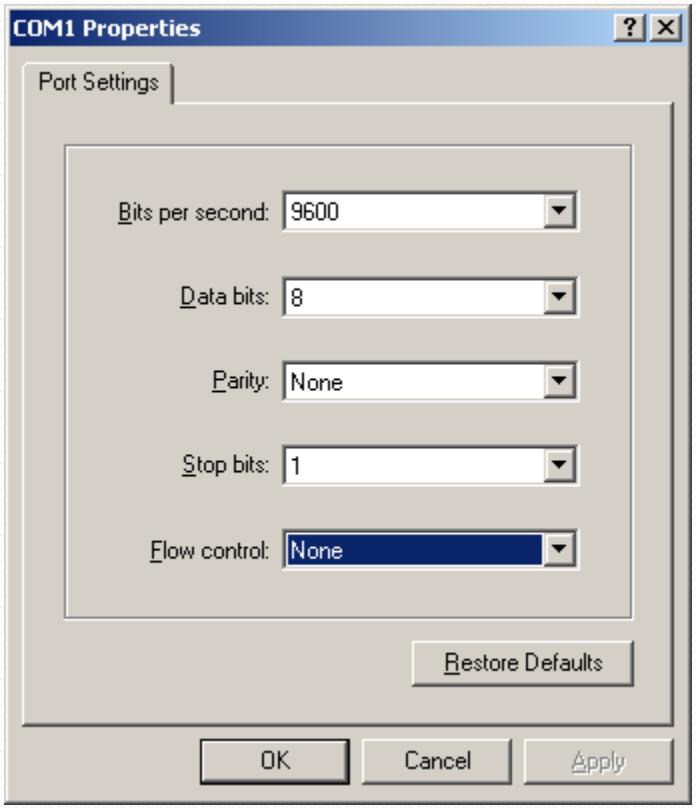
Internal Components of a 2600 Router



Computer/Terminal Console Connection



HyperTerminal Session Properties



Establishing a HyperTerminal Session

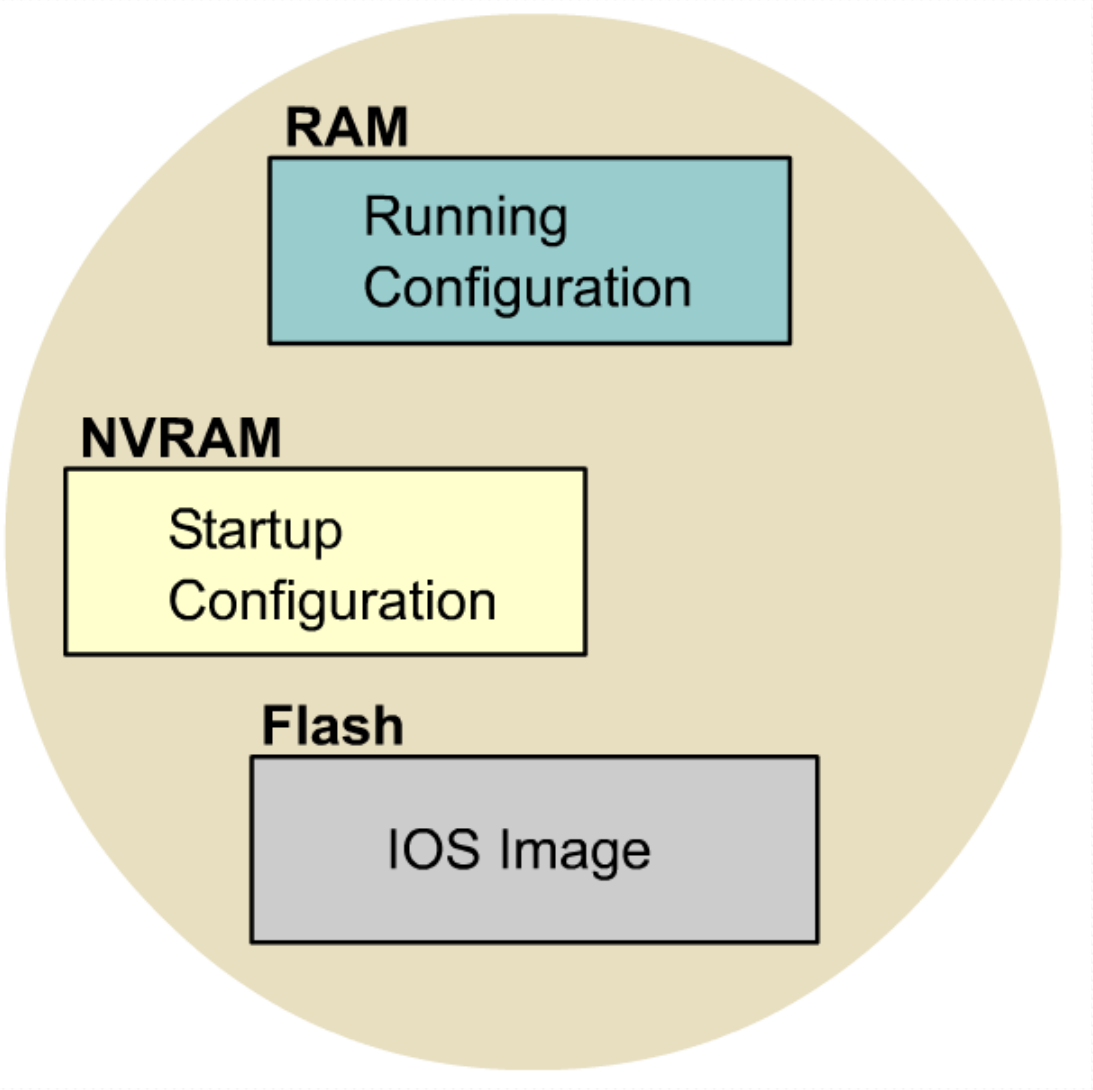
Take the following steps to connect a terminal to the console port on the router:

First, connect the terminal using the RJ-45 to RJ-45 rollover cable and an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.

Then, configure the terminal or PC terminal emulation software for 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

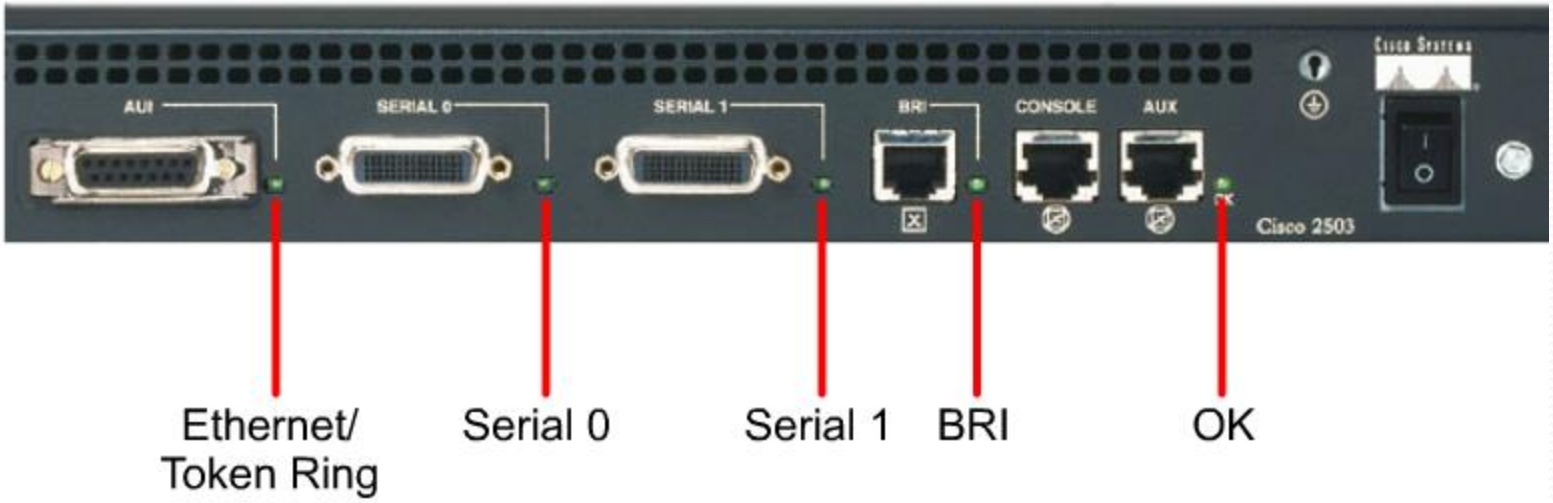
Router Command Line Interface

IOS File System Overview



Router LED Indicators

Cisco routers use LED indicators to provide status information. Depending upon the Cisco router model, the LED indicators will vary. An interface LED indicates the activity of the corresponding interface. If an LED is off when the interface is active and the interface is correctly connected, a problem may be indicated. If an interface is extremely busy, its LED will always be on. The green OK LED to the right of the AUX port will be on after the system initializes correctly.



Router Configuration

Router User Interface Modes

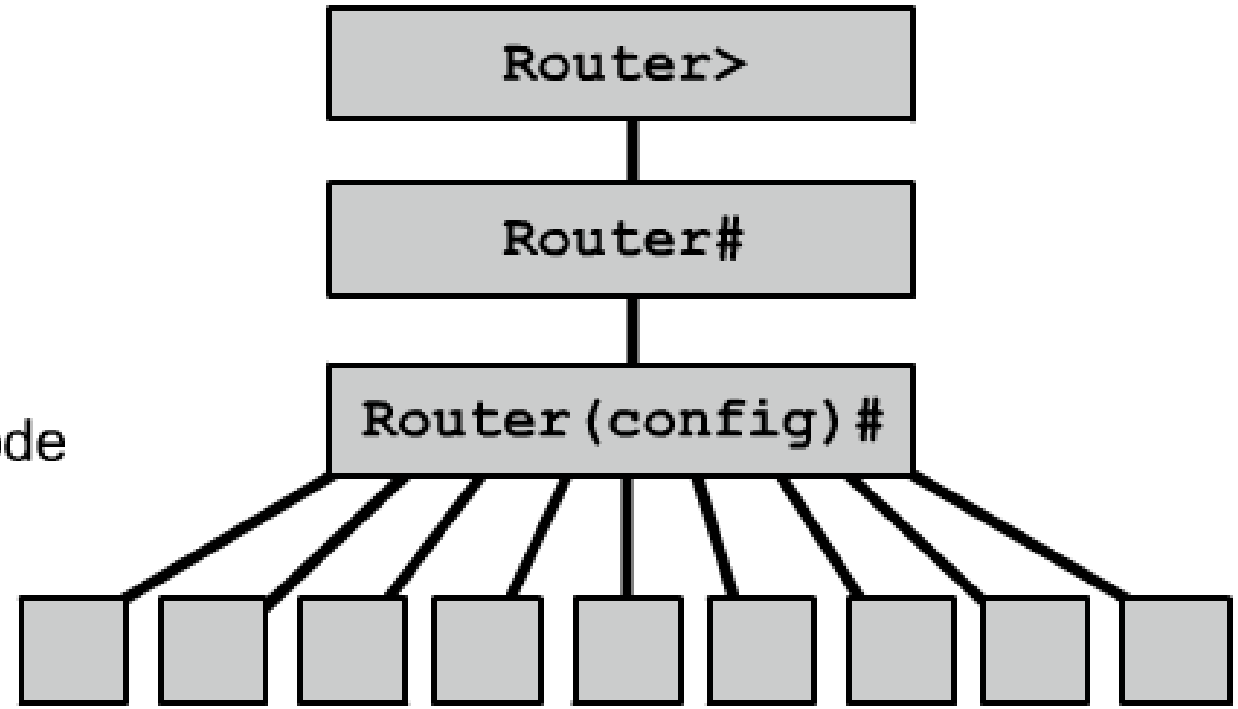
The Cisco command-line interface (CLI) uses a hierarchical structure. This structure requires entry into different modes to accomplish particular tasks.

Each configuration mode is indicated with a distinctive prompt and allows only commands that are appropriate for that mode.

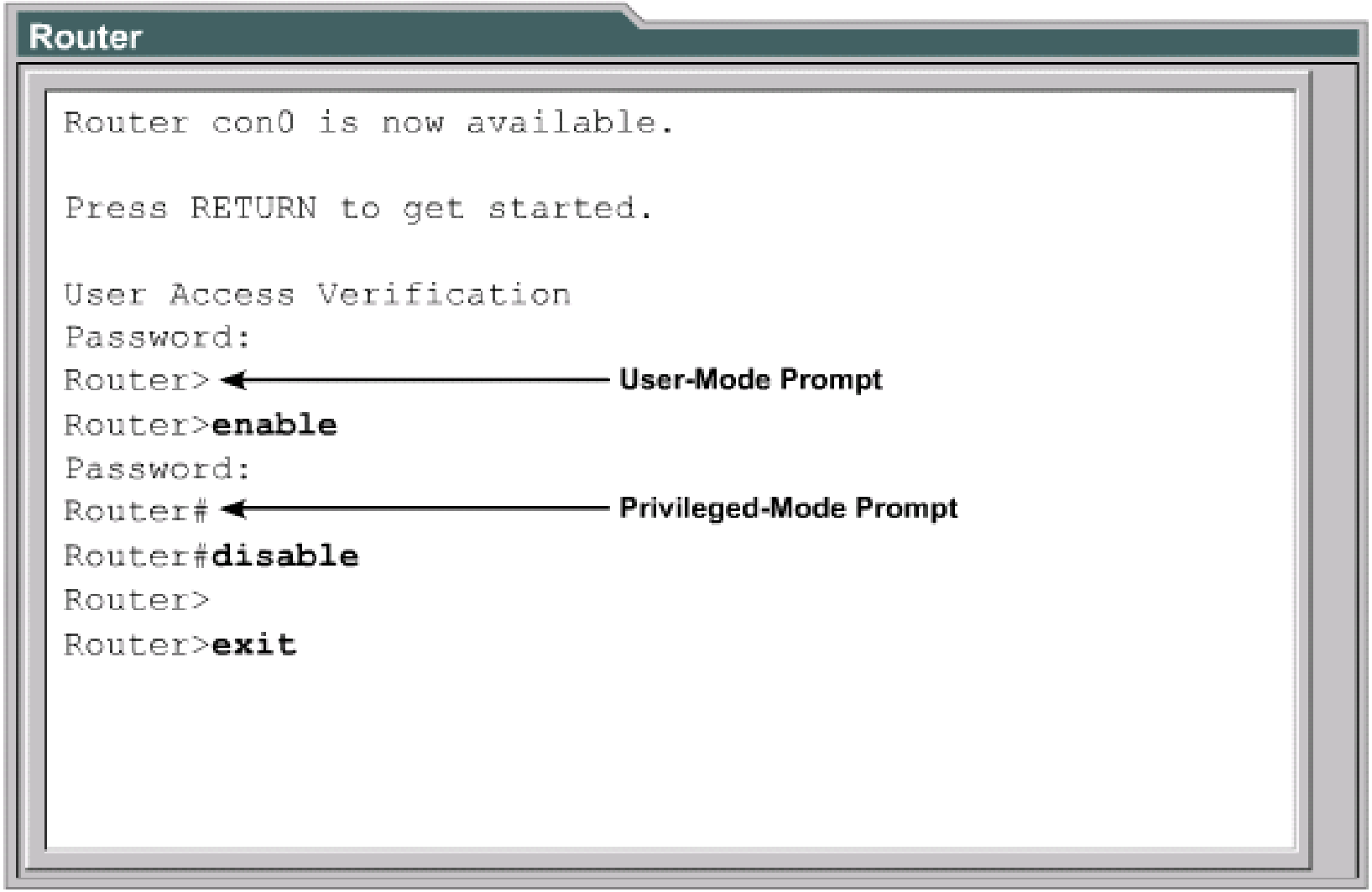
As a security feature the Cisco IOS software separates sessions into two access levels, user EXEC mode and privileged EXEC mode. The privileged EXEC mode is also known as enable mode.

Overview of Router Modes

- User EXEC mode
- Privileged EXEC mode
- Global configuration mode
- Specific configuration modes



Router Modes



CLI Command Modes

All command-line interface (CLI) configuration changes to a Cisco router are made from the global configuration mode. Other more specific modes are entered depending upon the configuration change that is required.

Global configuration mode commands are used in a router to apply configuration statements that affect the system as a whole.

The following command moves the router into global configuration mode

Router#**configure terminal** **(or config t)**
Router(config)#

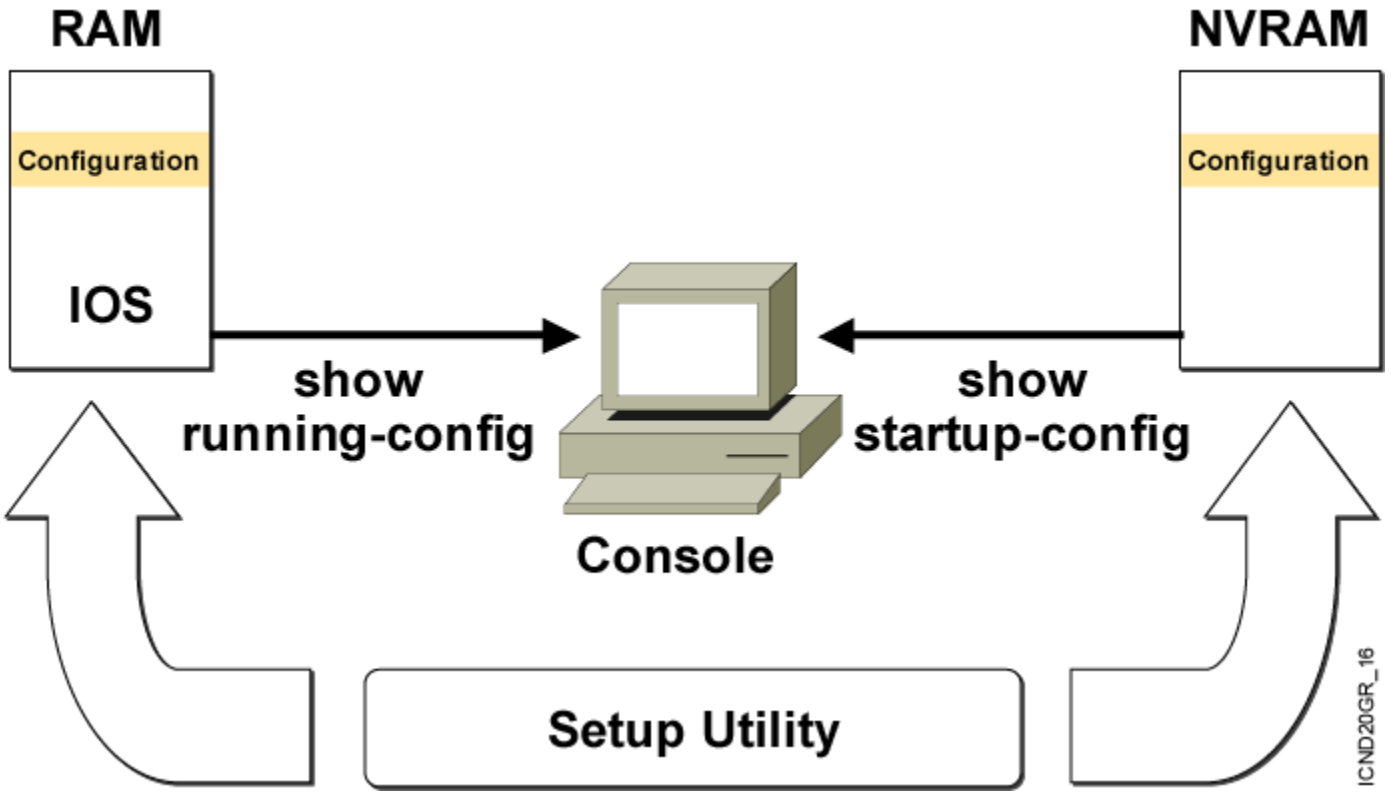
When specific configuration modes are entered, the router prompt changes to indicate the current configuration mode.

Typing **exit** from one of these specific configuration modes will return the router to global configuration mode. Pressing **Ctrl-Z** returns the router to all the way back privileged EXEC mode.

Show Version Command

```
wg_ro_a#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 08-Feb-99 18:18 by phanguye
Image text-base: 0x03050C84, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), RELEASE SOFTWARE(fc1)

wg_ro_a uptime is 20 minutes
System restarted by reload
System image file is "flash:c2500-js-l_120-3.bin"
(output omitted)
--More--

Configuration register is 0x2102
```

Viewing the Configuration



show running-config and show startup-config Commands

In RAM

```
wg_ro_c#show running-config
Building configuration...

Current configuration:
!
version 12.0
!
     -- More --
```

In NVRAM

```
wg_ro_c#show startup-config
Using 1359 out of 32762 bytes
!
version 12.0
!
     -- More --
```

- **Displays the current and saved configuration**

Saving Configurations

Configurations in two locations - RAM and NVRAM.

- The running configuration is stored in RAM.
- Any configuration changes to the router are made to the running-configuration and take effect immediately after the command is entered.
- The startup-configuration is saved in NVRAM and is loaded into the router's running-configuration when the router boots up.
- To save the running-configuration to the startup configuration, type the following from privileged EXEC mode (i.e. at the "Router#" prompt.)

```
Router# copy run start
```

Command Abbreviation

- Show Configuration – sh runn
- Configure Terminal – conf t
- Line auxillary – line aux
- Line console – line con

Configuring a Router's Name

A router should be given a unique name as one of the first configuration tasks.

This task is accomplished in global configuration mode using the following commands:

```
Router(config)#hostname NetworkPlus
NetworkPlus(config)#
```

As soon as the Enter key is pressed, the prompt changes from the default host name (Router) to the newly configured host name (which is NetworkPlus in the example above).

Router

```
Cisco#cl?
clear  clock
Cisco#clock
% Incomplete command.
Cisco#clock ?
  set  Set the time and date
Cisco#clock set
% Incomplete command.
Cisco#clock set ?
  hh:mm:ss  Current Time
Cisco#clock set 19:50:00
% Incomplete command.
Cisco#clock set 19:50:00 ?
  <1-31>  Day of the month
  MONTH   Month of the year
Cisco#clock set 19:50:00 14 7
                            ^
% Invalid input detected at '^' marker.
Cisco#clock set 19:50:00 14 July
% Incomplete command.
Cisco#clock set 19:50:00 14 July ?
  <1993-2035>  Year
Cisco#clock set 19:50:00 14 July 2003
Cisco#
```

Message Of The Day (MOTD)

A message-of-the-day (MOTD) banner can be displayed on all connected terminals.

Enter global configuration mode by using the command **config t**

Enter the command
banner motd # Welcome to NetworkPlus Training #.

Save changes by issuing the command **copy run start**

Privileged Mode Command

show startup-config
show running-config
show version
show flash
show interfaces
show interfaces s 0
show history
show terminal
terminal history size 25

Password

- Passwords restrict access to routers.
- Passwords should always be configured for virtual terminal lines and the console line.
- Passwords are also used to control access to privileged EXEC mode so that only authorized users may make changes to the configuration file.

Passwords

- There are five passwords for Router
  - Privileged Mode Password – 2
  - Line Console Password
  - Auxiliary Port Password
  - Telnet Password

Privileged Mode Password

Gates(config)# enable password cisco

Encrypted privilege mode password

Gates(config)# enable secret cisco1

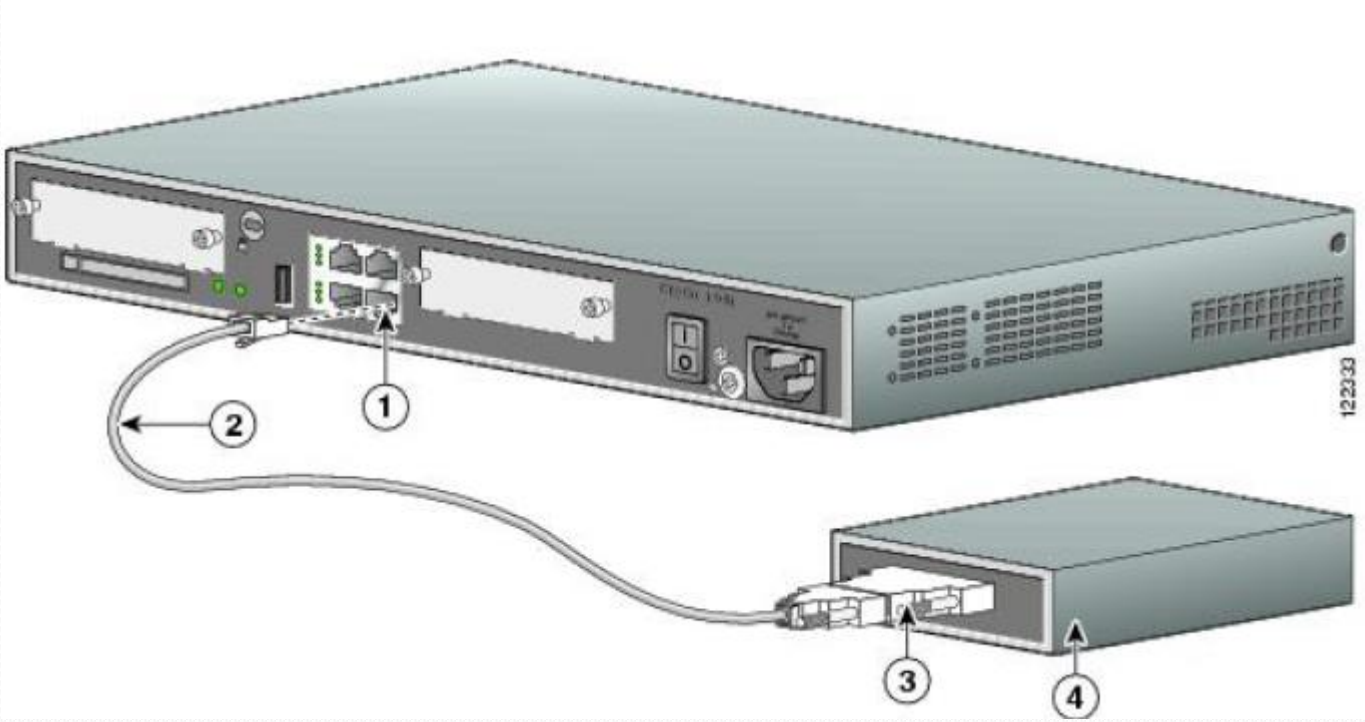
Line Password

```
Gates(config)# line console 0
Gates(config)# password cisco
Gates(config)# login
```

Aux Port Password

```
Gates(config)# line aux 0
Gates(config)# password cisco
Gates(config)# login
```

Connecting to Aux Port



1	Aux port (RJ-45)	3	DB-9-to-DB-25 modem adapter
2	Light blue console cable	4	Modem

Configuring a Telnet Password

- A password must be set on one or more of the virtual terminal (VTY) lines for users to gain remote access to the router using Telnet.
- Typically Cisco routers support five VTY lines numbered 0 through 4.

Telnet Password

```
Gates(config)# line vty 0 4
Gates(config)# password cisco
Gates(config)# login
```

Encrypting Passwords

- Only the enable secret password is encrypted by default
- Need to manually configure the user-mode and enable passwords for encryption
- To manually encrypt your passwords, use the service password-encryption command

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#service password-encryption
```

Disable Passwords

Gates(config)# no enable password

Gates(config)# no enable secret

For the Console

Gates(config)# line con 0

Gates(config)# no password

Gates(config)# line vty 0 4

Gates(config)# no password

Routing

Objectives

- Upon completion of this chapter, you will be able to complete the following tasks:
  - Distinguish the use and operation of static and dynamic routes
  - Configure and verify a static route
  - Identify how distance vector IP routing protocols such as RIP and IGRP operate on Cisco routers
  - Enable Routing Information Protocol (RIP)
  - Enable Interior Gateway Routing Protocol (IGRP)
  - Verify IP routing with show and debug commands

Routing

- The process of transferring data from one local area network to another
- Layer 3 devices
- Routed protocol Enables to forward packet from one router to another – Ex – IP, IPX
- Routing protocol sends and receives routing information packets to and from other routers – Ex -RIP, OSPF , IGRP
- Routing protocols gather and share the routing information used to maintain and update routing tables.
- That routing information is in turn used to route a routed protocol to its final destination

Routing

From

Raj

House #213, 4th Street

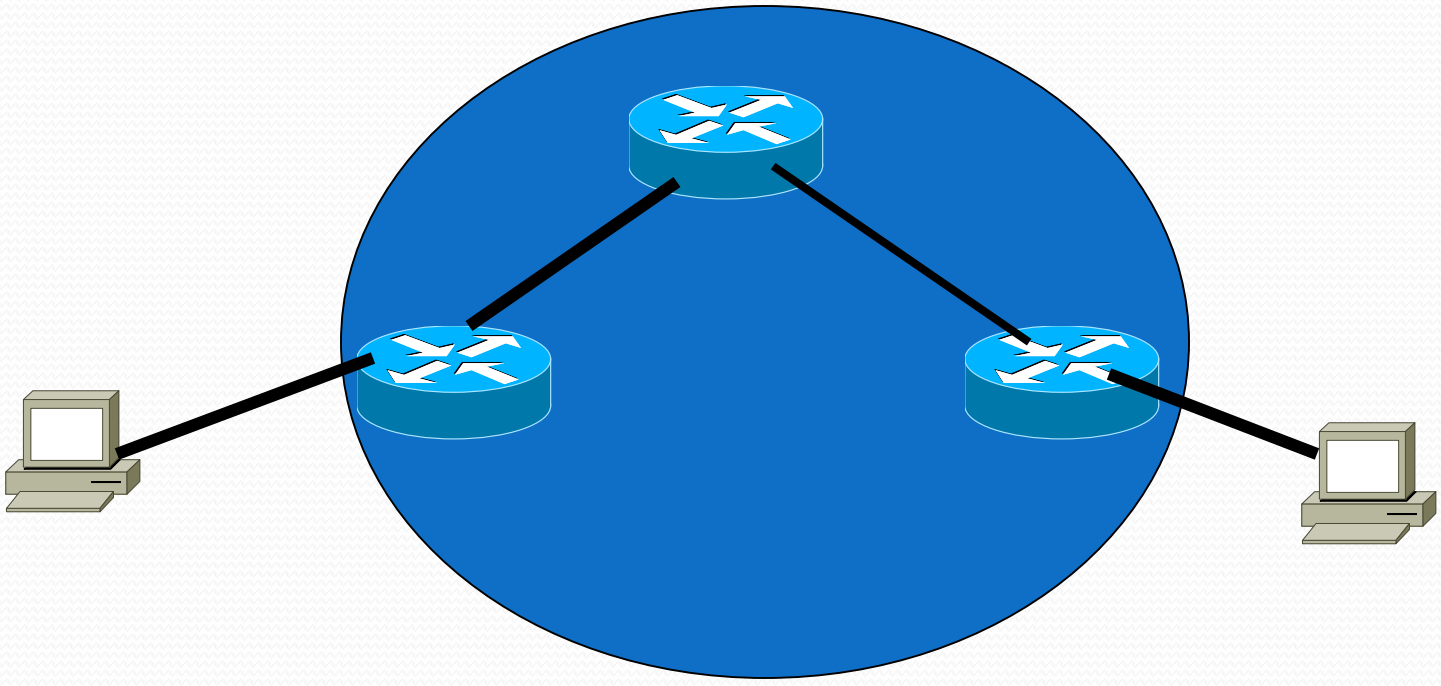
Jayanagar, Bangalore

To

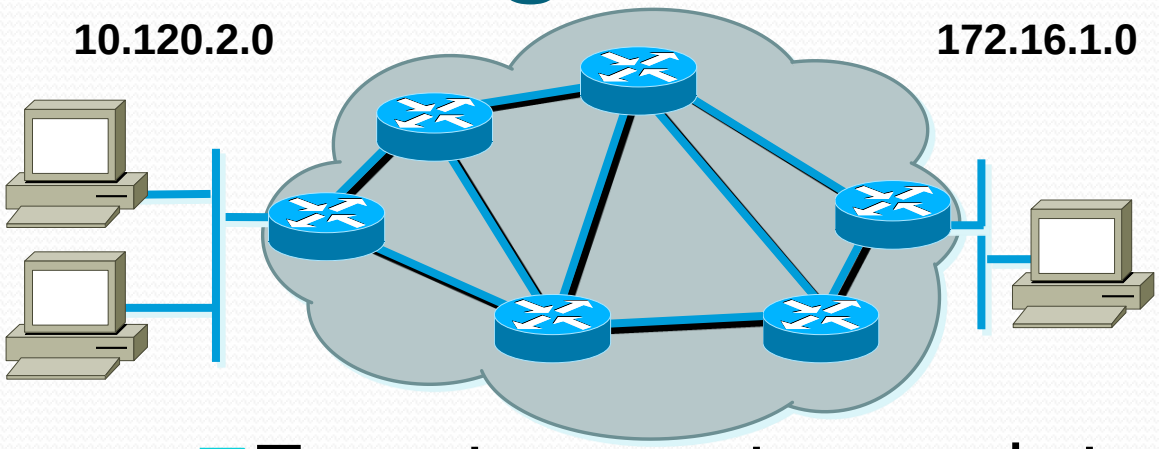
Ram

House #452, 2nd Street

Dadar, Mumbai

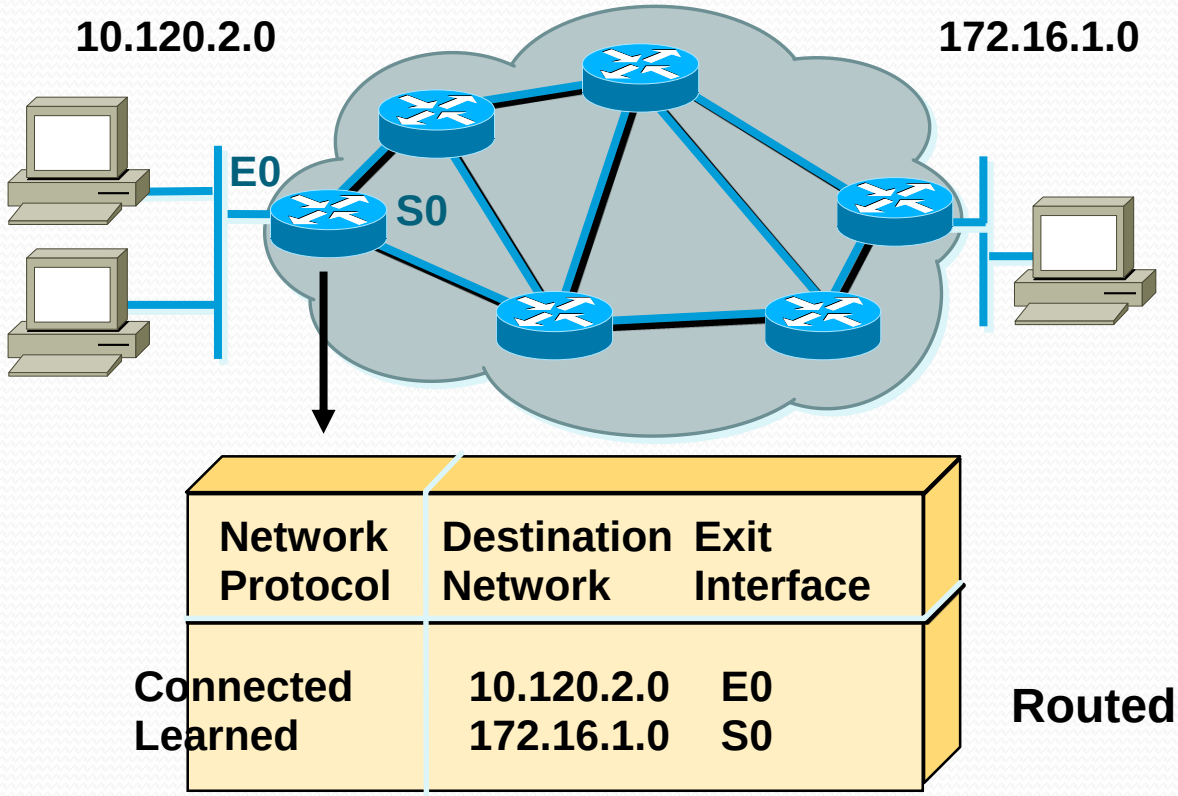


What is Routing?



- To route, a router needs to know:
  - Destination addresses
  - Sources it can learn from
  - Possible routes
  - Best route

What is Routing? (cont.)

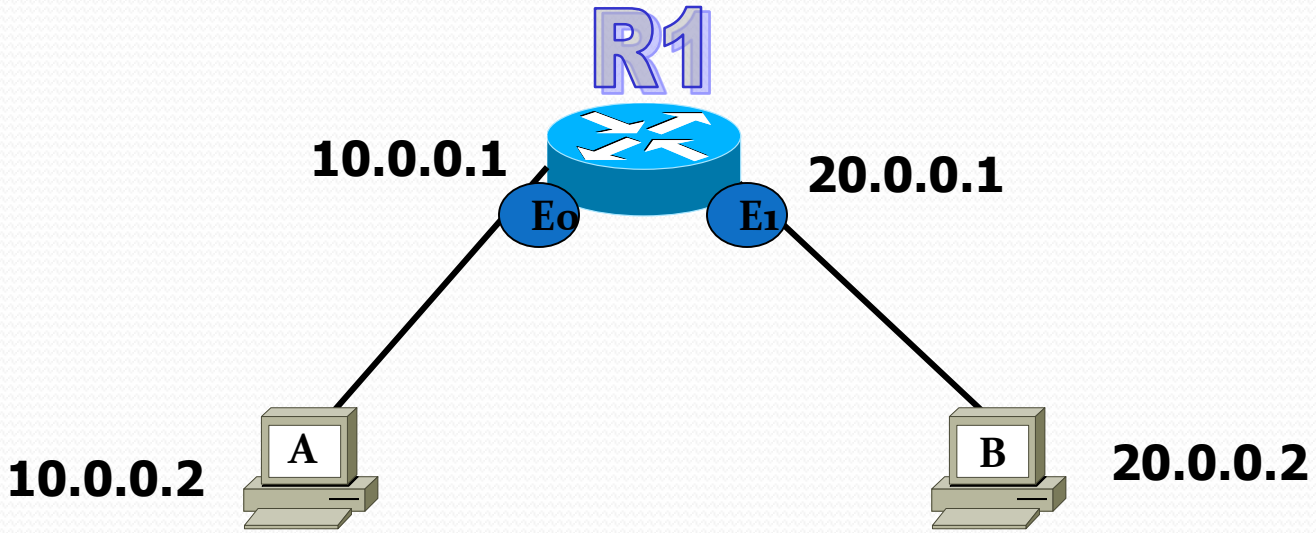


Routers must learn destinations that are not directly connected

Route Types

- Static routing - network administrator configures information about remote networks manually. They are used to reduce overhead and for security.
- Dynamic routing - information is learned from other routers, and routing protocols adjust routes automatically.
- Because of the extra administrative requirements, static routing does not have the scalability of dynamic routing.

IP Routing Process



- Step-by-step what happens when Host A wants to communicate with Host B on a different network
- A user on Host A pings Host B's IP address.

IP Routing

- The different types of routing are:
  - Static routing
  - Default routing
  - Dynamic routing

Static Routes

- **Benefits**
  - No overhead on the router CPU
  - No bandwidth usage between routers
  - Adds security
- **Disadvantage**
  - Administrator must really understand the internetwork
  - If a network is added to the internetwork, the administrator has to add a route to it on all routers
  - Not feasible in large networks

Static Route Configuration

```
R1(config)#ip route network   [mask]
{address | interface}[distance] [permanent]
```

- **R1(config)# iproute DestAddress SNM Nexthop address**

Static Route Configuration

ip route [*destination_network*] [*mask*] [*next-hop_address or exitinterface*] [*administrative_distance*] [permanent

- **ip route** The command used to create the static route.
- **destination_network** The network you're placing in the routing table.
- **mask** The subnet mask being used on the network.
- **next-hop_address** The address of the next-hop router that will receive the packet and forward it to the remote network. This is a router interface that's on a directly connected network.
- **exitinterface** You can use it in place of the next-hop address if you want, but it's got to be on a point-to-point link, such as a WAN
- **administrative_distance** By default, static routes have an administrative distance of 1 (or even 0 if you use an exit interface instead of a next-hop address)
- **permanent** If the interface is shut down, or the router can't communicate to the next-hop router, the route will automatically be discarded from the routing table. Choosing the permanent option keeps the entry in the routing table no matter what happens.

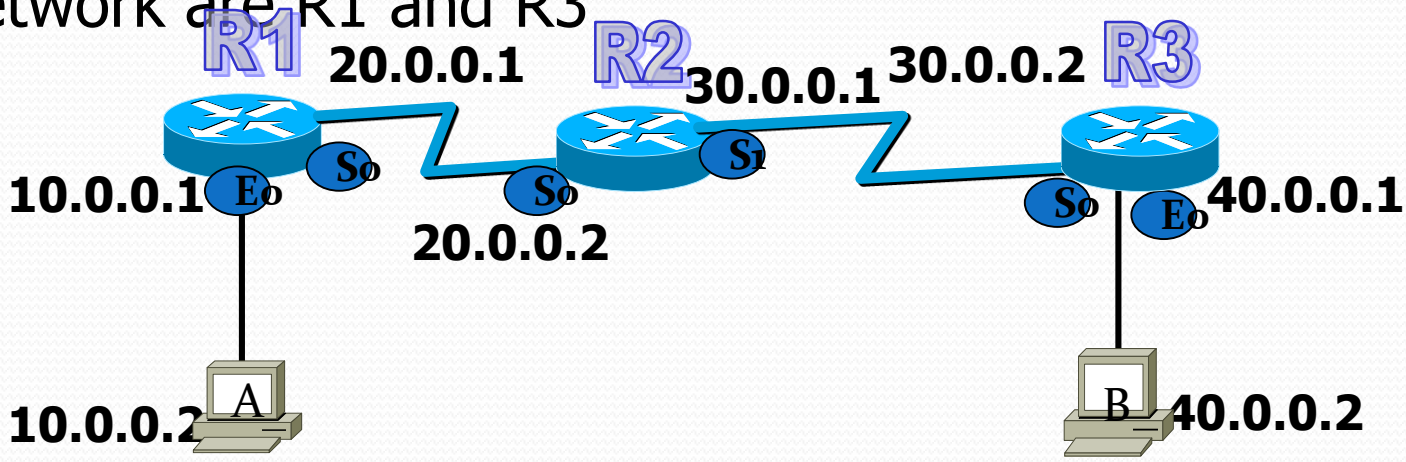
```
R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2
```

Verifying Static Route Configuration

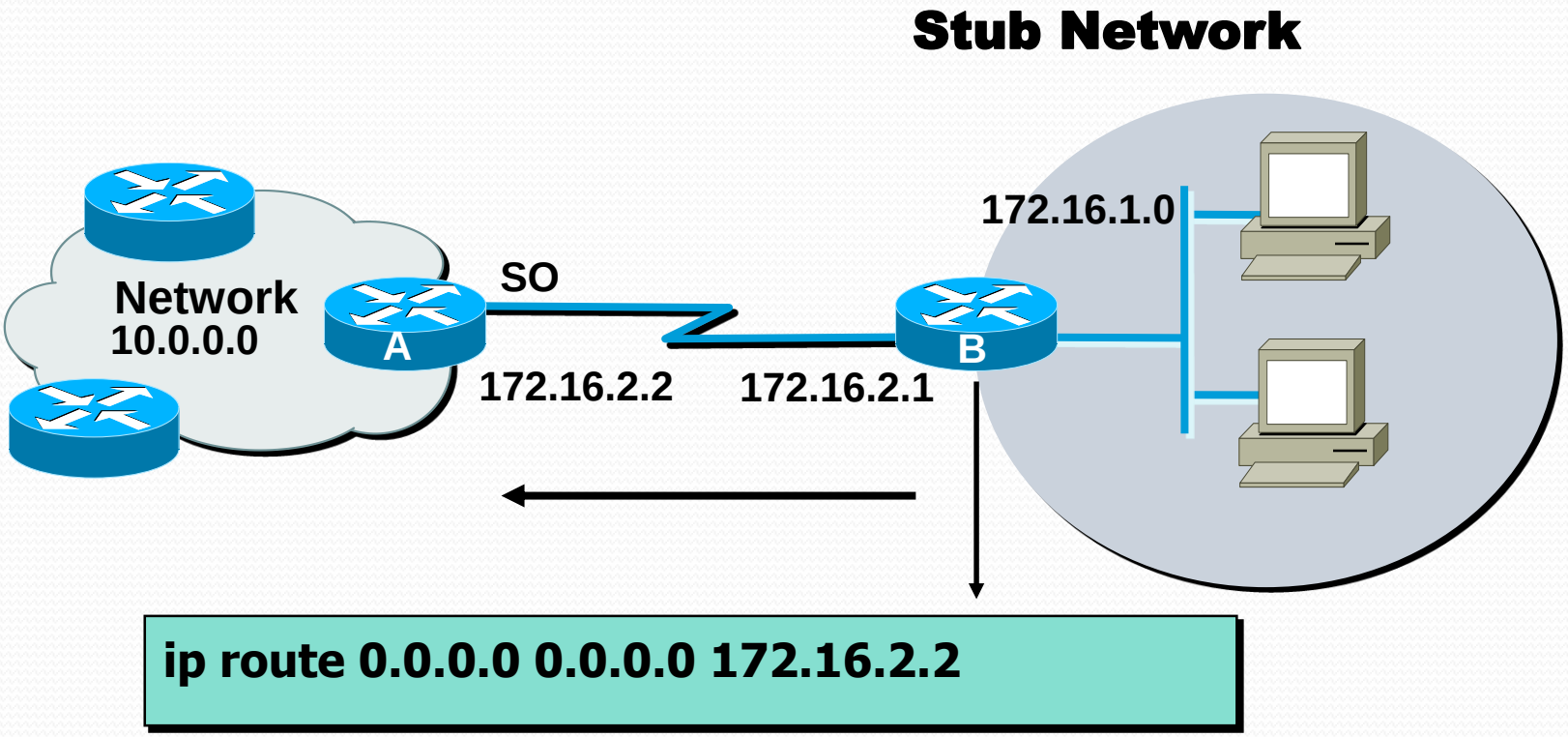
- After static routes are configured it is important to verify that they are present in the routing table and that routing is working as expected.
- The command **show running-config** is used to view the active configuration in RAM to verify that the static route was entered correctly.
- The **show ip route** command is used to make sure that the static route is present in the routing table.

Default Routes

- Can only use default routing on stub networks
- Stub networks are those with only one exit path out of the network
- The only routers that are considered to be in a stub network are R1 and R3



Default Routes



- This route allows the stub network to reach all known networks beyond router A.

Configuring Default Routes

Default routes are used to route packets with destinations that do not match any of the other routes in the routing table.

A default route is actually a special static route that uses this format:

ip route 0.0.0.0 0.0.0.0 [*next-hop-address* | *outgoing interface*]

This is sometimes referred to as a "Quad-Zero" route.

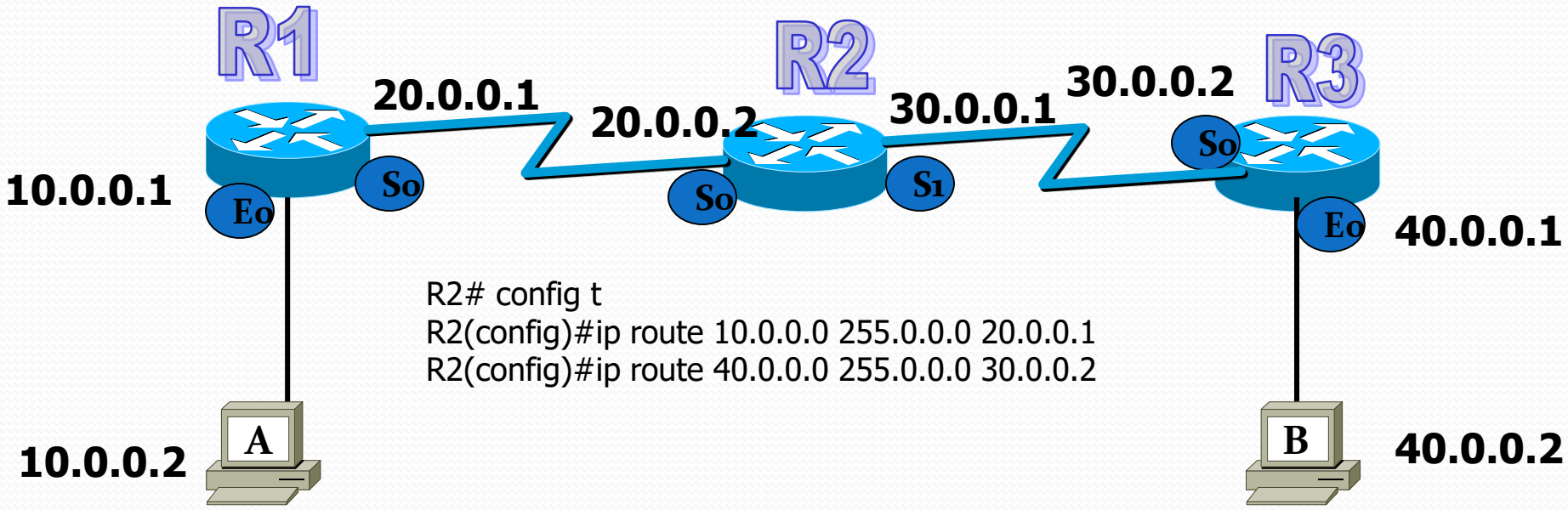
Example using next hop address:

Router(config)#**ip route 0.0.0.0 0.0.0.0 172.16.4.1**

Example using the exit interface:

Router(config)#**ip route 0.0.0.0 0.0.0.0 s0/0**

LAB – Static Route Configuration

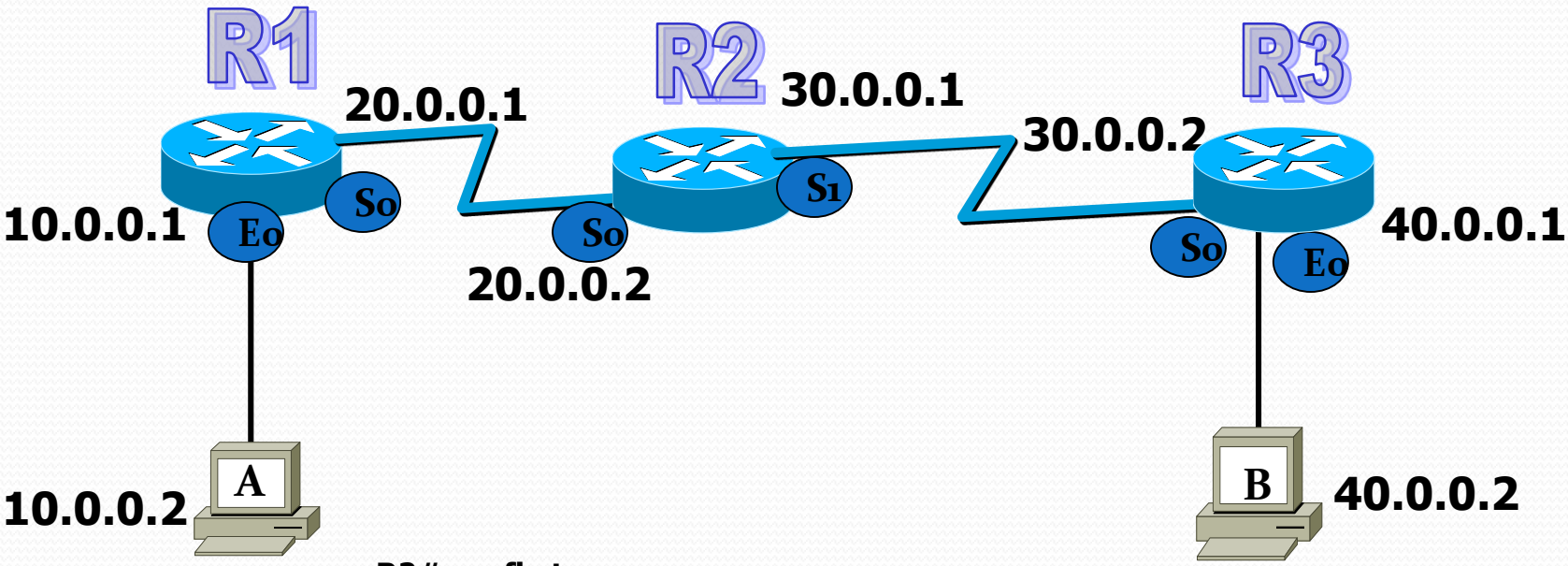


R2# config t
R2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
R2(config)#ip route 40.0.0.0 255.0.0.0 30.0.0.2

R1# config t
R1(config)#ip route 30.0.0.0 255.0.0.0 20.0.0.2
R1(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.2

R3# config t
R3(config)#ip route 10.0.0.0 255.0.0.0 30.0.0.1
R3(config)#ip route 20.0.0.0 255.0.0.0 30.0.0.1

Default Route LAB Configuration



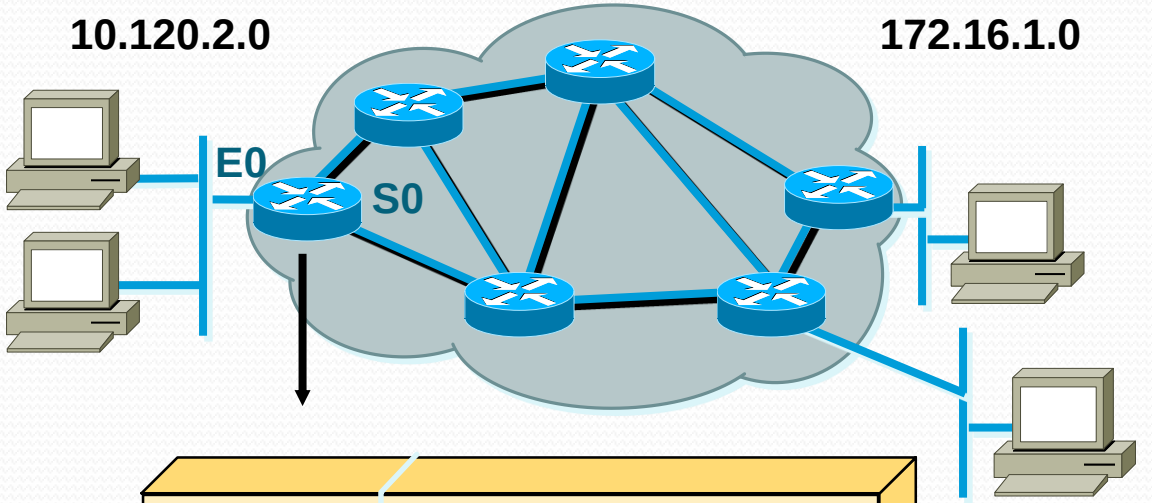
R2# config t
R2(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1
R2(config)#ip route 40.0.0.0 255.0.0.0 30.0.0.2

R1# config t
R1(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2

R3# config t
R3(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.1

What is a Routing Protocol?

- Routing protocols are used between routers to determine paths and maintain routing tables.
- Once the path is determined a router can route a routed protocol.



Network Protocol	Destination Network	Exit Interface
Connected	10.120.2.0	E0
RIP	172.16.1.0	S0
IGRP	172.17.3.0	S1

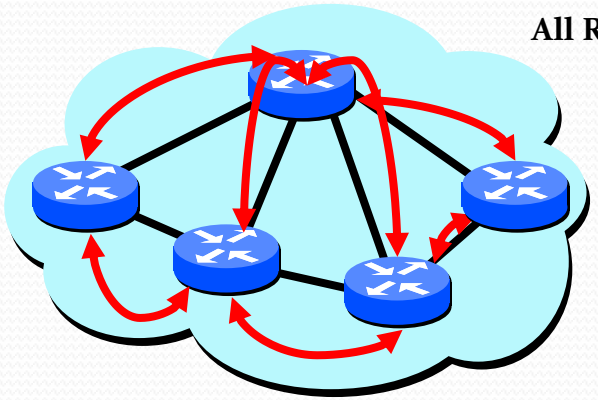
Routed Protocol: IP
Routing protocol: RIP, IGRP

Routing Categories

Autonomous System

- An Autonomous System (AS) is a group of IP networks, which has a single and clearly defined routing policy.
- Group of routers which can exchange updates
- AS are identified by numbers

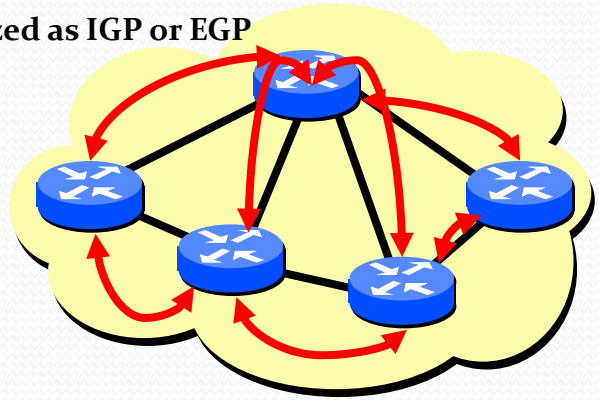
All Routing protocols are categorized as IGP or EGP



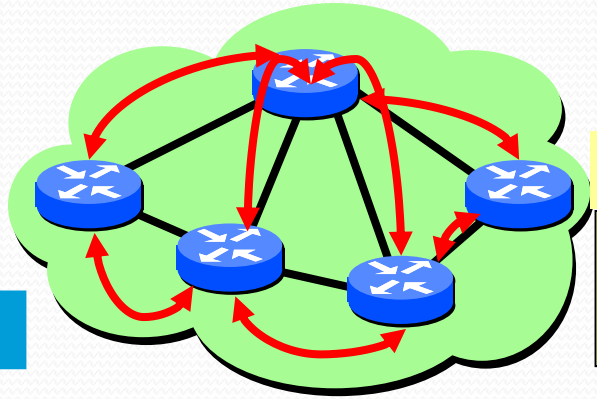
AS 1000

EGP

Exterior Gateway Protocols are used for routing between Autonomous Systems



AS 3000



AS 2000

IGP

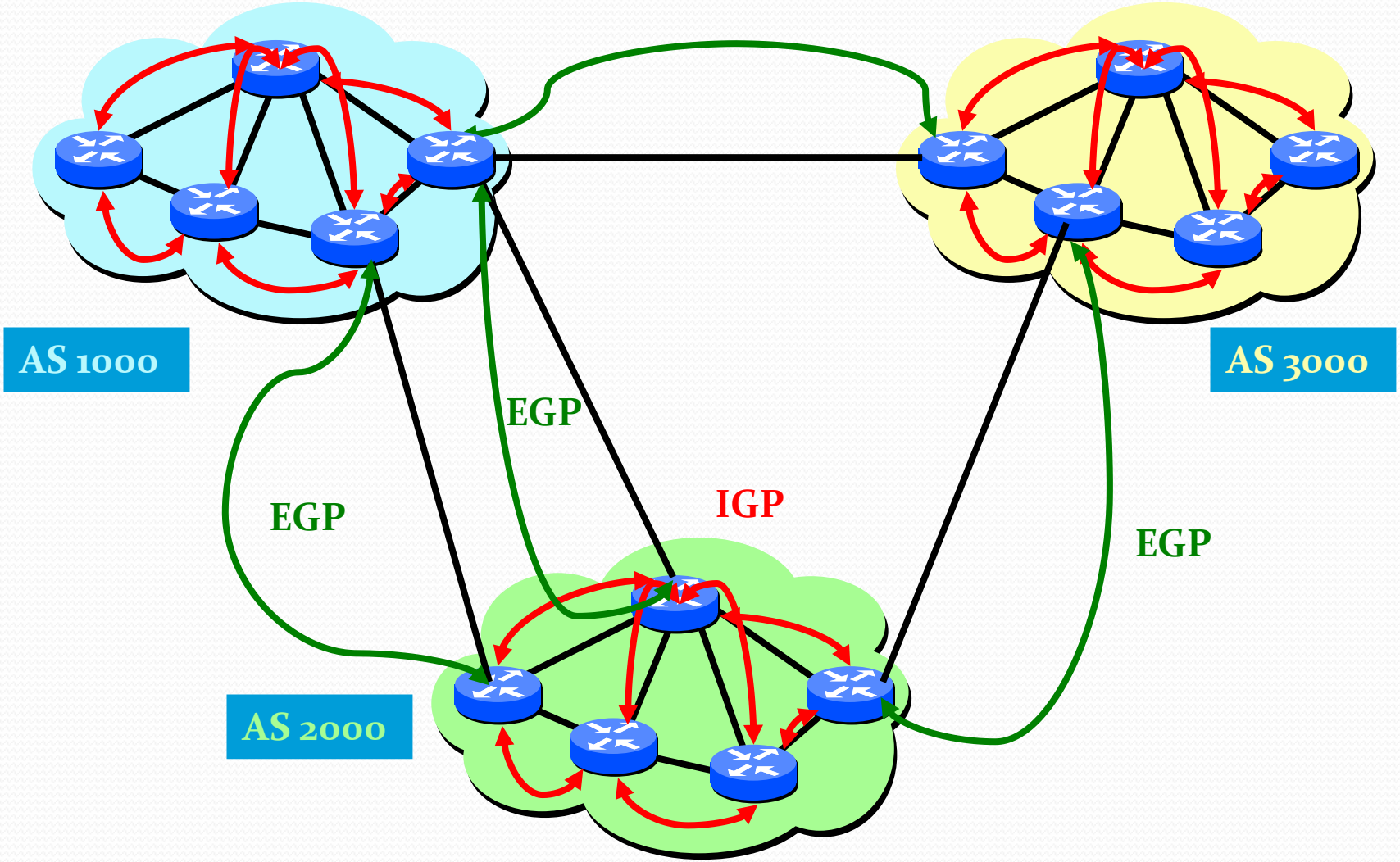
Interior Gateway Protocols are used for routing decisions within an Autonomous System.

Routing Categories

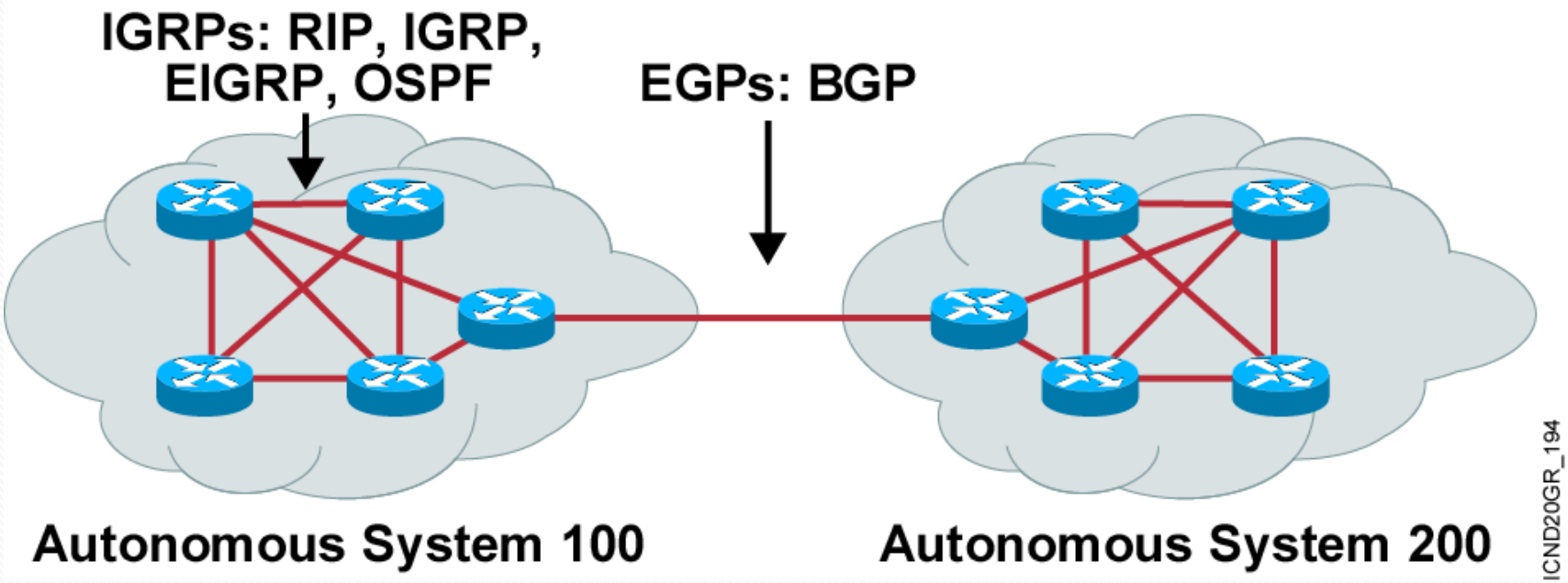
Interior Gateway Protocol (IGP)

Exterior Gateway Protocol (EGP)

Interior Gateway Protocol (IGP)



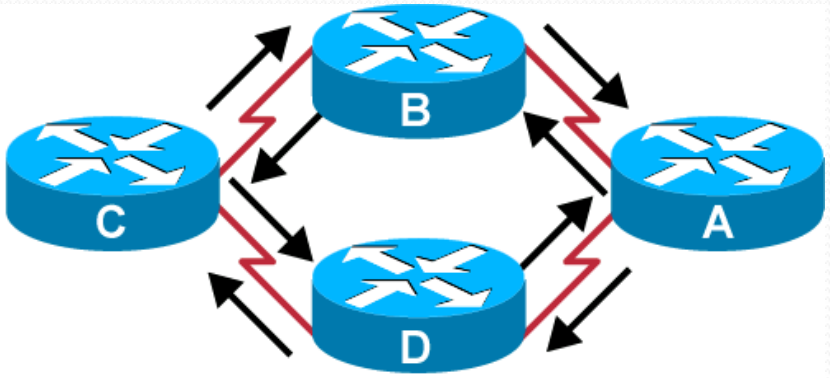
Autonomous Systems: Interior or Exterior Routing Protocols



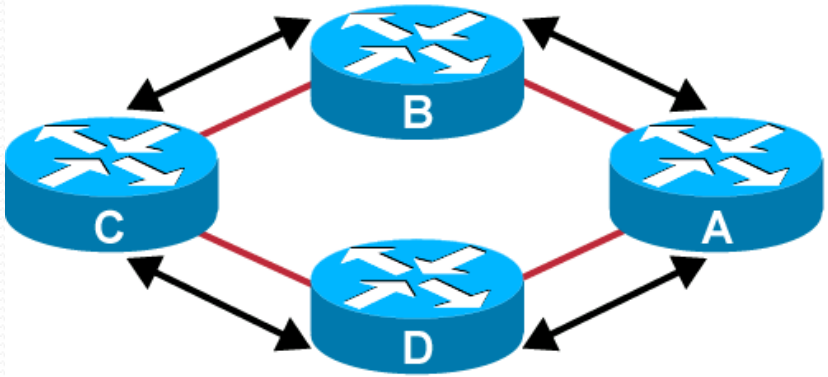
- An autonomous system is a collection of networks under a common administrative domain.
- IGPs operate within an autonomous system.
- EGPs connect different autonomous systems.

Types or Classes of Routing Protocols

Distance Vector



Hybrid Routing



Link State

ICND20GR_196

Types or Classes of Routing Protocols

- Distance Vector
  - RIP V1
  - IGRP
  - RIP V2
- Link state
  - OSPF
- Hybrid
  - EIGRP

Classful Routing Overview

- Classful routing protocols do not include the subnet mask with the route advertisement.
- Within the same network, consistency of the subnet masks is assumed.
- Summary routes are exchanged between foreign networks.
- Examples of classful routing protocols:
  - RIP Version 1 (RIPv1)
  - IGRP

Classless Routing Overview

- Classless routing protocols include the subnet mask with the route advertisement.
- Classless routing protocols support variable-length subnet masking (VLSM) and subnetting
- Examples of classless routing protocols:
  - RIP Version 2 (RIPv2)
  - EIGRP
  - OSPF
  - IS-IS

OSPF

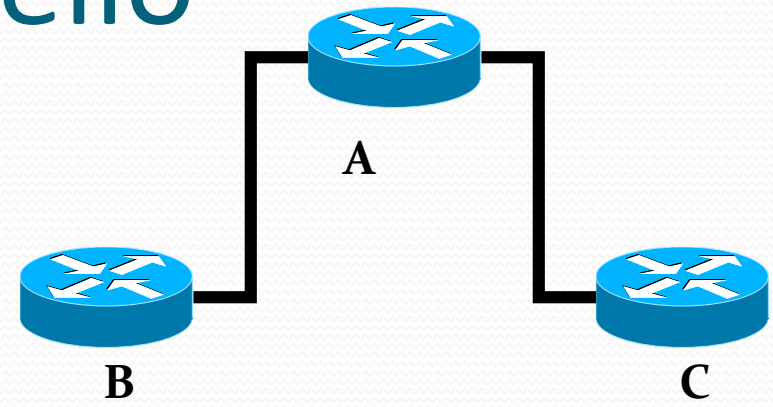
Open Shortest Path First (OSPF)

- OSPF is an open standards routing protocol
- This works by using the Dijkstra algorithm
- OSPF provides the following features:
  - Minimizes routing update traffic
  - Allows scalability (e.g. RIP is limited to 15 hops)
  - Has unlimited hop count
  - Supports VLSM/CIDR
  - Allows multi-vendor deployment (open standard)

Link State

- There are two types of Packets
  - Hello
  - LSA's

OSPF Hello



- When router A starts it send Hello packet – uses 224.0.0.5
- Hello packets are received by all neighbors
- B will write A's name in its neighbor table
- C also process the same way

"Hello" Packets

- Small frequently issued packets
- Discover neighbours and negotiate "adjacencies"
- Verify continued availability of adjacent neighbours
- Hello packets and Link State Advertisements (LSAs) build and maintain the topological database
- Hello packets are addressed to 224.0.0.5.

Link State Advertisement (LSA)

- An OSPF data packet containing link state and routing information that is shared among OSPF routers
- LSAs are shared only with routers with whom it has formed adjacencies
- LSA packets are used to update and maintain the topology database.

Link State

- There are three type of tables
  - Neighbor
  - Topology
  - Routing

Tables

- **Neighbor**
  - Contain information about the neighbors
  - Neighbor is a router which shares a link on same network
  - Another relationship is adjacency
  - Not necessarily all neighbors
  - LSA updates are only when adjacency is established

Tables

- **Topology**
  - Contain information about all network and path to reach any network
  - All LSA's are entered in to topology table
  - When topology changes LSA's are generated and send new LSA's
  - On topology table an algorithm is run to create a shortest path, this algorithm is known as SPF or dijkstra algorithm

Tables

- **Routing Table**
  - Also knows as forwarding database
  - Generated when an algorithm is run on the topology database
  - Routing table for each router is unique

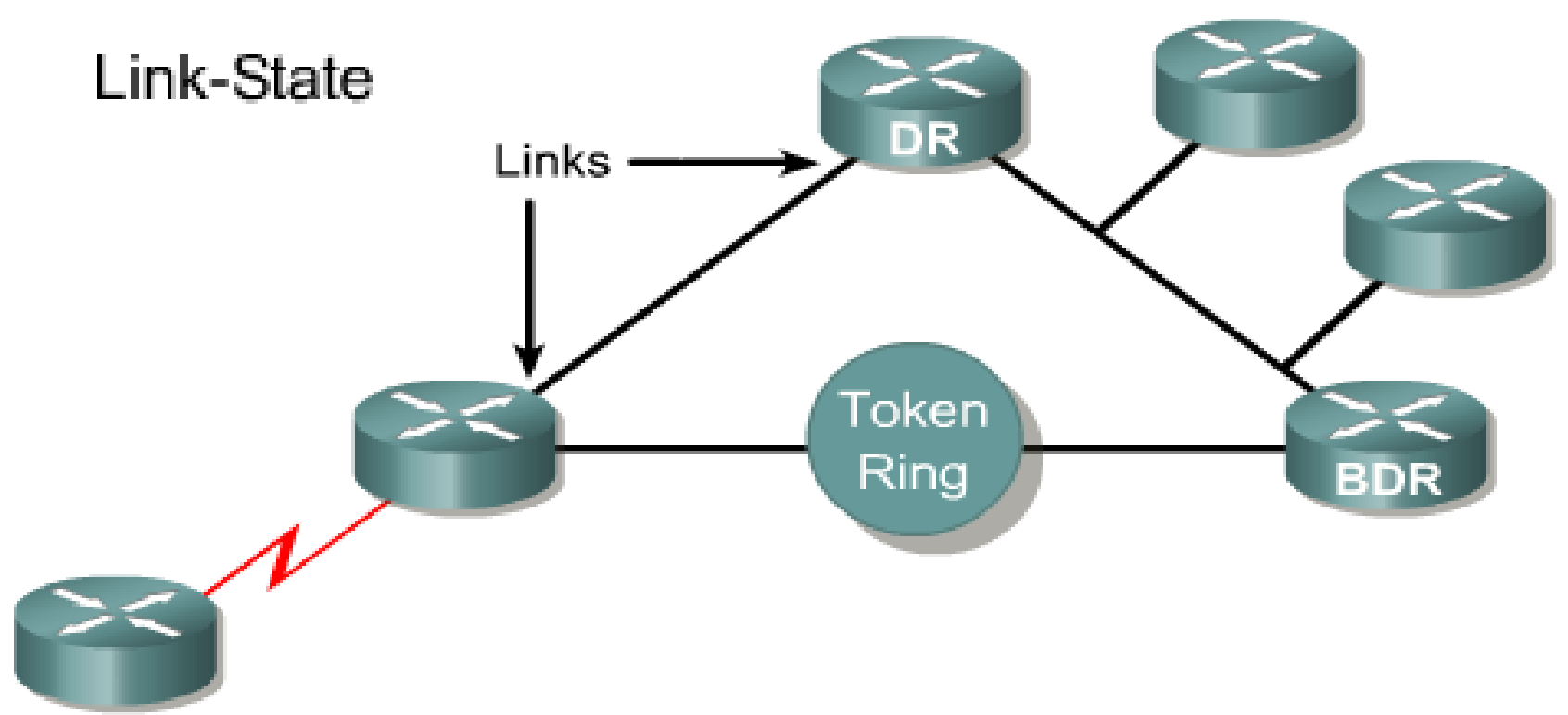
OSPF Terms

- Link
- Router ID
- Neighbours
- Adjacency
- OSPF Area
- Backbone area
- Internal routers
- Area Border Router (ABR)
- Autonomous System Boundary Router (ASBR)

Link

- A network or router interface assigned to a given network
- Link (interface) will have "state" information associated with it
  - Status (up or down)
  - IP Address
  - Network type (e.g. Fast Ethernet)
  - Bandwidth
  - Addresses of other routers attached to this interface

OSPF Term: Link State



- **Status of a link between two routers**
- **Information is shared between directly connected routers.**
- **This information propagates throughout the network unchanged and is also used to create a shortest path first (SPF) tree.**

Router ID

- The Router ID (RID) is an IP address used to identify the router
- Cisco chooses the Router ID by using the highest IP address of all configured loopback interfaces
- If no loopback interfaces are configured with addresses, OSPF will choose the highest IP address of all active physical interfaces.
- You can manually assign the router ID.
- The RID interface MUST always be up, therefore loopbacks are preferred

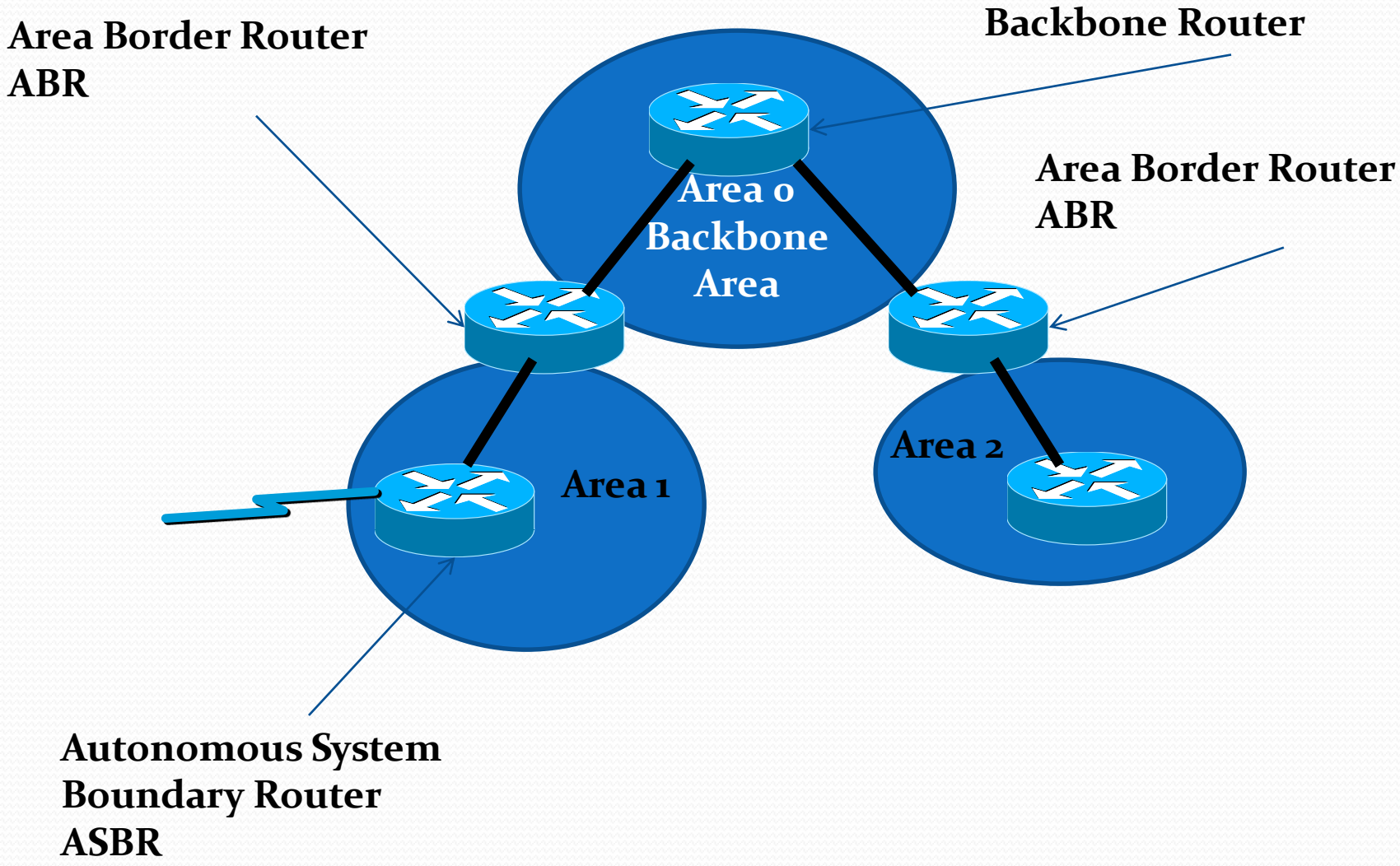
Neighbours

- Neighbours are two or more routers that have an interface on a common network
  - E.g. two routers connected on a serial link
  - E.g. several routers connected on a common Ethernet or Frame relay network
- Communication takes place between / among neighbours
- neighbours form "adjacencies"

Adjacency

- A relationship between two routers that permits the direct exchange of route updates
- Not all neighbours will form adjacencies
  - This is done for reasons of efficiency – more later

OSPF Design


Area Border Router
ABR
Backbone Router
Area Border Router
ABR
Area 0
Backbone
Area
Area 1
Area 2
Autonomous System
Boundary Router
ASBR

OSPF Areas

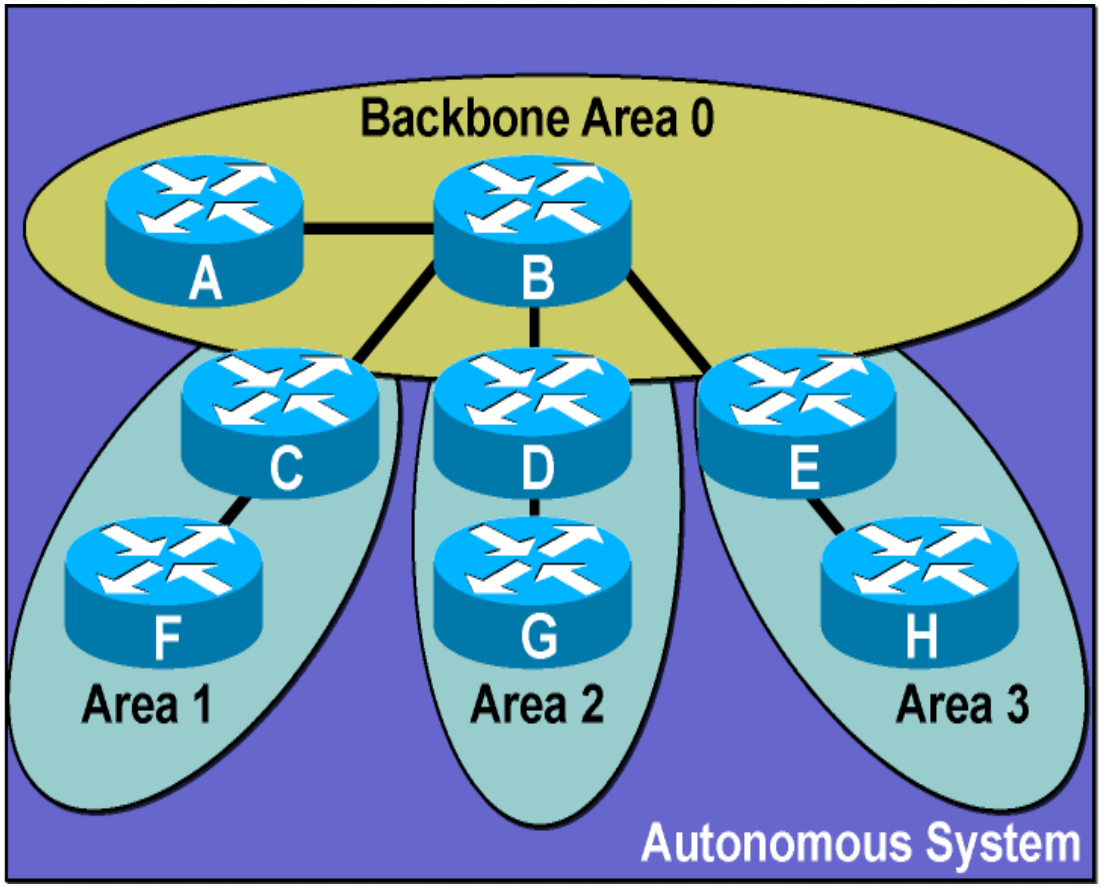
- An OSPF area is a grouping of contiguous networks and routers
  - Share a common ***area ID***
- A router can be a member of more than one area (area border router)
- All routers in the same area have the same topology database
- When multiple areas exist, there must always be an area 0 (the backbone) to which other areas connect

Why areas?

- Decreases routing overhead
  - Compare to multiple smaller broadcast domains instead of one large one
- Speeds convergence
- Confines network instability (e.g. route "flapping") to single area of the network
- Adds considerably to the complexity of setting up OSPF

Area Terminology

- Routers A and B are backbone routers.
- Backbone routers make up area 0.
- Routers C, D, and E are known as Area Border Routers (ABRs).
- ABRs attach all other areas to area 0.



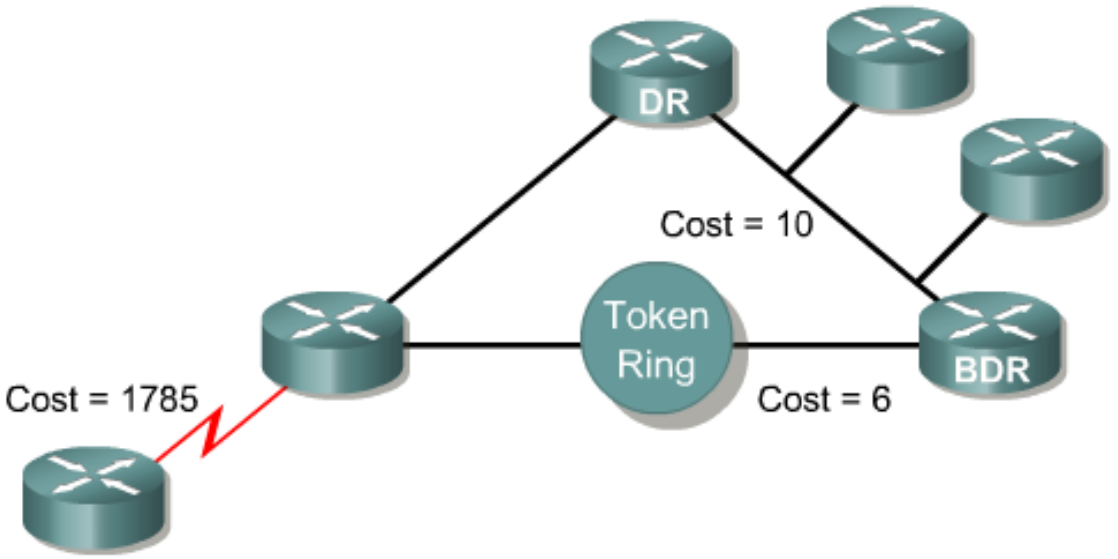
Path Calculation

- Changes to the topological database of a router trigger a recalculation to re-establish the best route(s) to known networks
  - Uses the SPF (shortest path first) algorithm developed by a computer scientist named Dijkstra
  - This is done by each individual router using its detailed "knowledge" of the whole network
  - Leads to rapid and accurate convergence
  - Based on detailed knowledge of every link in the area and the OSPF "cost" of each
  - builds an ***OSPF tree*** with itself at the route

Terminology: Cost

- Various criteria can be selected by the administrator to determine the metric
  - Usually, OSPF cost=10^8/bandwidth

Do not forget to configure the **bandwidth`** command on serial links to ensure correct default OSPF cost



Cost: The value assigned to a link. Rather than hops, link-state protocols assign a cost to a link, which is based on the bandwidth of the link (transmission speed).

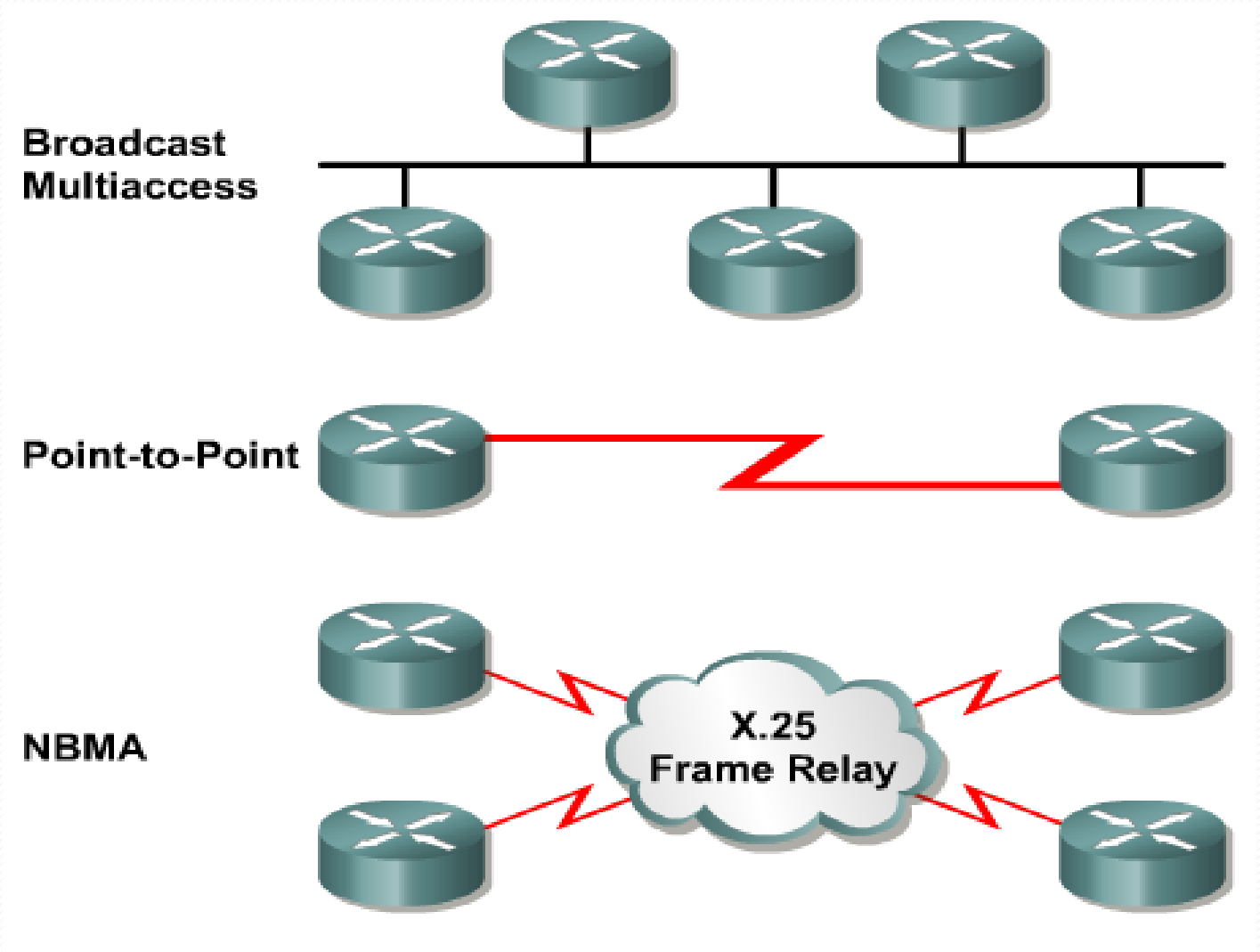
Pros and Cons

- Note that OSPF is a more sophisticated routing protocol
  - Converges rapidly and accurately
  - Can use a metric calculation that effectively selects the "best" route(s) primarily based on bandwidth, although an OSPF cost can be administratively assigned
- Use of OSPF requires
  - More powerful routing hardware
  - More detailed knowledge by the administrator, especially when large multi-area networks are used

Types of Neighbors

- OSPF can be defined for three type of neighbors
  - Broadcast Multi Access (BMA) ex- Ethernet
  - Point to Point
  - Non-Broadcast Multi Access (NBMA)

OSPF Network Types



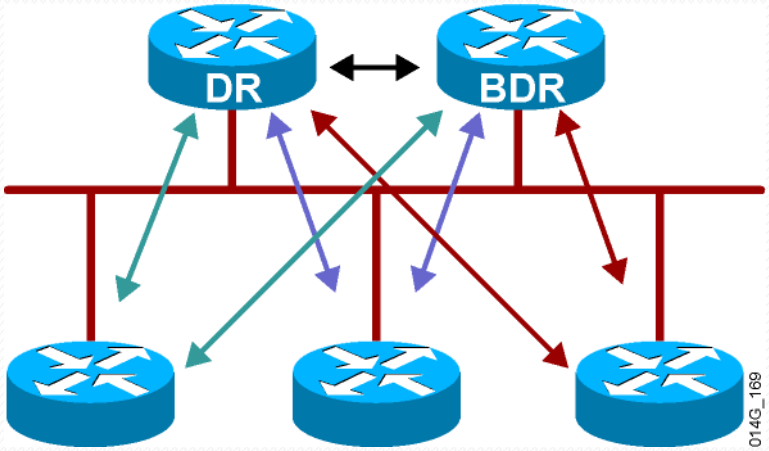
Adjacencies

- Point to Point all routers form adjacencies
- BMA & NBMA one router is elected as DR
- DR establish adjacency with every neighbor router
- LSA updates are exchanged only to DR
- DR is the router which has highest priority
- All CISCO routers has priority 1
- If priority is same then router id is seen
- The RID is highest IP address of all interfaces

Point-to-Point Links

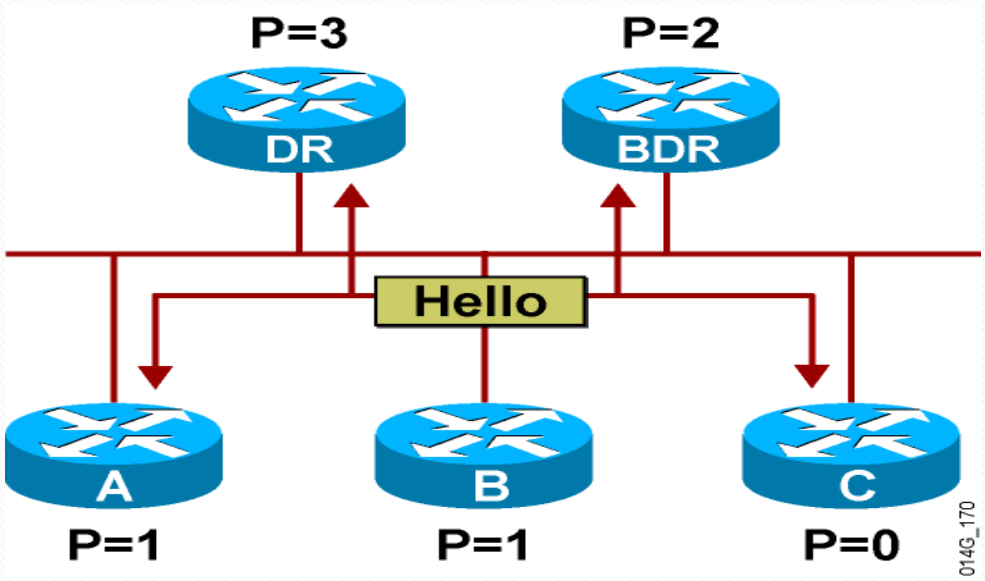
- Usually a serial interface running either PPP or HDLC
- No DR or BDR election required
- OSPF autodetects this interface type
- OSPF packets are sent using multicast 224.0.0.5
- All routers form adjacencies

Multi-access Broadcast Network



- Generally LAN technologies like Ethernet and Token Ring
- DR and BDR selection required
- All neighbor routers form full adjacencies with the DR and BDR only
- Packets to the DR use 224.0.0.6
- Packets from DR to all other routers use 224.0.0.5

Electing the DR and BDR



- Hello packets are exchanged via IP multicast.
- The router with the highest priority is selected as the DR.
- If Priority is same then Router ID is seen
- Use the OSPF router ID as the tie breaker.

OSPF Summary

- AD =110
- Hop count is unlimited
- Metric = Cost = 10^8/BW
- Classless, VLSM
- Load balance up to four routers
- Require more processing power

Basic OSPF Configuration

```
Router(config)# router ospf 1
```

- The number 1 in this example is a ***process-id #*** that begins an OSPF process in the router
  - More than one process can be launched in a router, but this is rarely necessary
  - Usually the same process-id is used throughout the entire network, but this is not required
  - The process-id # can actually be any value from 1 to "very large integer"
  - The process-id # cannot be ZERO
  - This is NOT the same as the AS# used in IGRP and EIGRP

Configuring OSPF Areas

- After identifying the OSPF process, you need to identify the interfaces that you want to activate OSPF communications

Lab_A#config t

Lab_A(config)#router ospf 1

Lab_A(config-router)#network 10.0.0.0 0.255.255.255

area ?

<0-4294967295> OSPF area ID as a decimal value

A.B.C.D OSPF area ID in IP address format

Lab_A(config-router)#network 10.0.0.0 0.255.255.255

area 0

- Every OSPF network must have an area 0 (the backbone area) to which other areas connect
  - So in a multiple area network, there must be an area 0
  - The wildcard mask represents the set of hosts supported by the network and is really just the inverse of the subnet mask.

OSPF Configuration

- OSPF Process ID number is irrelevant. It can be the same on every router on the network
- The arguments of the network command are the network number (10.0.0.0) and the wildcard mask (0.255.255.255)
- Wildcards - A 0 octet in the wildcard mask indicates that the corresponding octet in the network must match exactly
- A 255 indicates that you don't care what the corresponding octet is in the network number
- A network and wildcard mask combination of 1.1.1.1 0.0.0.0 would match 1.1.1.1 only, and nothing else.
- The network and wildcard mask combination of 1.1.0.0 0.0.255.255 would match anything in the range 1.1.0.0–1.1.255.255

OSPF and Loopback Interfaces

- Configuring loopback interfaces when using the OSPF routing protocol is important
- Cisco suggests using them whenever you configure OSPF on a router
- *Loopback interfaces* are logical interfaces, which are virtual, software-only interfaces; they are not real router interfaces
- Using loopback interfaces with your OSPF configuration ensures that an interface is always active for OSPF processes.
- The highest IP address on a router will become that router's RID
- The RID is used to advertise the routes as well as elect the DR and BDR.
- If you configure serial interface of your router with highest IP Address this Address becomes RID of t is the RID of the router because e router
- If this interface goes down, then a re-election must occur
- It can have an big impact when the above link is flapping

Configuring Loopback Interfaces

R1#**config t**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#**int loopback 0**

R1(config-if)#**ip address 172.16.10.1 255.255.255.255**

R1(config-if)#**no shut**

R1(config-if)#**^Z**

R1#

Verifying OSPF Operation

```
Router#
show ip protocols
```

- **Verifies the configured IP routing protocol processes, parameters and statistics**

```
Router#
show ip route ospf
```

- **Displays all OSPF routes learned by the router**

```
Router#
show ip ospf interface
```

- **Displays the OSPF router ID, area ID and adjacency information**

Verifying OSPF Operation (Cont.)

```
Router#
show ip ospf
```

- **Displays the OSPF router ID, timers, and statistics**

```
Router#
show ip ospf neighbor [detail]
```

- **Displays information about the OSPF neighbors, including Designated Router (DR) and Backup Designated Router (BDR) information on broadcast networks**

The show ip route ospf Command

```
RouterA# show ip route ospf

 Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile,
        B - BGP, D - EIGRP, EX - EIGRP external, O - OSPF,
        IA - OSPF inter area, E1 - OSPF external type 1,
        E2 - OSPF external type 2, E - EGP, i - IS-IS, L1
- IS-IS
        level-1, L2 - IS-IS level-2, * - candidate default

Gateway of last resort is not set
        10.0.0.0 255.255.255.0 is subnetted, 2 subnets
O       10.2.1.0 [110/10] via 10.64.0.2, 00:00:50,
Ethernet0
```

The show ip ospf interface Command

```
RouterA# show ip ospf interface e0

Ethernet0 is up, line protocol is up
  Internet Address 10.64.0.1/24, Area 0
  Process ID 1, Router ID 10.64.0.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 10.64.0.2, Interface address 10.64.0.2
  Backup Designated router (ID) 10.64.0.1, Interface address 10.64.0.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.64.0.2  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

The show ip ospf neighbor Command

```
RouterB# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time     Address         Interface
10.64.1.1       1     FULL/BDR        00:00:31      10.64.1.1       Ethernet0
10.2.1.1        1     FULL/-          00:00:38      10.2.1.1        Serial0
```

show ip ospf neighbor detail

Displays details list of neighbors, their priorities, and their state (for example: init, exstart, or full).

show ip ospf database

Displays the contents of the topological database maintained by the router. The command also shows the router ID and the OSPF process ID. A number of database types can be shown with this command using keywords. Refer to www.cisco.com for details about the keywords.

Setting Priority for DR Election

```
Router(config-if)#
ip ospf priority number
```

- This interface configuration command assigns the OSPF priority to an interface.
- Different interfaces on a router may be assigned different values.
- The default priority is 1. The range is from 0 to 255.
- 0 means the router is a DROTHER; it can't be the DR or BDR.

Administrative Distances

Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

Route Preference

- Route is selected as the best route in the routing table as the best route according to the following crieteria:

1. Route with the longest Prefix match
2. Route with the lower administrative distance
3. Route with the lower metric.

Switching

Layer 2 Switching

- Switching breaks up large collision domains into smaller ones
- Collision domain is a network segment with two or more devices sharing the same bandwidth.
- A hub network is a typical example of this type of technology
- Each port on a switch is actually its own collision domain, you can make a much better Ethernet LAN network just by replacing your hubs with switches

Switching Services

- Unlike bridges that use software to create and manage a filter table, switches use Application Specific Integrated Circuits (ASICs)
- Layer 2 switches and bridges are faster than routers because they don't take up time looking at the Network layer header information.
- They look at the frame's hardware addresses before deciding to either forward the frame or drop it.
- layer 2 switching so efficient is that no modification to the data packet takes place

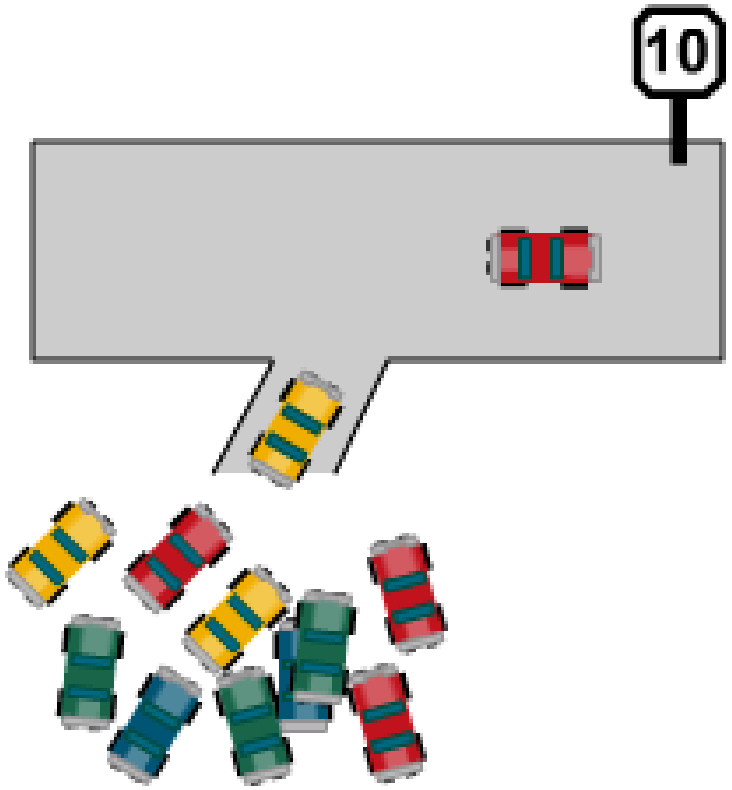
How Switches and Bridges Learn Addresses

Bridges and switches learn in the following ways:

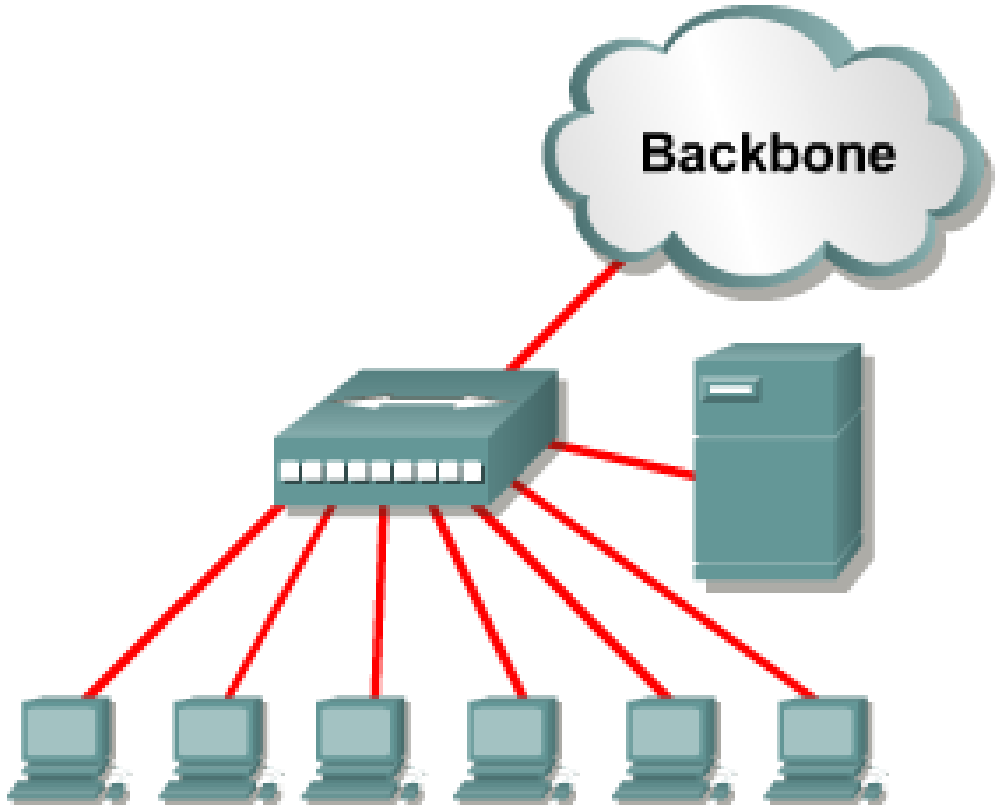
- Reading the source MAC address of each received frame or datagram
- Recording the port on which the MAC address was received.

In this way, the bridge or switch learns which addresses belong to the devices connected to each port.

Ethernet Access with Hubs

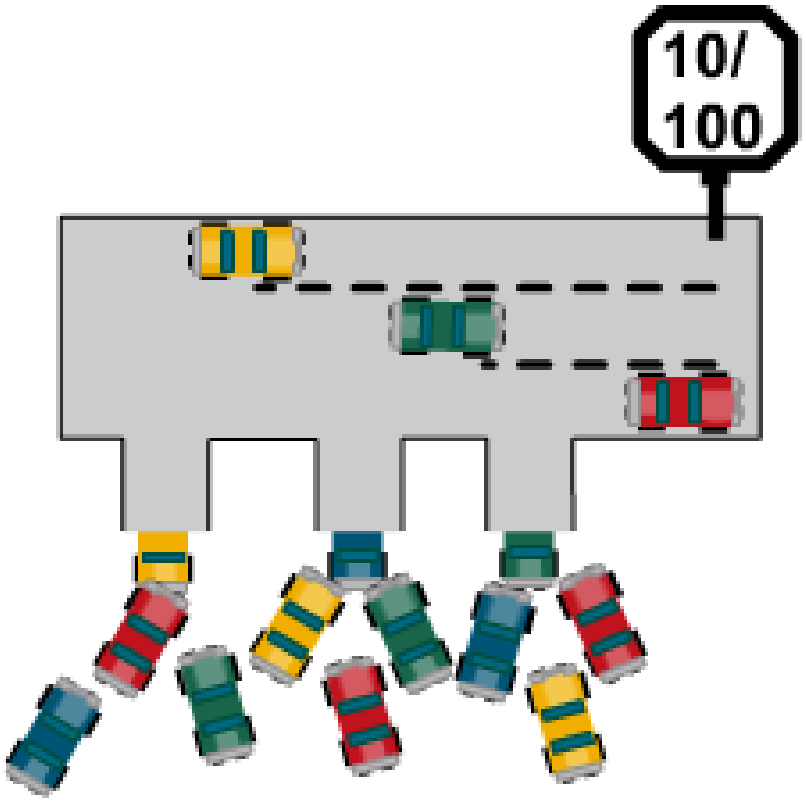


One device sending at a time

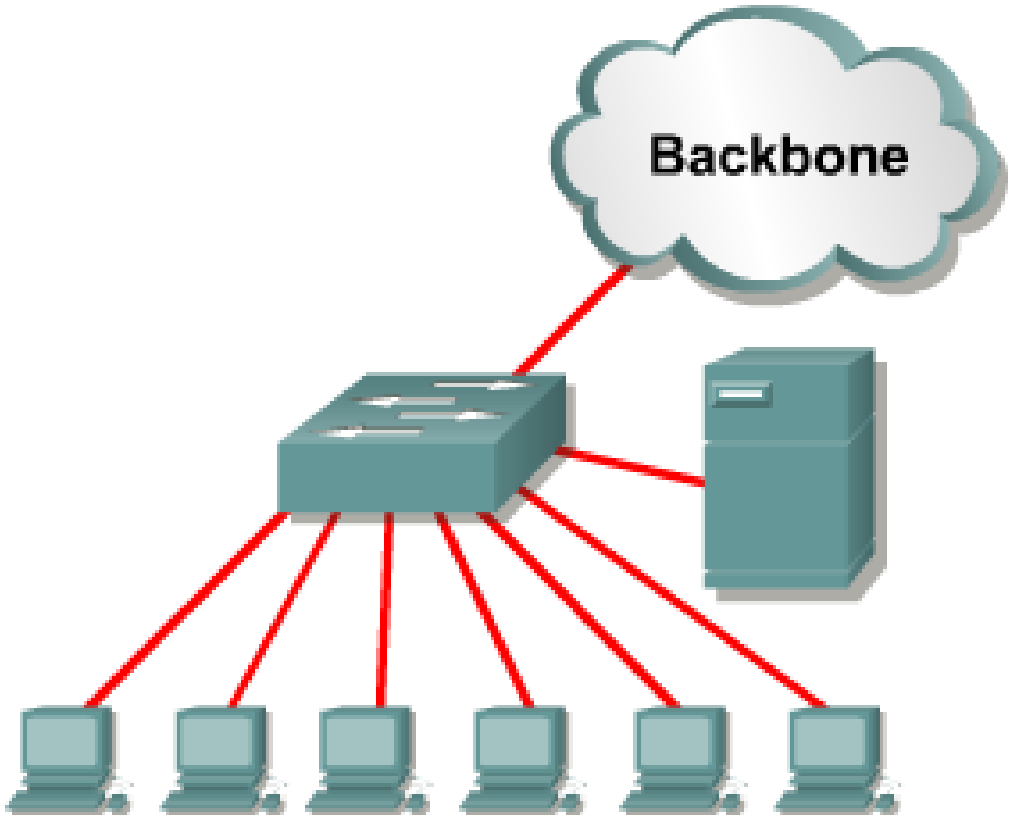


Each node shares 10 Mbps

Ethernet Access with Switches

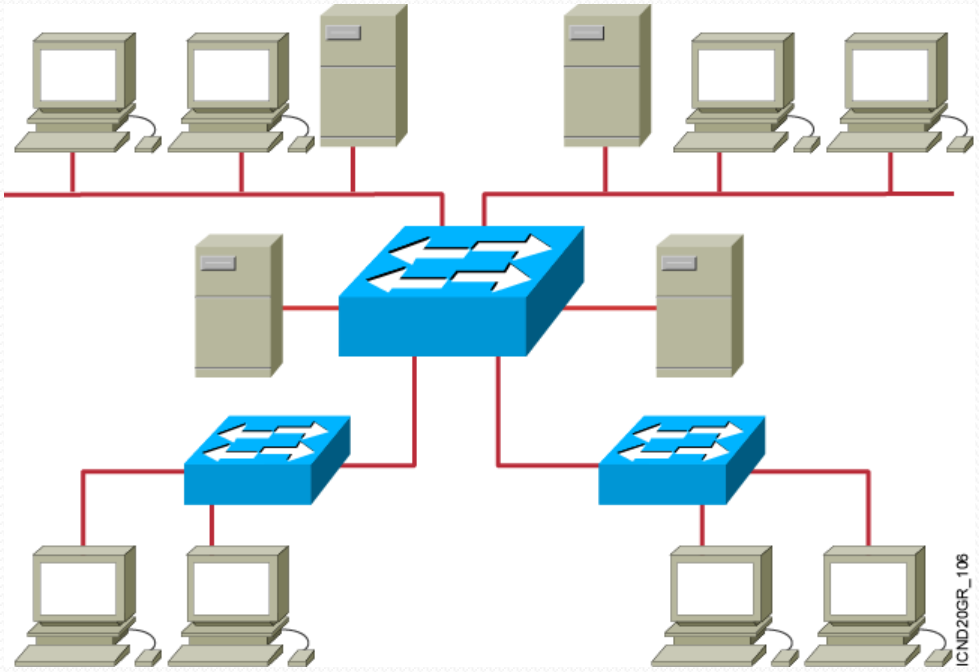


Multiple devices sending at the same time



Each node has 10/100 Mbps

Ethernet Switches and Bridges

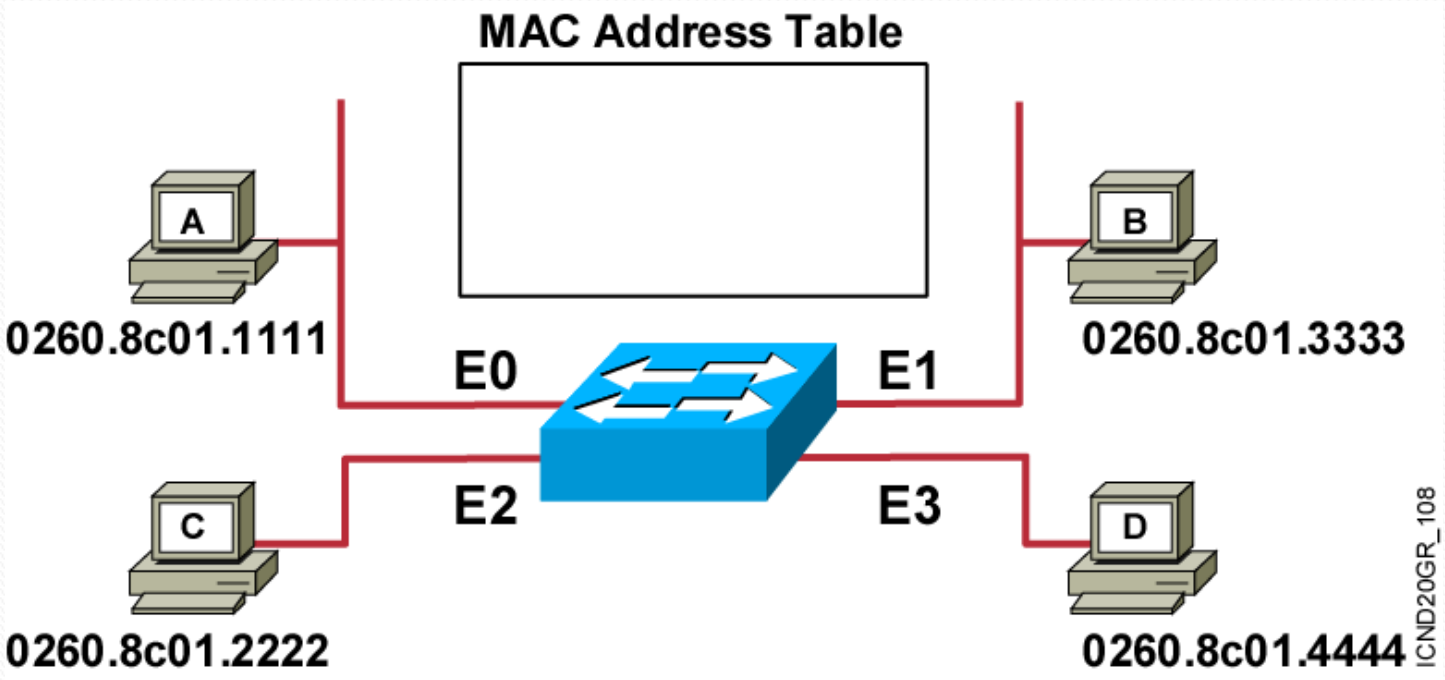


- Address learning
- Forward/filter decision
- Loop avoidance

Switch Features

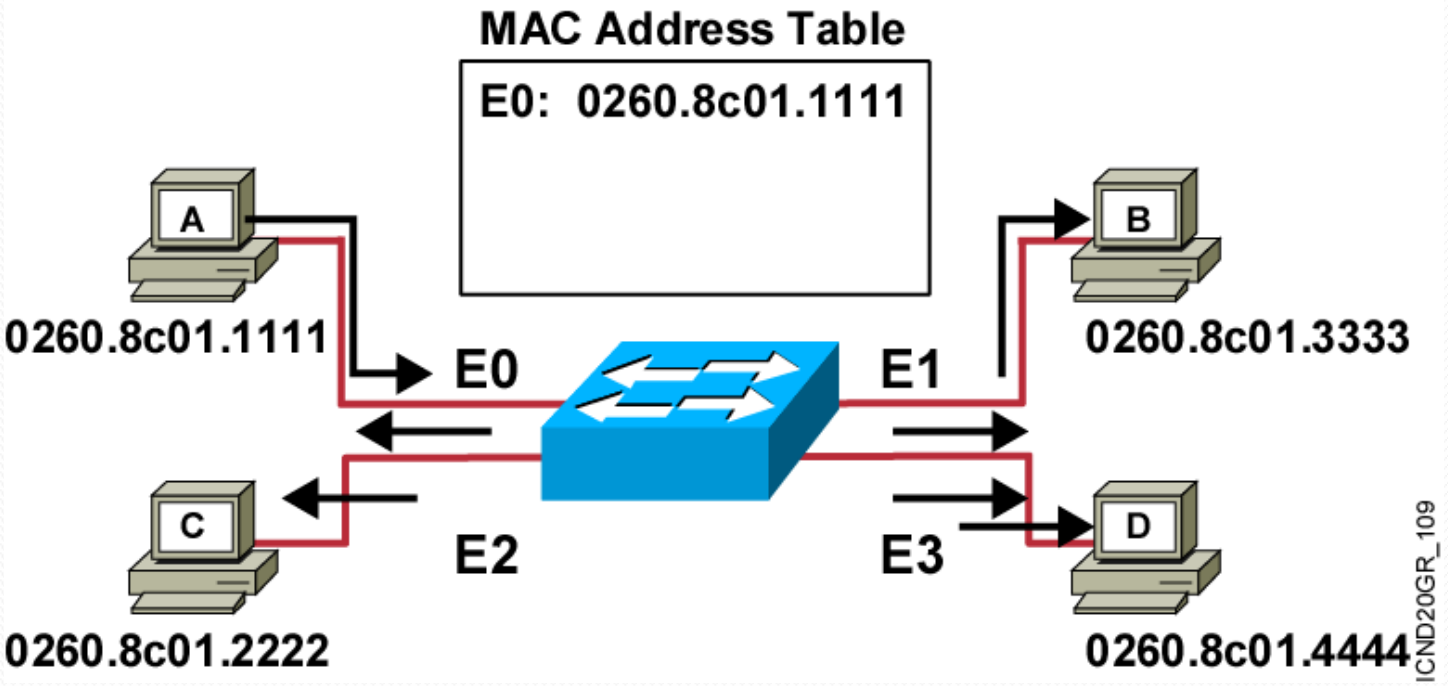
- There are three conditions in which a switch will flood a frame out on all ports except to the port on which the frame came in, as follows:
  - Unknown unicast address
  - Broadcast frame
  - Multicast frame

MAC Address Table



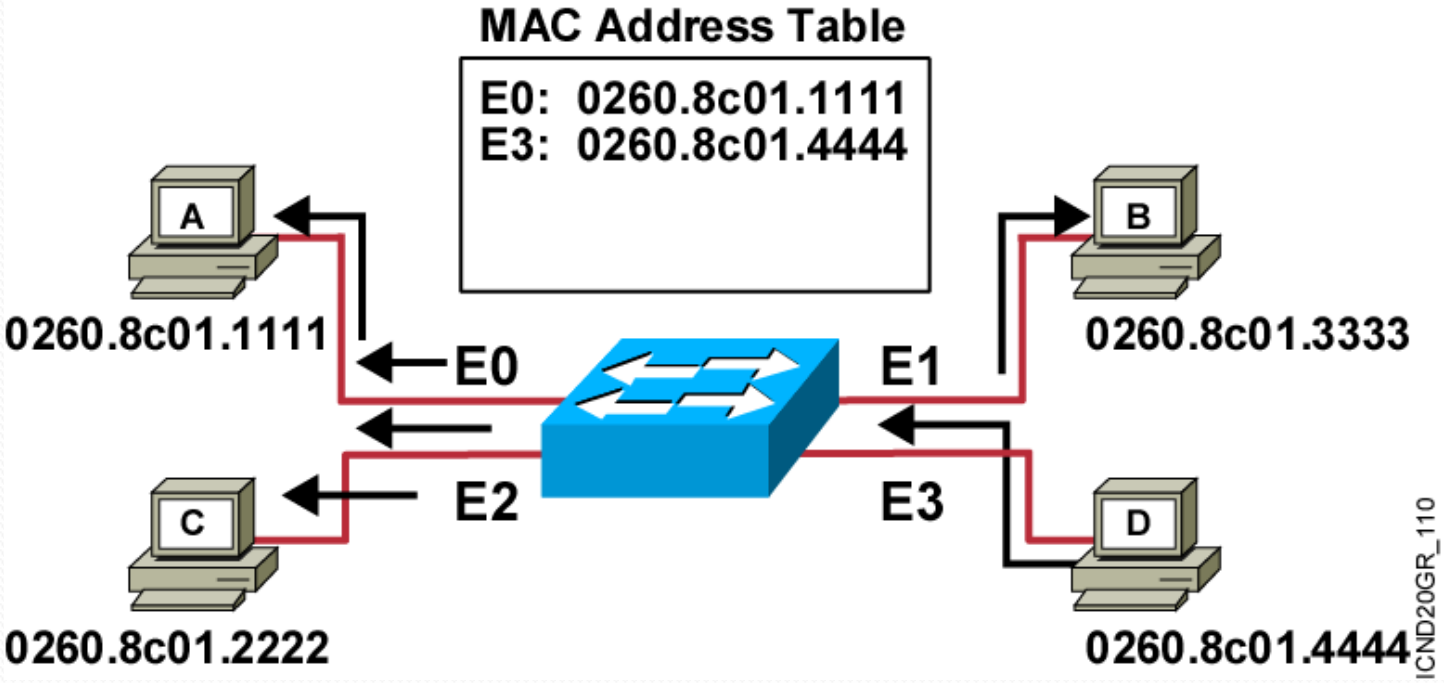
- **Initial MAC address table is empty.**

Learning Addresses



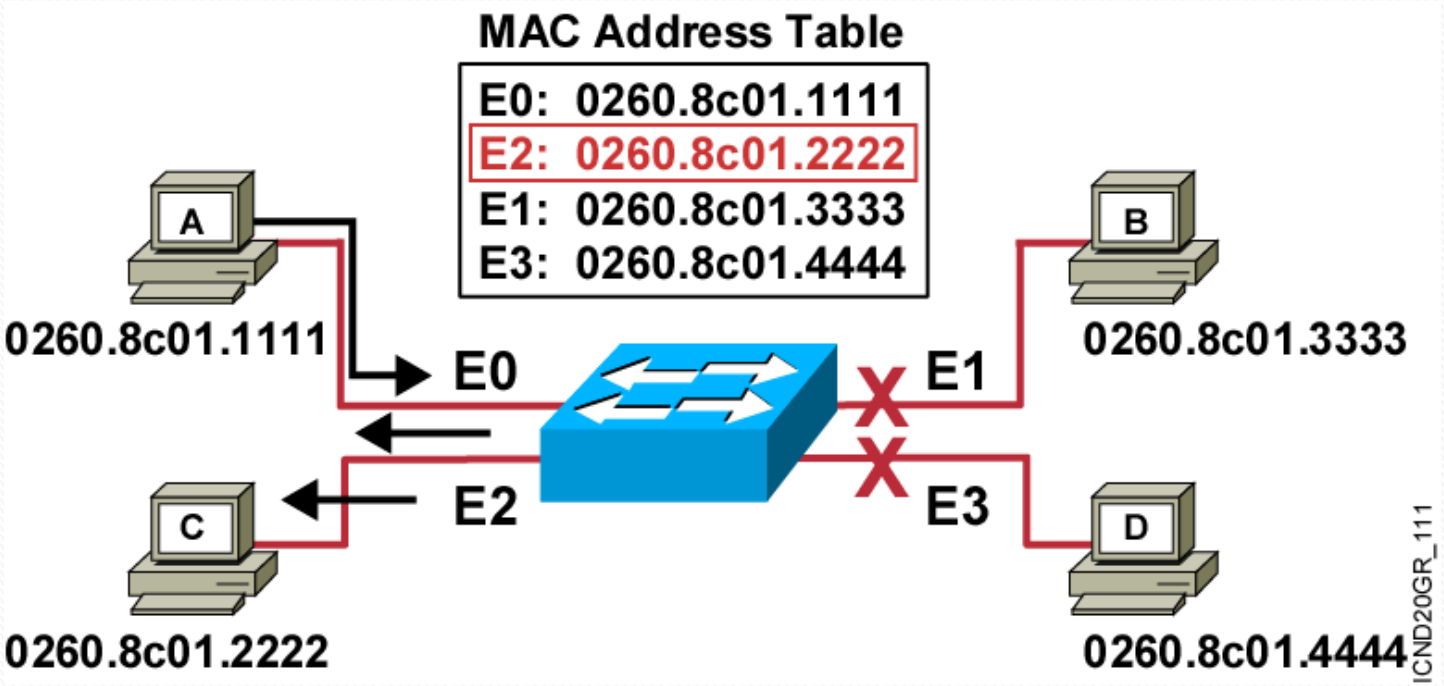
- **Station A sends a frame to station C.**
- **Switch caches the MAC address of station A to port Eo by learning the source address of data frames.**
- **The frame from station A to station C is flooded out to all ports except port Eo (unknown unicasts are flooded).**

Learning Addresses (Cont.)



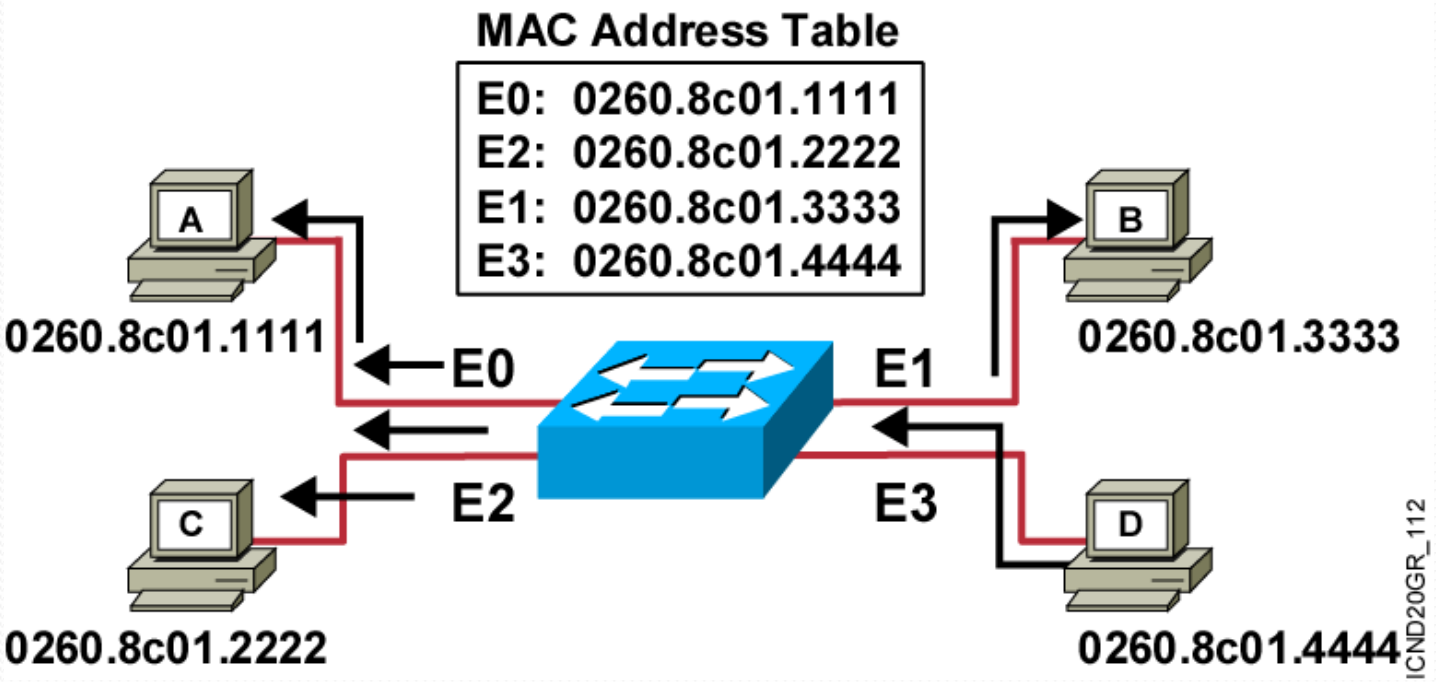
- **Station D sends a frame to station C.**
- **Switch caches the MAC address of station D to port E3 by learning the source address of data frames.**
- **The frame from station D to station C is flooded out to all ports except port E3 (unknown unicasts are flooded).**

Filtering Frames



- **Station A sends a frame to station C.**
- **Destination is known; frame is not flooded.**

Broadcast and Multicast Frames



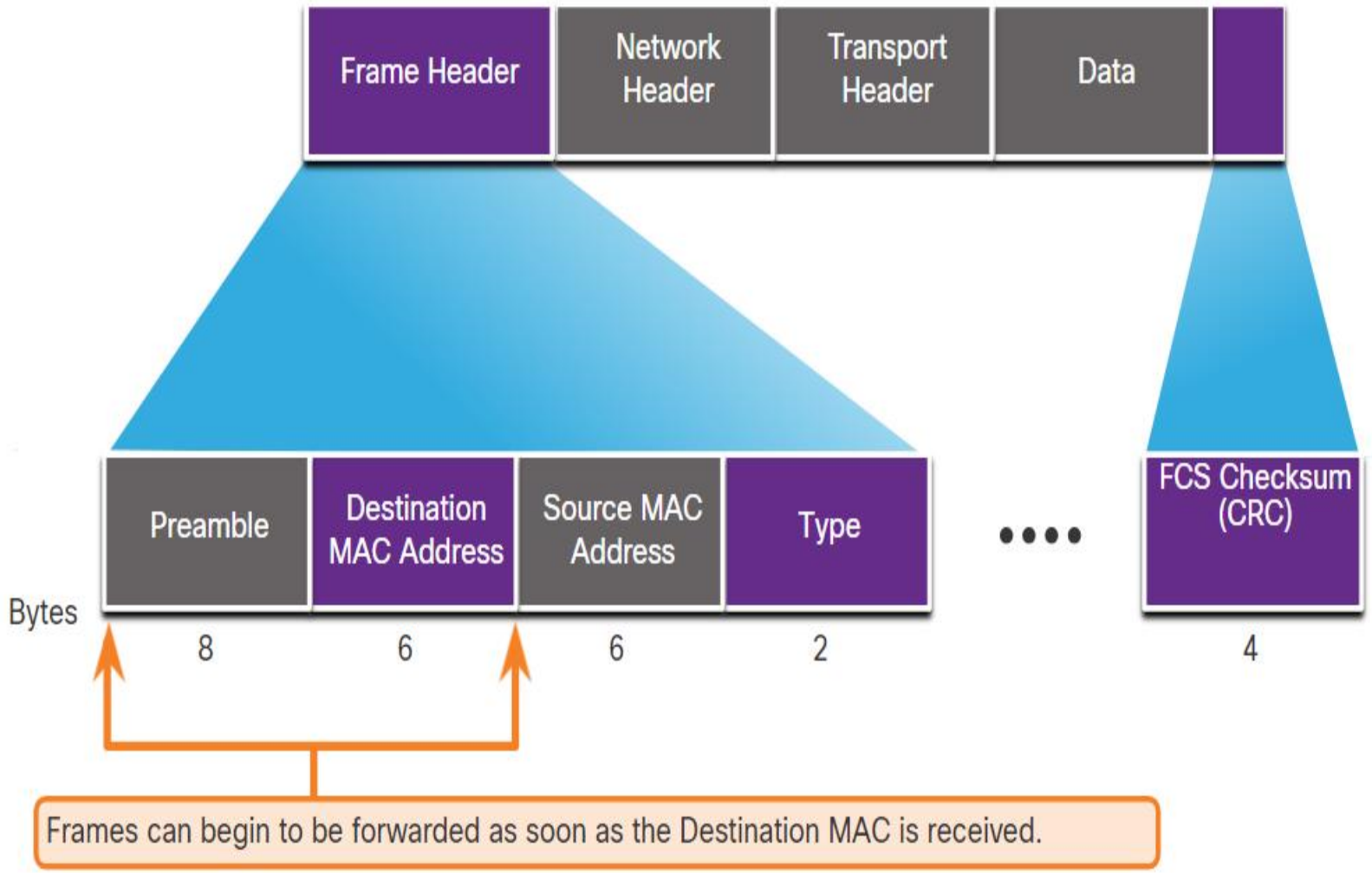
- **Station D sends a broadcast or multicast frame.**
- **Broadcast and multicast frames are flooded to all ports other than the originating port.**

Forward/Filter Decision

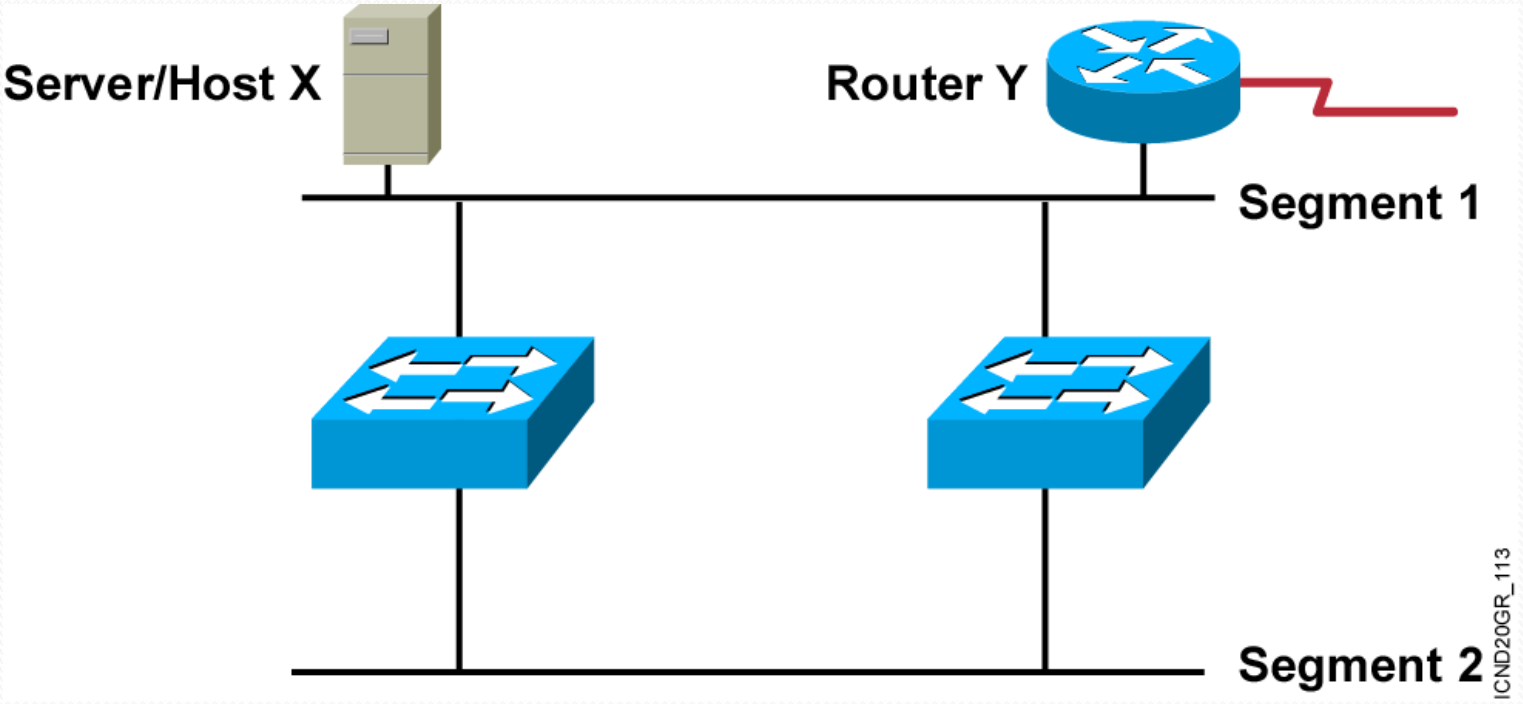
- When a frame arrives at a switch interface, the destination hardware address is compared to the forward/ filter MAC database.
- If the destination hardware address is known and listed in the database, the frame is sent out only the correct exit interface
- If the destination hardware address is not listed in the MAC database, then the frame is flooded out all active interfaces except the interface the frame was received on.
- If a host or server sends a broadcast on the LAN, the switch will flood the frame out all active ports except the source port.

Methods of Switching

- There are three methods of switching:
- **Store and Forward:** The frame is fully received, and checked for FCS before it is being forwarded.
- **Fragment-Free:** The frame is received until the first 64 bytes of data before the frame is get forwarded to make sure the forwarded frame doesn't have collisions and is not a runt frame.
- **Cut Through:** The frame is received until the destination mac address before it is being forwarded. This method considred as the quickest switching method

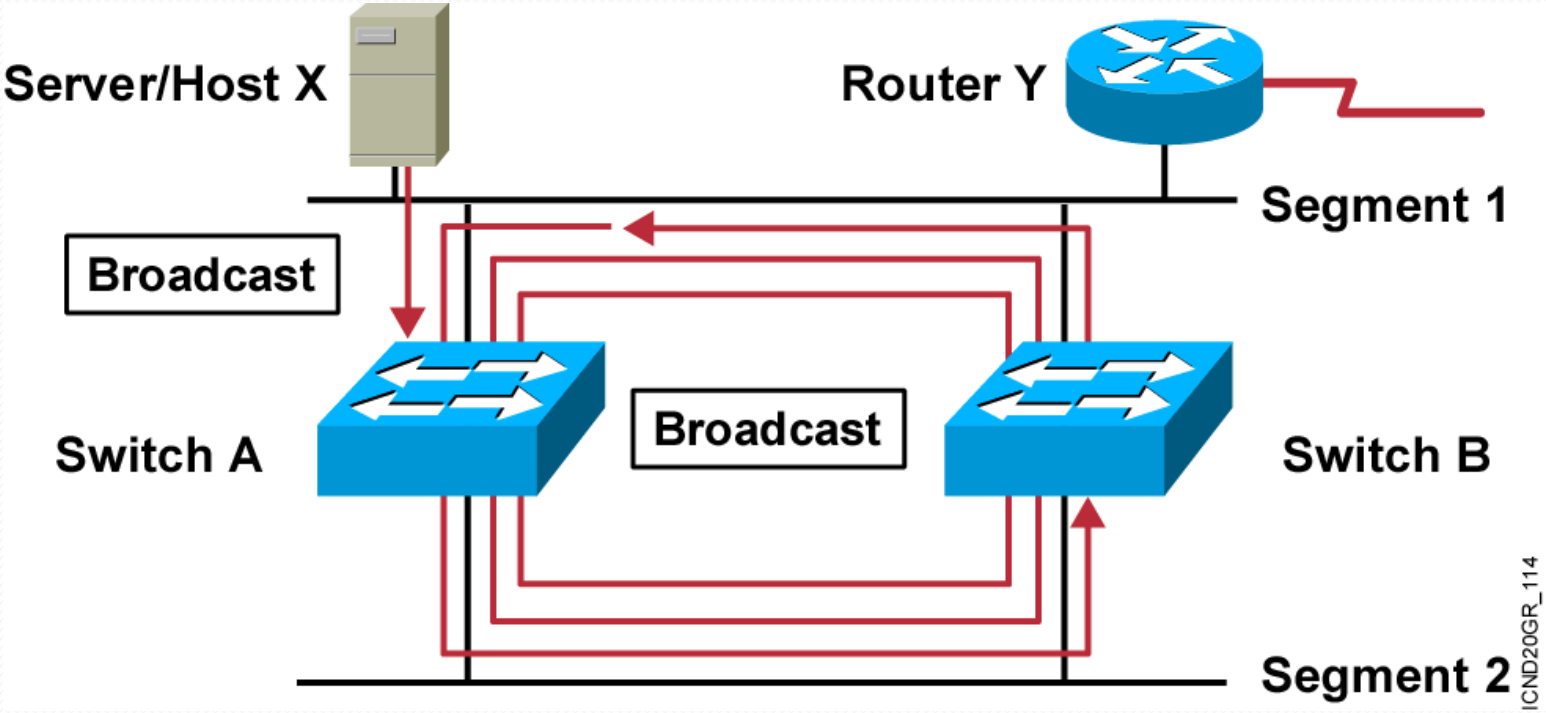

Frame Header
Network Header
Transport Header
Data
Preamble
Destination MAC Address
Source MAC Address
Type
FCS Checksum (CRC)
Bytes
8
6
6
2
4
Frames can begin to be forwarded as soon as the Destination MAC is received.

Redundant Topology



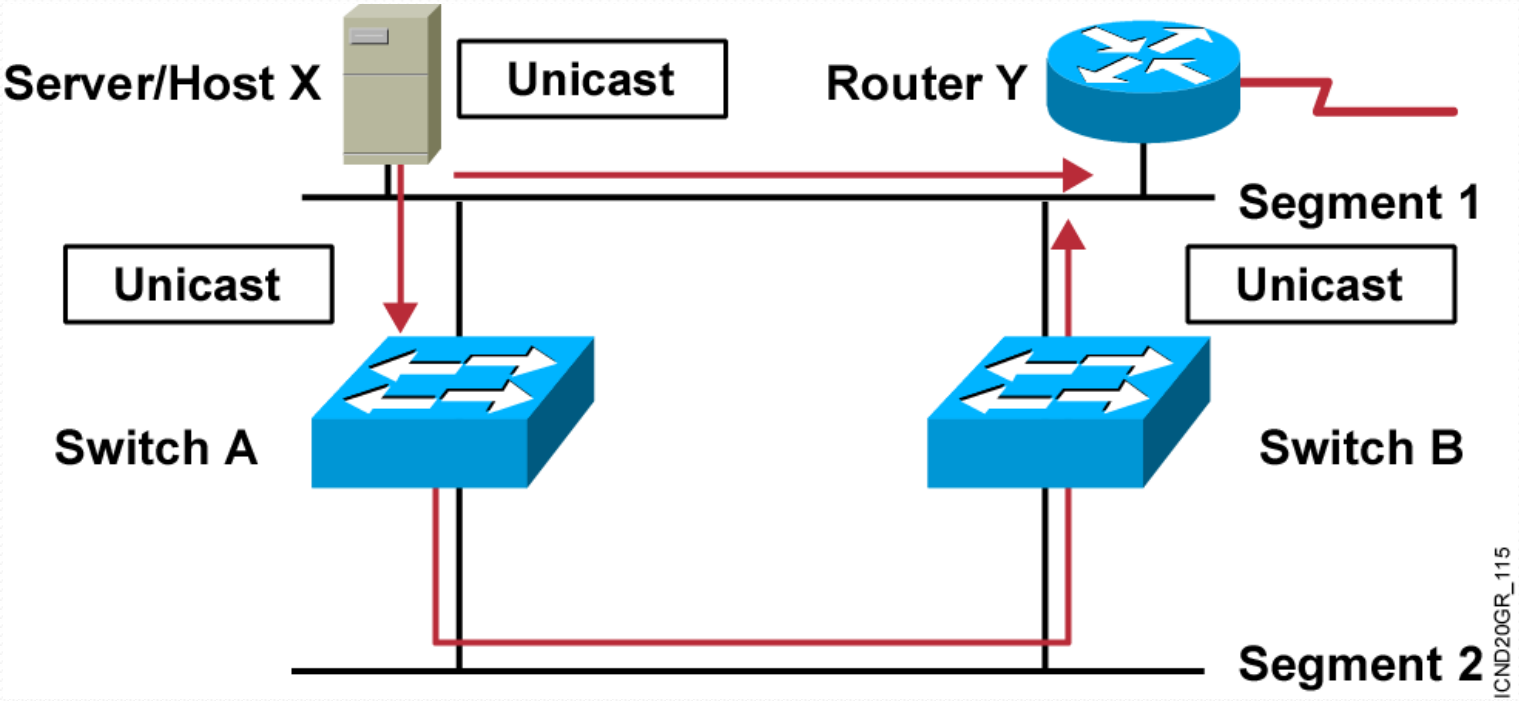
- Redundant topology eliminates single points of failure.
- Redundant topology causes broadcast storms, multiple frame copies, and MAC address table instability problems.

Broadcast Storms



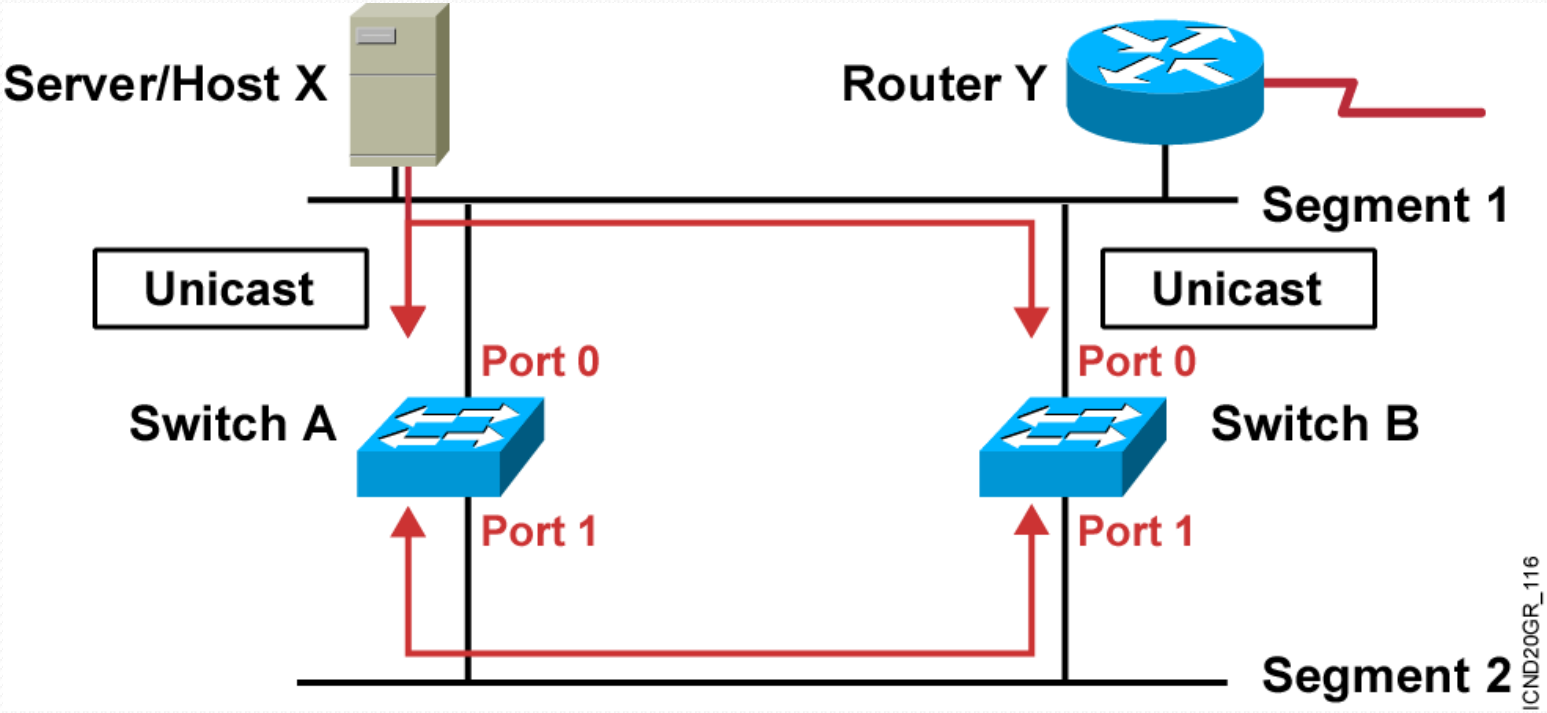
- Host X sends a broadcast.
- Switches continue to propagate broadcast traffic over and over.

Multiple Frame Copies



- Host X sends a unicast frame to router Y.
- MAC address of router Y has not been learned by either switch yet.
- Router Y will receive two copies of the same frame.

MAC Database Instability



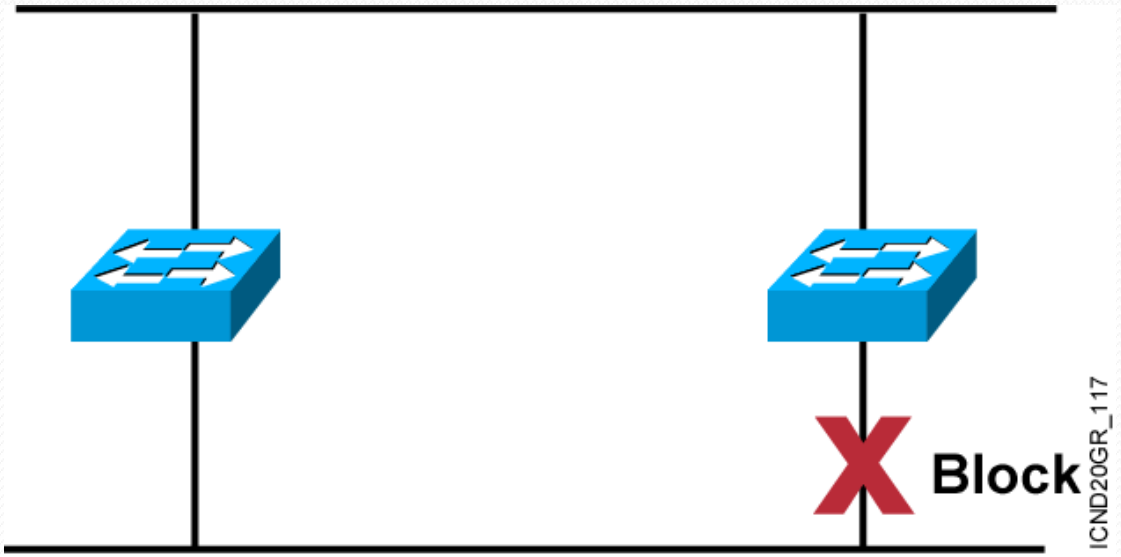
- Host X sends a unicast frame to router Y.
- MAC address of router Y has not been learned by either switch.
- Switches A and B learn the MAC address of host X on port 0.
- The frame to router Y is flooded.
- Switches A and B incorrectly learn the MAC address of host X on port 1.

Spanning Tree

Overview

- Redundancy in a network is extremely important because redundancy allows networks to be fault tolerant.
- Redundant topologies based on switches and bridges are subject to broadcast storms, multiple frame transmissions, and MAC address database instability.
- Therefore network redundancy requires careful planning and monitoring to function properly.
- The Spanning-Tree Protocol is used in switched networks to create a loop free network

Spanning-Tree Protocol



- **Provides a loop-free redundant network topology by placing certain ports in the blocking state.**

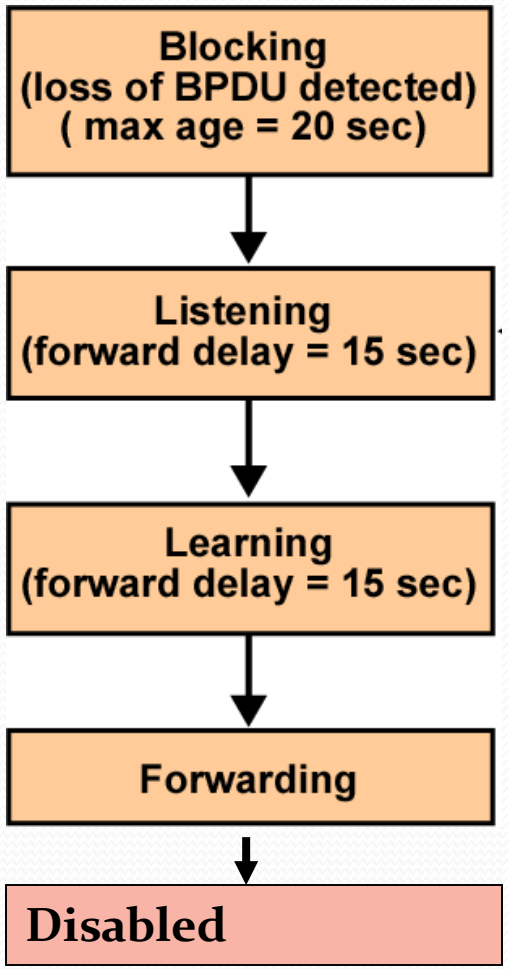
Spanning Tree Protocol

- **Spanning Tree Protocol resides in Data link Layer**

- **Ethernet bridges and switches can implement the IEEE 802.1D Spanning-Tree Protocol and use the spanning-tree algorithm to construct a loop free network.**

Spanning-Tree Port States

- **Spanning-tree transits each port through several different states:**



Selecting the Root Bridge

- The first decision that all switches in the network make, is to identify the root bridge.
- When a switch is turned on, the spanning-tree algorithm is used to identify the root bridge. BPDUs are sent out with the Bridge ID (BID).
- The BID consists of a bridge priority that defaults to 32768 and the switch base MAC address.
- When a switch first starts up, it assumes it is the root switch and sends BPDUs. These BPDUs contain BID.
- All bridges see these and decide that the bridge with the smallest BID value will be the root bridge.
- A network administrator may want to influence the decision by setting the switch priority to a smaller value than the default.

Spanning Tree Protocol Terms

❑**BPDU Bridge Protocol Data Unit (BPDU)** - All the switches exchange information to use in the selection of the root switch

❑**Bridge ID** - The bridge ID is how STP keeps track of all the switches in the network. It is determined by a combination of the bridge priority (32,768 by default on all Cisco switches) and the base MAC address.

❑**Root Bridge** -The bridge with the lowest bridge ID becomes the root bridge in the network.

❑**Nonroot bridge** - These are all bridges that are not the root bridge.

❑**Root port** - The root port is always the link directly connected to the root bridge or the shortest path to the root bridge. If more than one link connects to the root bridge, then a port cost is determined by checking the bandwidth of each link.

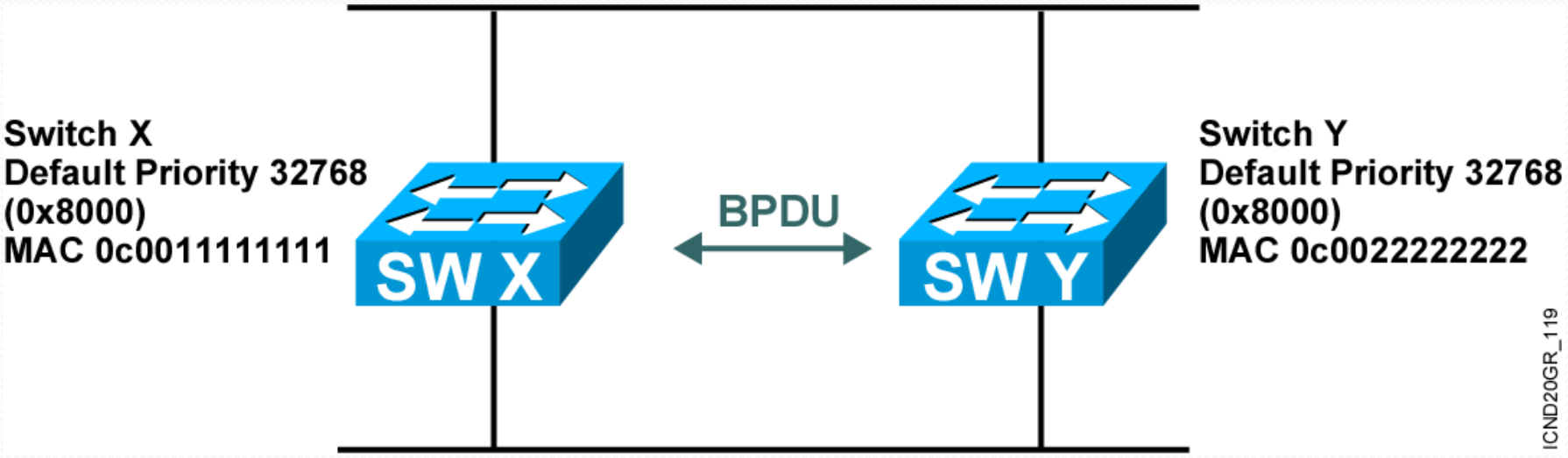
❑**Designated port** - A designated port is one that has been determined as having the best (lowest) cost. A designated port will be marked as a forwarding port

❑**Nondesignated Port** - A nondesignated port is one with a higher cost than the designated port. Nondesignated ports are put in blocking mode

❑**Forwarding Port -** A forwarding port forwards frames

❑**Blocked Port -** A blocked port is the port that will not forward frames, in order to prevent loops

Spanning-Tree Protocol
Root Bridge Selection

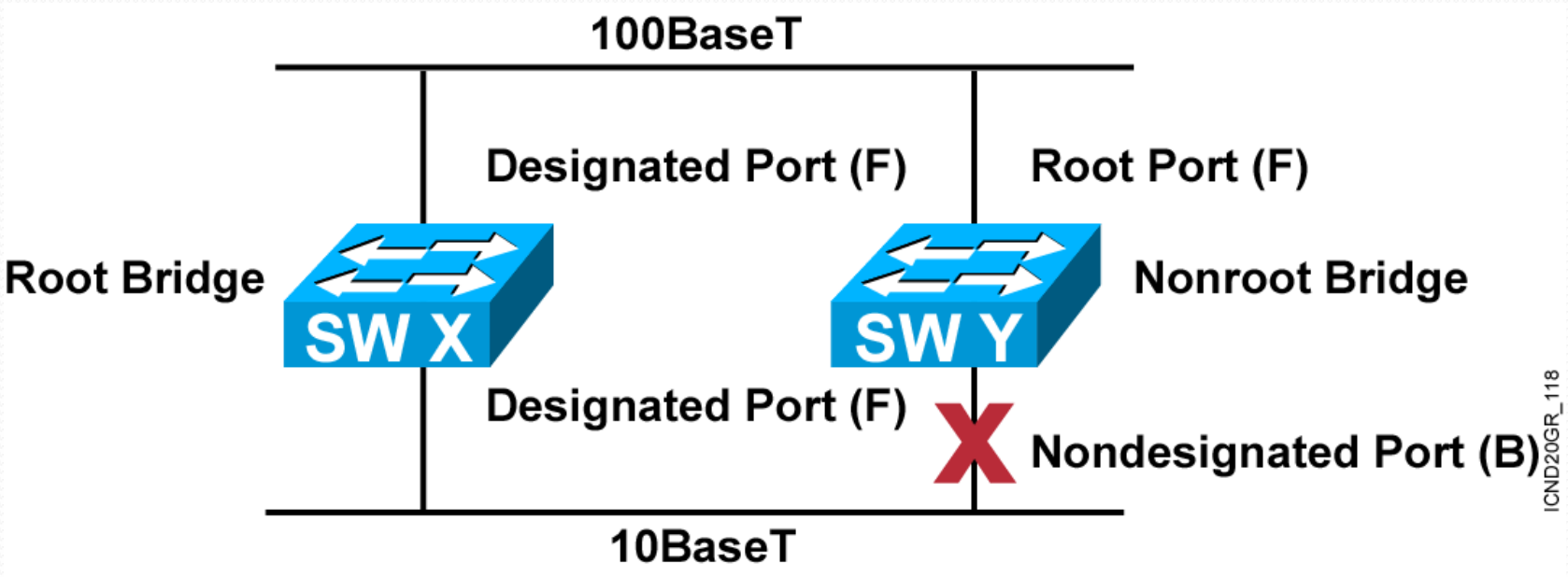


- Bpdu = Bridge Protocol Data Unit
  (default = sent every two seconds)
- Root bridge = Bridge with the lowest bridge ID
- Bridge ID =

- In the example, which switch has the lowest bridge ID?

Spanning-Tree Operation

- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment
- Nondesignated ports are unused



Selecting the Root Port

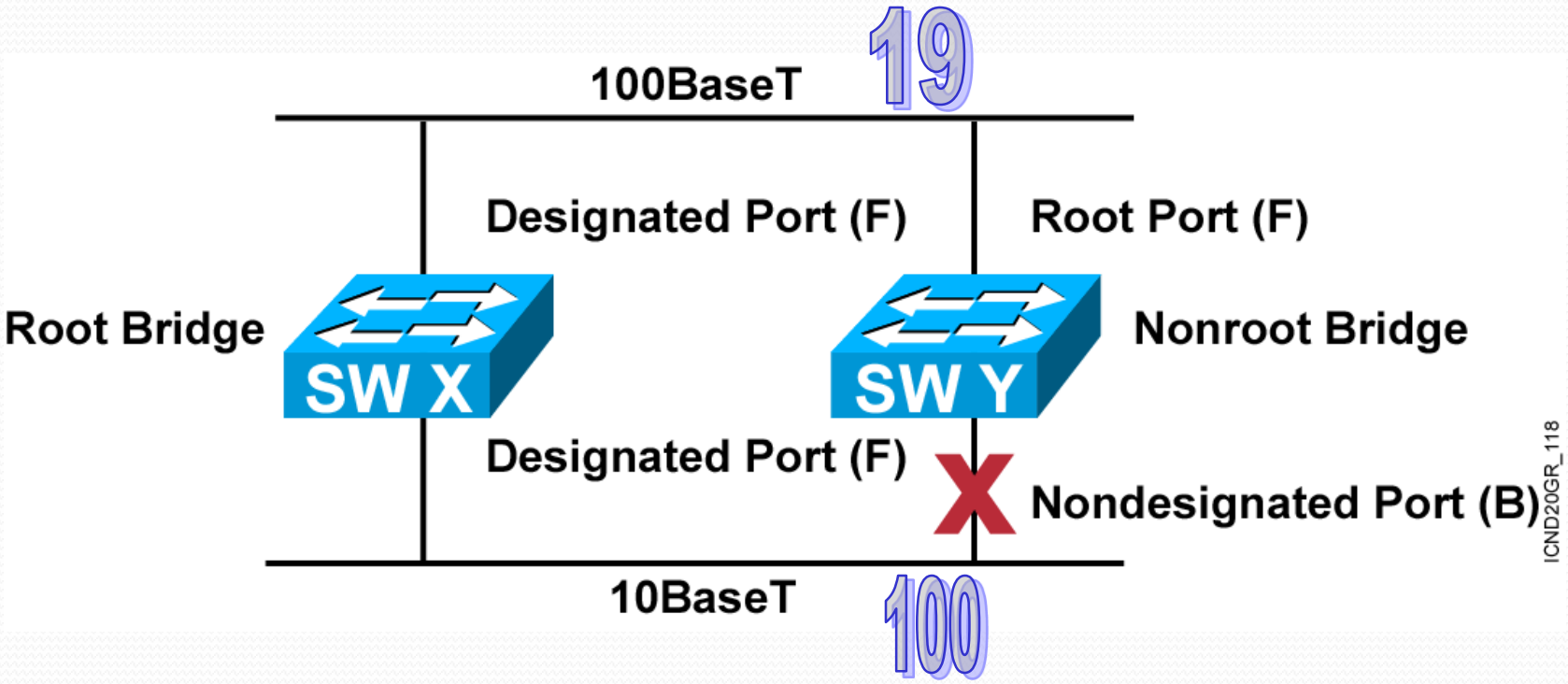
- The STP cost is an accumulated total path cost based on the rated bandwidth of each of the links
- This information is then used internally to select the root port for that device

Link Speed	Cost (Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

ICND20GR_121

Spanning-Tree Operation

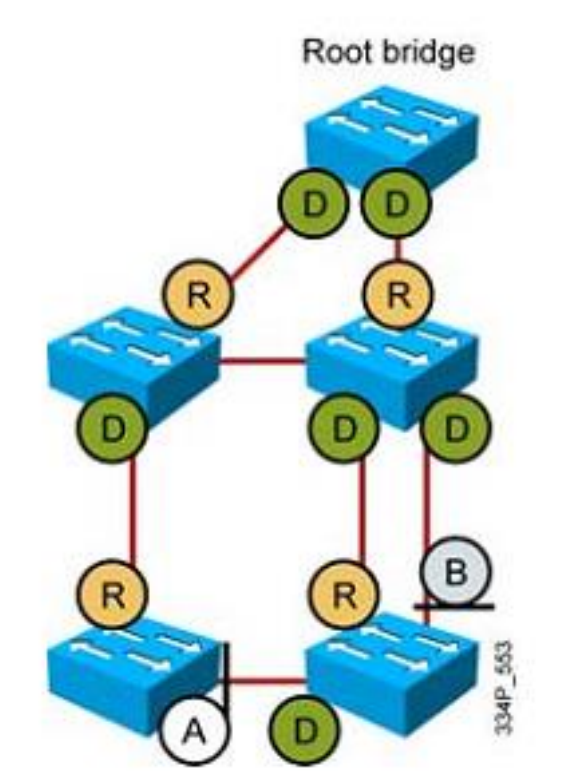
- One root bridge per network
- One root port per nonroot bridge
- One designated port per segment
- Nondesignated ports are unused



Rapid Spanning Tree

RSTP Port Roles

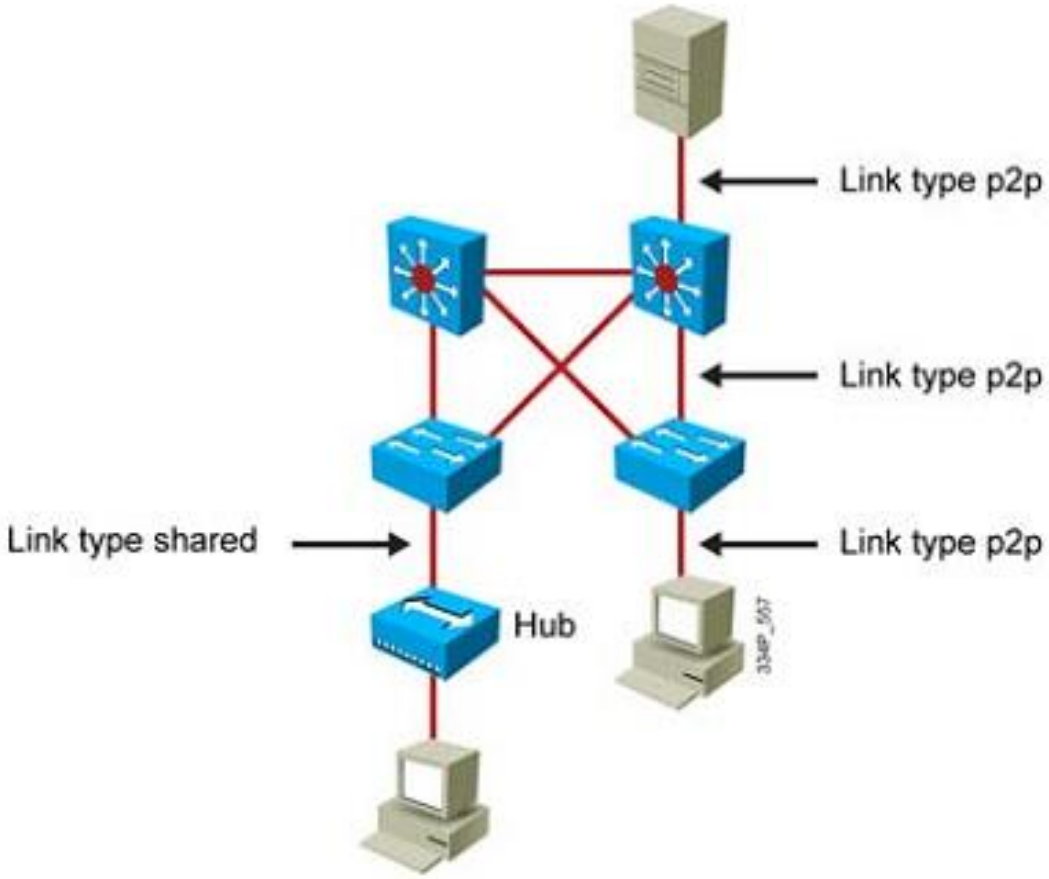
- **Port in forwarding mode:**
  - **Root: chosen path to root bridge**
  - **Designated: port that sends the best BPDU on the segment to which it is connected**
- **Port in blocking mode:**
  - **Alternate: receives more useful BPDUs from another bridge**
  - **Backup: receives more useful BPDUs from the same bridge**



Spanning-Tree Port Types and States

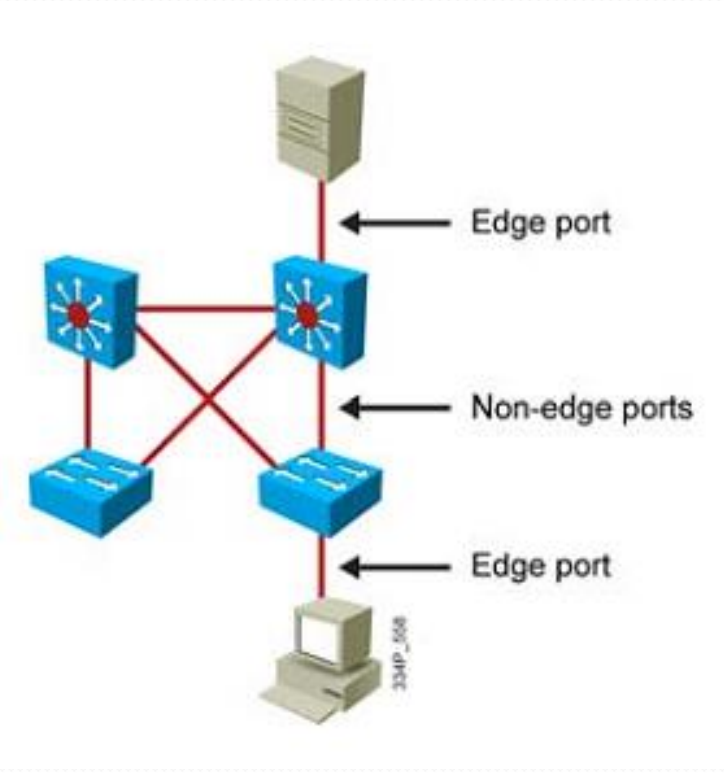
STP Port Role	RSTP Port Role	STP Port State	RSTP Port State
Root port	Root port	Forwarding	Forwarding
Designated port	Designated port	Forwarding	Forwarding
Nondesignated port	Alternative or backup port	Blocking	Discarding
Disabled	Disabled	—	Discarding
Transition	Transition	Listening Learning	Learning

RSTP Link Types



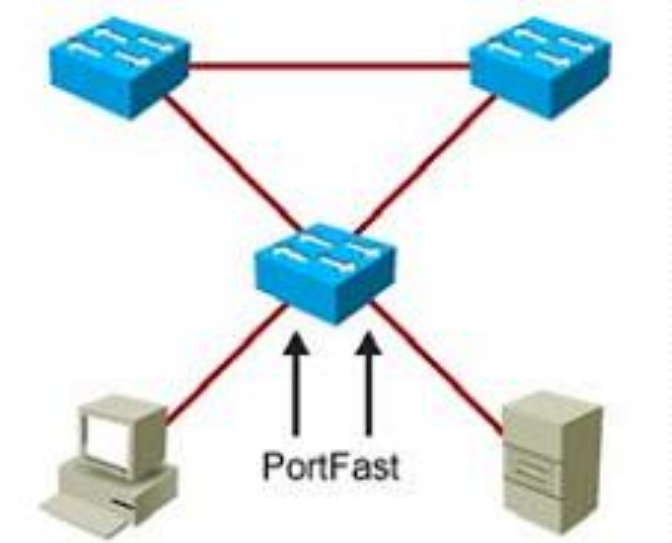
RSTP Edge Ports

- **Will never have a switch conneteced to it**
- **Immediately transitions to forwarding**
- **Functions similarly to PortFast**
- **Is configured with *spanning-tree portfast* command**



PortFast Configuration

- Configure PortFast on edge ports connected to nonswitch devices
- PortFasts transition directly to forwarding, bypassing listening and learning states of spanning-tree



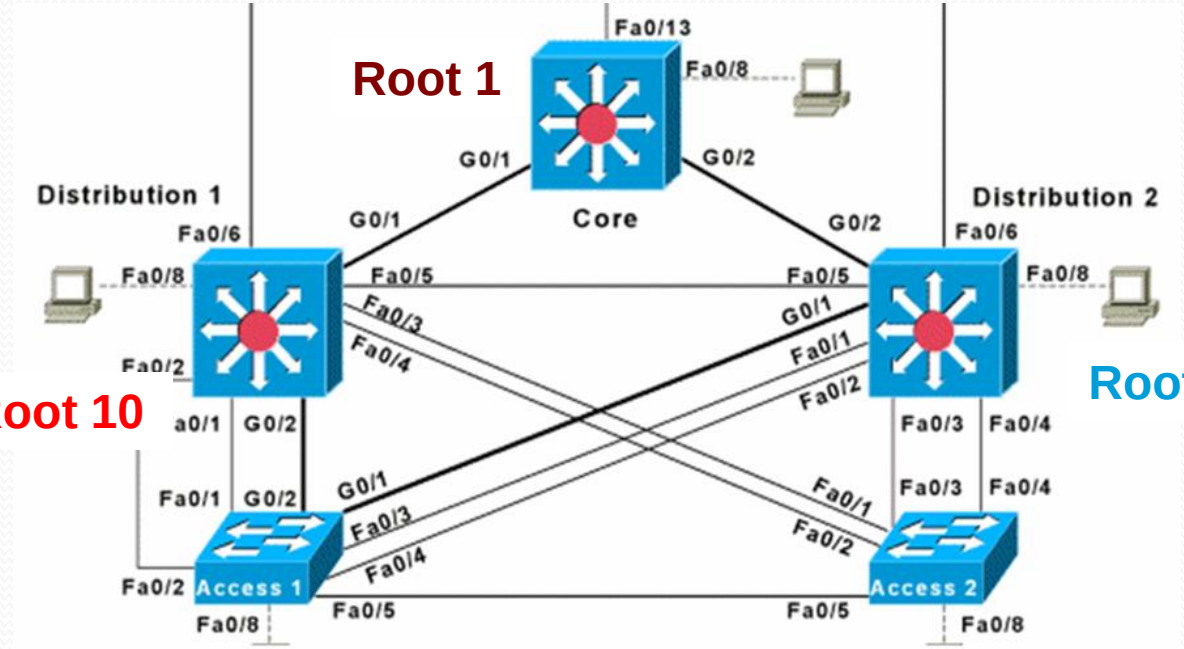

```
switch(config)# spanning-tree portfast default
```

Enables PortFast on all nontrunking interfaces

```
switch(config-if)# spanning-tree portfast [trunk]
```

- **Configure PortFast on an interface**
- **Use trunk parameter for trunk interfaces with no switches connected (e.g. routers or servers with trunks)**

PVST+




```
Core(config)#spanning-tree vlan 1 root primary

Distribution1(config)#spanning-tree vlan 10 root primary

Distribution2(config)#spanning-tree vlan 20 root primary
```

STP Enhancements

BPDUFilter

- BPDU Filter behaves differently when enabled globally or per interface
- BPDU Filter when enabled at the interface level, it immediately stops sending and receiving BPDU, and if any BPDU is received, the port will drop the BPDUs and keep forwarding.
- BPDU Filter when enabled at the Global configuration, It will be enabled on portfast ports.

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

- It will also stop sending the BPDUs.
- However, If any BPDU is received Later, The port will disable portfast feature and removes BPDU filter and function normally as any STP port

BPDUfilter Configuration

- To enable BPDU filter globally:

  spanning-tree portfast default

  spanning-tree portfast bpdufilter default

- To enable BPDU filter on particular port

  spanning-tree bpdufilter enable

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

BPDUguard

- BPDUGuard works almost the same when enabled globally or per port level.
- It simply prevents the port from receiving any BPDUs, and if received any BPDU, the port will automatically moves to err-disabled state.
- BPDUGuard on global configuration can work only with portfast.

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

BPDUguard Configuration

- To configure BPDU GUARD using global command:

  spanning-tree portfast default

  spanning-tree portfast bpduguard default

- To configure on particular interface:

  spanning-tree bpduguard enable

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

Rootguard

- Rootguard feature disables the port, if it receives any superior bpdus.
- However the port will automatically recover, if the port stops receiving those superior root bpdus.
- Unlike BPDUguard, which requires manual recovery for err-disabled ports.

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

Rootguard Configuration

- Rootguard can be enabled only on the interface level as follows:
- **Spanning-tree guard root**

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

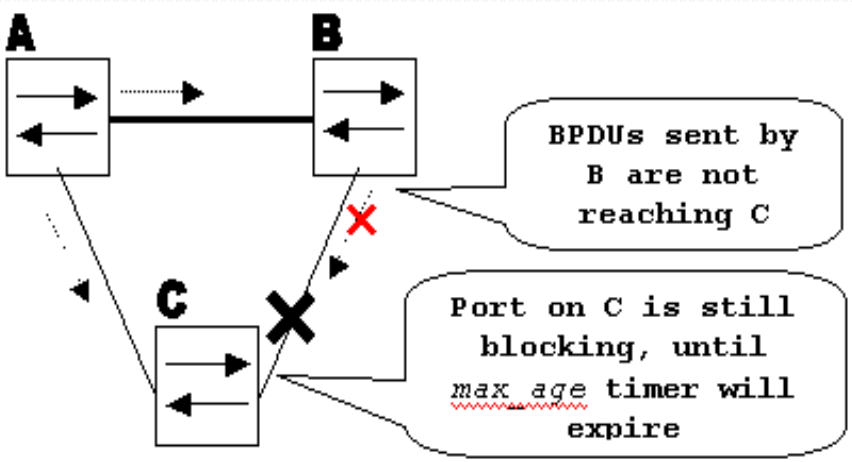
Loopguard

- Loopguard prevents loops in unidirectional links.
- Loopguard moves blocked ports into err-disabled when they don't receive bpdus to unidirectional problem, instead of moving them to forwarding and create the loop.

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

STP without Loopguard

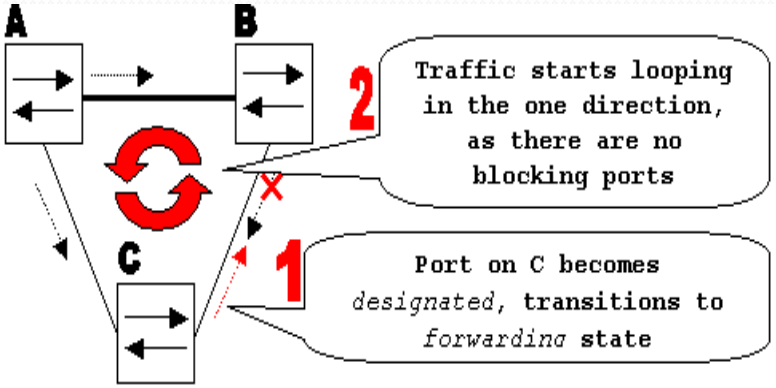
- Assume link C-B has a failure on its RX.



Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

STP without Loopguard

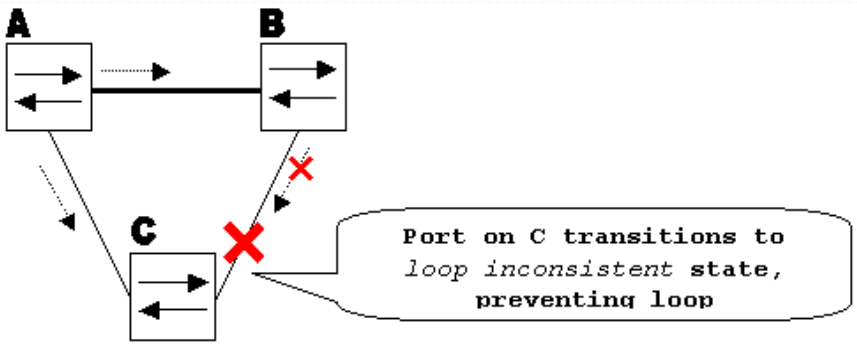
- Port C-B on Switch B will stop receiving the BPDUs, and It will start transitioning to forwarding.
- Thus the loop occurs, because ports will be forwarding in this case.



Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

STP with Loopguard

- When loopguard is enabled on the blocked port, It will place the port into loop inconsistent when stops receiving the BPDUs.
- Thus preventing the loop
- Loop Guard can't be enabled on a portfast or guard root port.
- LoopGuard if enabled in the global configuration mode, it is enabled in point-to-point links



Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

Loopguard Configuration

- Loopguard can be enabled on the interface level:

  Router(config)#**interface gigabitEthernet 1/1**

  Router(config-if)#**spanning-tree guard loop**

- It can also be enabled gobally:
- Router(config)#**spanning-tree loopguard default**

Developed By:Waleed Hashim Ali Adlan -0123125530-
waleed_hashim@hotmail.com

Switch Configuration

Physical Startup of the Catalyst Switch

- Switches are dedicated, specialized computers, which contain a CPU, RAM, and an operating system.
- Switches usually have several ports for the purpose of connecting hosts, as well as specialized ports for the purpose of management.
- A switch can be managed by connecting to the console port to view and make changes to the configuration.
- Switches typically have no power switch to turn them on and off. They simply connect or disconnect from a power source.

Switch Command Modes

- Switches have several command modes.
- The default mode is User EXEC mode, which ends in a greater-than character (**>**).
- The commands available in User EXEC mode are limited to those that change terminal settings, perform basic tests, and display system information.
- The **enable** command is used to change from User EXEC mode to Privileged EXEC mode, which ends in a pound-sign character (**#**).
- The **configure** command allows other command modes to be accessed.

Show Commands in User-Exec Mode

Commands	Description
`show version`	Gives version information for software and hardware. Used to see exactly which modules and software are in use.
`show running-config`	Displays the current configuration file of the switch.
`show interface`	Displays the administrative and operational status of a switching port, packets in/out, and errors.
`show interface status`	Display the operational mode of the port.
`show controllers ethernet-controller`	Gives discarded frames, deferred frames, alignment errors, collisions, and so on.
`show post`	Tells if the switch passed the Power-On Self Test (POST).

Tasks

- Setting the passwords (Password must be between 4 and 8 characters)
- Setting the hostname
- Configuring the IP address and subnet mask
- Erasing the switch configurations

Setting Switch Hostname
Setting Passwords on Lines

```
Switch(config)#hostname ALSwitch
ALSwitch(config)#line con 0
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
ALSWitch(config-line)#line vty 0 4
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
```

Switch Configuration

- There are two reasons to set the IP address information on the switch:
  - To manage the switch via Telnet or other management software
  - To configure the switch with different VLANs and other network functions
- See the default IP configuration = show IP command

Configure IP Address

```
sw1(config-if)#interface vlan 1
sw1(config-if)#ip address 10.0.0.1 255.0.0.0
sw1(config-if)#no shut
sw1(config-if)#exit
sw1(config)ip default-gateway 10.0.0.254
```

Configuring Interface Descriptions

- You can administratively set a name for each interface on the switches

```
SW1#config t
Enter configuration commands, one per line. End with CNTL/Z
SW1(config)#int e0/1
SW1(config-if)#description Finance
SW1(config-if)#int f0/26
SW1(config-if)#description trunk_to_Building_4
SW1(config-if)#
```

- Setting Port Security

  Sw1(config-if)#switchport port-security mac-address mac-address

  - Now only this one MAC address is allowed on this switch port

Switch Configuration

Connect two machine to a switch

To view the MAC table

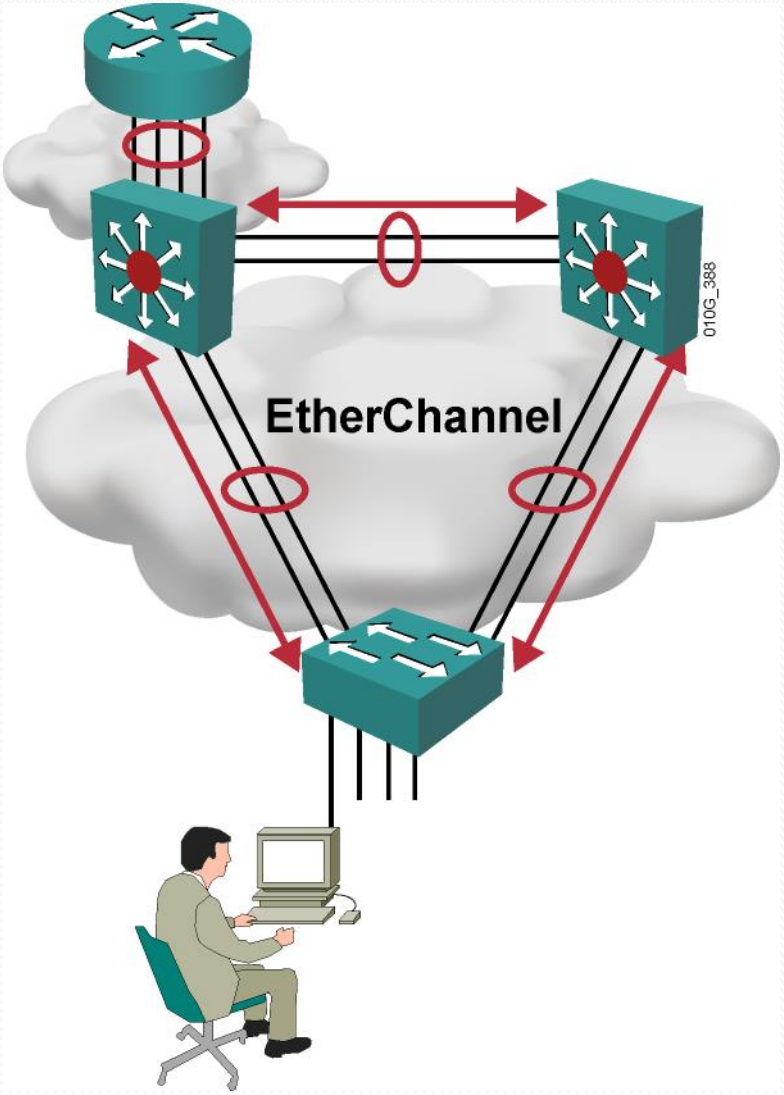
sw1#show mac-address-table dynamic
Sw1#sh spanning-tree
Sw1(config)#spanning-tree vlan 1 priority ?
Sw1(config)#spanning-tree vlan 1 priority 4096

Erase the configuration

Configuring Link Aggregation with EtherChannel

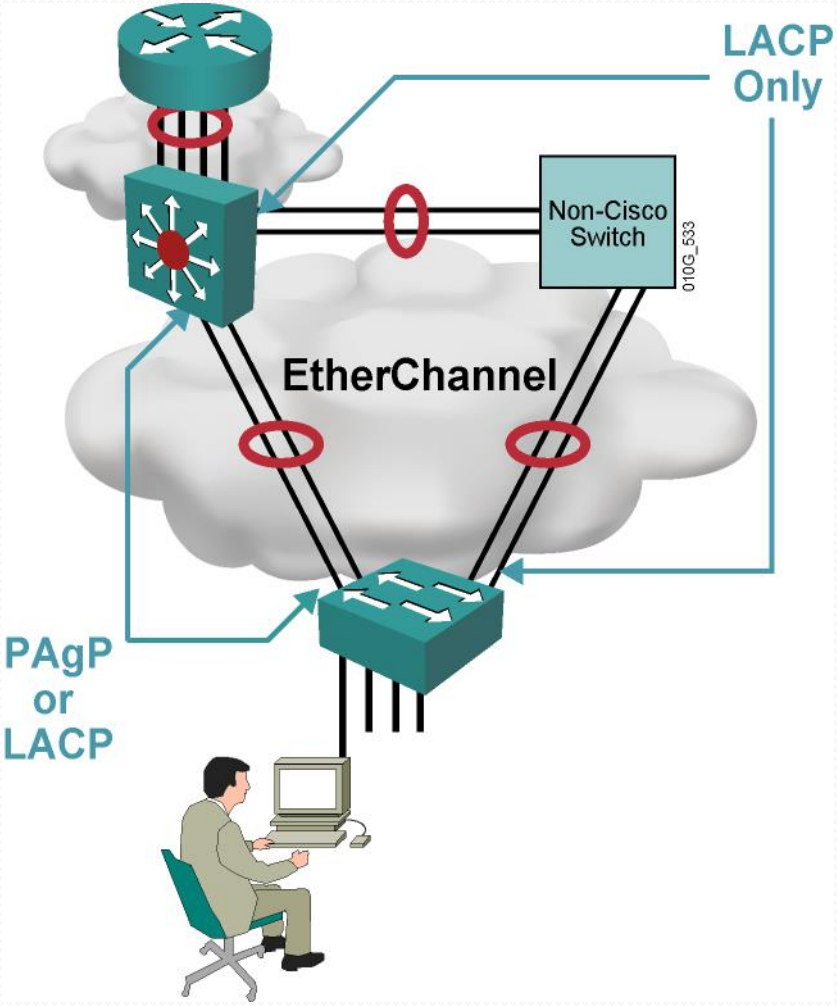
EtherChannel

- Logical aggregation of similar links
- Load balances
- Viewed as one logical port
- Redundancy



Dynamic Trunk Negotiation Protocols

- PAgP Port Aggregation Control Protocol
  - Cisco proprietary
- LACP Link Aggregation Control Protocol
  - IEEE 802.3ad standard



About EtherChannel Configuration Commands

- Configure PAgP
  - interface port-channel {*channel-group-number}*
  - channel-protocol pagp
  - channel-group 1 mode {*mode}*
- Verify
  - show interfaces fastethernet 0/1 etherchannel
  - show etherchannel 1 port-channel
  - show etherchannel 1 summary

Configuring Layer 2 EtherChannel

```
Switch(config)#interface range interface slot/port - port
```

- Specifies the interfaces to configure in the bundle

```
Switch(config-if-range)#channel-protocol {pagp | lacp}
```

- Specifies the channel protocol—either PAgP or LACP

```
Switch(config-if-range)#channel-group number mode {active
| on | auto | desirable | passive}
```

- Creates the port-channel interface and places the interfaces as members

VLANs

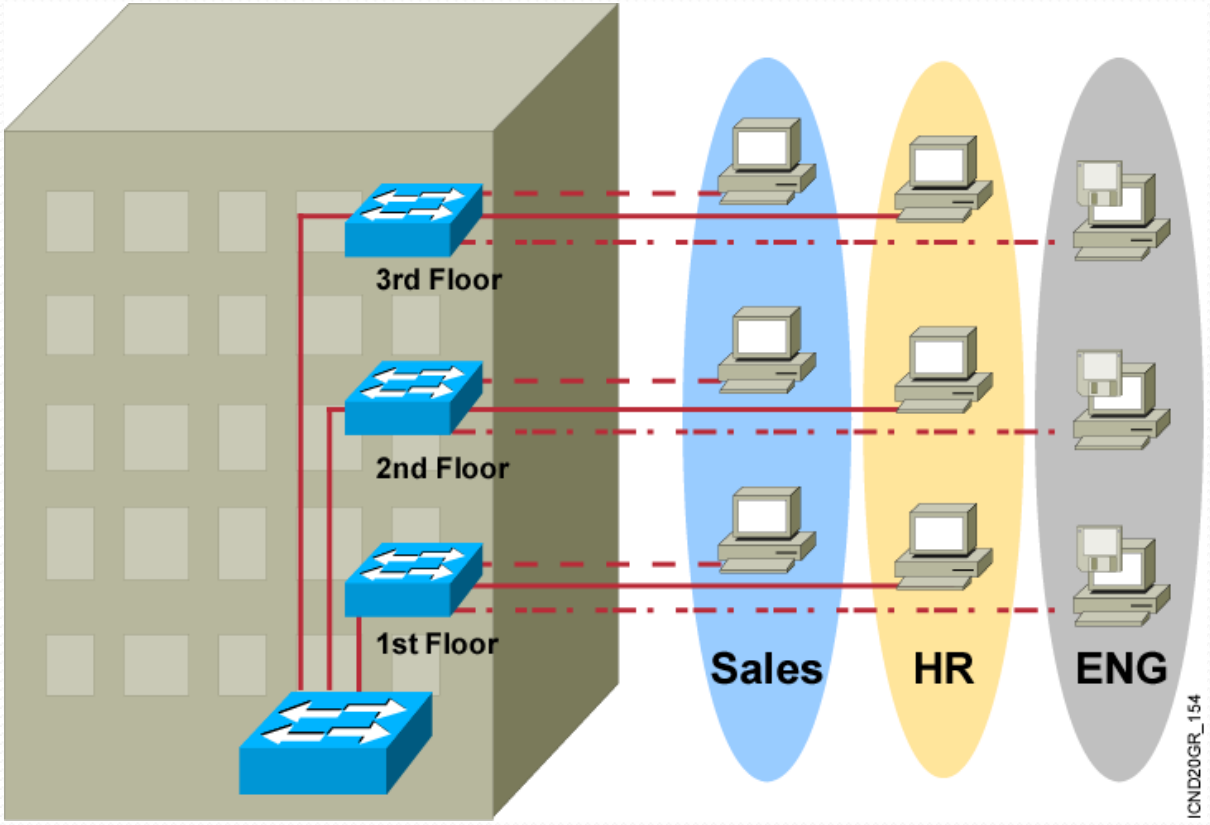
VLANs

- A VLAN is a logical grouping of network users and resources connected to administratively defined ports on a switch.
- Ability to create smaller broadcast domains within a layer 2 switched internetwork by assigning different ports on the switch to different subnetworks.
- Frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN
- By default, no hosts in a specific VLAN can communicate with any other hosts that are members of another VLAN,
- For Inter VLAN communication you need routers

VLANs

- VLAN implementation combines Layer 2 switching and Layer 3 routing technologies to limit both collision domains and broadcast domains.
- VLANs can also be used to provide security by creating the VLAN groups according to function and by using routers to communicate between VLANs.
- A physical port association is used to implement VLAN assignment.
- Communication between VLANs can occur only through the router.
- This limits the size of the broadcast domains and uses the router to determine whether one VLAN can talk to another VLAN.
- *NOTE: This is the only way a switch can break up a broadcast domain!*

VLAN Overview



- **Segmentation**
- **Flexibility**
- **Security**

A VLAN = A Broadcast Domain = Logical Network (Subnet)

Security

- A Flat internetwork's security used to be tackled by connecting hubs and switches together with routers
- This arrangement is ineffective because
  - Anyone connecting physical network could access network resources located on that physical LAN
  - Can observe the network traffic by plugging network analyzer into the HUB
  - Users could join a workgroup by just plugging their workstations into the existing hub
- By creating VLAN's administrators have control over each port and user

How VLANs Simplify Network Management

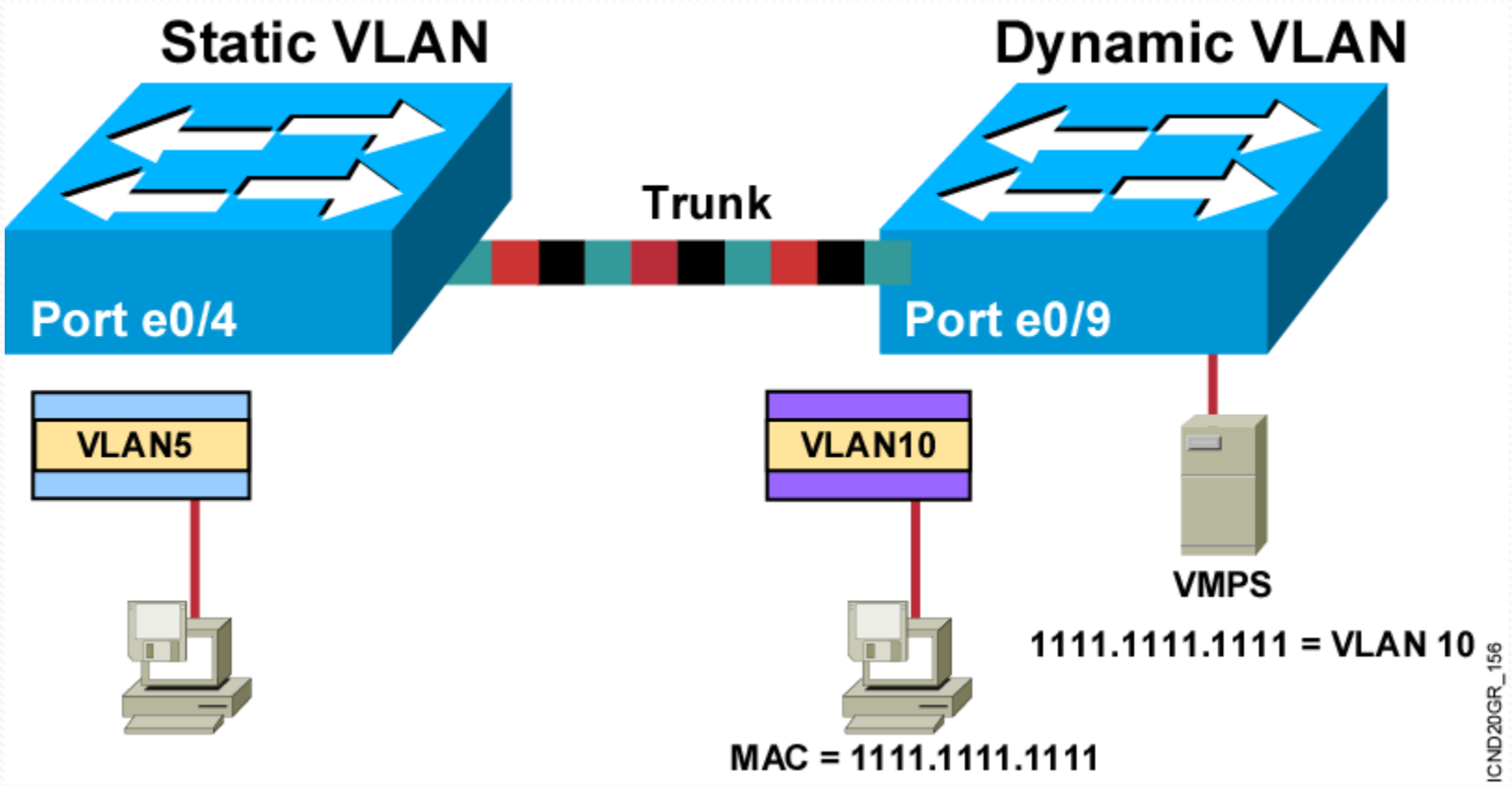
- If we need to break the broadcast domain we need to connect a router
- By using VLAN's we can divide Broadcast domain at Layer-2
- A group of users needing high security can be put into a VLAN so that no users outside of the VLAN can communicate with them.
- As a logical grouping of users by function, VLANs can be considered independent from their physical locations.

VLAN Memberships

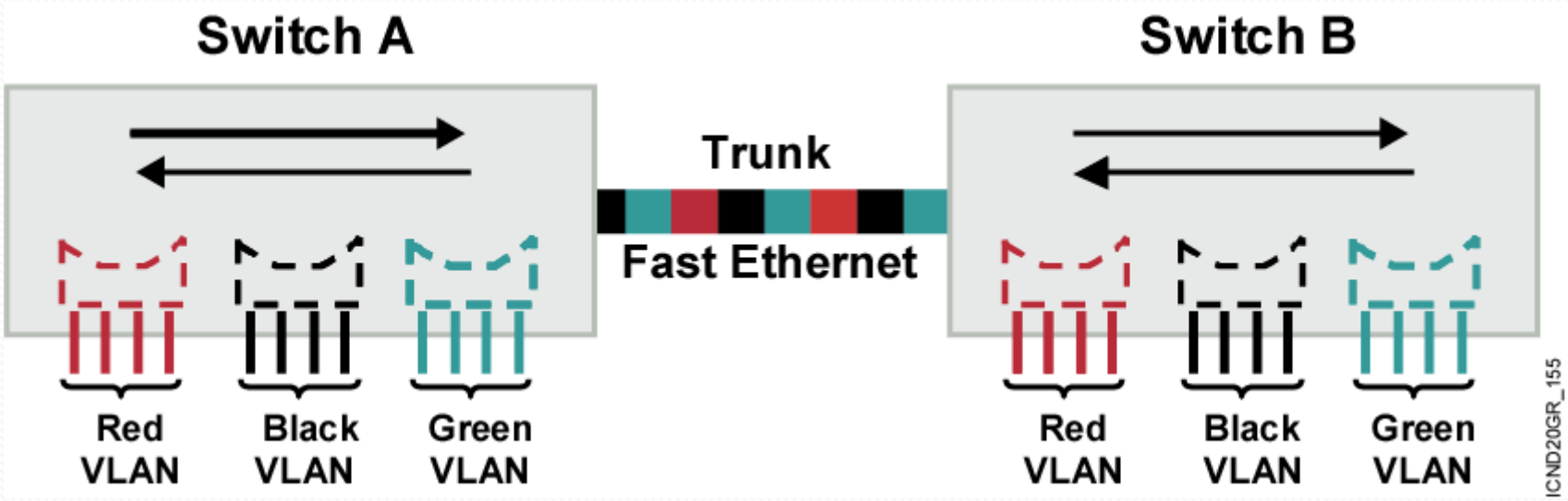
- VLAN created based on port is known as Static VLAN.

- VLAN assigned based on hardware addresses into a database, is called a dynamic VLAN

VLAN Membership Modes



VLAN Operation



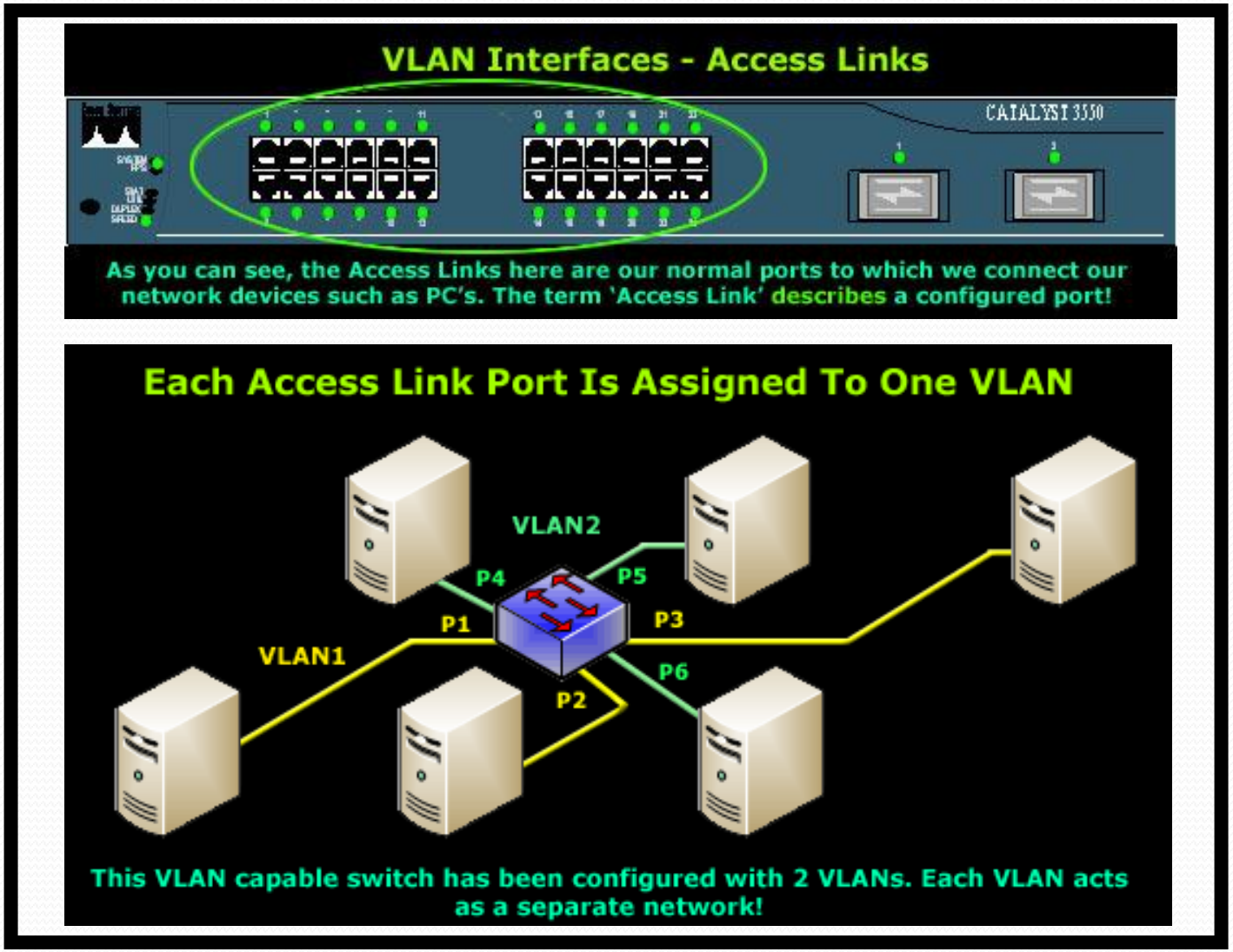
- VLANs can span across multiple switches.
- Trunks carry traffic for multiple VLANs.
- Trunks use special encapsulation to distinguish between different VLANs.

Types of Links

- **Access links**
  - This type of link is only part of one VLAN
  - It's referred to as the *native VLAN* of the port.
  - Any device attached to an *access link* is unaware of a VLAN
  - Switches remove any VLAN information from the frame before it's sent to an access-link device.

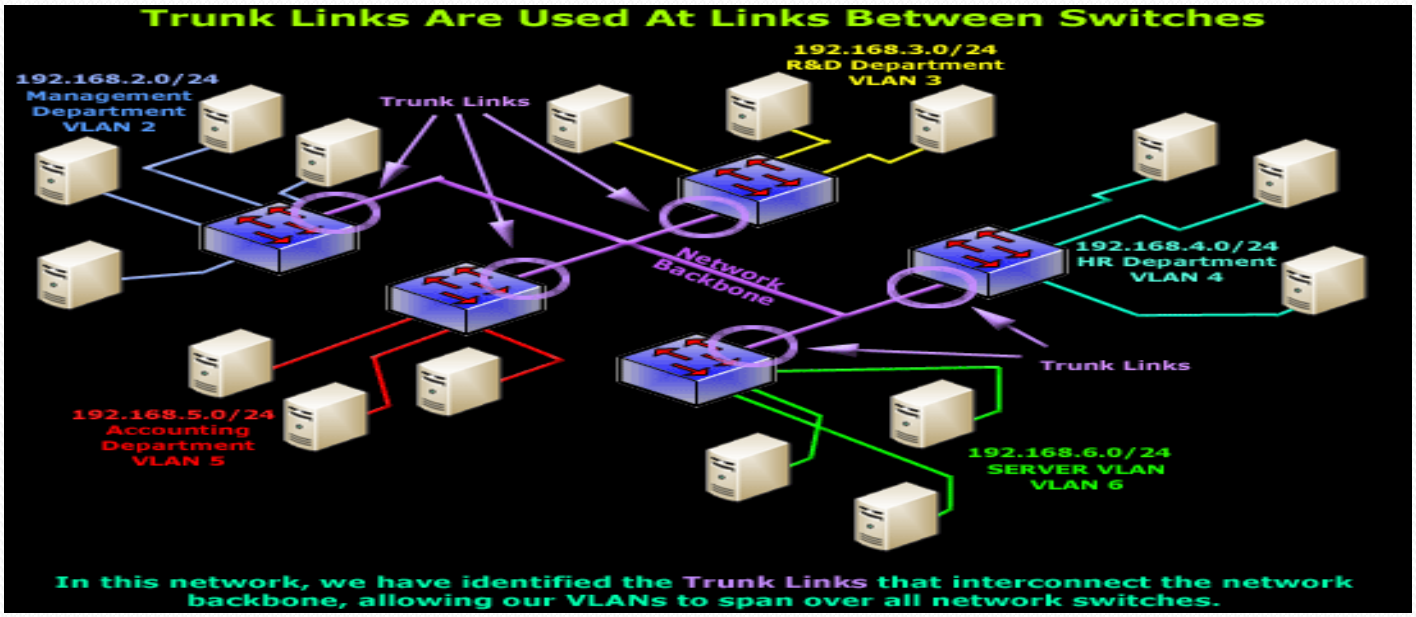
- **Trunk links**
  - Trunks can carry multiple VLANs
  - These carry the traffic of multiple VLANs
  - A trunk link is a 100- or 1000Mbps point-to-point link between two switches, between a switch and router.

Access links



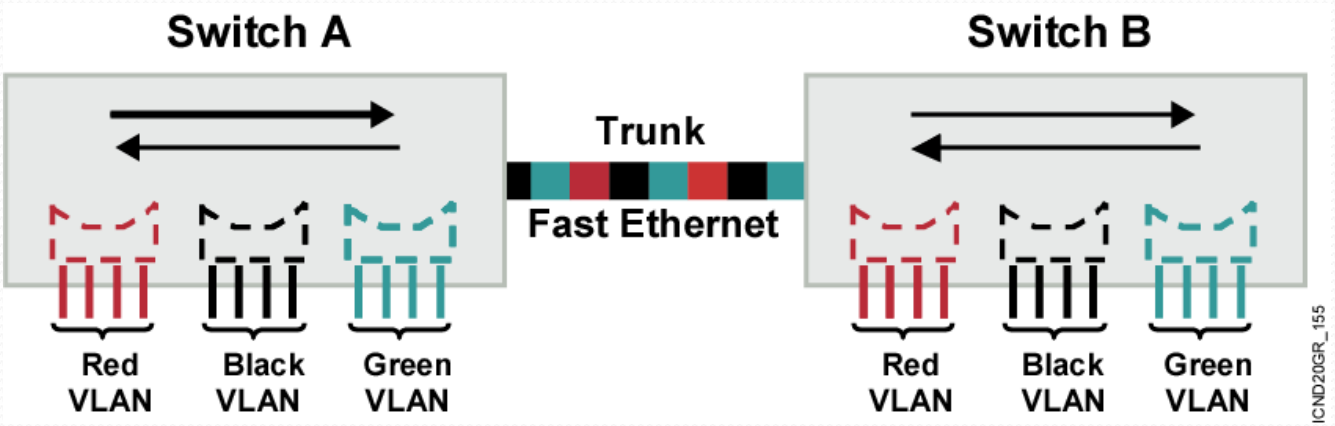
Trunk links

VLAN Interfaces - Trunk Links
CATALYST 3550
Our purple circle indicates the Trunk Links on this Catalyst 3550 switch. These Gigabit ports are usually configured as Trunk Links as in our diagram above.


Trunk Links Are Used At Links Between Switches
192.168.2.0/24
Management
Department
VLAN 2
Trunk Links
192.168.3.0/24
R&D Department
VLAN 3
Network
Backbone
192.168.4.0/24
HR Department
VLAN 4
Trunk Links
192.168.5.0/24
Accounting
Department
VLAN 5
192.168.6.0/24
SERVER VLAN
VLAN 6
In this network, we have identified the Trunk Links that interconnect the network backbone, allowing our VLANs to span over all network switches.

Frame Tagging

- Can create VLANs to span more than one connected switch
- Hosts are unaware of VLAN
- When host A Create a data unit and reaches switch, the switch adds a Frame tagging to identify the VLAN
- Frame tagging is a method to identify the packet belongs to a particular VLAN
- Each switch that the frame reaches must first identify the VLAN ID from the frame tag
- It finds out what to do with the frame by looking at the information in the filter table
- Once the frame reaches an exit to an access link matching the frame's VLAN ID, the switch removes the VLAN identifier

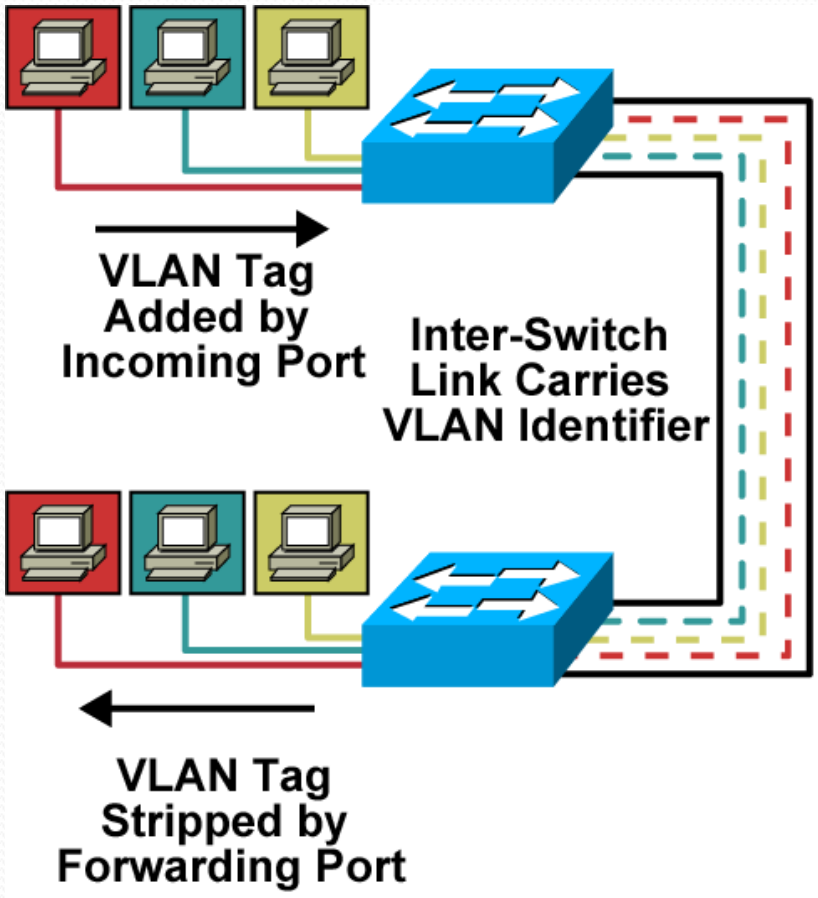


Frame Tagging Methods

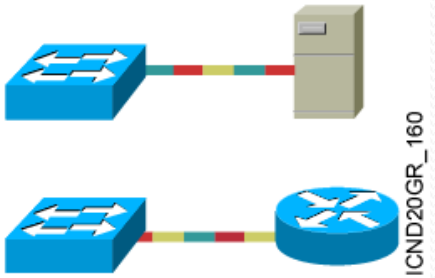
- There are two frame tagging methods
  - Inter-Switch Link (ISL)
  - IEEE 802.1Q
- Inter-Switch Link (ISL)
  - proprietary to Cisco switches
  - used for Fast Ethernet and Gigabit Ethernet links only
- IEEE 802.1Q
  - Created by the IEEE as a standard method of frame tagging
  - it actually inserts a field into the frame to identify the VLAN
  - If you're trunking between a Cisco switched link and a different brand of switch, you have to use 802.1Q for the trunk to work.

ISL Tagging

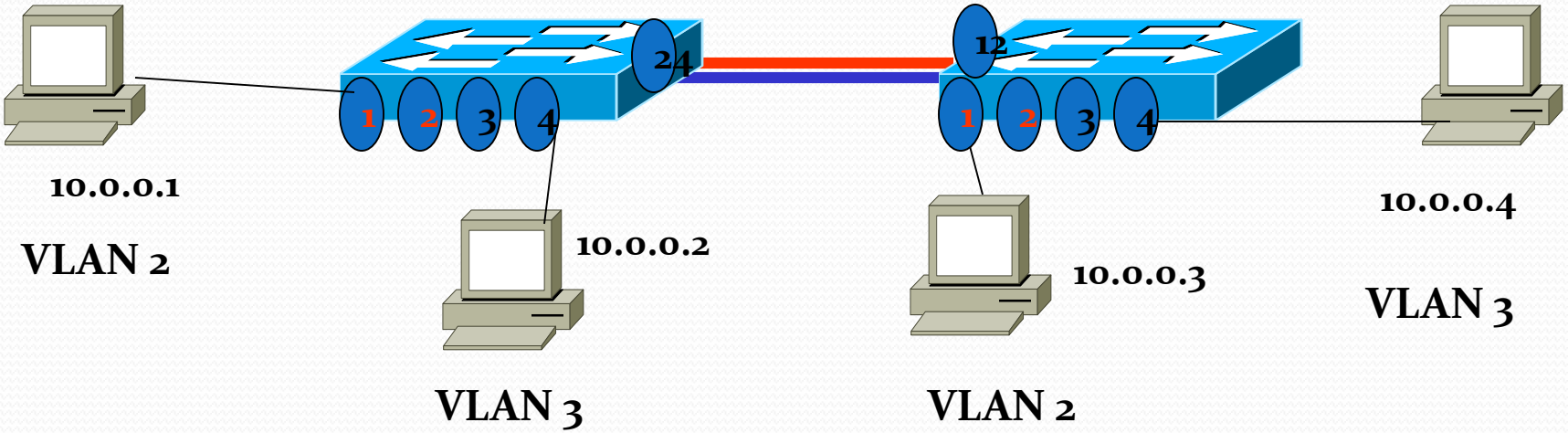
ISL trunks enable VLANs across a backbone.



- Performed with ASIC
- ISL header not seen by client
- Effective between switches, and between routers and switches



VLAN Configuration



VLAN Configuration Steps

- **VLAN Creation:**

!SW1/SW2

Vlan 2

Name Red

Vlan 3

Name Blue

Exit

- **Port Assignment:**

!SW1/SW2

Interface Fa0/1

Switchport access vlan 2

!

Interface fa0/4

Switchport access vlan 3

- **Trunk Configuration:**

!SW1

Int erface fa0/24

Switchport trunk encapsulation dot1q

Switchport mode trunk

Switchport Mode Interactions

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	**Access**	**Trunk**	**Trunk**	**Access**
Dynamic Desirable	**Trunk**	**Trunk**	**Trunk**	**Access**
Trunk	**Trunk**	**Trunk**	**Trunk**	**Not recommended**
Access	**Access**	**Access**	**Not recommended**	**Access**

Note: Table assumes DTP is enabled at both ends.

- show dtp interface – to determine current setting

Verifying the VLAN Configuration

```
Switch#show vlan [id | name] [vlan_num | vlan_name]
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/5, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/11, Fa0/12
                                                 Gi0/1, Gi0/2
2    VLAN0002                          active
51   VLAN0051                          active
52   VLAN0052                          active
…

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
2    enet  100002     1500  -      -      -        -    -        0      0
51   enet  100051     1500  -      -      -        -    -        0      0
52   enet  100052     1500  -      -      -        -    -        0      0
…

Remote SPAN VLANs
------------------------------------------------------------------------------
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Verifying the VLAN Port Configuration

```
Switch#show running-config interface {fastethernet |
gigabitethernet} slot/port
```

- Displays the running configuration of the interface

```
Switch#show interfaces [{fastethernet | gigabitethernet}
slot/port] switchport
```

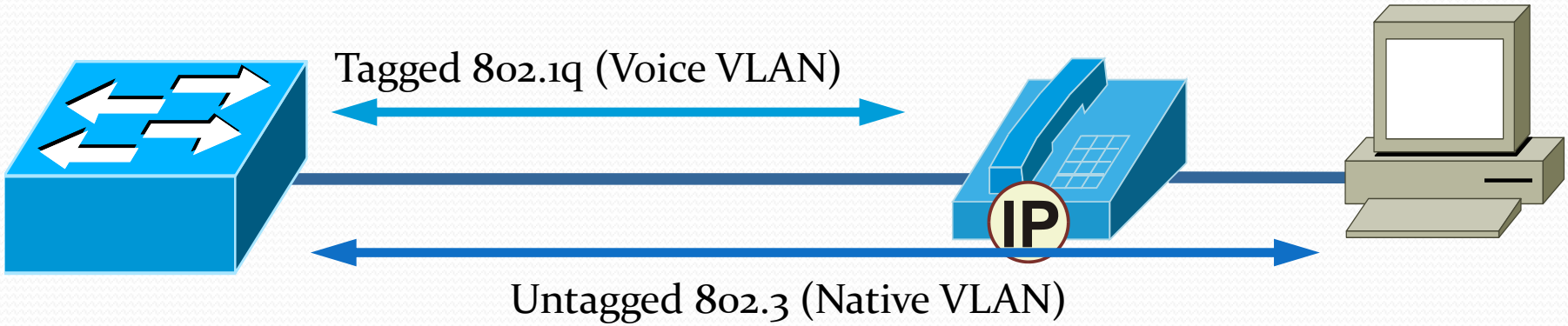
- Displays the switch port configuration of the interface

```
Switch#show mac-address-table interface interface-id [vlan
vlan-id] [ | {begin | exclude | include} expression]
```

- Displays the MAC address table information for the specified interface in the specified VLAN

Configuring Auxiliary VLANs

- An *access* port able to handle 2 VLANs
- *Native* VLAN (PVID) and *Auxiliary* VLAN (VVID)
- Hardware set to *dot1q trunk*



Configuring Auxiliary VLANs (Cont.)

Example 3550 switch or EtherSwitch Network Module

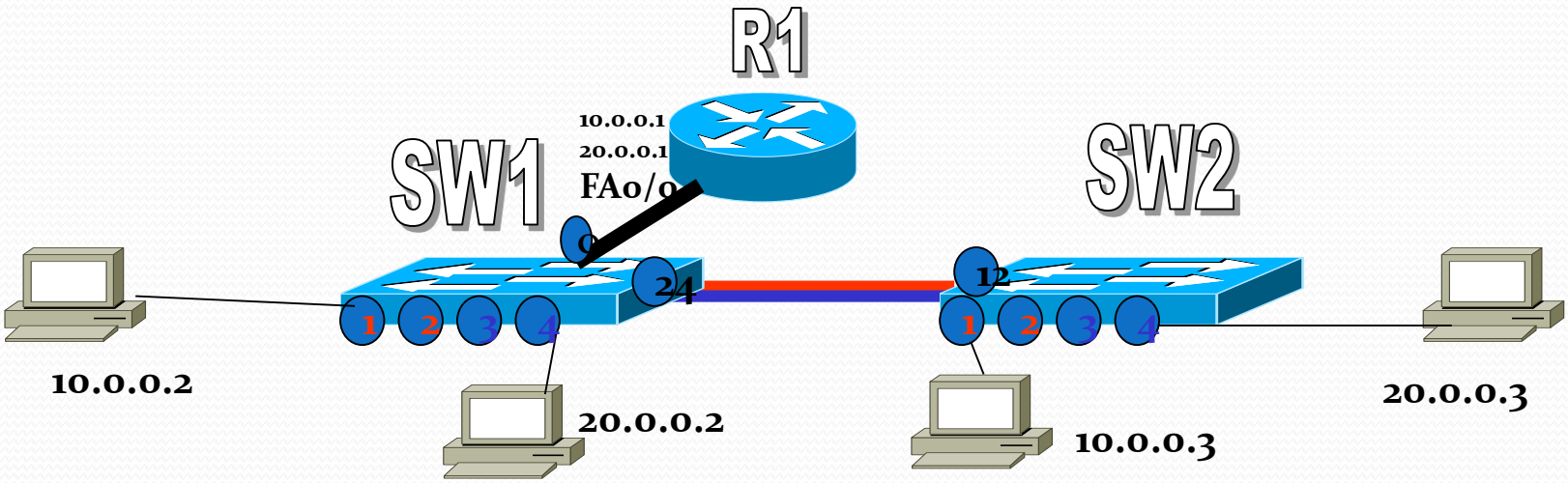
```
SW1(config)#interface FastEthernet0/2
SW1(config-if)#switchport access vlan 10
SW1(Config)#switchport voice vlan 20
!
SW1(config)#interface FastEthernet0/3
SW1(config-if)#switchport access vlan 10
SW1(Config-if)#switchport voice vlan 20
SW1(Config-if)# interface fa0/1
SW1(Config-if)switchport mode trunk
```

- 802.1q trunking is enabled on the port
- The access VLAN is used for the PC plugged into the IP phone
- The voice VLAN is used for voice and signaling that originates and terminates on the IP phone
- Spanning tree portfast enables the port to initialize quickly

VLAN to VLAN

- If you want to connect between two VLANs you need a layer 3 device

Router on Stick



Router On Stick (creating Vlans)

Create two VLAN's on each switches

```
#vlan database
sw(vlan)#vlan 2 name red
sw(vlan)#vlan 3 name blue
sw(vlan)#exit
sw#config t
sw(config)#int fastethernet 0/1
sw(config-if)#switchport access vlan 2
sw(config)#int fastethernet 0/4
sw(config-if)#switchport  access vlan 3
```

To see Interface status

```
#show interface status
```

Router On Stick (Trunk Configuration)

- **Trunk Port Configuration**

- sw#config t
- sw(config)#int fastethernet 0/24
- sw(config-if)#switchport trunk encapsulation dot1q
- sw(config-if)#switchport mode trunk

Router On Stick (Router Configuration)

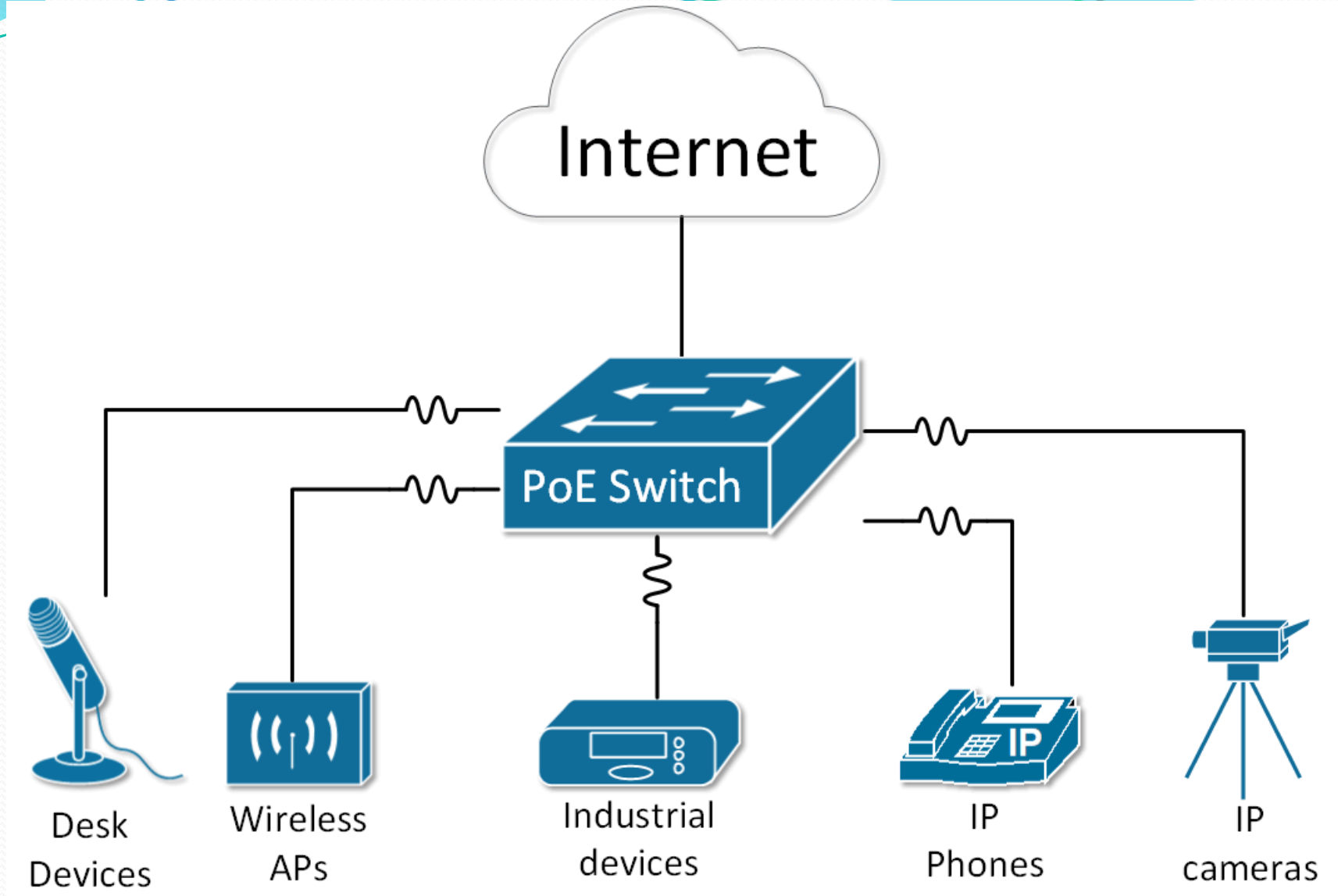
- **Router Configuration**
- R1#config t
- R1(config)#int fastethernet 0/0
- R1(config-if)# no shut
- R1(config)#int fastethernet 0/0.1
- R1(config-if)#encapsulation dot1q 2
- R1(config-if)#ip address 10.0.0.1 255.0.0.0
- R1(config-Iif)# EXIT
- R1(config)#int fastethernet 0/0.2
- R1(config-if)# encapsulation dot1q 3
- R1(config-if)#ip address 20.0.0.1 255.0.0.0

Router On Stick (Switch-Router Port Configuration)

- **Router-Switch Port to be made as Trunk**
- sw(config)#int fastethernet 0/9
- sw(config-if)#switchport trunk enacapsulation dot1q
- sw(config-if)#switchport mode trunk

Power Over Ethernet

- Power over Ethernet (PoE) is a widely used LAN technology that provides DC power to endpoints over existing copper Ethernet cabling used for data connectivity. Power is passed from Power Sourcing Equipment (PSE) over the twisted pairs to Powered Devices (PD) such as IP phones, IP cameras, card readers, selling machines, wireless access points, and other industrial and building appliances.


Internet
PoE Switch
IP
Desk Devices
Wireless APs
Industrial devices
IP Phones
IP cameras

POE Standards

- **IEEE 802.3af (PoE):**
- Provides up to 15.4 watts per port.
- Suitable for low-power devices like IP phones or basic cameras.

- **IEEE 802.3at (PoE+):**
- Provides up to 25.5 watts per port.
- Suitable for devices requiring more power, like PTZ (Pan-Tilt-Zoom) cameras or advanced wireless access points.

- **IEEE 802.3bt (PoE++ or 4PPoE):**
- Provides up to 60 watts (Type 3) or 100 watts (Type 4).
- Ideal for high-power devices like LED lighting or networked displays.

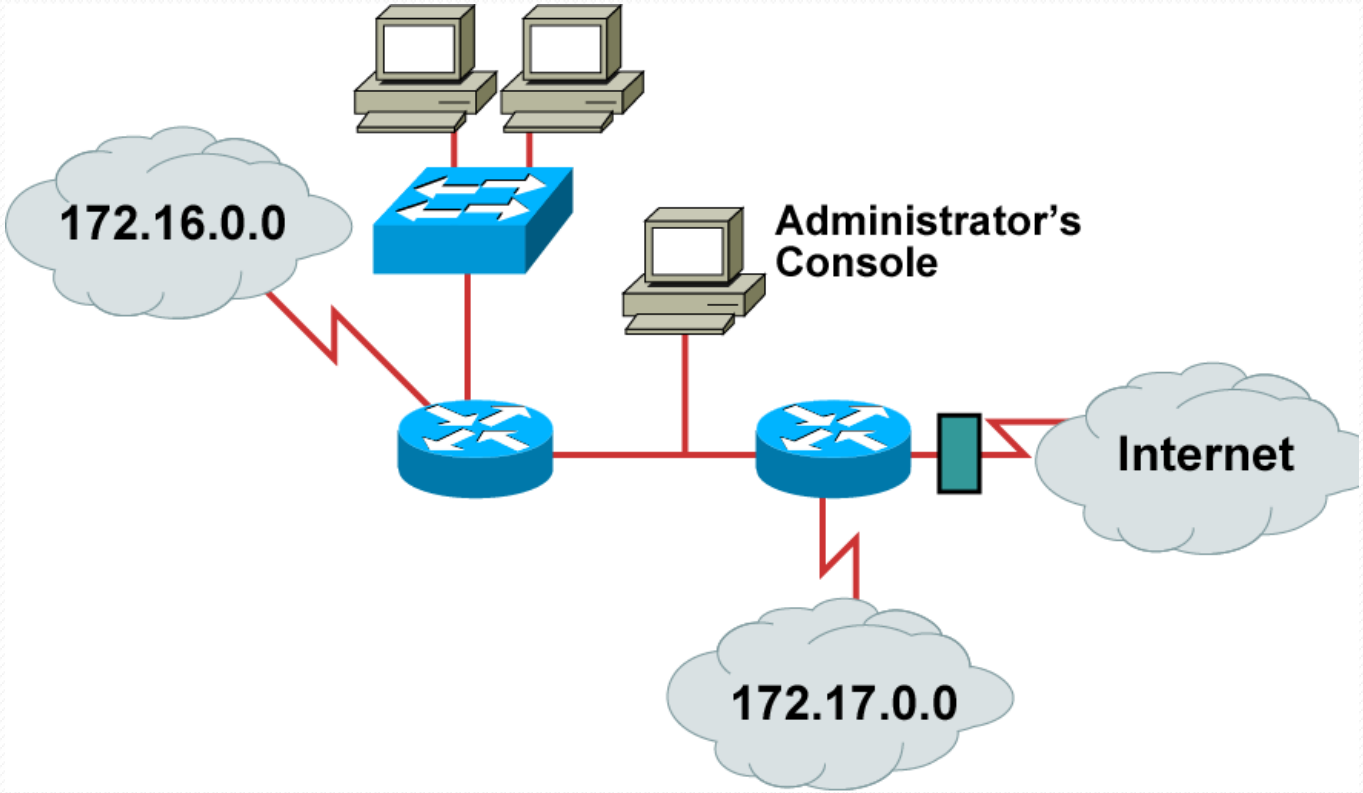
POE Classes

- When you connect an end device to a PoE enabled interface, the switch sends out a detection pulse and waits for a valid detection signature (as defined in 802.3af/at). When the end device responds to this pulse by drawing a standard amount of current, which tells the switch what PoE class the end client is.

Class	Power
Class 0	Up to 12.95 W
Class 1	Up to 3.84 W
Class 2	3.84W to 6.49W
Class 3	6.49W to 12.95W
Class 4	12.95W to 25.5W
Class 5	25.5W to 40W
Class 6	40W to 51W
Class 7	51W to 62W
Class 8	62W to 71.3W

Access Control Lists

Why Use Access Lists?



- Manage IP traffic as network access grows
- Filter packets as they pass through the router

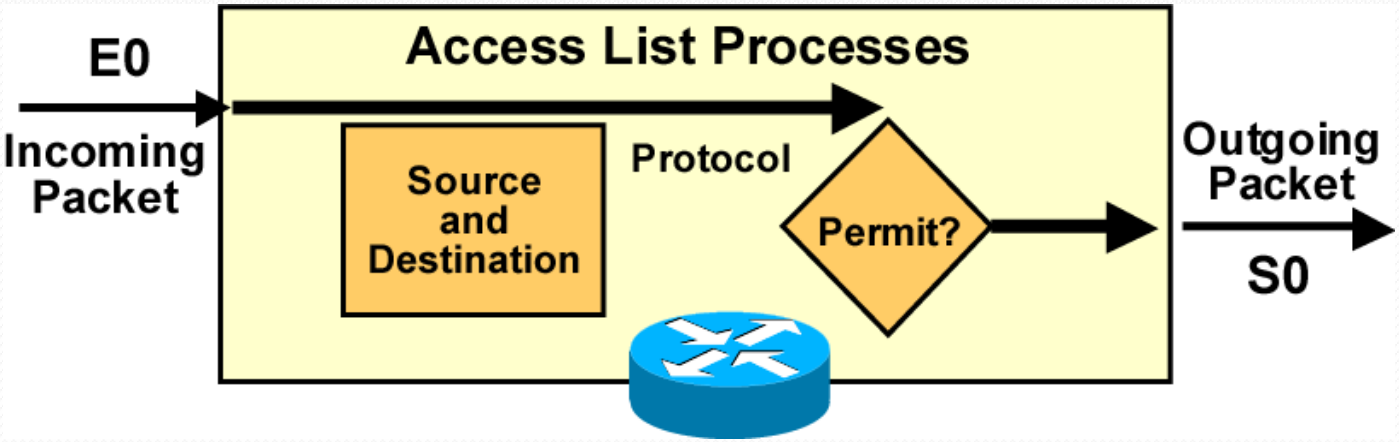
What are ACLs?

- ACLs are lists of conditions that are applied to traffic traveling across a router's interface.
- These lists tell the router what types of packets to accept or deny.
- Acceptance and denial can be based on specified conditions.
- ACLs can be configured at the router to control access to a network or subnet.
- Some ACL decision points are source and destination addresses, protocols, and upper-layer port numbers.

ACL's

- Different access list for Telnet
- When configuring ISDN you need to use access list
- Implicit deny at bottom
- All restricted statements should be on first
- There are two types
  - Standard
  - Extended

Types of Access Lists



- Standard
  - Checks source address
  - Permits or denies entire protocol suite
- Extended
  - Checks source and destination address
  - Generally permits or denies specific protocols

How to Identify Access Lists

Access List Type		Number Range/Identifier
IP	Standard	1-99, 1300-1999
	Extended	100-199, 2000-2699
	Named	Name

ICND20GR_57

- Standard IP lists (1-99) test conditions of all IP packets from source addresses.
- Extended IP lists (100-199) test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports.
- Standard IP lists (1300-1999) (expanded range).
- Extended IP lists (2000-2699) (expanded range).

Standard ACLs

- The full syntax of the standard ACL command is:

- Router(config)#**access-list** *access-list-number* {deny | permit} source [*source-wildcard*]

- The no form of this command is used to remove a standard ACL. This is the syntax:
- Router(config)#**no access-list** *access-list-number*

Config# Access-list 1 deny 192.168.1.0 0.0.0.255
Config# access-list 1 permit any

Wildcard Mask

Access-list 99 permit 192.168.1.1 wildcard mask

All 32 bits of an IP Address can be filtered

Wildcard inverse mask

0=must match

1= ignore

MASK (192.168.1.1)	Matching IP
0.0.0.0 (host)	192.168.1.1
0.0.0.255	192.168.1.0-255
0.0.255.255	192.168.0-255.0-255
0.255.255.255	192.0-255.0-255.0-255
255.255.255.255	0-255.0-255.0-255.0-255 (any)

The ANY and HOST keyword

Access-list 1 permit 0.0.0.0 255.255.255.255

Or

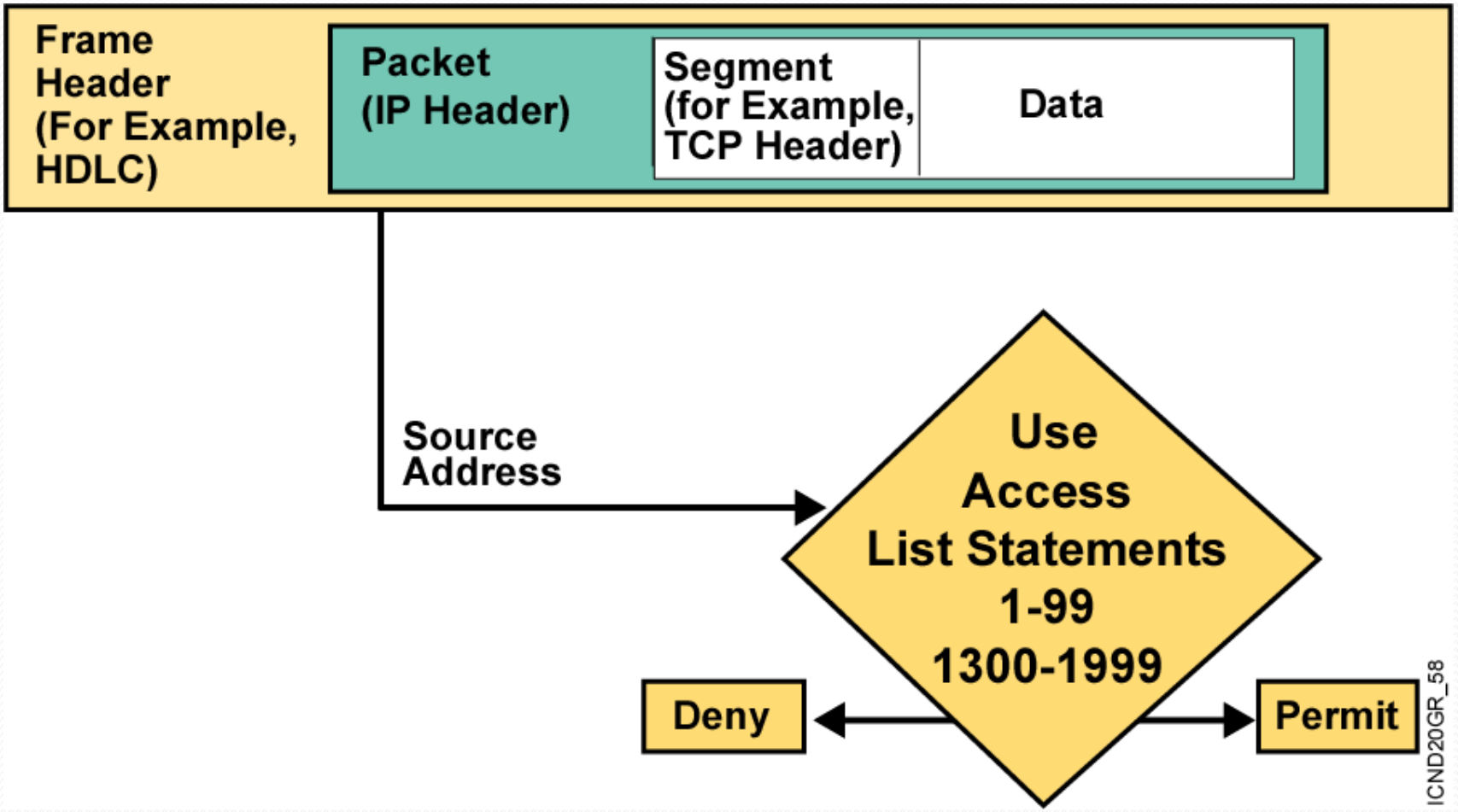
permit any

Access-list 1 permit 200.0.0.9 0.0.0.0

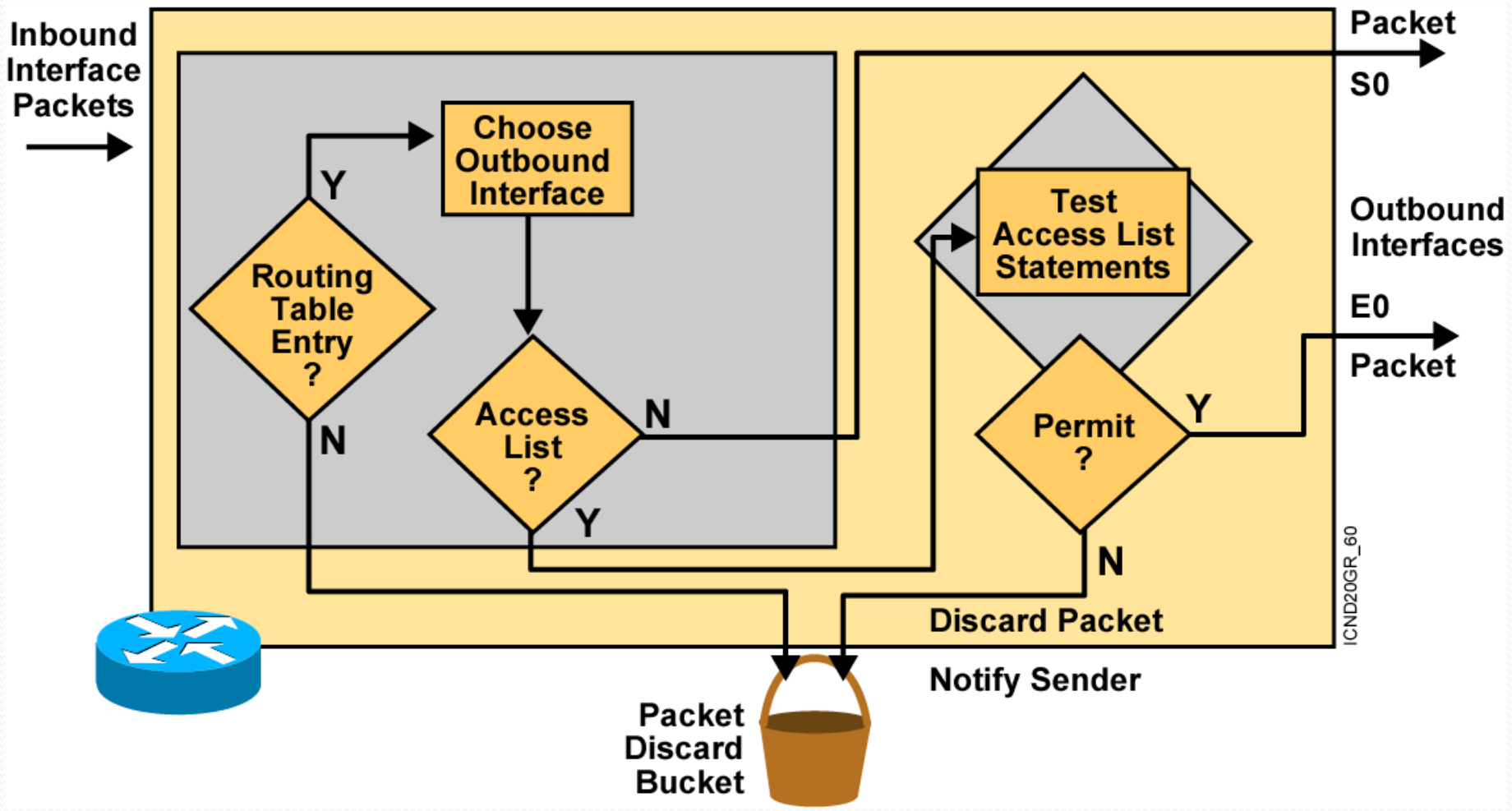
Or

permit host 200.0.0.9

Testing Packets with Standard Access Lists



Outbound ACL Operation



- If no access list statement matches, then discard the packet.

Reading an ACL

- First Hit or Best Fit?

1. Access-list 99 deny 192.168.1.1 0.0.0.0
   access-list 99 permit any

2. Access-list 99 permit 192.168.1.0 0.0.0.255
   Access-list 99 deny host 192.168.1.1
   access-list 99 permit any

3. Access-list 99 deny host 192.168.1.1

- Implicit deny at the end of every ACL

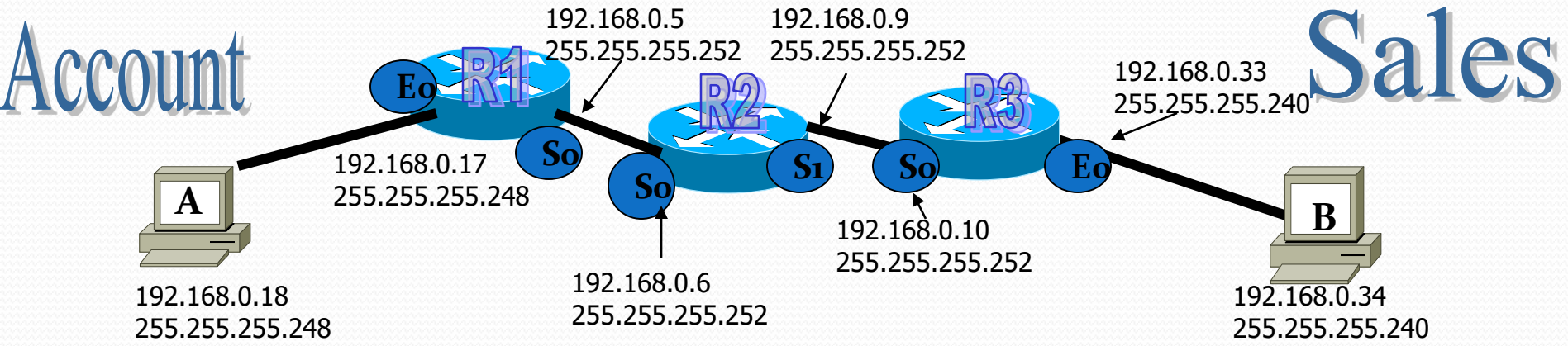
The ip access-group command

Next, you need to apply ACLs to an interface by using the **access-group** command, as in this example:

`Router(config-if)#{protocol}` **access-group** *access-list-number* { **in** | **out** }

All the ACL statements identified by *access-list-number* are associated with one or more interfaces. Any packets that pass the ACL test conditions can be permitted to use any interface in the access group of interfaces.

Exercise – Standard Access List

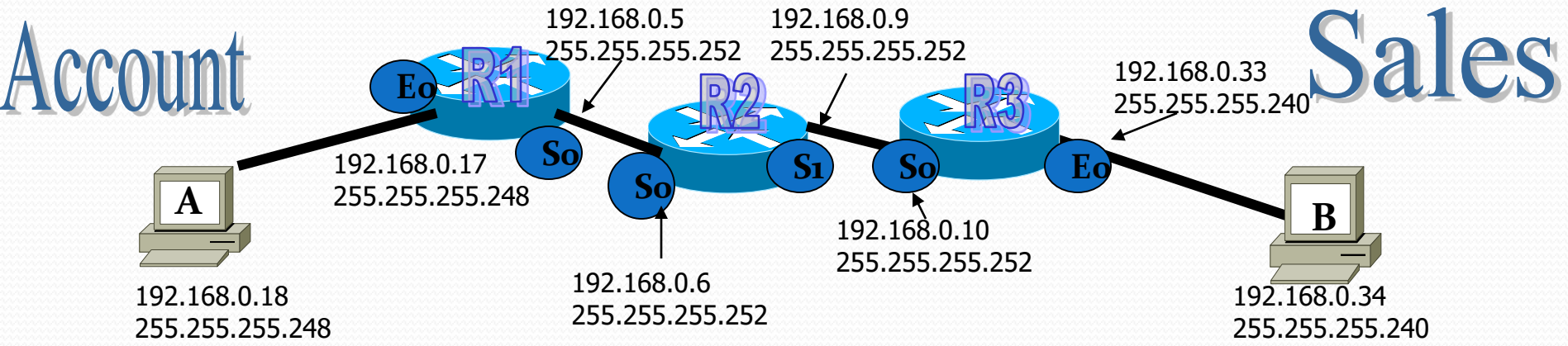


Account should be denied access to Sales

To steps to configure

- Create a standard Access list
- Apply ACL to proper interface inbound or outbound

Exercise – Standard Access List



Creating access list

Config# Access-list 1 deny 192.168.0.18 0.0.0.7
Config# access-list 1 permit any

Applying access list

Config#int e 0
Config-if# ip access-group 1 out

Extended ACLs

- Extended ACLs are used more often than standard ACLs because they provide a greater range of control.
- Extended ACLs check the source and destination packet addresses as well as being able to check for protocols and port numbers.
- At the end of the extended ACL statement, additional precision is gained from a field that specifies the optional Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number.
- Logical operations may be specified such as, equal (eq), not equal (neq), greater than (gt), and less than (lt), that the extended ACL will perform on specific protocols.
- Extended ACLs use an access-list-number in the range 100 to 199 (also from 2000 to 2699 in recent IOS).

Configuration

- Access-list acl# {permit/Deny}
  - Protocol
  - Src IP src WCM
  - Dst IP dst WCM
  - Opetrator port

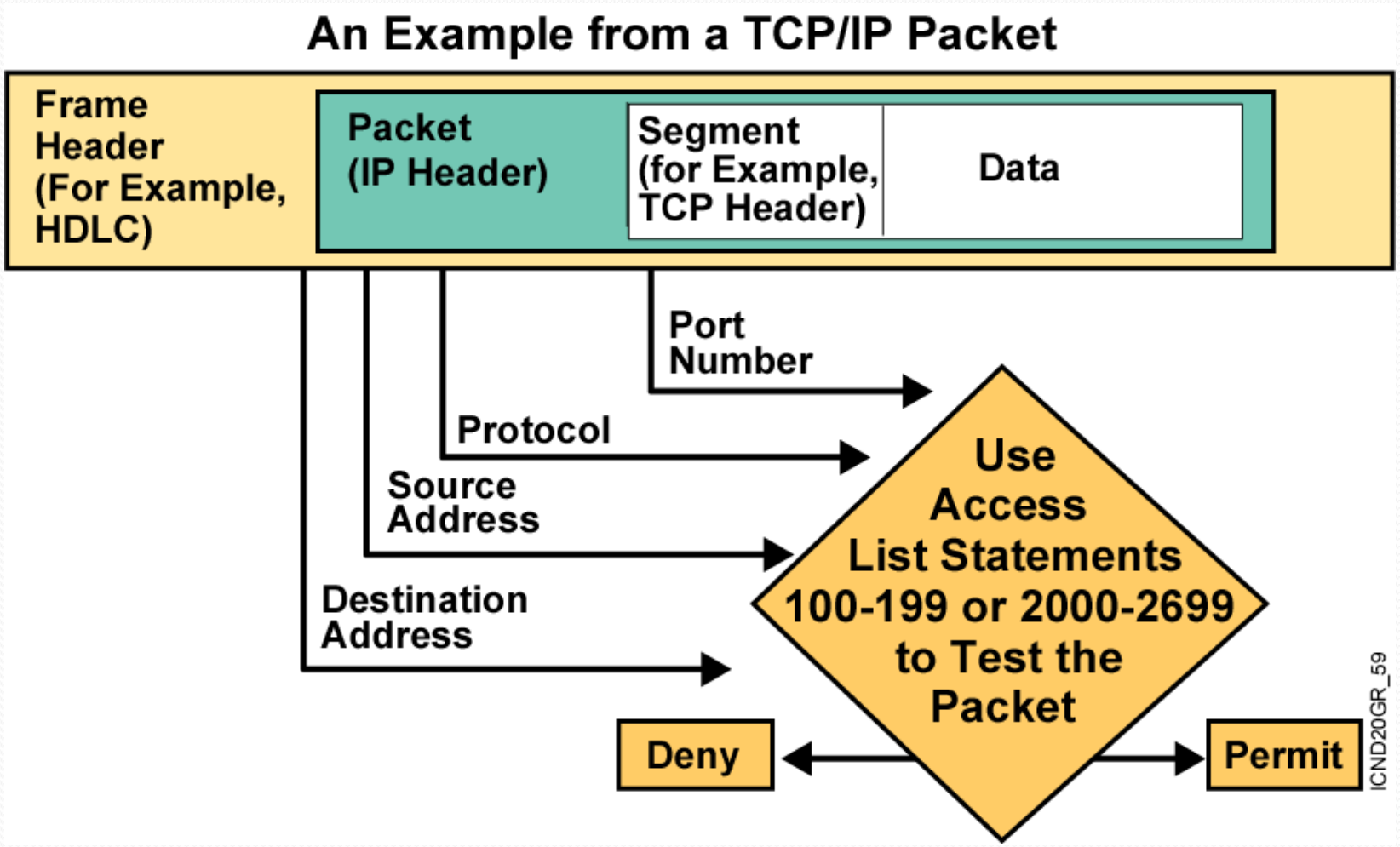
- **Protocol**
  - OSPF
  - EIGRP
  - ICMP
  - TCP
  - UDP

RP If you need to Block a routing protocol

IP

- **Operator**
  - eq
  - gt
  - lt
  - neq

Testing Packets with Extended Access Lists



Extended ACL Syntax

```
Router(config)#access-list access-list-number {permit | deny}
protocol source
[source-mask destination destination-mask operator operand]
```

Paramter	Description
access-list-number	Identifies the list using a number in the range 100 to 199.
permit | **deny**	Indicates whether this entry allows or blocks the specified address.
protocol	The protocol, such as IP, TCP, UDP, ICMP, GRE, or IGRP.
source and **destination**	Identifies source and destination addresses.
source-mask and *destination-mask*	Wildcard mask; zeros indicate positions that must match, ones indicate do not care positions.
operator operand	lt, gt, eq, neq (less than, greater than, equal, not equal), and a port number.
established	Allows TCP traffic to pass if the packet uses an established connection (for example, has ACK bits set).

Verify Access List

Command	Effect
`show access-list`	Displays all access lists and their parameters configured on the router. This command does not show you which interface the list is set on.
`show access-list 110`	Shows only the parameters for the access list 110. This command does not show you the interface the list is set on.
`show ip access-list`	Shows only the IP access lists configured on the router.
`show ip interface`	Shows which interfaces have access lists set.
`show running-config`	Shows the access lists and which interfaces have access lists set.

Network Address Translation

New Addressing Concepts

- Problems with IPv4
  - **Shortage of IPv4 addresses**
  - **Allocation of the last IPv4 addresses was for the year 2005**
  - **Address classes were replaced by usage of CIDR, but this is not sufficient**

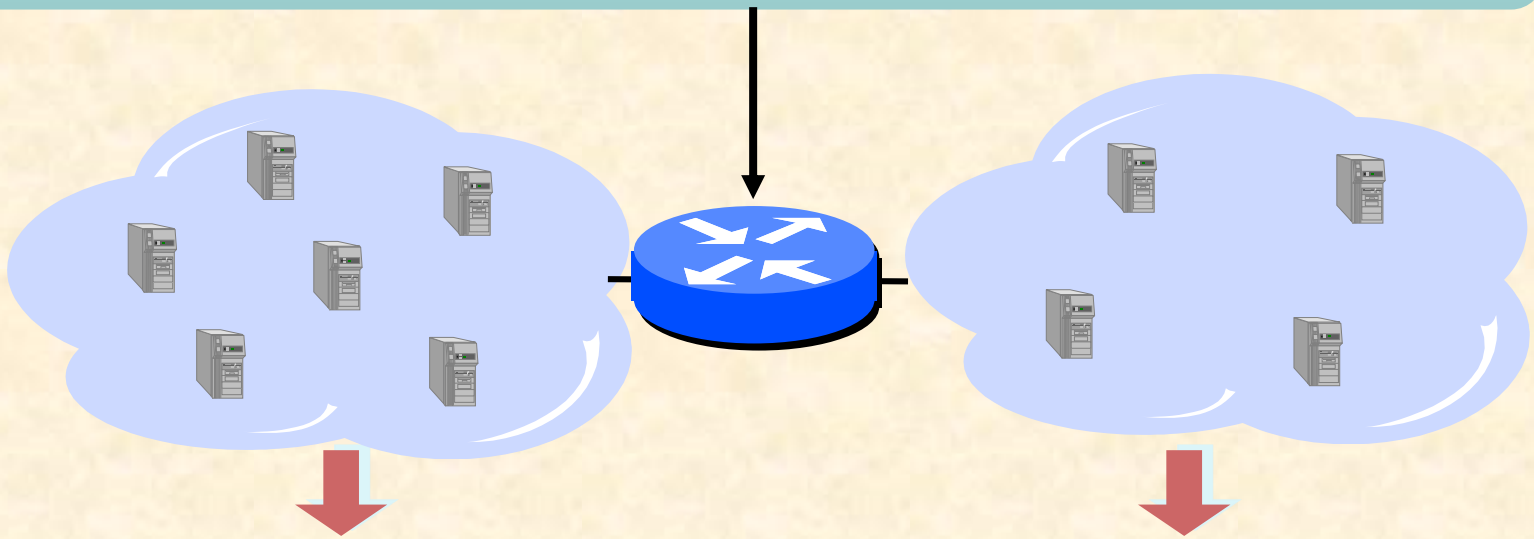
- Short term solution
  - **NAT: Network Address Translator**

- Long term solution
  - **IPv6 = IPng (IP next generation)**
  - **Provides an extended address range**

Fig. 2 Address shortage and possible solutions (TI1332EU02TI_0003 New Address Concepts, 5)

NAT: Network Address Translator

- NAT
  - **Translates between local addresses and public ones**
  - **Many private hosts share few global addresses**

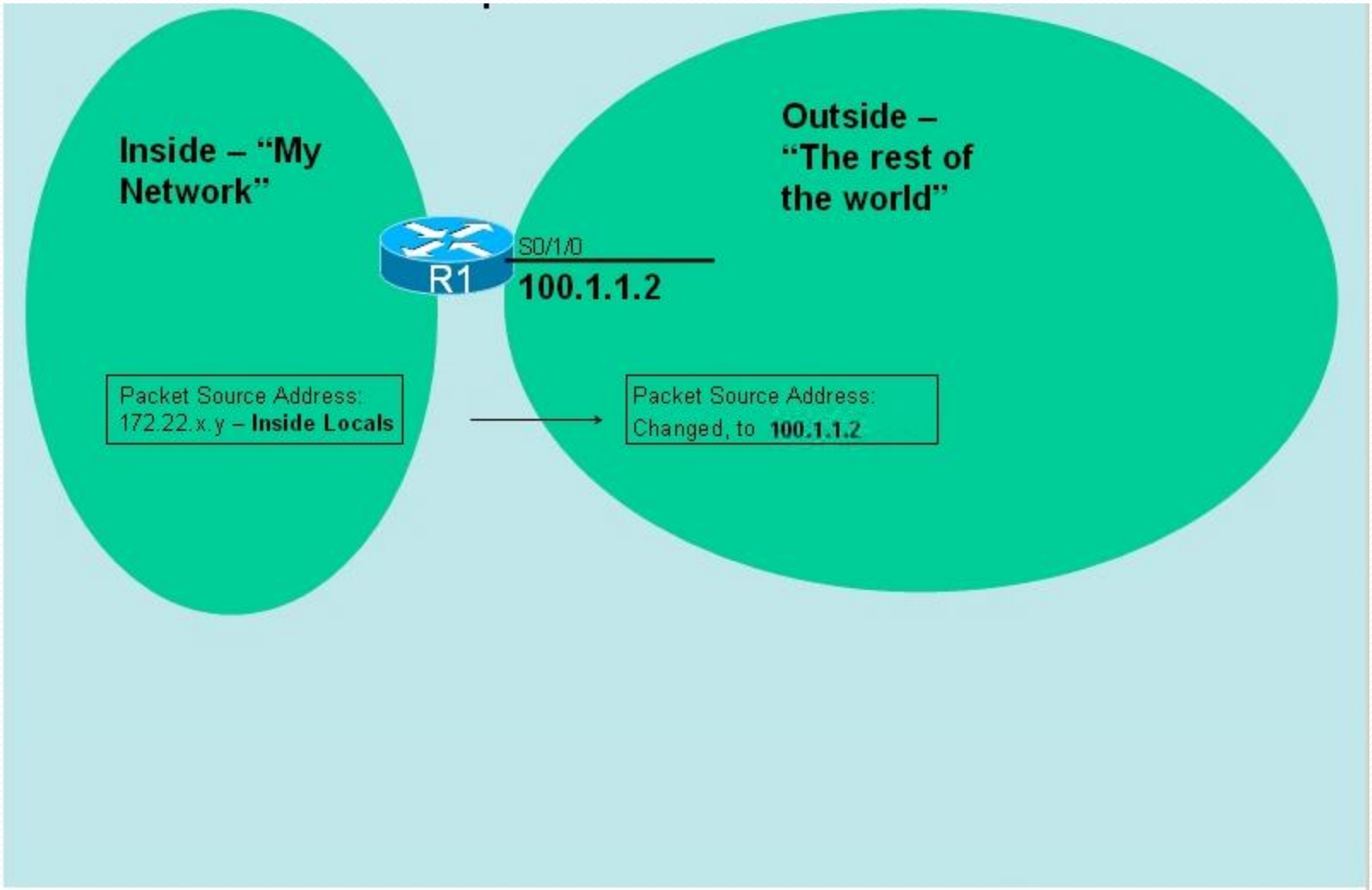


- Private Network
  - **Uses private address range (local addresses)**
  - **Local addresses may not be used externally**
- Public Network
  - **Uses public addresses**
  - **Public addresses are globally unique**

Private Addressing

Address Class	Reserved Address Space
Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

Inside/Outside



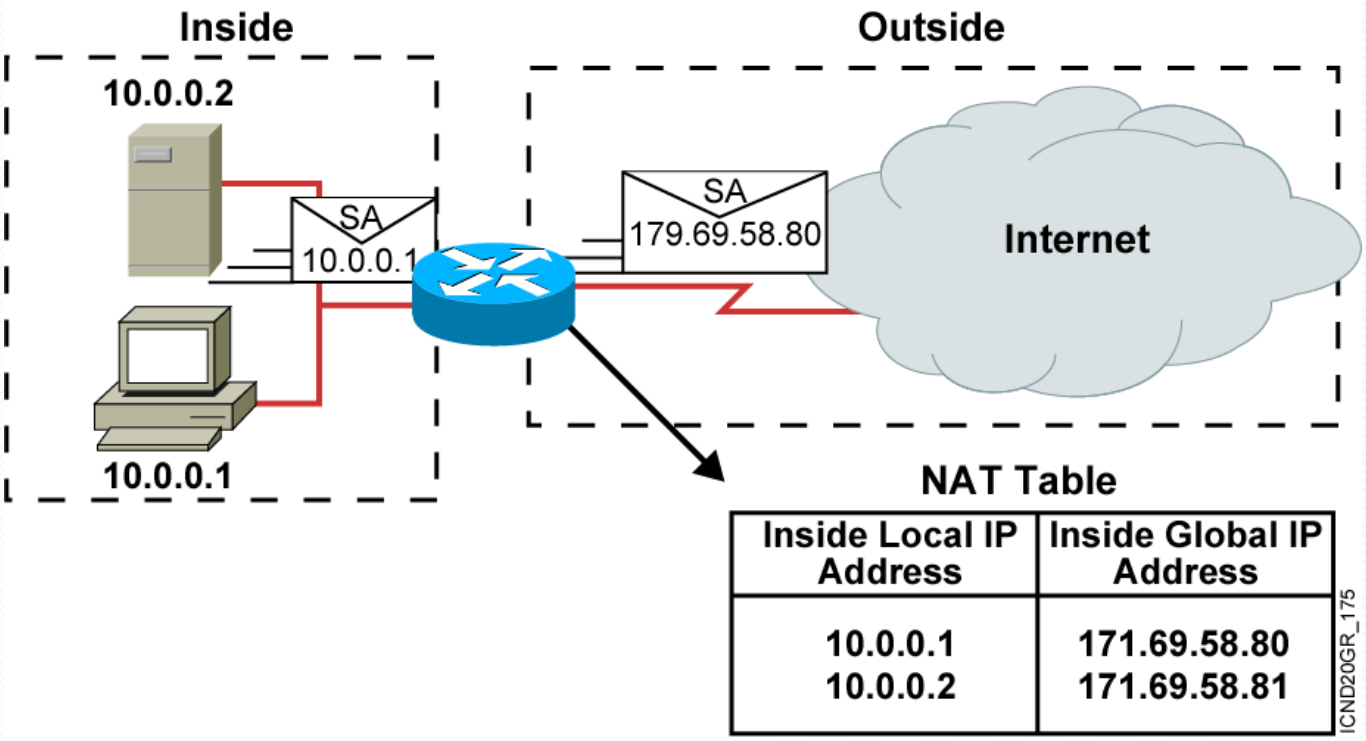
NAT Addressing Terms

- Inside Local
  - The term "inside" refers to an address used for a host inside an enterprise. It is the actual IP address assigned to a host in the private enterprise network.
- Inside Global
  - NAT uses an inside global address to represent the inside host as the packet is sent through the outside network, typically the Internet.
  - A NAT router changes the source IP address of a packet sent by an inside host from an inside local address to an inside global address as the packet goes from the inside to the outside network.

NAT Addressing Terms

- Outside Global
  - The term "outside" refers to an address used for a host outside an enterprise, the Internet.
  - An outside global is the actual IP address assigned to a host that resides in the outside network, typically the Internet.
- Outside Local
  - NAT uses an outside local address to represent the outside host as the packet is sent through the private network.
  - This address is outside private, outside host with a private address

Network Address Translation



- **An IP address is either local or global.**
- **Local IP addresses are seen in the inside network.**

Types Of NAT

- There are different types of NAT that can be used, which are
  - Static NAT
  - Dynamic NAT
  - Overloading NAT with PAT (NAPT)

Static NAT

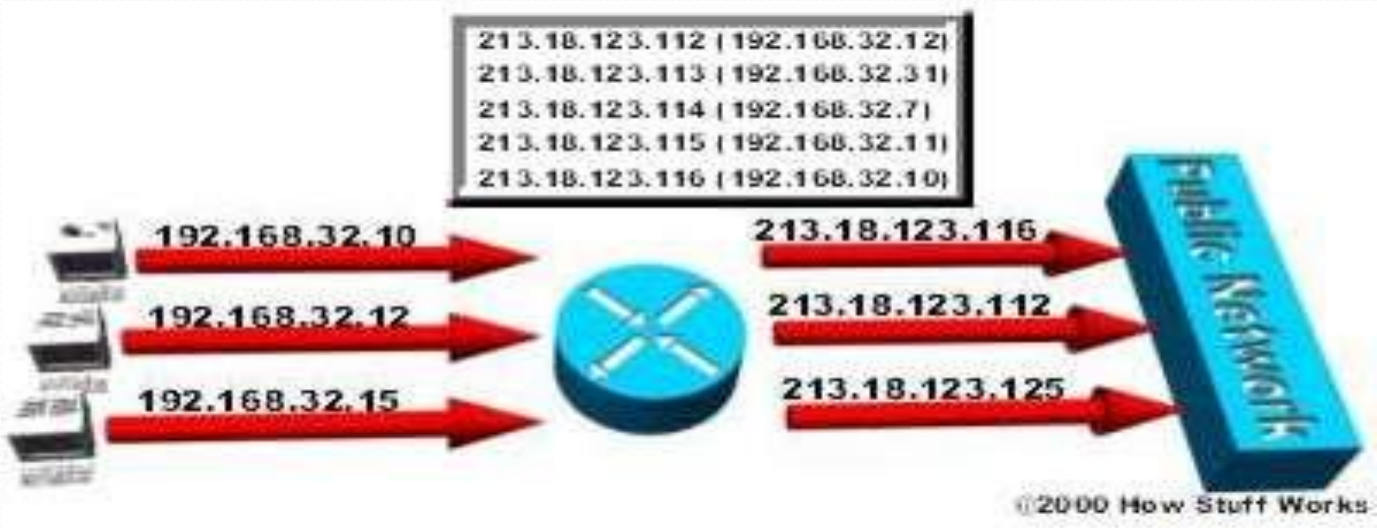
- **Static NAT - Mapping an unregistered IP address to a registered IP address on a one-to-one basis. Particularly useful when a device needs to be accessible from outside the network.**

- **In static NAT, the computer with the IP address of 192.168.32.10 will always translate to 213.18.123.110.**

Dynamic NAT

- Dynamic NAT - Maps an unregistered IP address to a registered IP address from a group of registered IP addresses.

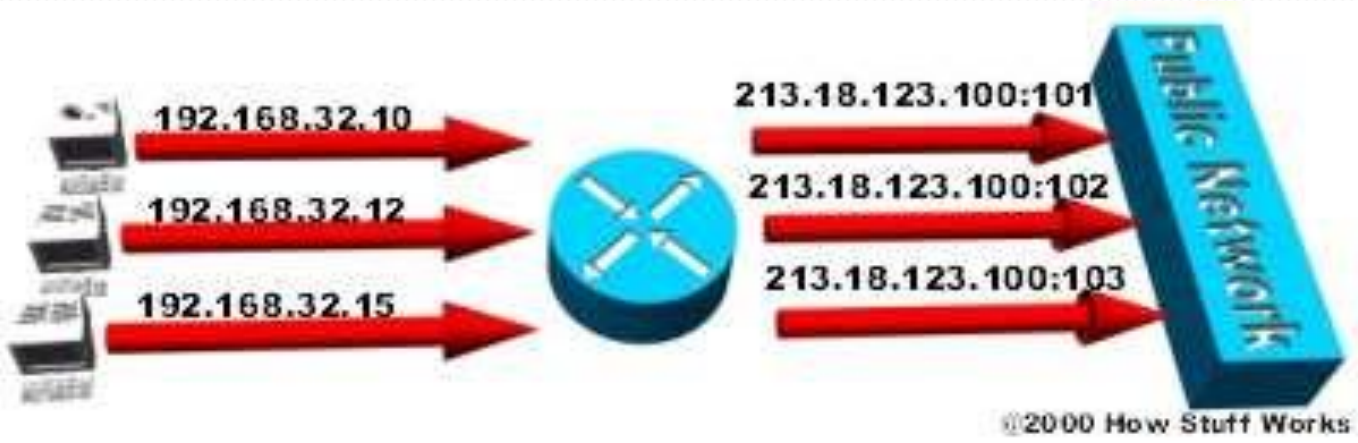
- In dynamic NAT, the computer with the IP address 192.168.32.10 will translate to the first available address in the range from 213.18.123.100 to 213.18.123.150.



Overloading NAT with PAT (NAPT)

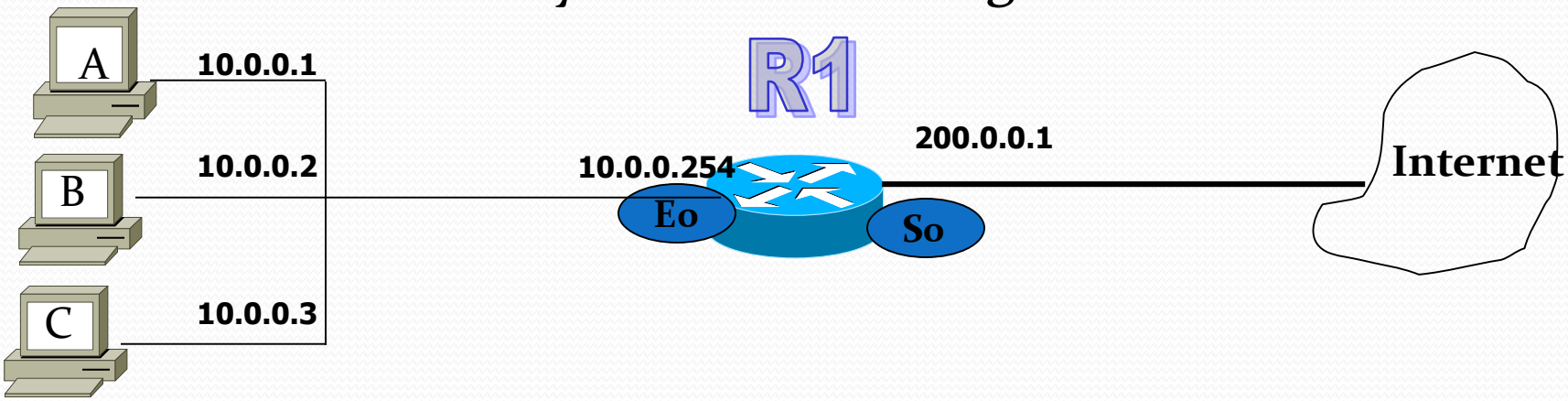
- Overloading - A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. This is known also as PAT (Port Address Translation), single address NAT or port-level multiplexed NAT.

- In overloading, each computer on the private network is translated to the same IP address (213.18.123.100), but with a different port number assignment..



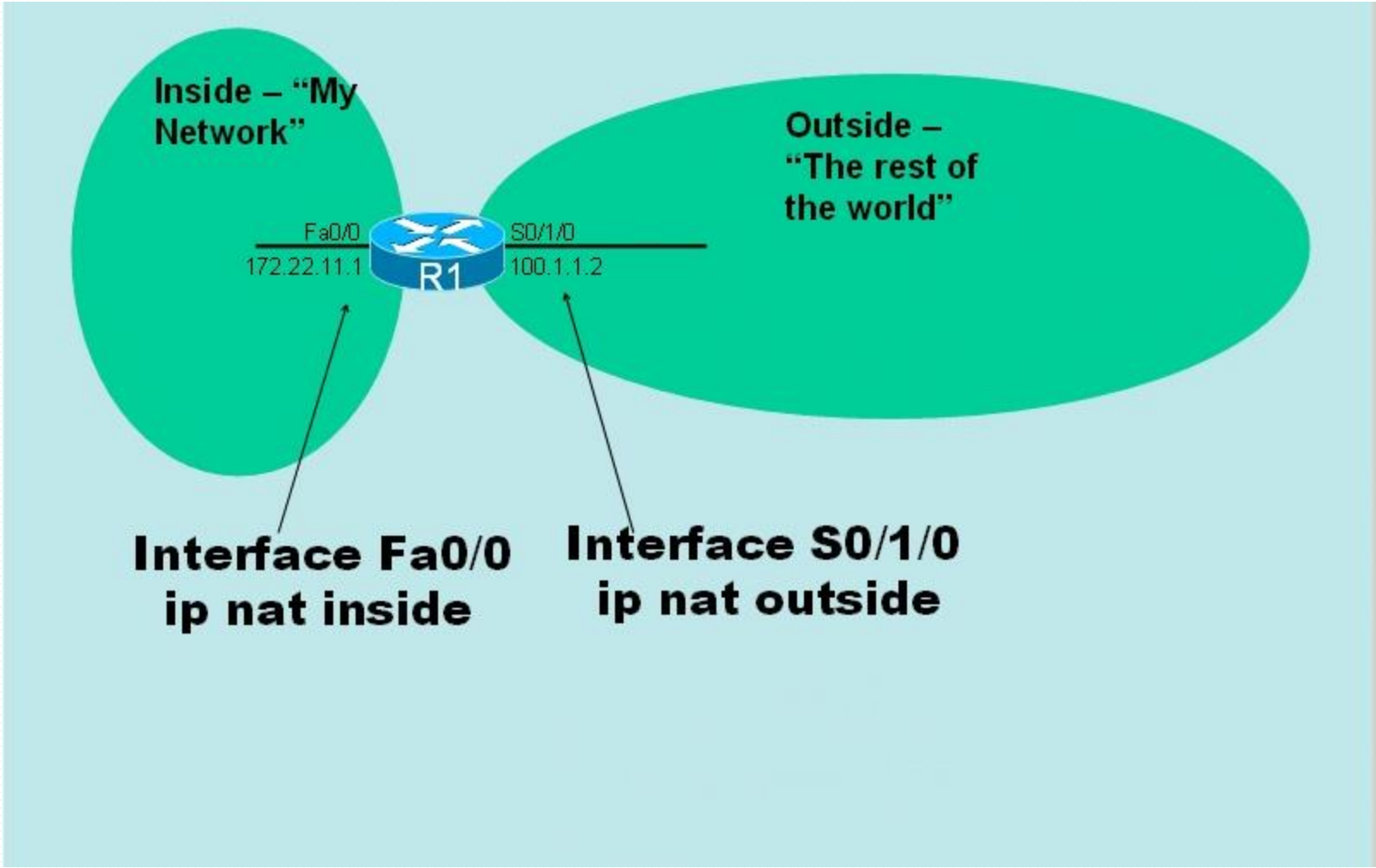
Static NAT Configuration

- For each interface you need to configure INSIDE or OUTSIDE



R1(config)#Int fastethernet 0/0
R1(config-if)# IP NAT inside
R1(config-if)#Int s 0/0
R1(config-if)# IP NAT outside
R1(config-if)# Exit
R1(config)# ip NAT inside source static 10.0.0.1 200.0.0.1
To see the table
R1#show ip nat translations
R1#show ip nat statistics

INSIDE/OUTSIDE



Dynamic NAT

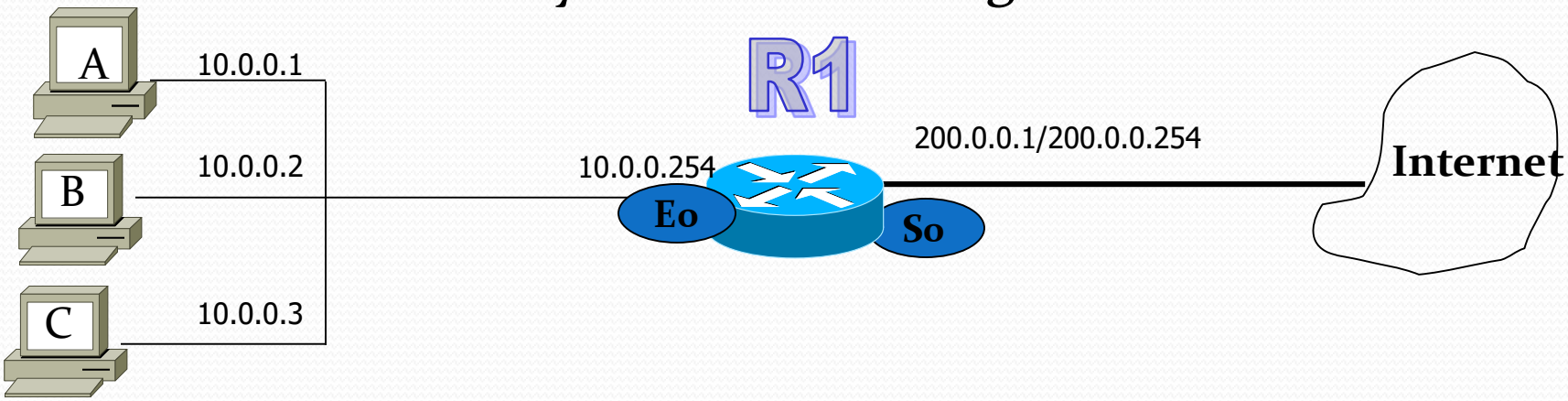
- Dynamic NAT sets up a pool of possible inside global addresses and defines criteria for the set of inside local IP addresses whose traffic should be translated with NAT.
- The dynamic entry in the NAT table stays in there as long as traffic flows occasionally.
- If a new packet arrives, and it needs a NAT entry, but all the pooled IP addresses are in use, the router simply discards the packet.

Dynamic NAT

- Instead of creating static IP, create a pool of IP Address, Specify a range
- Create an access list and permit hosts
- Link Access list to the Pool

Dynamic NAT Configuration

- For each interface you need to configure INSIDE or OUTSIDE



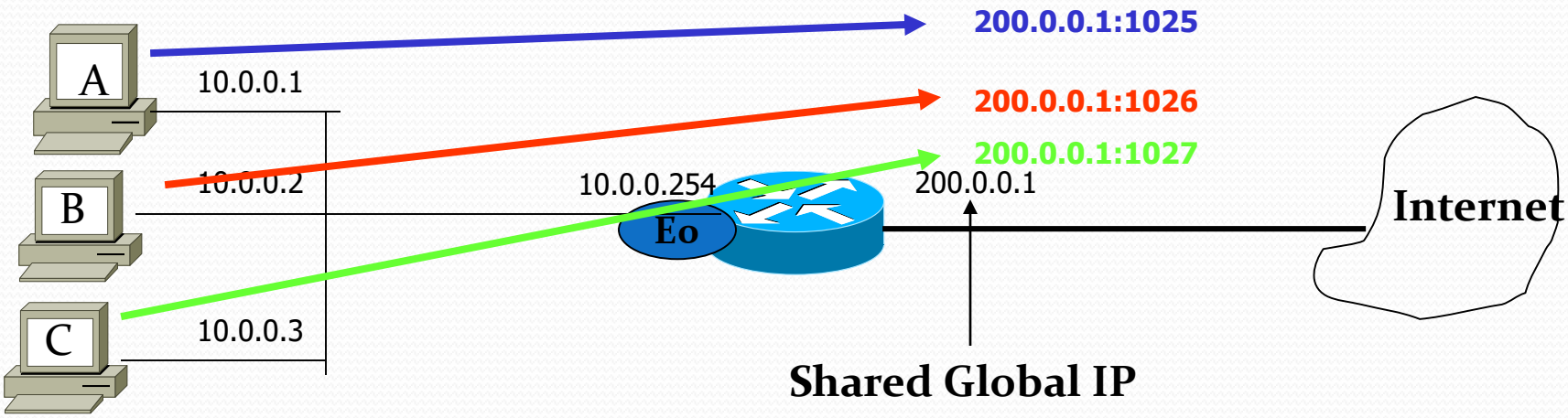
Create an Access List
R1(config)# Access-list 1 permit 10.0.0.0 0.255.255.255

Configure NAT dynamic Pool
R1(config)# IP NAT pool cisco 200.0.0.1 200.0.0.254 netmask 255.255.255.0

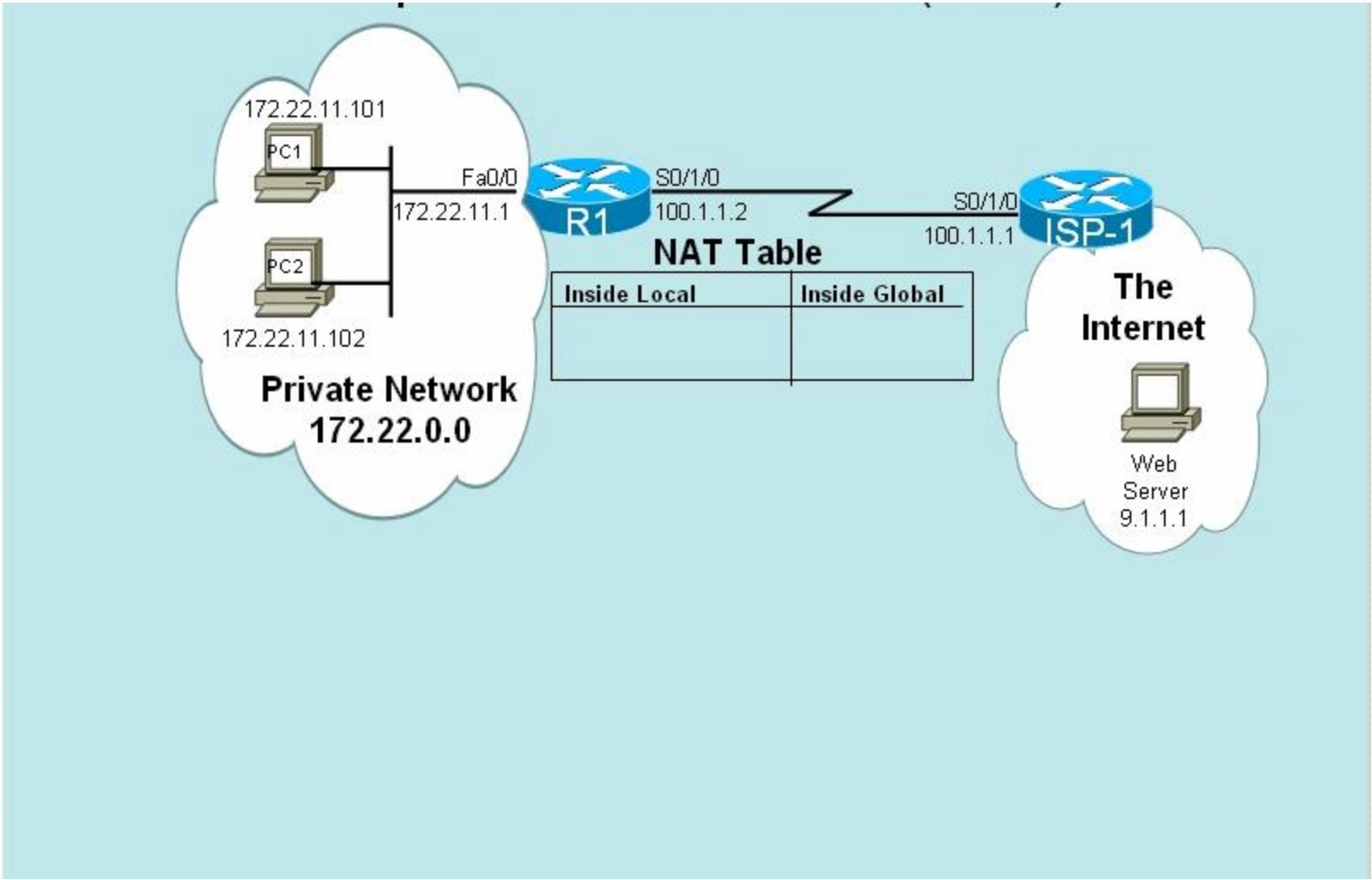
Link Access List to Pool
R1(config)# IP NAT inside source list 1 pool cisco

PAT

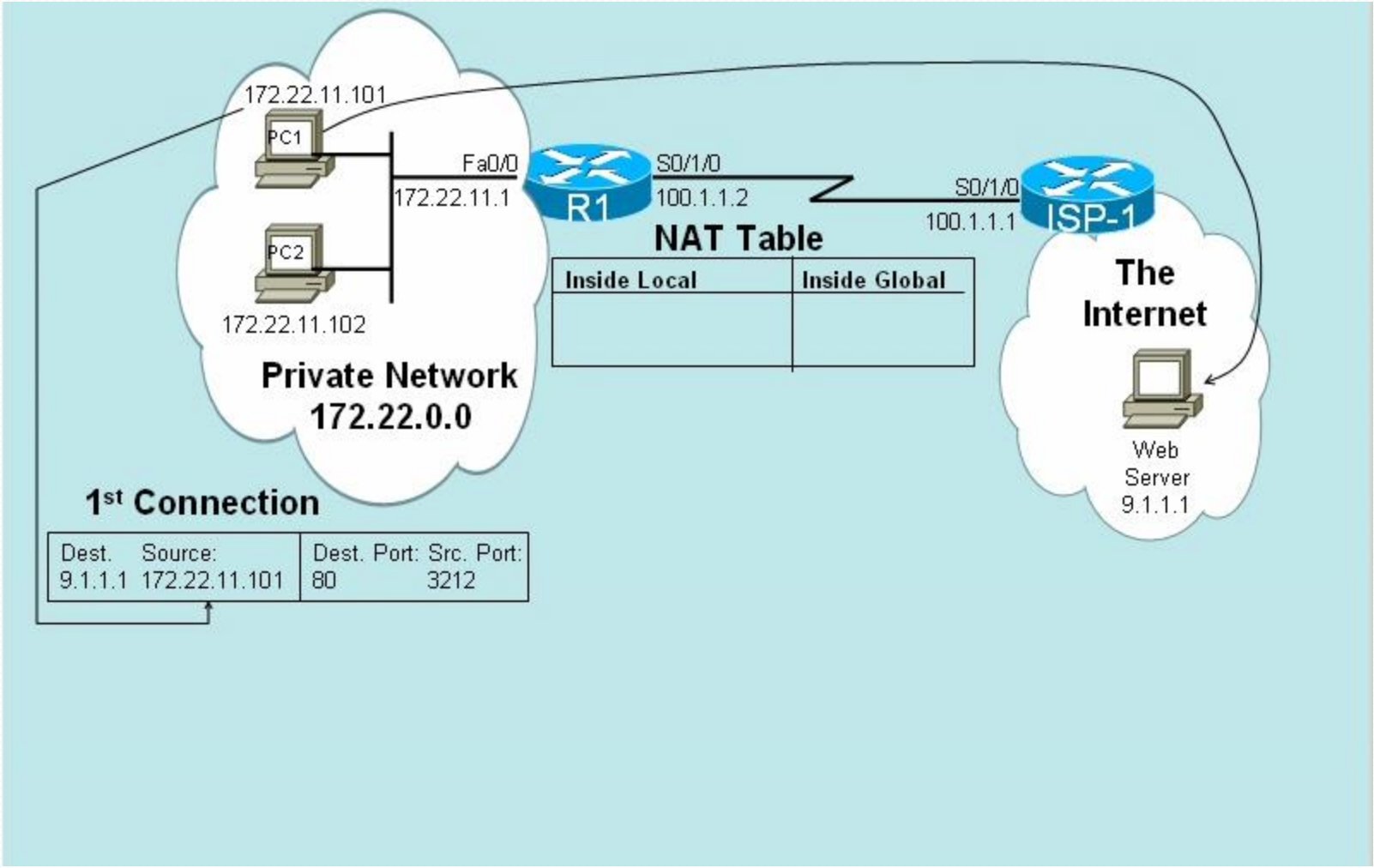
- Overloading an inside global address
- NAT overload only one global IP shared among all hosts



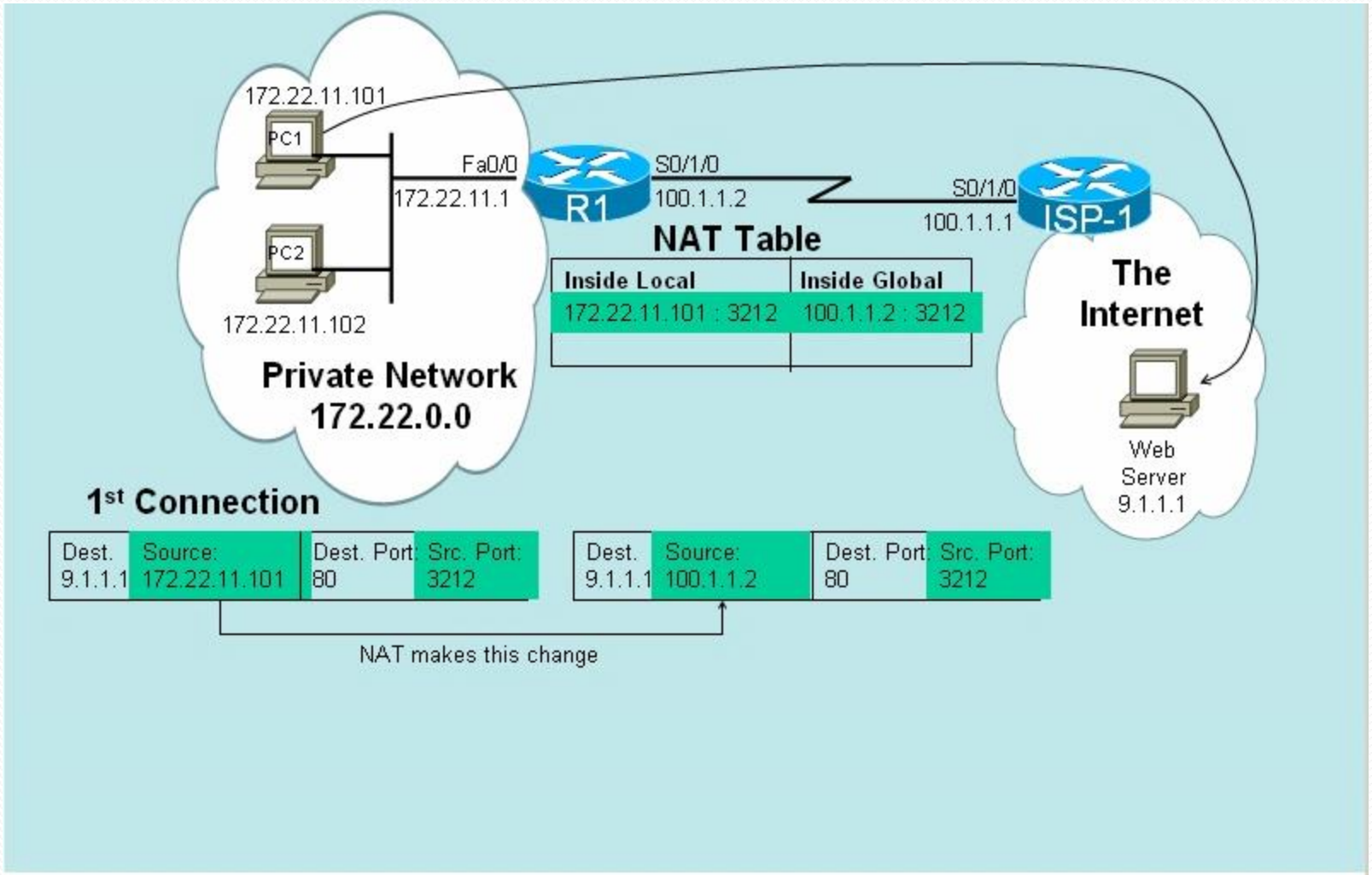
PAT


172.22.11.101
PC1
Fa0/0
172.22.11.1
R1
S0/1/0
100.1.1.2
S0/1/0
100.1.1.1
ISP-1
NAT Table
Inside Local
Inside Global
PC2
172.22.11.102
Private Network
172.22.0.0
The Internet
Web Server
9.1.1.1

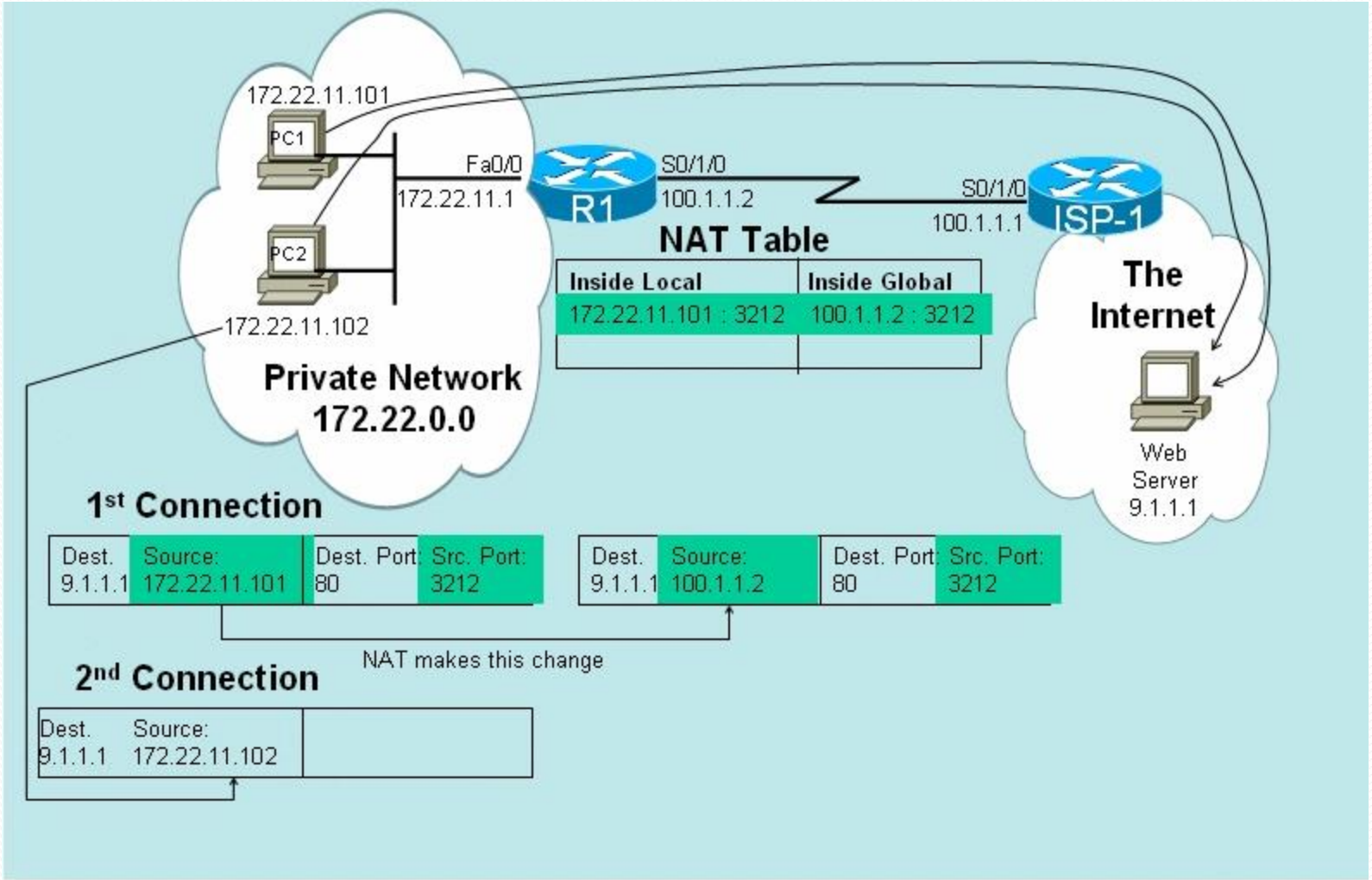
PAT


172.22.11.101
PC1
Fa0/0
172.22.11.1
PC2
172.22.11.102
Private Network
172.22.0.0
R1
S0/1/0
100.1.1.2
S0/1/0
100.1.1.1
ISP-1
NAT Table
Inside Local
Inside Global
The Internet
Web Server
9.1.1.1
1st Connection
Dest. Source:
9.1.1.1 172.22.11.101
Dest. Port: Src. Port:
80 3212

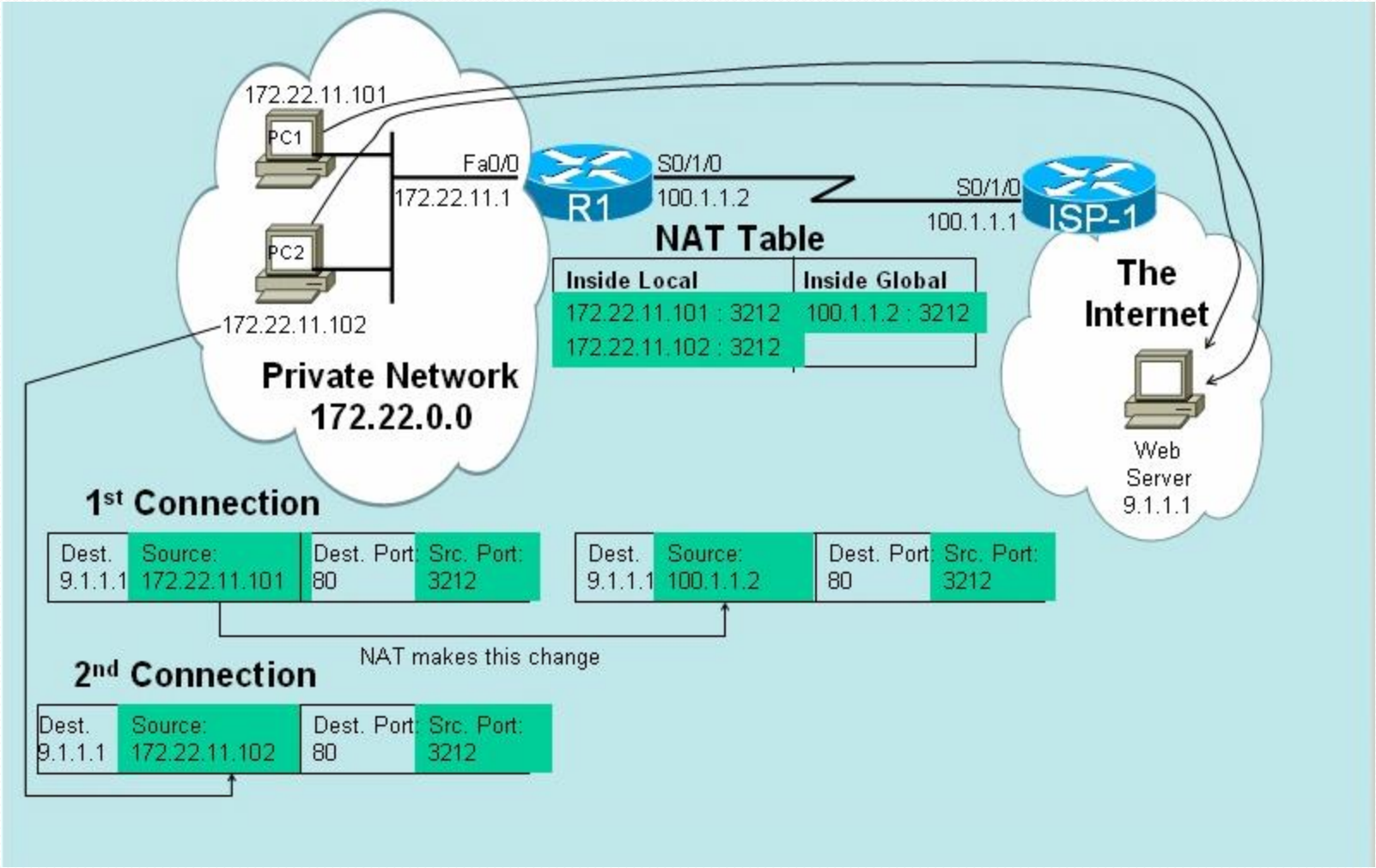
PAT


172.22.11.101
PC1
Fa0/0
172.22.11.1
R1
S0/1/0
100.1.1.2
S0/1/0
100.1.1.1
ISP-1
PC2
172.22.11.102
NAT Table
Inside Local
Inside Global
172.22.11.101 : 3212
100.1.1.2 : 3212
The Internet
Private Network
172.22.0.0
Web Server
9.1.1.1
1st Connection
Dest. 9.1.1.1
Source: 172.22.11.101
Dest. Port: 80
Src. Port: 3212
Dest. 9.1.1.1
Source: 100.1.1.2
Dest. Port: 80
Src. Port: 3212
NAT makes this change

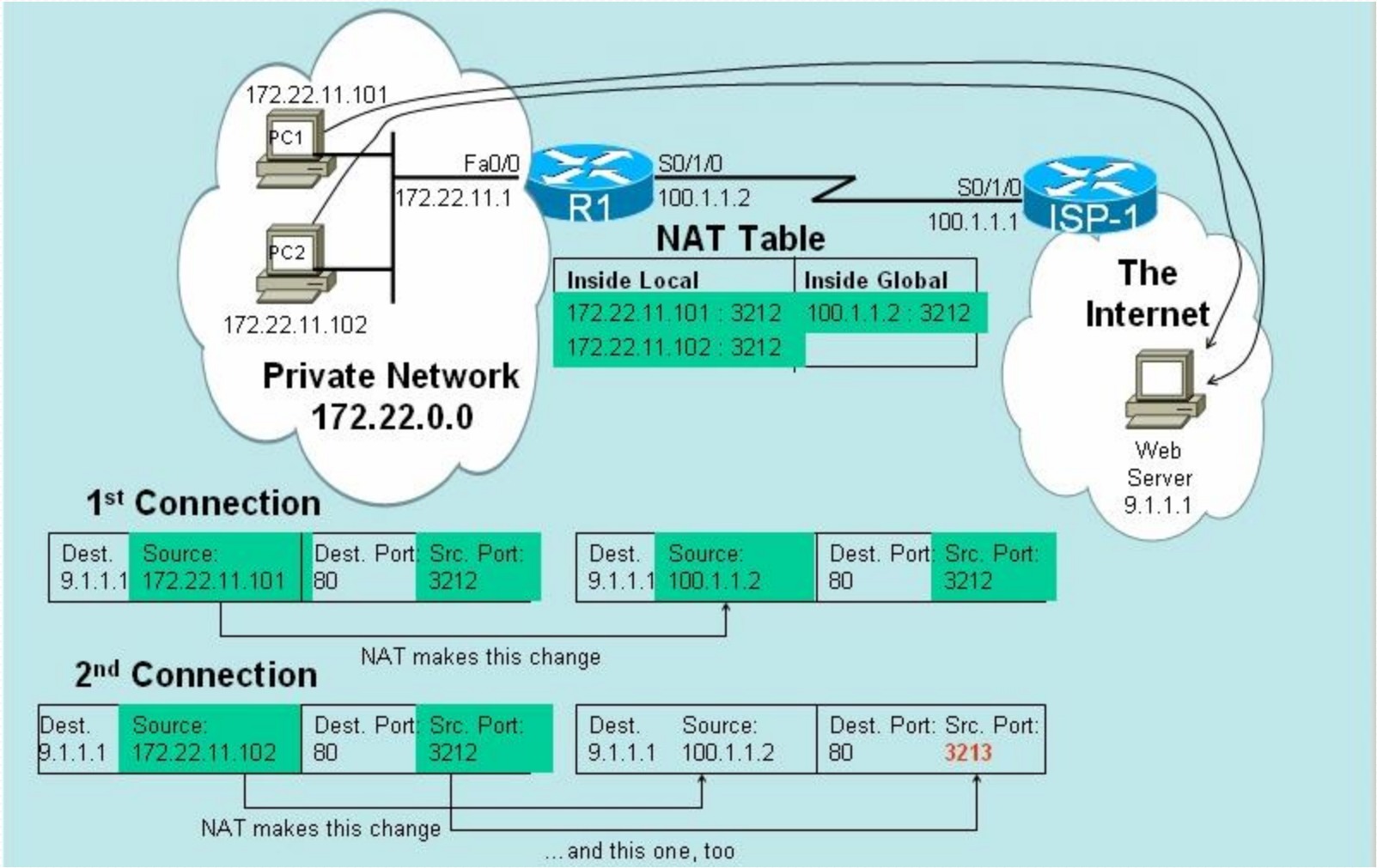
PAT


172.22.11.101
PC1
Fa0/0
172.22.11.1
R1
S0/1/0
100.1.1.2
S0/1/0
100.1.1.1
ISP-1
PC2
172.22.11.102
Private Network
172.22.0.0
NAT Table
Inside Local
Inside Global
172.22.11.101 : 3212
100.1.1.2 : 3212
The Internet
Web Server 9.1.1.1
1st Connection
Dest. 9.1.1.1
Source: 172.22.11.101
Dest. Port: 80
Src. Port: 3212
Dest. 9.1.1.1
Source: 100.1.1.2
Dest. Port: 80
Src. Port: 3212
NAT makes this change
2nd Connection
Dest. 9.1.1.1
Source: 172.22.11.102

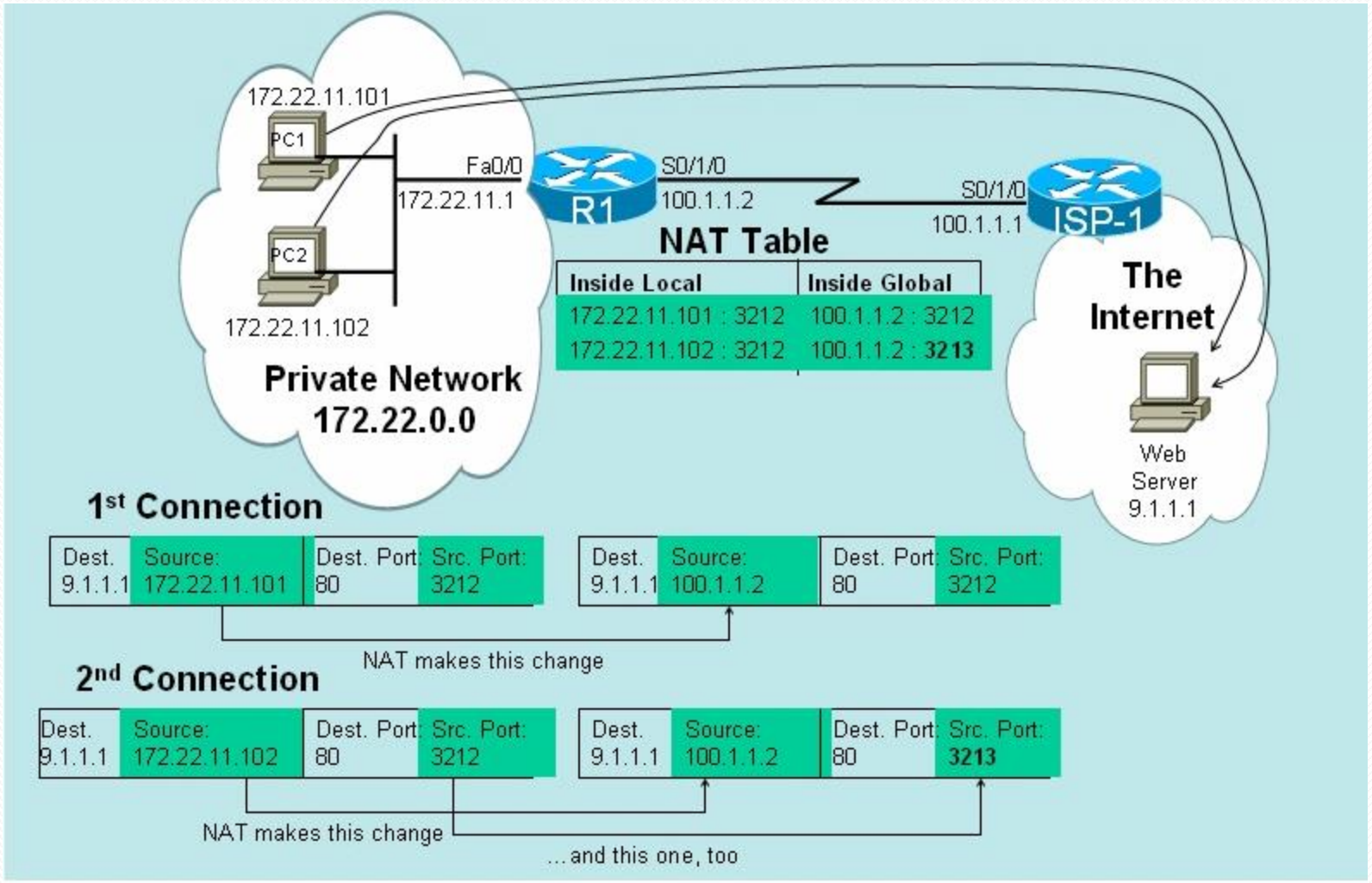
PAT


172.22.11.101
PC1
Fa0/0
172.22.11.1
R1
S0/1/0
100.1.1.2
S0/1/0
100.1.1.1
ISP-1
NAT Table
Inside Local
Inside Global
172.22.11.101 : 3212
100.1.1.2 : 3212
172.22.11.102 : 3212
PC2
172.22.11.102
Private Network
172.22.0.0
The Internet
Web Server
9.1.1.1
1st Connection
Dest. 9.1.1.1
Source: 172.22.11.101
Dest. Port: 80
Src. Port: 3212
Dest. 9.1.1.1
Source: 100.1.1.2
Dest. Port: 80
Src. Port: 3212
NAT makes this change
2nd Connection
Dest. 9.1.1.1
Source: 172.22.11.102
Dest. Port: 80
Src. Port: 3212

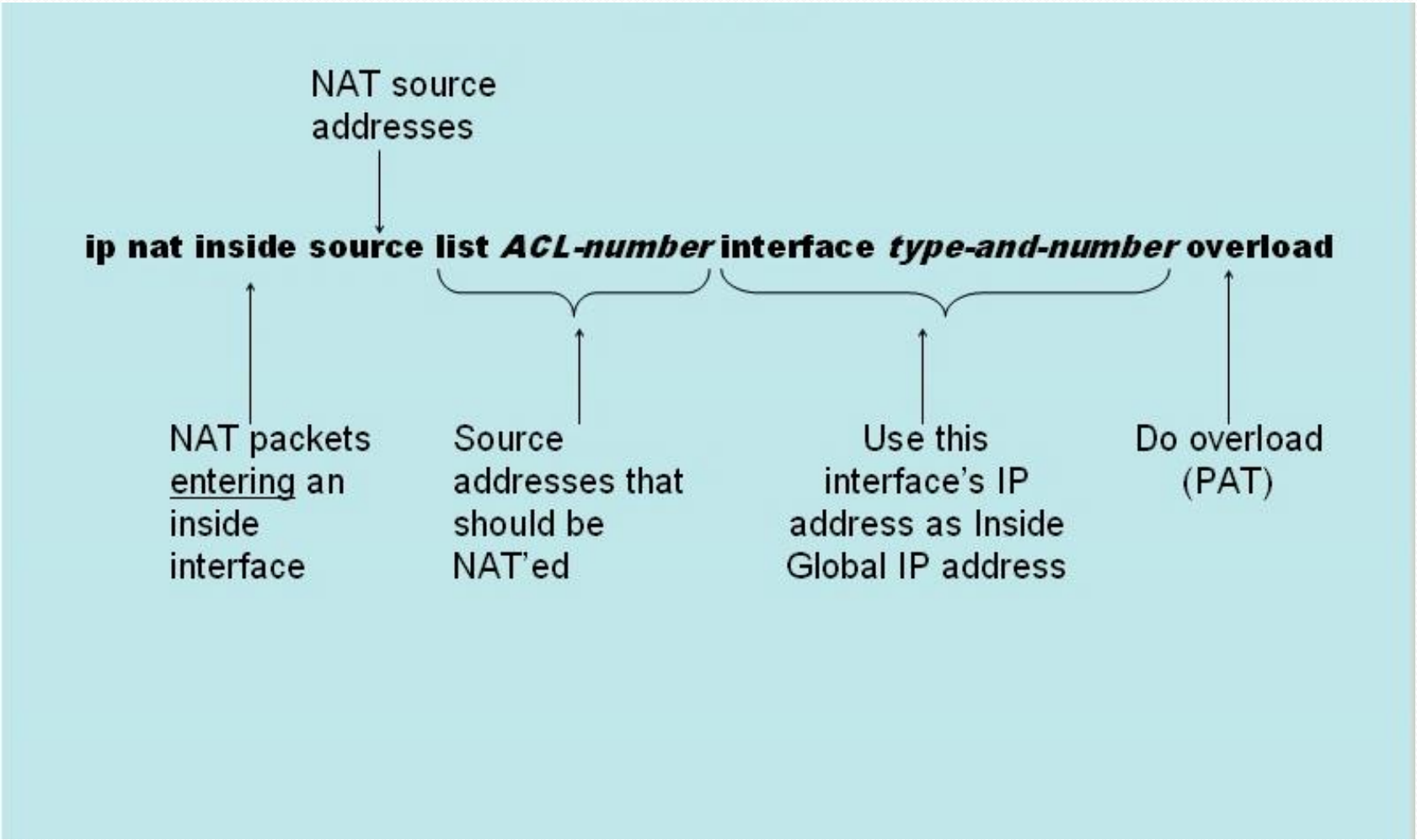
PAT


172.22.11.101
PC1
Fa0/0
172.22.11.1
PC2
172.22.11.102
Private Network
172.22.0.0
R1
S0/1/0
100.1.1.2
S0/1/0
100.1.1.1
ISP-1
The Internet
Web Server
9.1.1.1
NAT Table
Inside Local
Inside Global
172.22.11.101 : 3212
100.1.1.2 : 3212
172.22.11.102 : 3212
1st Connection
Dest. 9.1.1.1
Source: 172.22.11.101
Dest. Port: 80
Src. Port: 3212
Dest. 9.1.1.1
Source: 100.1.1.2
Dest. Port: 80
Src. Port: 3212
NAT makes this change
2nd Connection
Dest. 9.1.1.1
Source: 172.22.11.102
Dest. Port: 80
Src. Port: 3212
Dest. 9.1.1.1
Source: 100.1.1.2
Dest. Port: 80
Src. Port: 3213
NAT makes this change
...and this one, too

PAT


172.22.11.101
PC1
Fa0/0
172.22.11.1
R1
S0/1/0
100.1.1.2
S0/1/0
100.1.1.1
ISP-1
PC2
172.22.11.102
Private Network
172.22.0.0
NAT Table
Inside Local
Inside Global
172.22.11.101 : 3212
100.1.1.2 : 3212
172.22.11.102 : 3212
100.1.1.2 : 3213
The Internet
Web Server 9.1.1.1
1st Connection
Dest. 9.1.1.1
Source: 172.22.11.101
Dest. Port: 80
Src. Port: 3212
Dest. 9.1.1.1
Source: 100.1.1.2
Dest. Port: 80
Src. Port: 3212
NAT makes this change
2nd Connection
Dest. 9.1.1.1
Source: 172.22.11.102
Dest. Port: 80
Src. Port: 3212
Dest. 9.1.1.1
Source: 100.1.1.2
Dest. Port: 80
Src. Port: 3213
NAT makes this change
...and this one, too

Configuration



IPV6

What is IPv6?

- IPv6 was originally created as the answer to IPv4's address-exhaustion crisis.
- It has been improved to bring us the flexibility, efficiency, capability, and optimized functionality that can truly meet our ever-increasing needs.
- The amount of people and devices that connect to networks increases each and every day.
- 128 bit in length that gives 3.4x10^38 IP
- or more exactly:

(340,282,366,920,938,463,463,374,607,431,768,211,456)

What is IPv6? (Cont'd)

- More Hierarchal design that gives flexible architecture
- No Broadcast, just multicast
- Three address types: Unicast, Multicast and Anycast (to place the same address on many devices, and the packet is routed to the nearest device)

IPv6 Addressing

IPv6 addresses are 128 bits written in Hexadecimal notation

Eight groups of numbers separated by : not .

Shortened Expression

First, you can drop any leading zeros in each of the individual blocks.

Ex:

2001:0db8:3c4d:0012:0000:0000:1234:56ab

Could be written

2001:db8:3c4d:12:0:0:1234:56ab

All blocks of zeros can be removed by replacing them with double colons, like this:

2001:db8:3c4d:12::1234:56ab

413

Shortened Expression (Cont'd)

Only one contiguous block of zeros can be replaced on the address

Example:

2001:0000:0000:0012:0000:0000:1243:56ab

Will be written as

2001::12:0:0:1243:56ab

Address Types

- **Unicast**

  -Global Unicast : Public (Real) IP addresses

  -Link-local : Automatically assigned, and is limited to the link, not routable

  -Unique Local : is unique over the links, routable

- **Multicast**

415

Address Types (Cont'd)

- **Anycast**

  - More than one device can obtain the same address and the routers determine the nearest one to get the packet to

Note: The interface can have multiple IPs of different types at the same time

Special Addresses

0:0:0:0:0:0:0:0	Equals :: This is the equivalent of IPv4's 0.0.0.0
0:0:0:0:0:0:0:1	Equals ::1. The equivalent of 127.0.0.1 in IPv4.
0:0:0:0:0:0:192.168.100.1	This is how an IPv4 address would be written in a mixed IPv6/IPv4 network environment.
2000::/3	The global unicast address range.

Special Addresses (Cont'd)

- **FC00::/7** The unique local unicast range.
- **FE80::/10** The link-local unicast range.
- **FF00::/8** The multicast range.
- **3FFF:FFFF::/32** Reserved for examples and documentation.
- **2001:0DB8::/32** Also reserved for examples and documentation.
- **2002::/16** Used with 6to4, which is the transition system—the structure that allows IPv6 packets to be transmitted over an IPv4 network without the need to configure explicit tunnels.

Configuring IPv6

In order to enable IPv6 on a router

Corp(config)#**ipv6 unicast-routing**

IPv6 isn't enabled by default on any interfaces either, so we have to go to each interface individually and enable it.

You use the interface configuration command
ipv6 address <ipv6prefix>/<prefix-length> [eui-64]
to get this done.

Example:

Corp(config-if)#**ipv6 address**
2001:db8:3c4d:1:0260:d6FF:FE73:1987/64

419

Configuring IPv6 (Cont'd)

- You can specify the entire 128-bit global IPv6 address or you can use the eui-64 option. Remember, the eui-64 format allows the device to use its MAC address and pad it to make the interface ID.
  - Corp(config-if)#**ipv6 address 2001:db8:3c4d:1::/64 eui-64**

- IPv6 can also be enabled on the interface by typing the command
- Corp(config-if)# **ipv6 enable**
- But this will make it use link-local address which will only allow it to communicate to that local subnet

Configuring IPv6 Static and Default Route

- Static Routes
- !R1
- ipv6 route 2004::/64 2003::2
- or
- ipv6 route 2004::/64 fa0/1 2003::2

- Default Routes
- !R1
- ipv6 route ::/0 2003::2

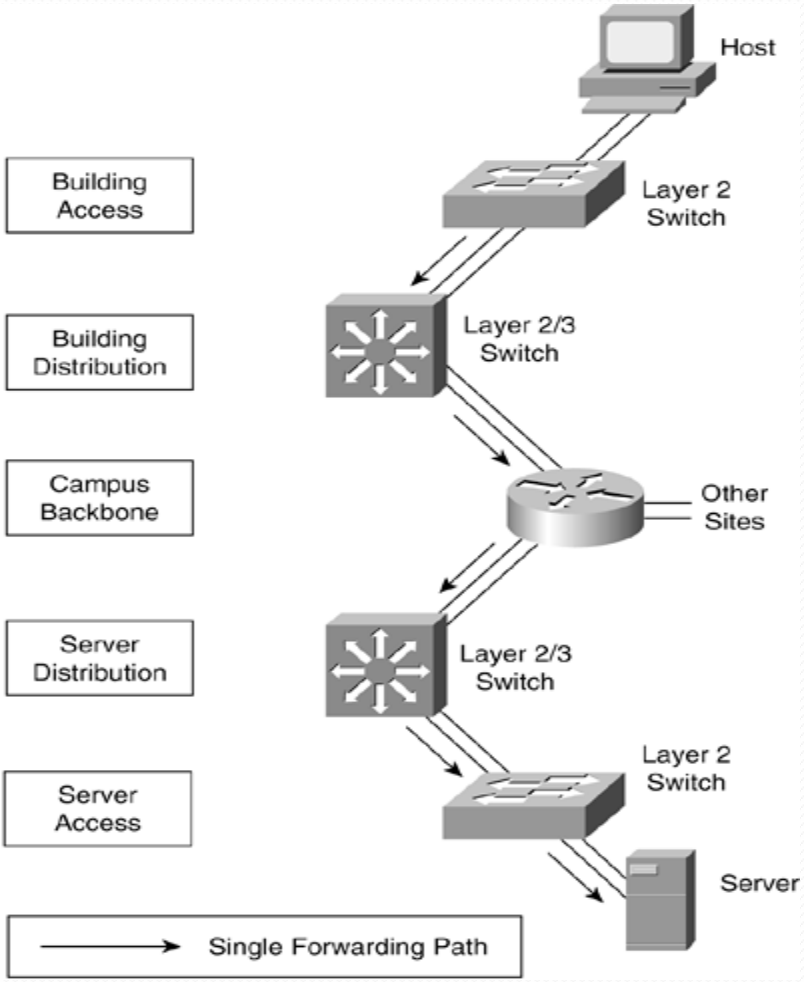
IPv6 Floating Default Routes

- !R1
- ipv6 route ::/0 2003::2 5
- ipv6 route ::/0 2005::a 10

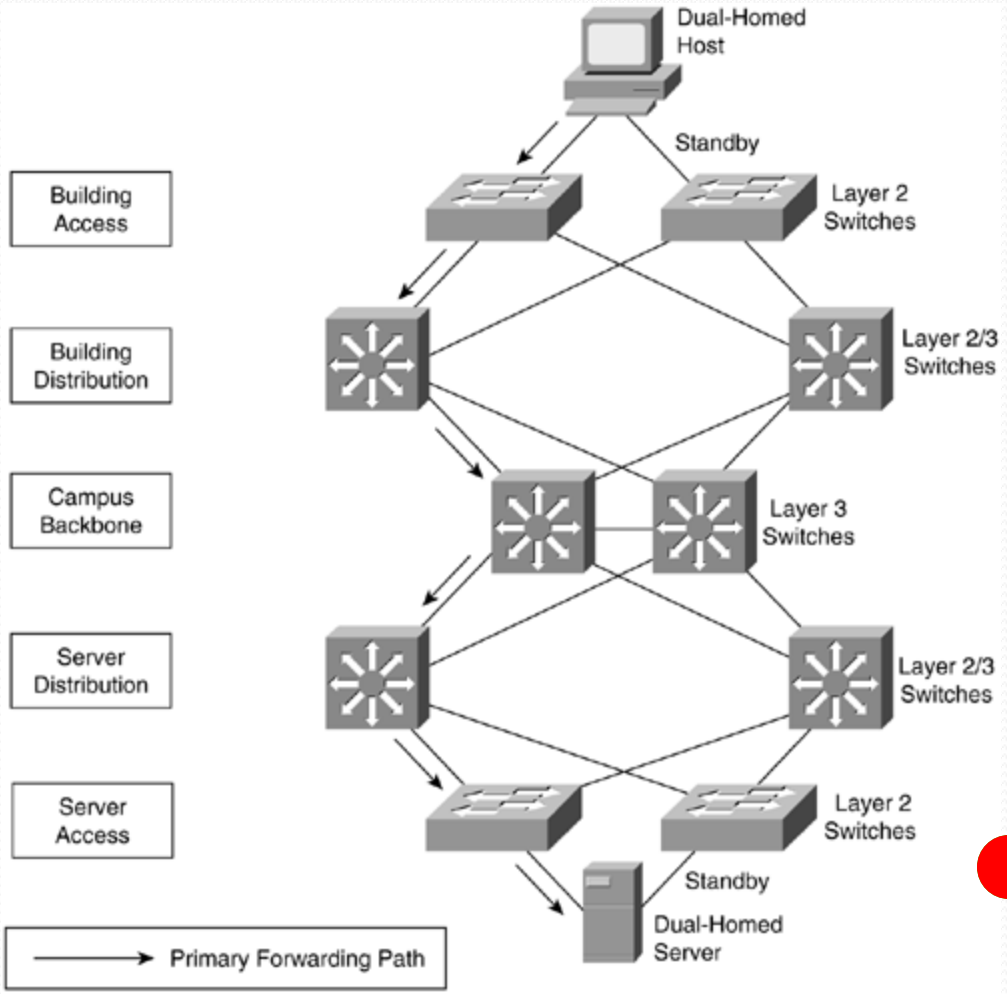
FHRP

Single Forwarding Path vs Redundancy

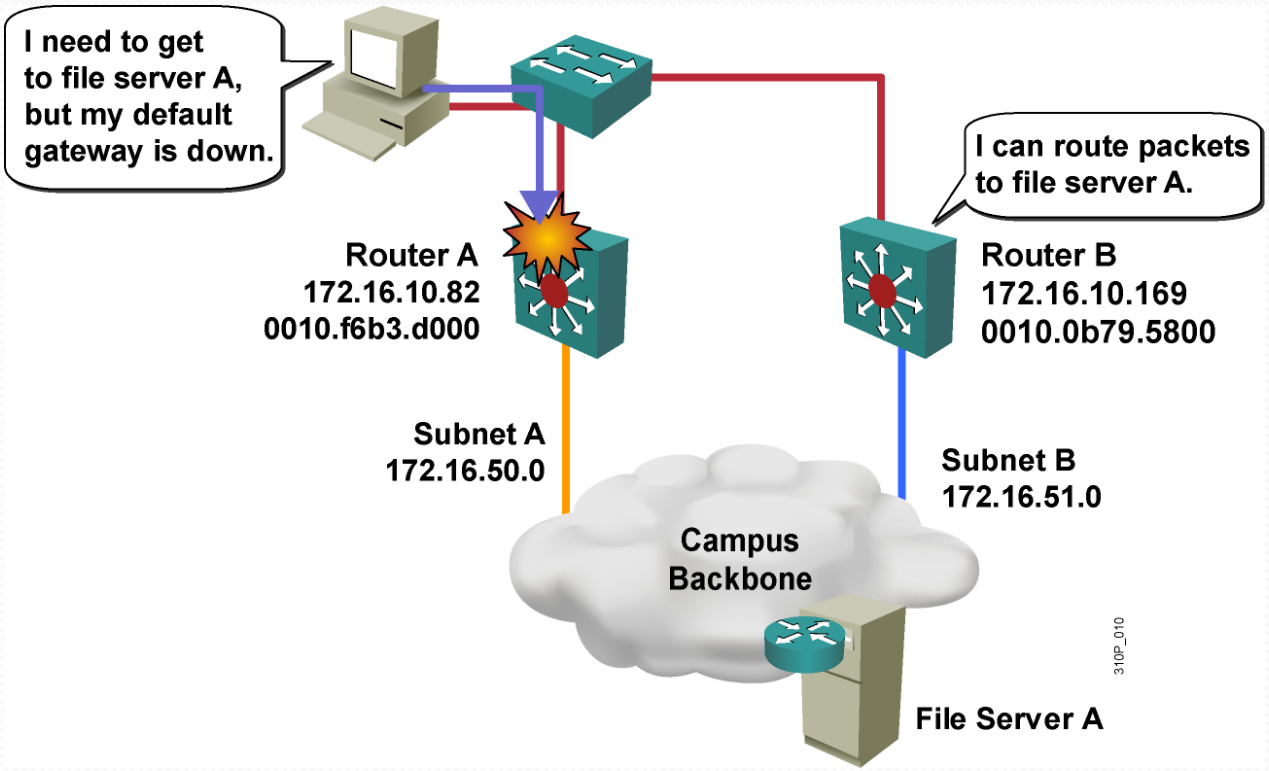
Single Forwarding Path



Adding Redundancy



Implementing Default Gateway Router Redundancy in Multilayer Switched Networks



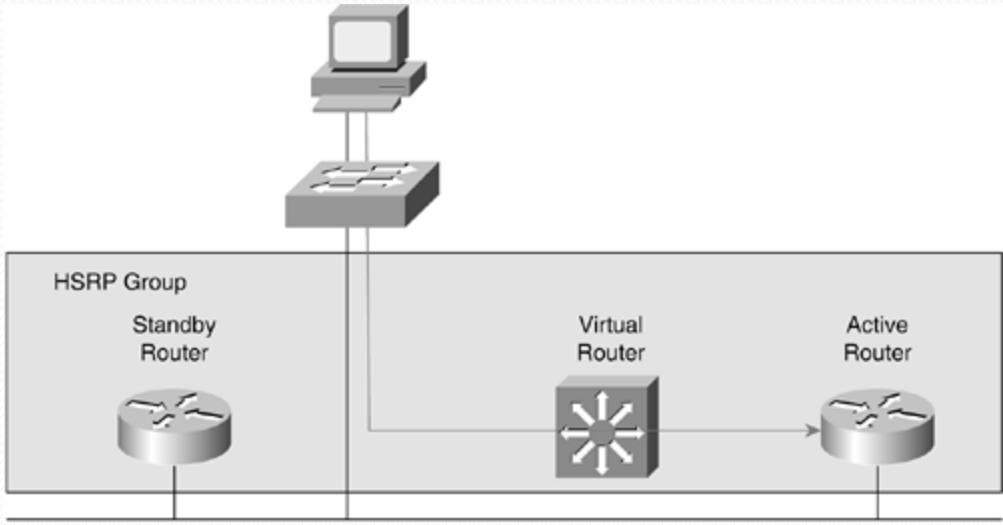
Redundancy Protocols

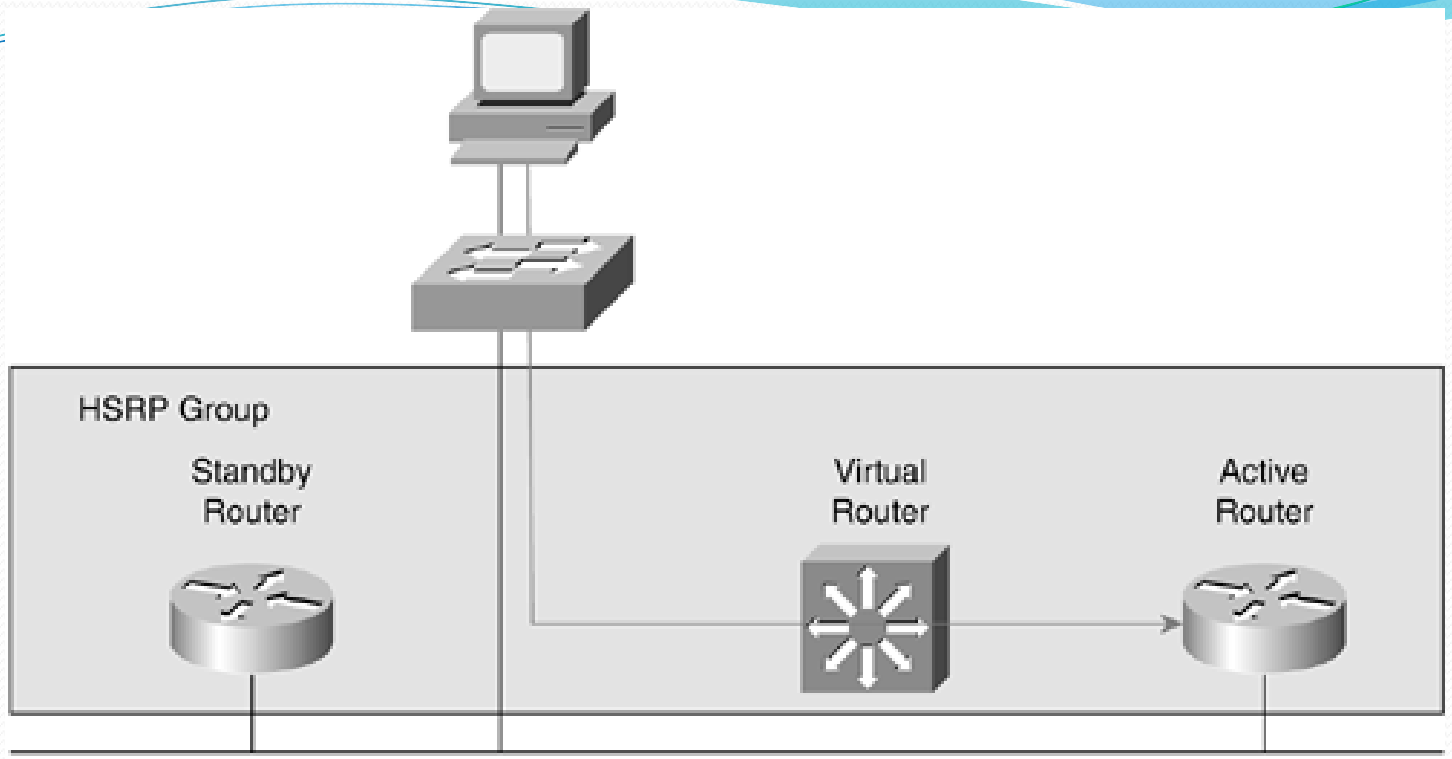
- Cisco IOS offers several features to provide a redundant default gateway to end devices.
- The following are the default gateway redundancy features supported by Cisco IOS routers and switches:
  - **Hot Standby Routing Protocol (HSRP)**
  - **Virtual Router Redundancy Protocol (VRRP)**
  - **Gateway Load Balancing Protocol (GLBP)**

HSRP
Hot Standby Router Protocol

HSRP (Hot Standby Routing Protocol)

- Cisco proprietary protocol
- RFC 2281
- Method of providing IP address sharing and redundancy for default gateways.
- The protocol consists of a:
  - Virtual MAC address
  - IP address
- Shared between two routers:
  - Active Router
  - Standby Router
- Routers exchange HSRP hello messages at regular intervals





One standby router

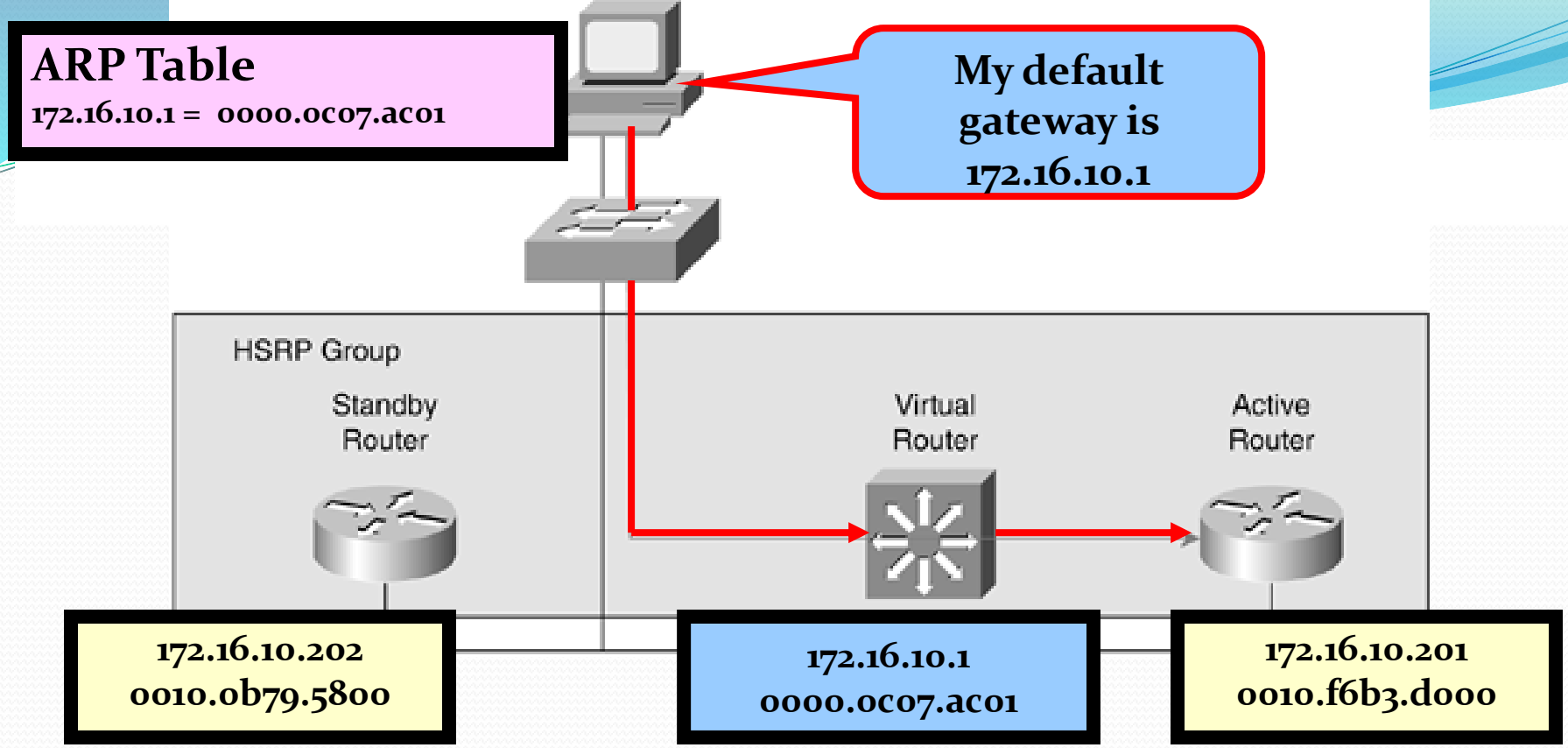
- The backup router in case the active router fails for the subnet.
- It will then forward traffic destined to the virtual IP address.

One virtual router

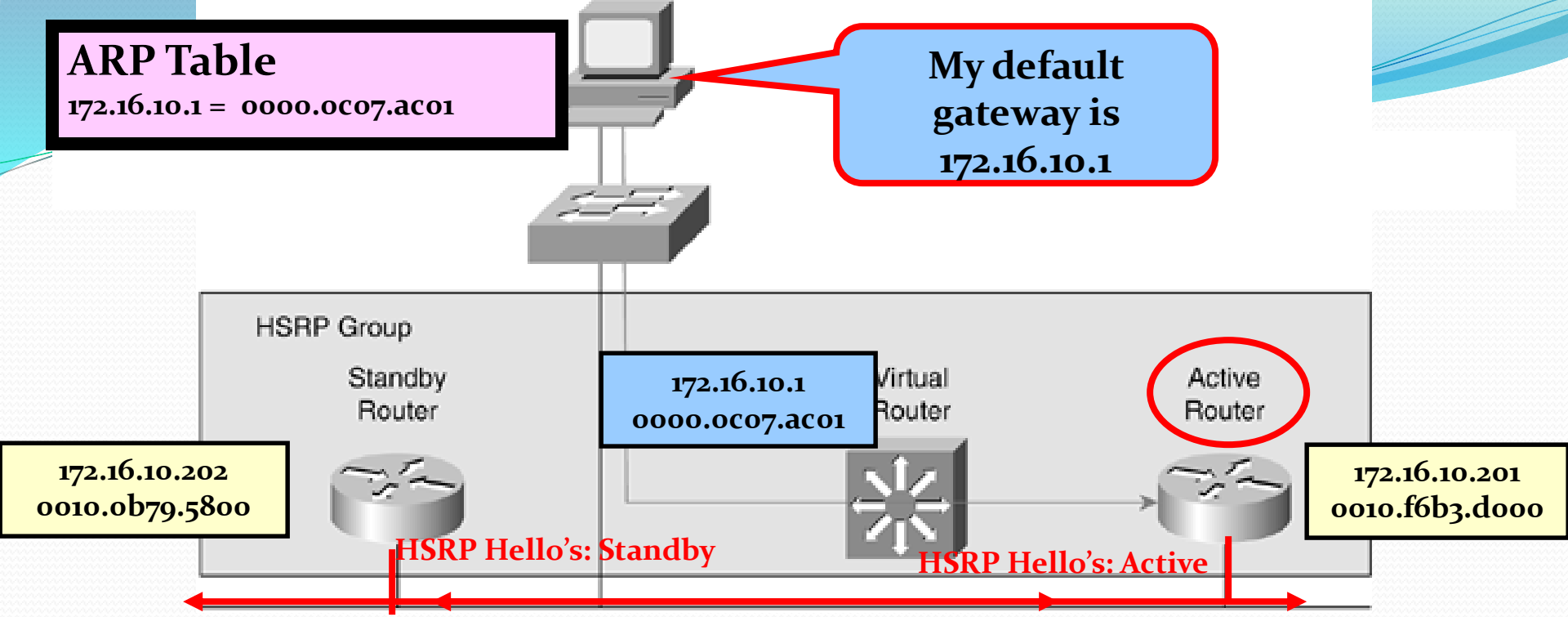
- The virtual router is **not** an actual router.
- Represents the HSRP group acting as one virtual router.
- It is the **default gateway** as far as hosts on the subnet are concerned.

One active router

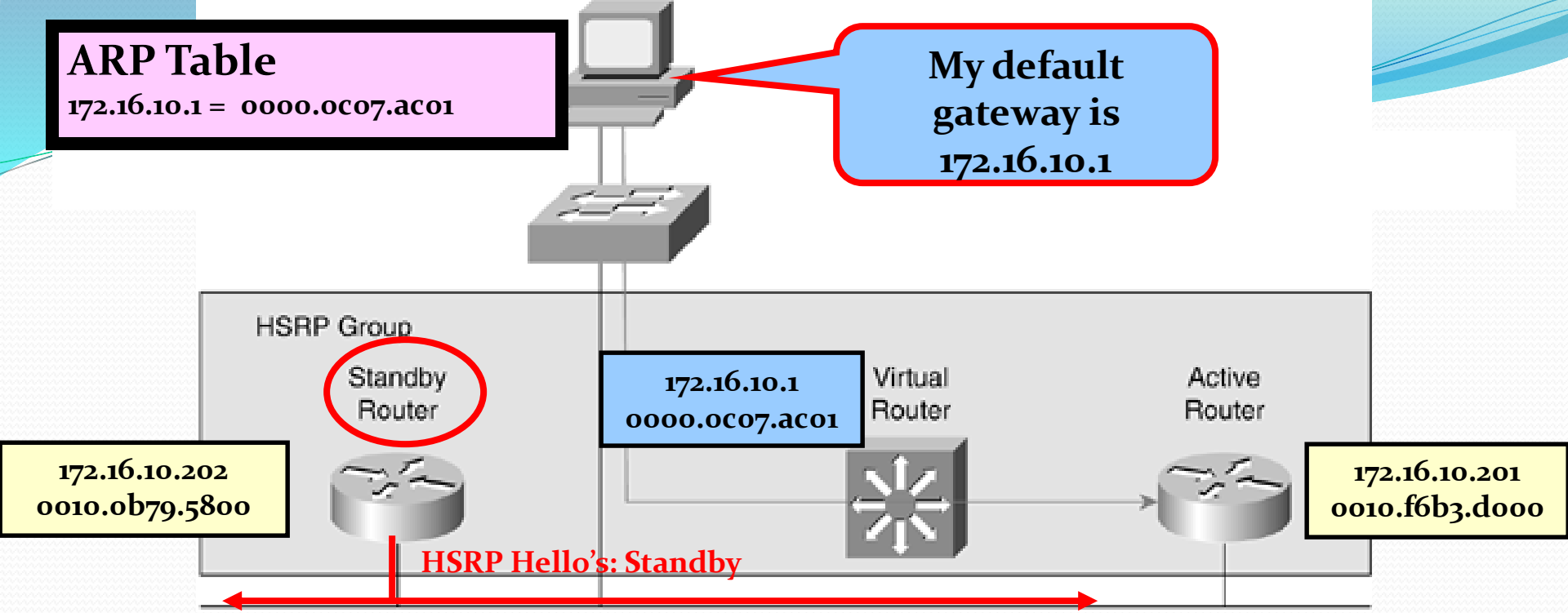
- The active router forwards traffic destined to the virtual IP address.



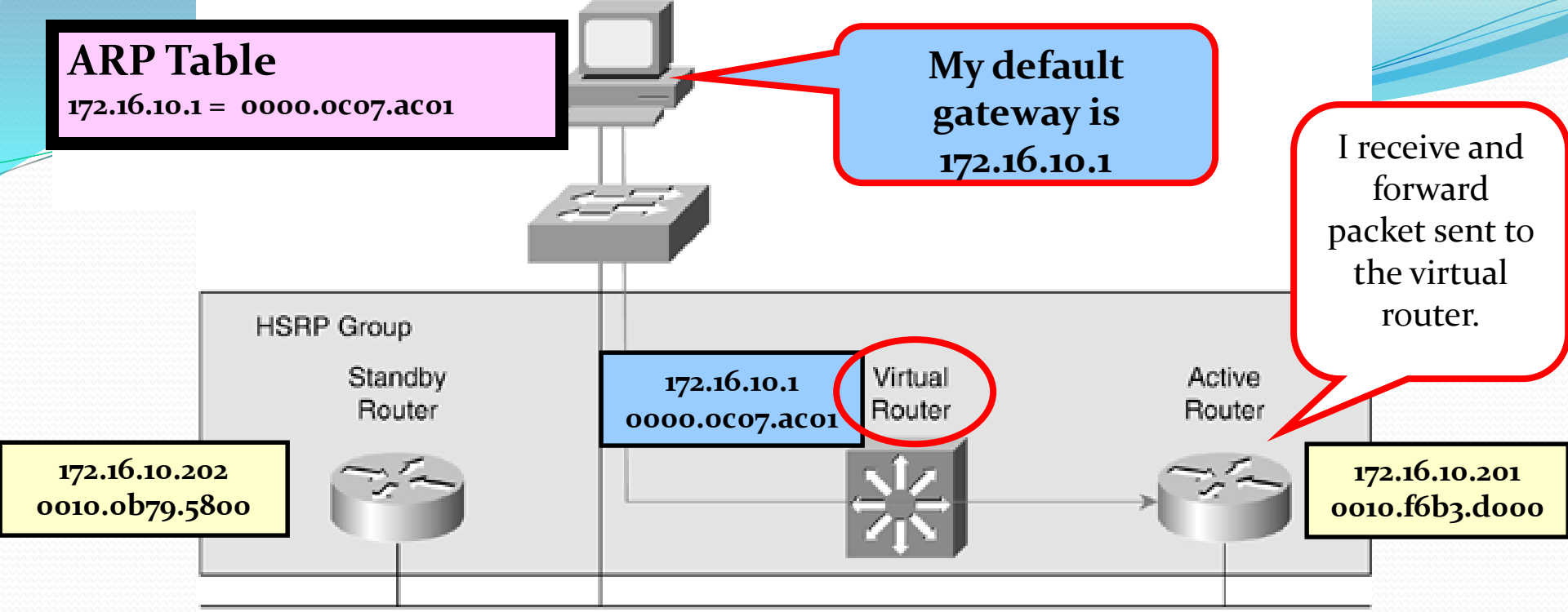
- The **host** connected to the switch sends the packet destined for the **virtual router**, but in reality the **active router** does the packet **forwarding**.
- **Note**: *Additional HSRP member routers*— Other routers are neither active nor standby, but they are configured to participate in the same HSRP group.
  - They monitor the current active and standby routers and transition into one of those roles if the current router fails for the subnet.



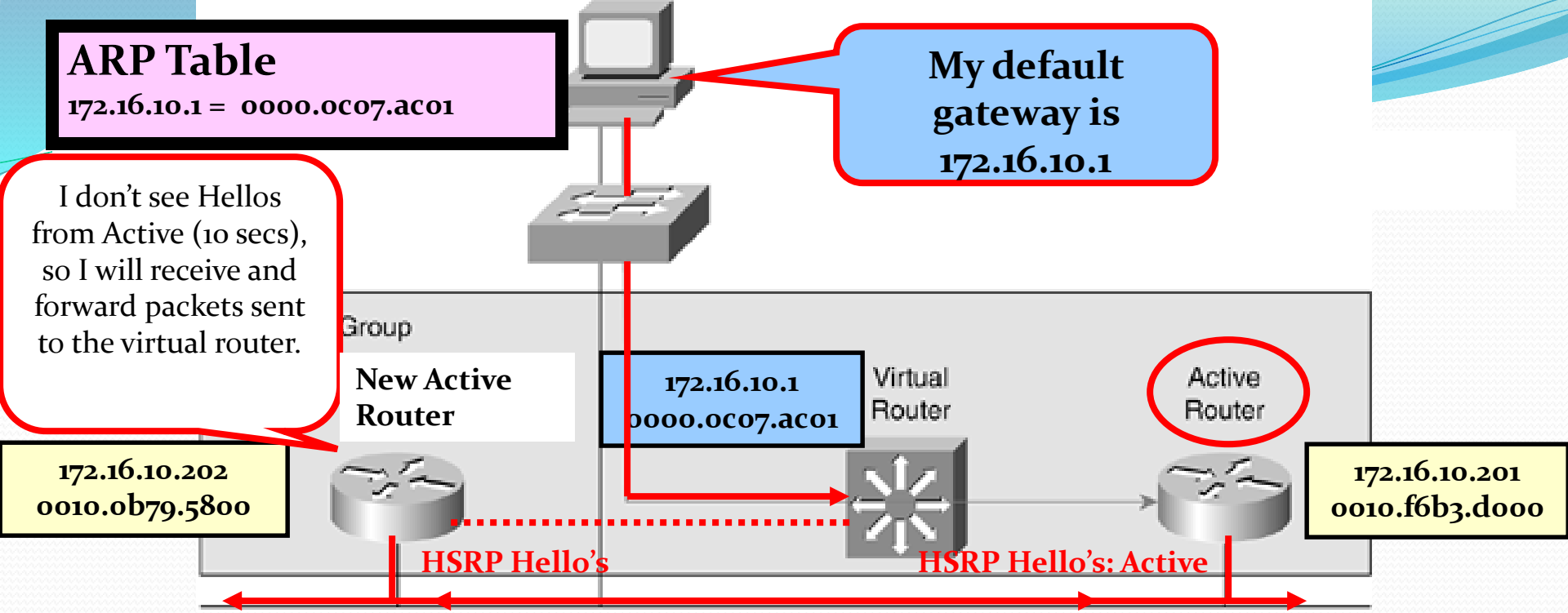
- The **active router** assumes and maintains its active role through the transmission of **hello messages (default every 3 seconds)**.
  - Sent by active and standby routers.
  - Multicast 224.0.0.2 ("all routers") using UDP port 1985
- The router with the **highest standby priority** - **active router**.
  - **0 to 255**
  - **Default = 100** (configurable)
  - Otherwise, the router with the highest IP address
- When the **preempt option** is **not configured**, the **first router to initialize** HSRP becomes the active router. (*May not be what you want!*)



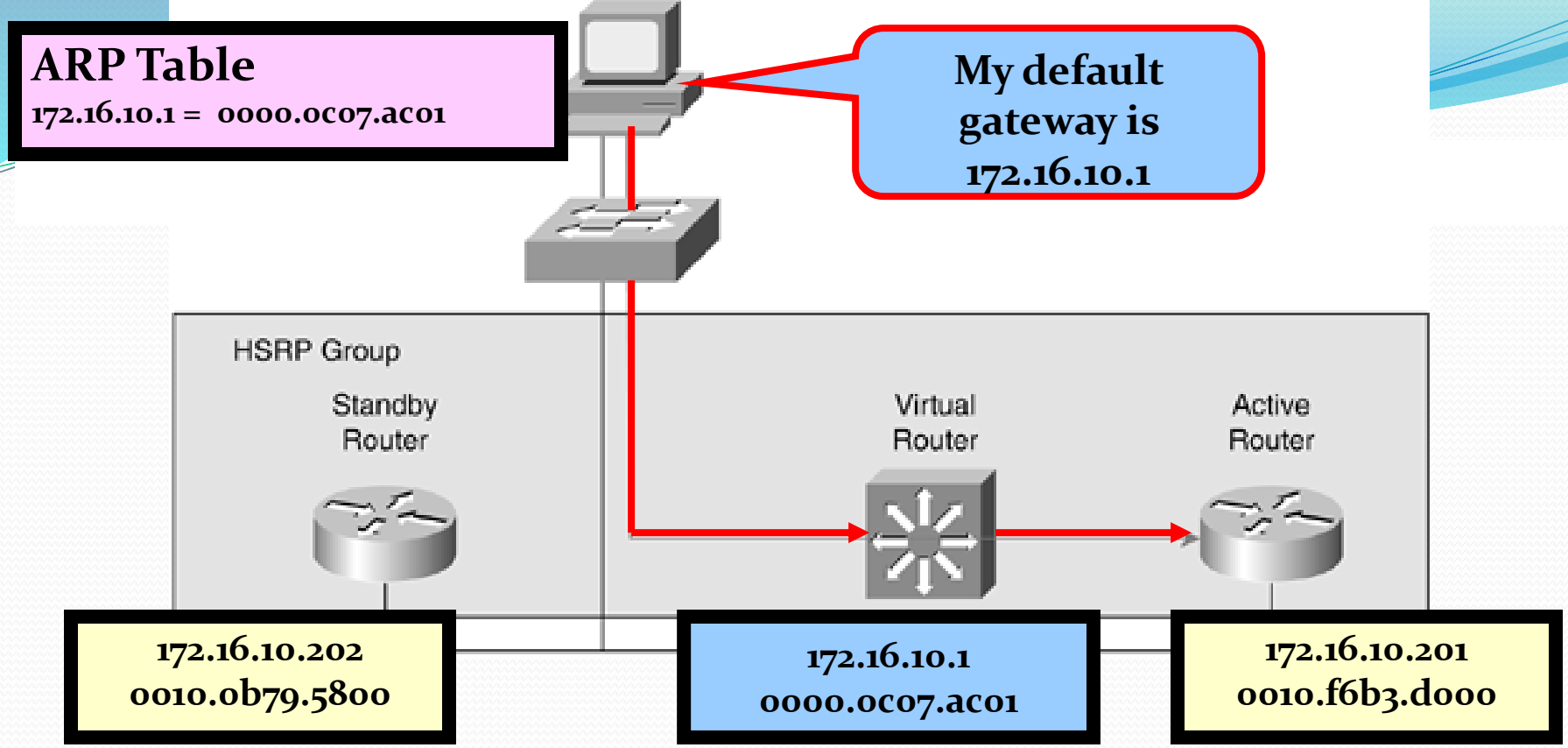
- The **second router** in the HSRP group to initialize or second highest priority is elected as the **standby router**.
  - **Monitor the operational status of the HSRP group**
  - Quickly assumes packet-forwarding responsibility if the active router becomes inoperable.
- The standby router **also transmits hello messages** to inform all other routers in the group of its **standby router role** and status.



- The **virtual router** presents a consistent available router (default gateway) to the hosts.
  - Assigned its:
    - **Own IP address**
    - **Own virtual MAC address**
  - The **active router** acting as the virtual router actually forwards the packets.
- **Additional HSRP member routers**: These routers in listen state monitor the hello messages but do not respond.
  - Do forward any packets addressed to the routers' IP addresses.
  - Do not forward packets destined for the virtual router because they are not the active router.



- When the **active router fails**, the other HSRP routers stop receiving hello messages and the standby router assumes the role of the active router.
  - When the ***holdtime* expires (default 10 seconds)**.
- Because the **new active router assumes both the IP address and virtual MAC address of the virtual router, the end stations see no disruption in service.**



- When the **active router only fails:**
  - **Standby** takes over.
  - If there are other routers participating in the group, those routers then **contend to be the new standby** router.
  - The **new active router remains the forwarding router** even when the former active router with the higher priority regains service in the network unless **preempt** is configured (coming).
- If **both the active and standby routers fail:**
  - All routers in the HSRP group contend for the active and standby router roles.

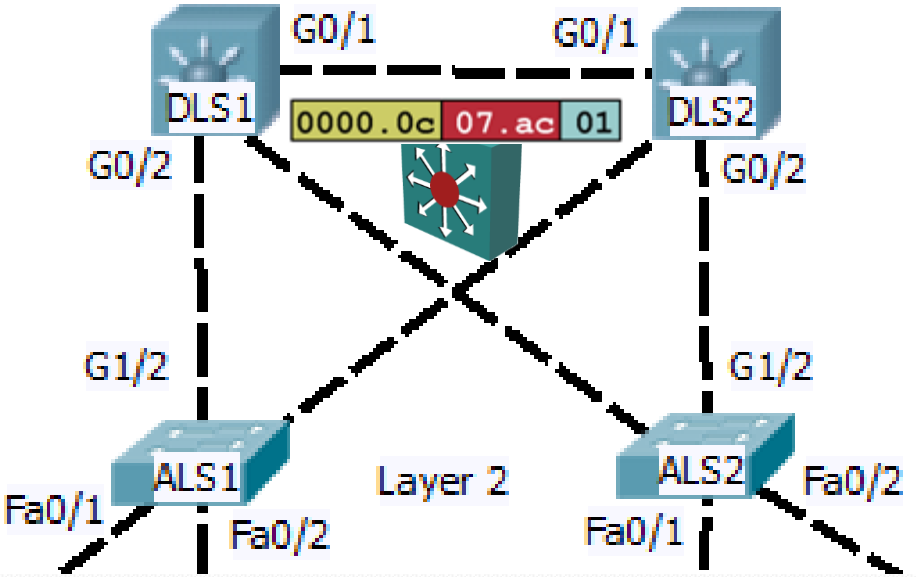
Virtual IP

- To configure a router as a member of an HSRP standby group, enter this command in interface configuration mode:

  (Physical interface or VLAN interface if VLANs are used)

`Switch(config-if)#`**`standby`** *`group-number`* **`ip`** *`virtual-ip-address`*

- ***group-number*** refers to the HSRP standby group number.
  - The group number can range from **0 to 255.**
- ***virtual-ip-address*** indicates the virtual IP address of the HSRP group.

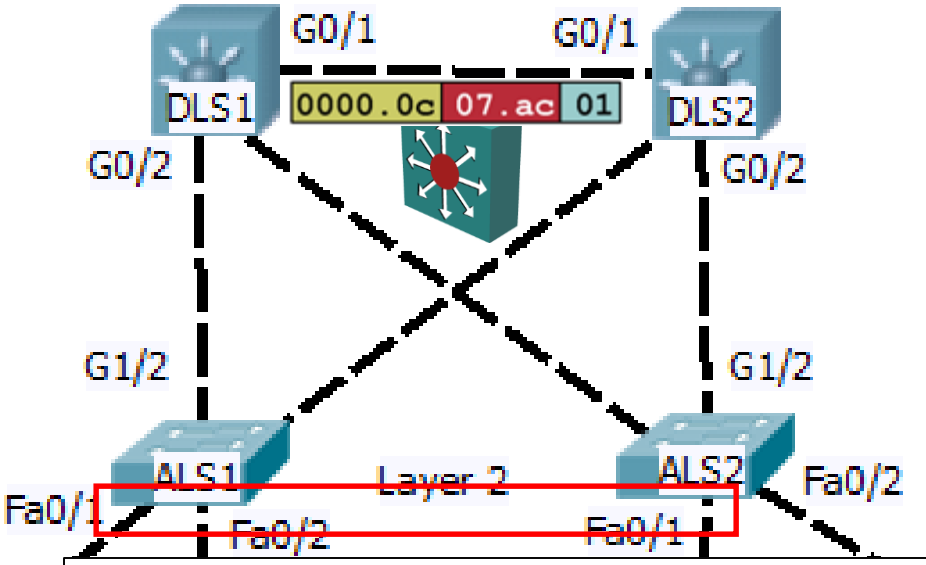



```
DLS1
interface vlan 10
  ip add 172.16.10.201 255.255.255.0
  standby 1 priority 200
  standby 1 ip 172.16.10.1
  standby 1 preempt


Router B
interface vlan 10
  ip add 172.16.10.202 255.255.255.0
  standby 1 priority 100
  standby 1 ip 172.16.10.1
  standby 1 preempt
```

Virtual IP

```
Switch(config-if)#standby group-number ip virtual-ip-address
```

- ***group-number*** refers to the HSRP standby group number.
  - The group number can range from **0 to 255.**
  - 0 is the default
  - Most Cisco switches support only up 16 groups.
  - Each VLAN does NOT have to have it's own group number.
  - Group numbers are locally significant to that VLAN or interface.




```
DLS1
interface vlan 10
  ip add 172.16.10.201 255.255.255.0
  standby 1 priority 200
  standby 1 ip 172.16.10.1
  standby 1 preempt


interface vlan 20
  ip add 172.16.20.202 255.255.255.0
  standby 1 priority 210
  standby 1 ip 172.16.20.1
  standby 1 preempt

interface vlan 30
  ip add 172.16.30.202 255.255.255.0
  standby 1 priority 220
  standby 1 ip 172.16.30.1
  standby 1 preempt
```

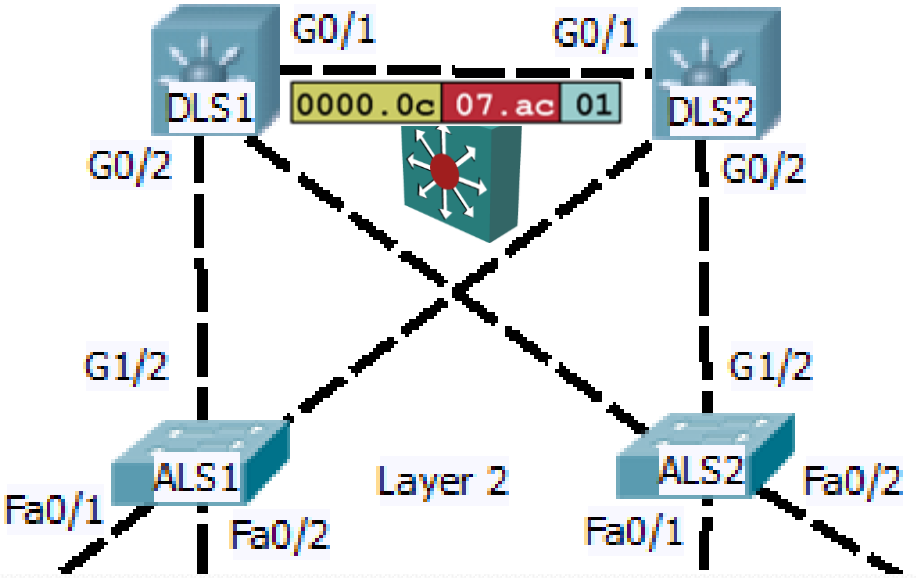
Priority

- To set the priority value of a router, enter this command in interface configuration mode:

```
Switch(config-if)#standby group-number priority priority-value
```

  - The ***priority-value*** indicates the number that prioritizes a potential standby router.
  - The range is **0 to 255**; the **default is 100**.
  - Some documentation states 1 to 255.
  - During the election process, the router in an HSRP group with the **highest priority becomes the forwarding router**.

- If several routers have the same priority, the physical IP address of the router's interface is used as a tiebreaker.
  - The router with the numerically **highest IP address wins**.
- In reality the router that boots up first will most likely become the active router.
  - Best to use the preempt command (coming)




```
DLS1
interface vlan 10
  ip add 172.16.10.201 255.255.255.0
  standby 1 priority 200
  standby 1 ip 172.16.10.1
  standby 1 preempt


Router B
interface vlan 10
  ip add 172.16.10.202 255.255.255.0
  standby 1 priority 100
  standby 1 ip 172.16.10.1
  standby 1 preempt
```

Timers

Both the *hellotime* and the *holdtime* parameters are configurable.

```
Switch(config-ig)# standby group timers [msec] hellotime
   [msec] holdtime
```

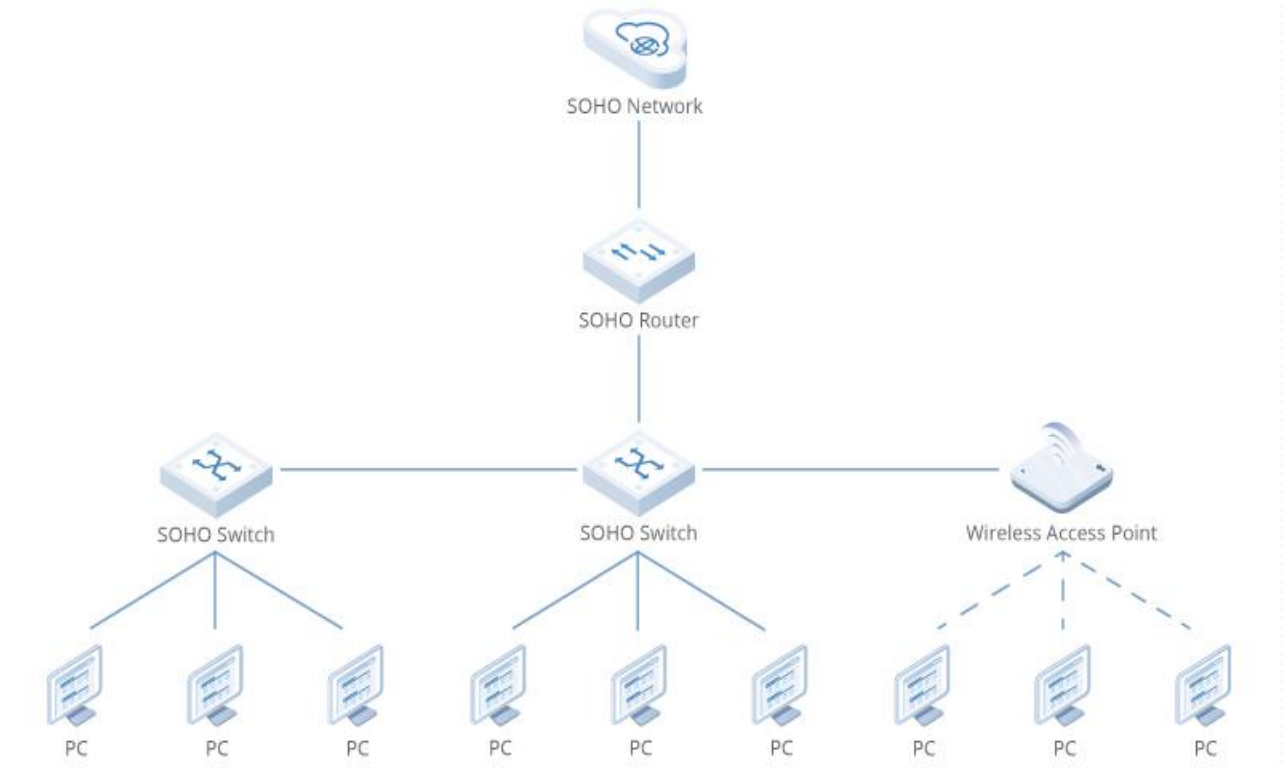
- ***Hellotime***
  - Default = **3 seconds**
  - Value varies from 1 to 255.
- ***Holdtime***
  - Default = **10 seconds**
  - Value varies from 1 to 255.
- Timers will be in milliseconds (1/1,000th) of the **msec** keyword precedes a value.
- To reinstate the default standby timer values, enter the following command:

  no standby *group-number* timers

SOHO Network

SOHO Network

- The Small Office/Home Office (SOHO) concept in networking refers to the design and implementation of network solutions tailored for small-scale businesses or home-based offices.



Key Features of SOHO Networking

- **Simple Setup:**
- Designed for easy installation and configuration, often using plug-and-play devices.
- Minimal technical expertise required.

- **Cost-Effectiveness:**
- Uses affordable, off-the-shelf networking equipment such as routers, switches, and wireless access points.

- **Connectivity:**
- Provides wired and wireless connectivity to devices like computers, printers, smartphones, and tablets.
- Includes internet access, often through a broadband connection (DSL, cable, or fiber).

- **Scalability:**
- Built to accommodate a small number of users (typically 1–20 users) but can be scaled up slightly if needed.

- **Integrated Devices:**
- Equipment like SOHO routers often combine multiple functions such as routing, switching, firewall, and wireless access in a single device.

- **Security:**
- Basic security features like firewalls, WPA/WPA2 encryption for Wi-Fi, and VPN support for secure remote access.

- **Performance:**
- Optimized for small-scale operations, with sufficient bandwidth for typical office activities like email, web browsing, file sharing, and video conferencing.

Example of Cisco SOHO Devices

- **Cisco RV160W:** A compact wireless router designed for small offices or home offices
- **Cisco SG250 Series:** Managed switches that offer features like VLANs, QoS, and PoE (Power over Ethernet) for small office networks.
- **Cisco WAP121:** A small business wireless-N access point that provides reliable Wi-Fi coverage for small offices or homes
- **Cisco Meraki MX67:** Integrated firewall, content filtering, and advanced threat protection
- **Cisco 1000 Series:** Advanced security features, integrated wireless capabilities, and support for SD-WAN

VPN
Virtual Private Network

What is VPN?

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.

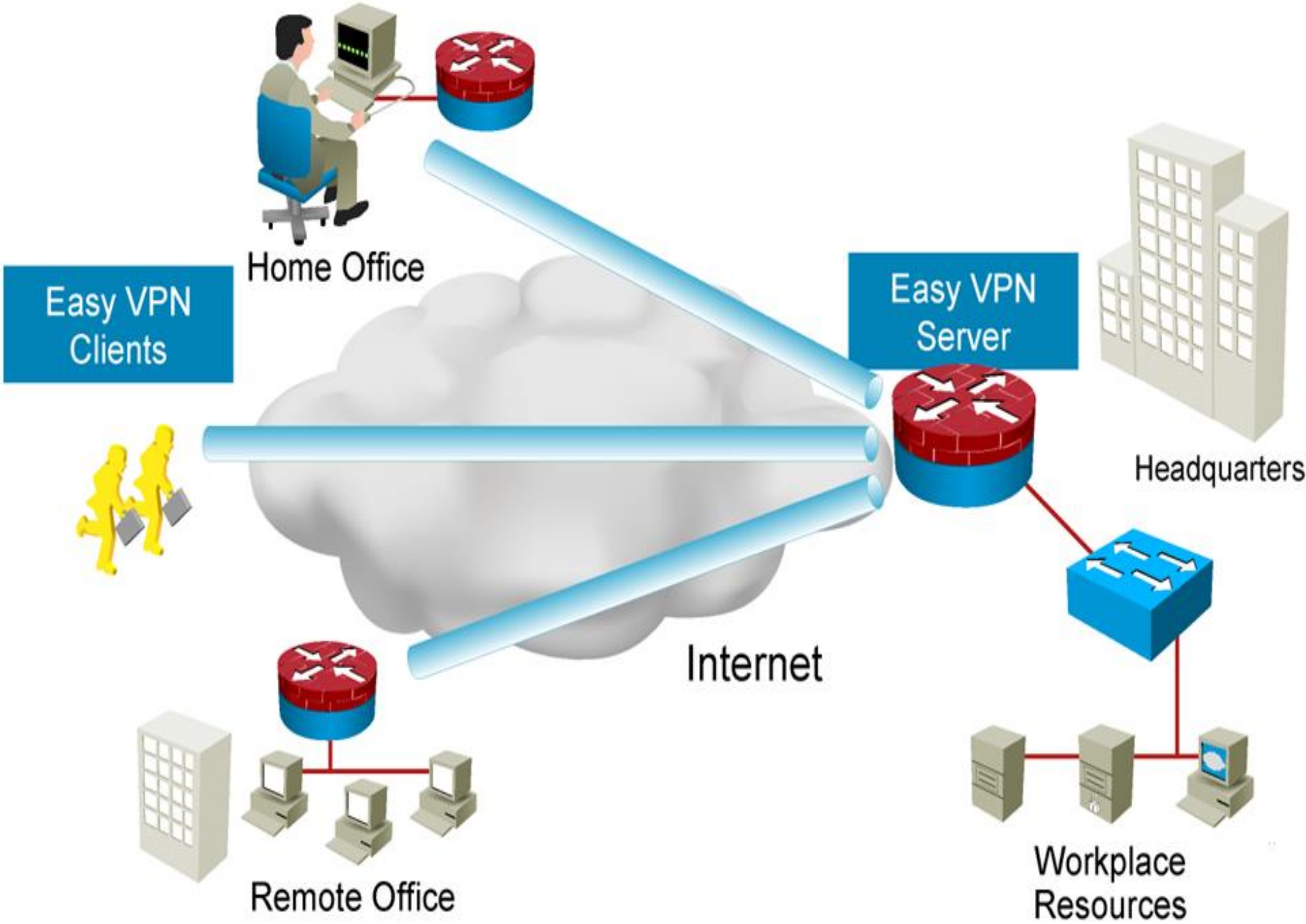
- Became popular as more employees worked in remote locations.

Types of VPN

- The two types of VPN are named based upon the role they play in business
- **Remote access VPN**
- **Site-to-Site VPN**

VPN Types

- **Remote access VPN** : allow remote users like telecommuters to securely access the corporate network wherever and whenever they need.
- **Site-to-Site VPN** : or (intranet VPN) allow a company to connect to its remote sites securely over a public medium like internet instead of expensive dedicated connection


Home Office
Easy VPN Clients
Easy VPN Server
Headquarters
Internet
Remote Office
Workplace Resources

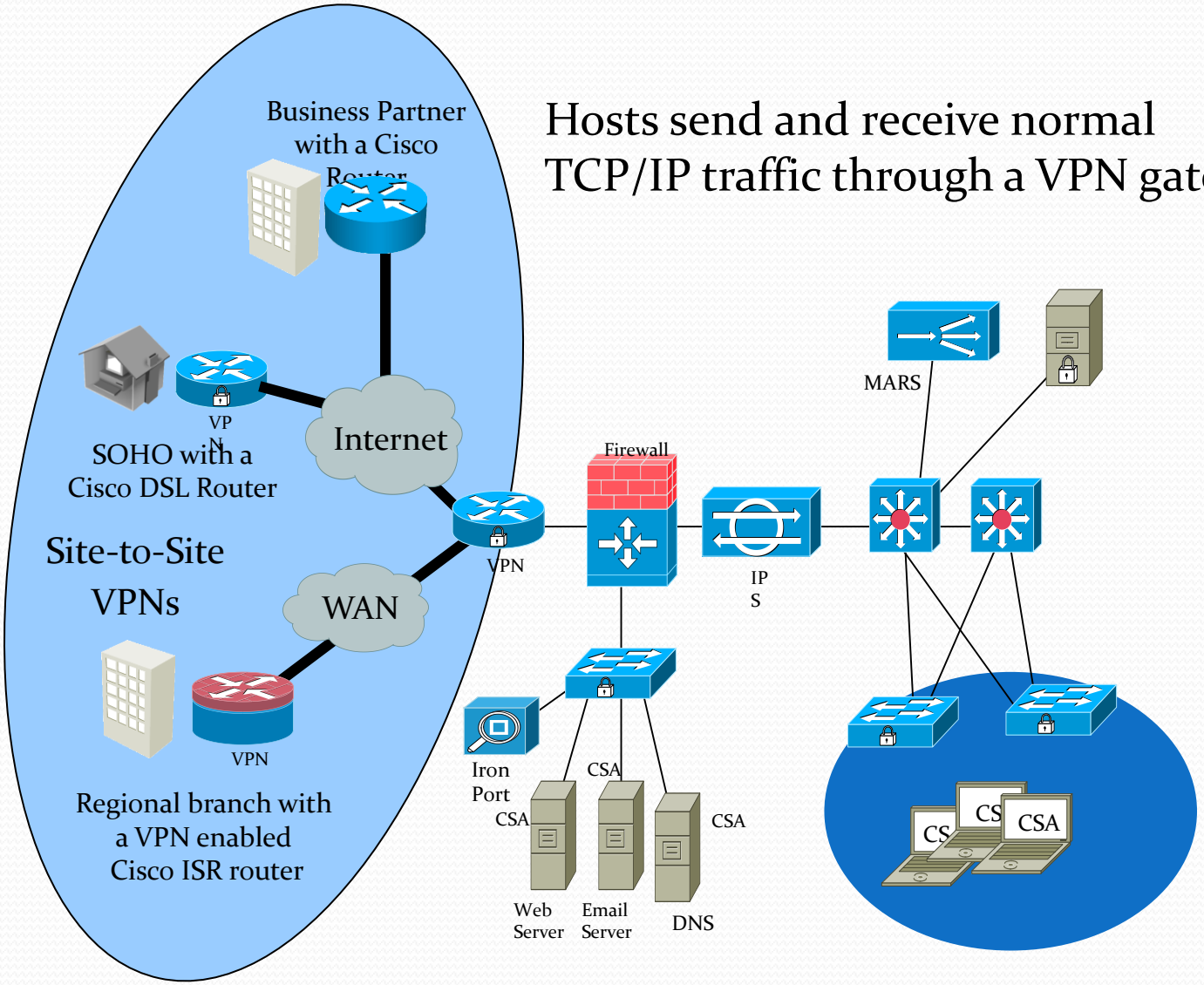
Four Critical Functions

- Authentication – validates that the data was sent from the sender.
- Access control – limiting unauthorized users from accessing the network.
- Confidentiality – preventing the data to be read or copied as the data is being transported.
- Data Integrity – ensuring that the data has not been altered

IPSec

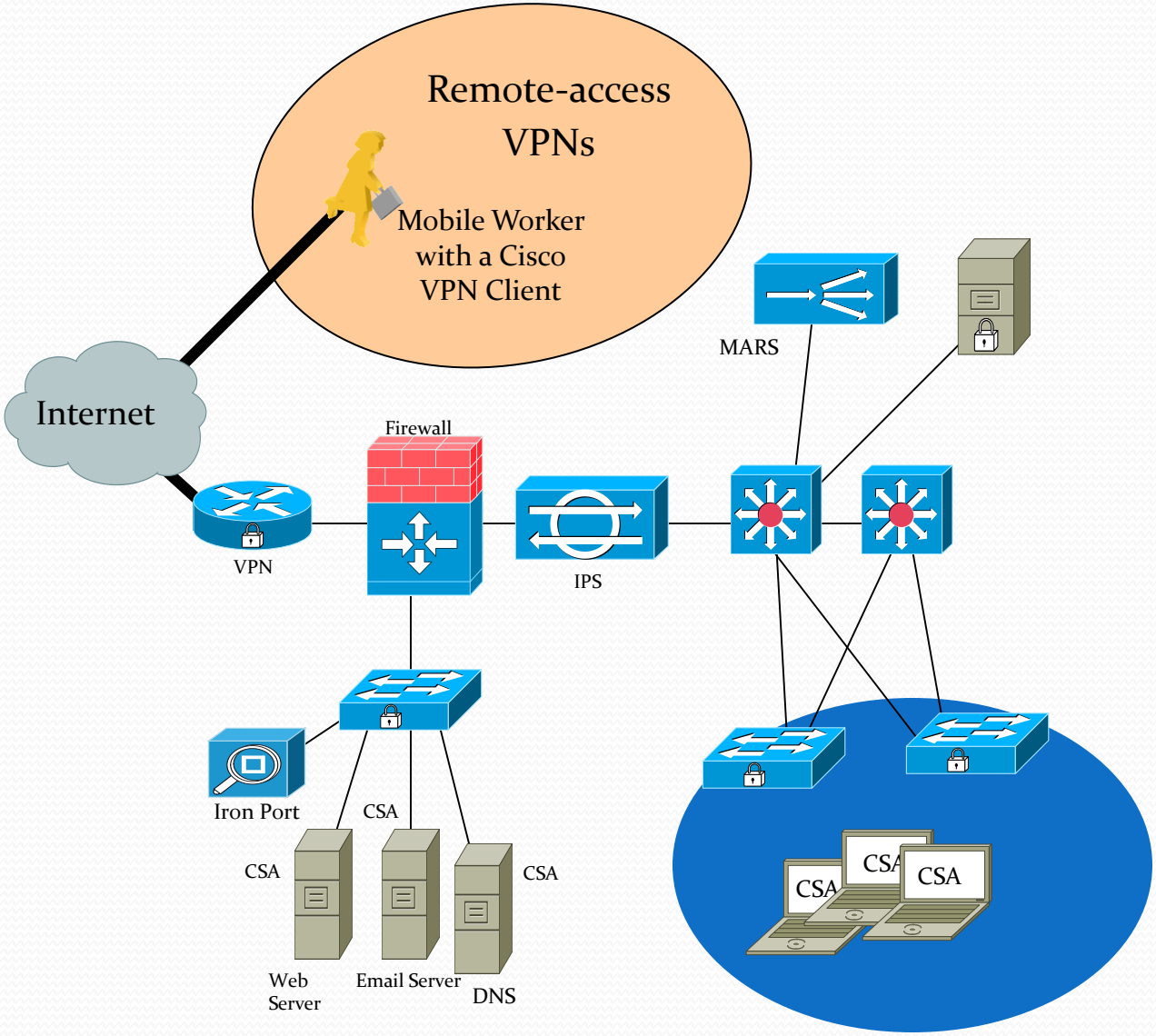
- IP security is an industry standard suite of protocols and algorithms that allows for secure data transmission over IP based network

Site-to-Site VPN

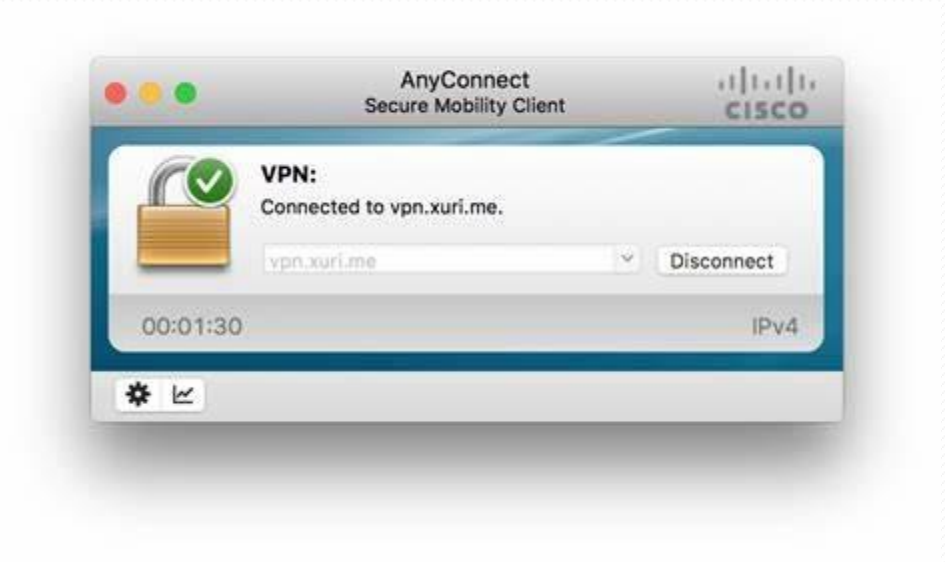


Hosts send and receive normal TCP/IP traffic through a VPN gateway

Remote-Access VPNs

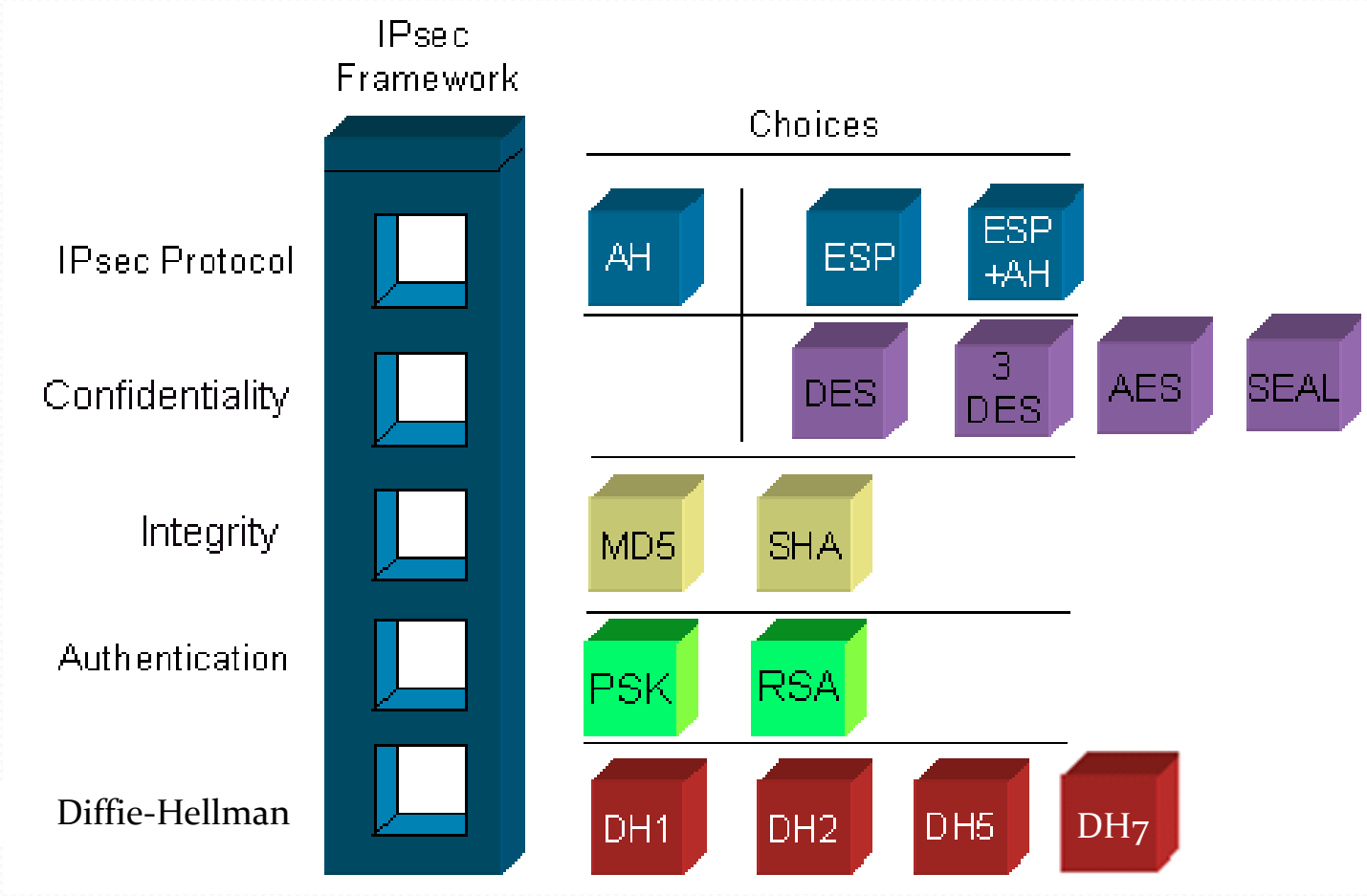


VPN Client Software



In a remote-access VPN, each host typically has Cisco AnyConnect software

IPSec Framework



Internet Key Exchange (IKE)

- Security Associations
- IKE Phases
- IKE Phase 1 – ISAKAMP
- IKE Phase 2 - IPSEC

Layer2 Discovery Protocols

CDP

- Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that networking applications use to learn about nearby, directly connected devices.
- Cisco Discovery Protocol is enabled by default
- CDP sends periodic advertisement to a well-known multicat mac address 01:00:0C:CC:CC:CC
- CDP is enabled by default on Cisco devices

- To disable CDP, issue the command: **no cdp run**
- To reenable it again issue the command: **cdp run**
- To enable the CDP on a specific interface issue the command: **cdp enable** in the interface command
- **Router(config)# cdp timer** *seconds,* specifies the frequency of the cdp updates
- **Router# show cdp neighbors** , display the cisco devices neighbors and their detail.
- **CDP Default Hello** timer is 60 seconds and the holdtime period is 180 seconds

Information Gathered by CDP

This information may include the

Operating System version,

Hostname,

Every address (IP Address)

The port identifier from which the announcement was sent,

Device type and model,

Duplex setting,

Native vlan,

Power draw (for POE devices),

Other device specific information

LLDP

- Link Layer Discovery Protocol is the is the IEEE equivalent CDP protocol.
- LLDP is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network.
- LLDP standard is IEEE 802.1AB
- LLDP messages used to advertise to the following multicast addresses
  01:80:c2:00:00:0e, or
  01:80:c2:00:00:03, or
  01:80:c2:00:00:00

- To enable lldp globally, **lldp run**
- To disable lldp reception on the interface, **no lldp receive** , interface command
- To disable lldp transmission the interface, **no lldp transmit**
- To show the neighbor brief information, **show lldp neighbor**
- **Default** Hello timer is 30 seconds, and update timer is 120 seconds.

Information Gathered By LLDP

- System name and description
- Port name and description
- VLAN name(But not native vlan Identification)
- IP management address
- System capabilities (switching, routing, etc.)
- MAC information
- Power

Quality of Service

What Is Quality of Service (QoS)?

The ability of the network to provide better or "special" service to users/applications.

Data, Video, Voice

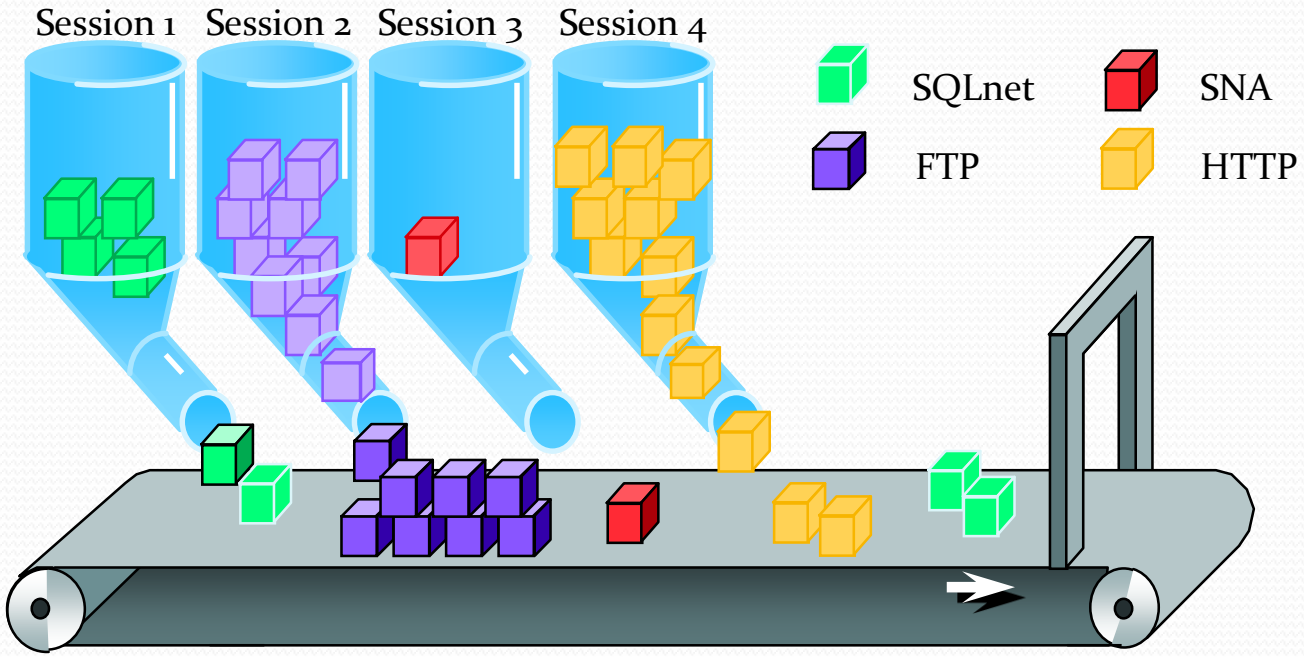
Consistent Predictable Performance

Quality of Service Building Blocks

- Classification
- Policing
- Shaping
- Congestion Management

Congestion Management—Fancy Queuing

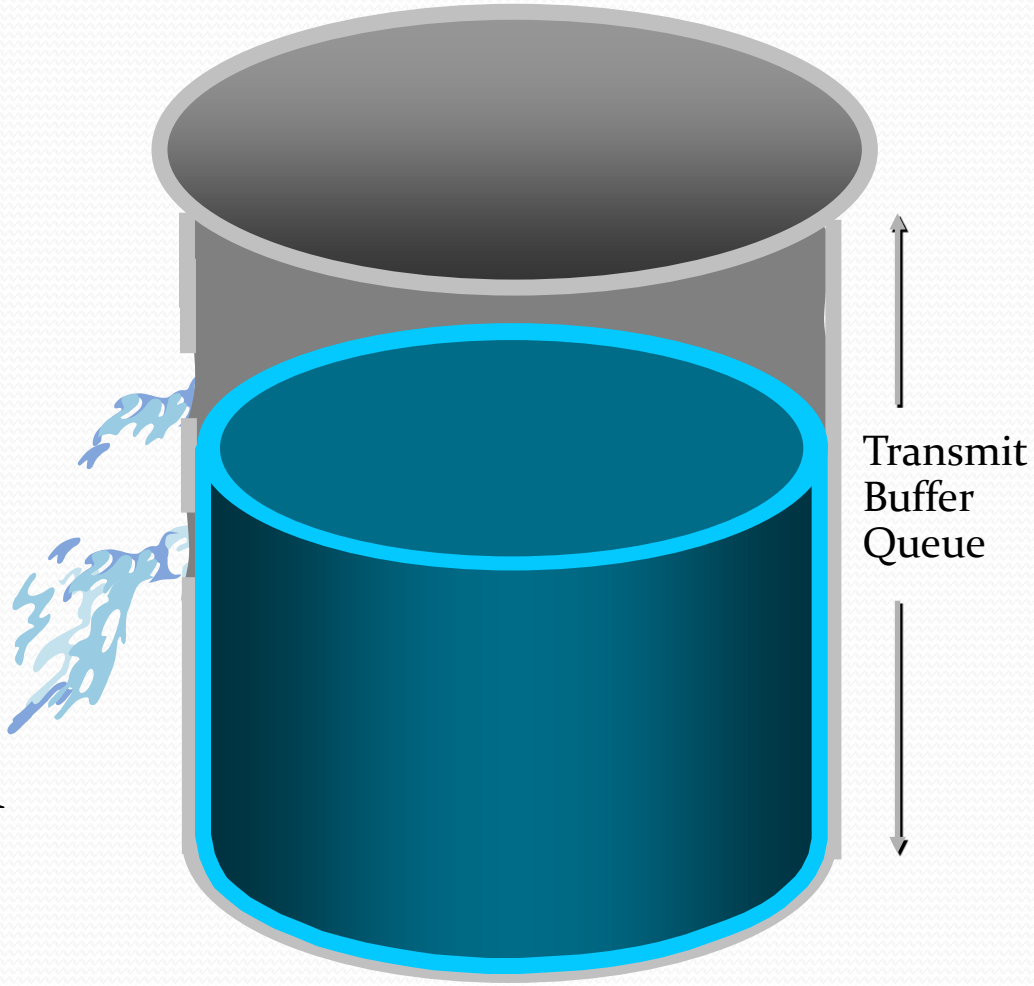
- Weighted Fair Queuing
  - Automatically allocates bandwidth "fairly"



Other queuing options include FIFO, priority queuing, and custom queuing

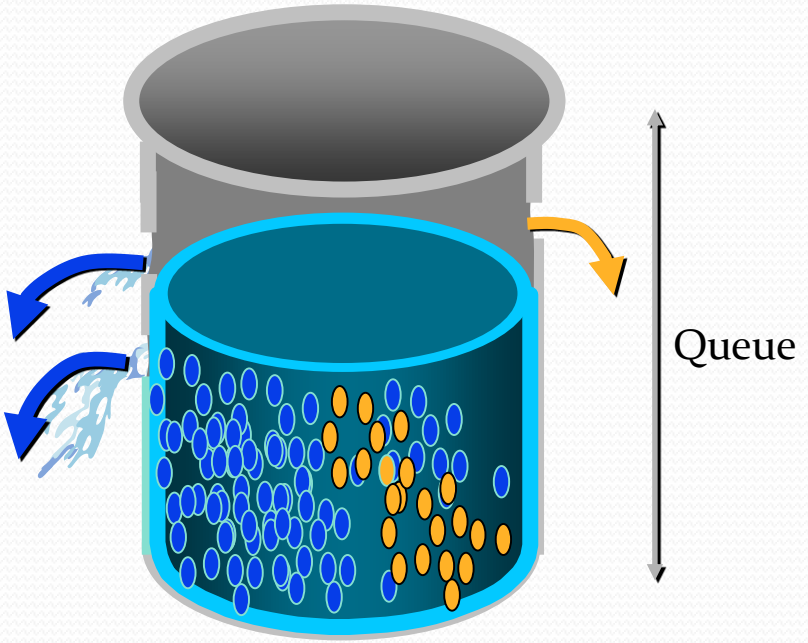
Random Early Detection (RED)

- RED reduces long-term average queue
- Packet drops are randomized throughout queue depth
- Drop rate is increased as queue depth is increased



Weighted RED

- WRED addresses:
  - In the event packets need to be dropped, what class of packets should be dropped



Packets classified as blue start dropping at a 50% queue depth. Drop rate is increased as queue depth is increased.

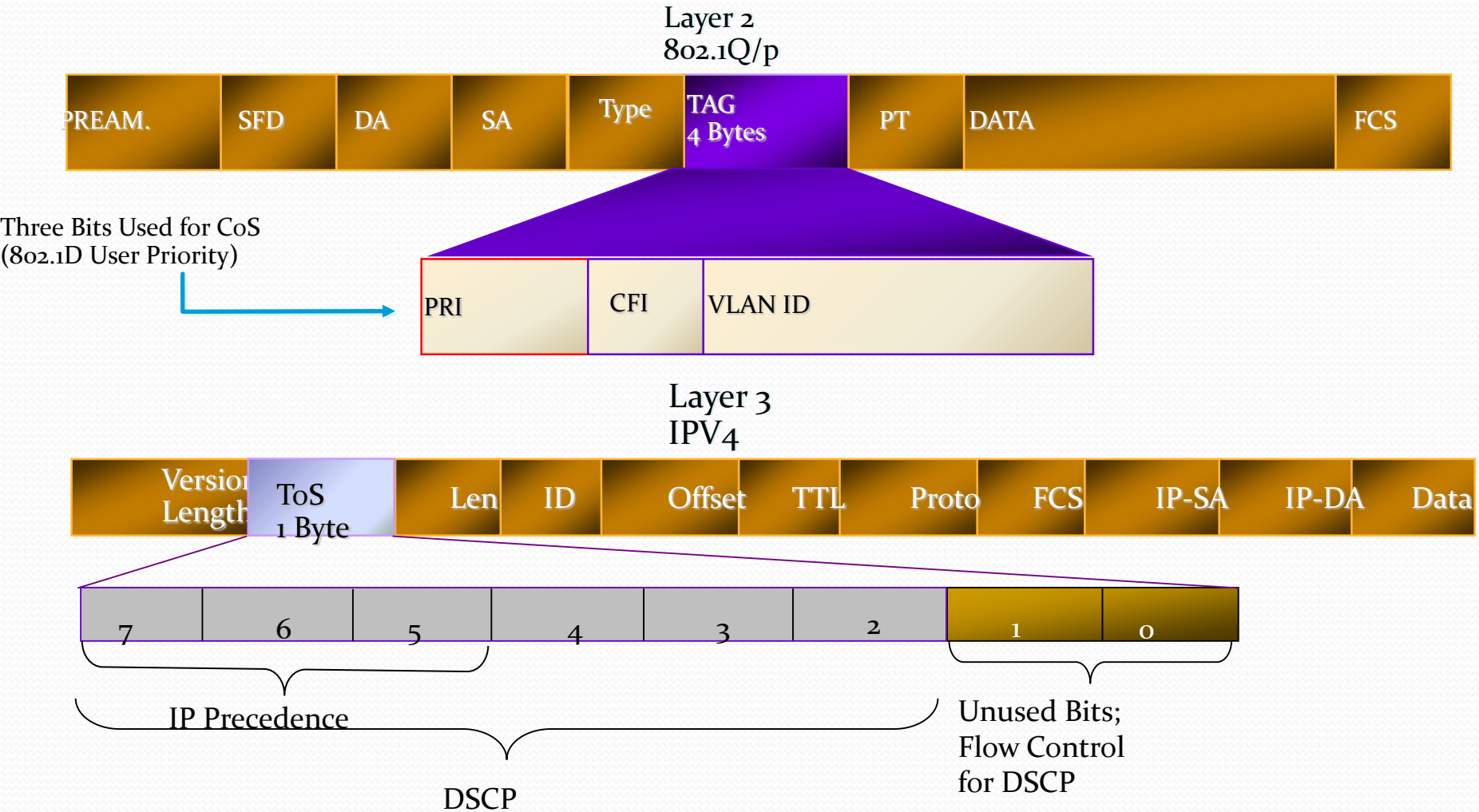
Packets classified as gold are dropped at 90% queue depth.

QoS Terminology

- QoS labels are used to prioritize traffic

  COS, TOS, DSCP
- Classification is selection of traffic based on labels, policy
- Marking is application of QoS labels to traffic
- Policing is process by which the switch limits the bandwidth consumed by a flow of traffic
- Queuing is placing of traffic in different transmit queues
- Scheduling is process of emptying the transmit queues

Layer 2 and 3 Traffic Classification



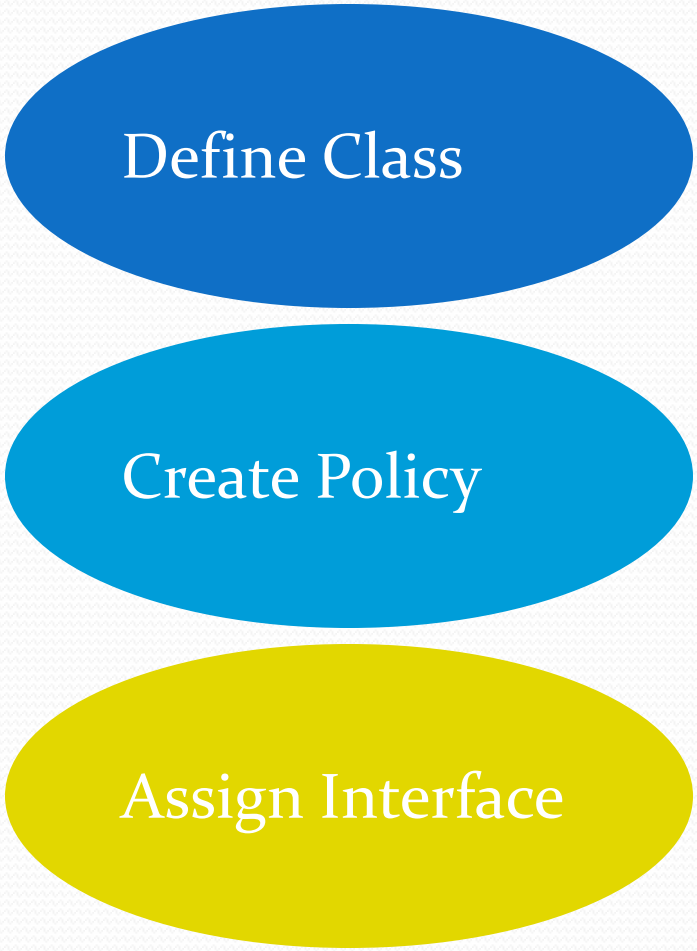
DiffServ Behaviors (RFC's: 2474, 2475, 2597 & 2598)

Per-Hop Behaviours (PHB)				DiffServ Code Points (DSCP)
Expedited Forwarding	EF			101110
Assured Forwarding	Low Drop Pref	Med Drop Pref	High Drop Pref	
Class Selector (CS) 1	AF11	AF12	AF13	001010 001100 001110
Class Selector (CS) 2	AF21	AF22	AF23	010010 010100 010110
Class Selector (CS) 3	AF31	AF32	AF33	011010 011100 011110
Class Selector (CS) 4	AF41	AF42	AF43	100010 100100 100110
Best Effort				000000

QoS Examples

- Rewrite all packets from a specific host with high-priority DSCP
- Trust DSCP of VOIP packets and place in Strict Priority Tx Queue
- Police all multicast to 30 mbps
- Mark down vlan 7 traffic beyond 50mbps
- Put video in Tx queue 2 and shape to 20mbps

QoS Syntax : Modular QoS CLI



- Various Criteria to match packets (ACL, IP Prec, IP-DSCP)
- If a packet matches criteria, it is a member of this “class”.

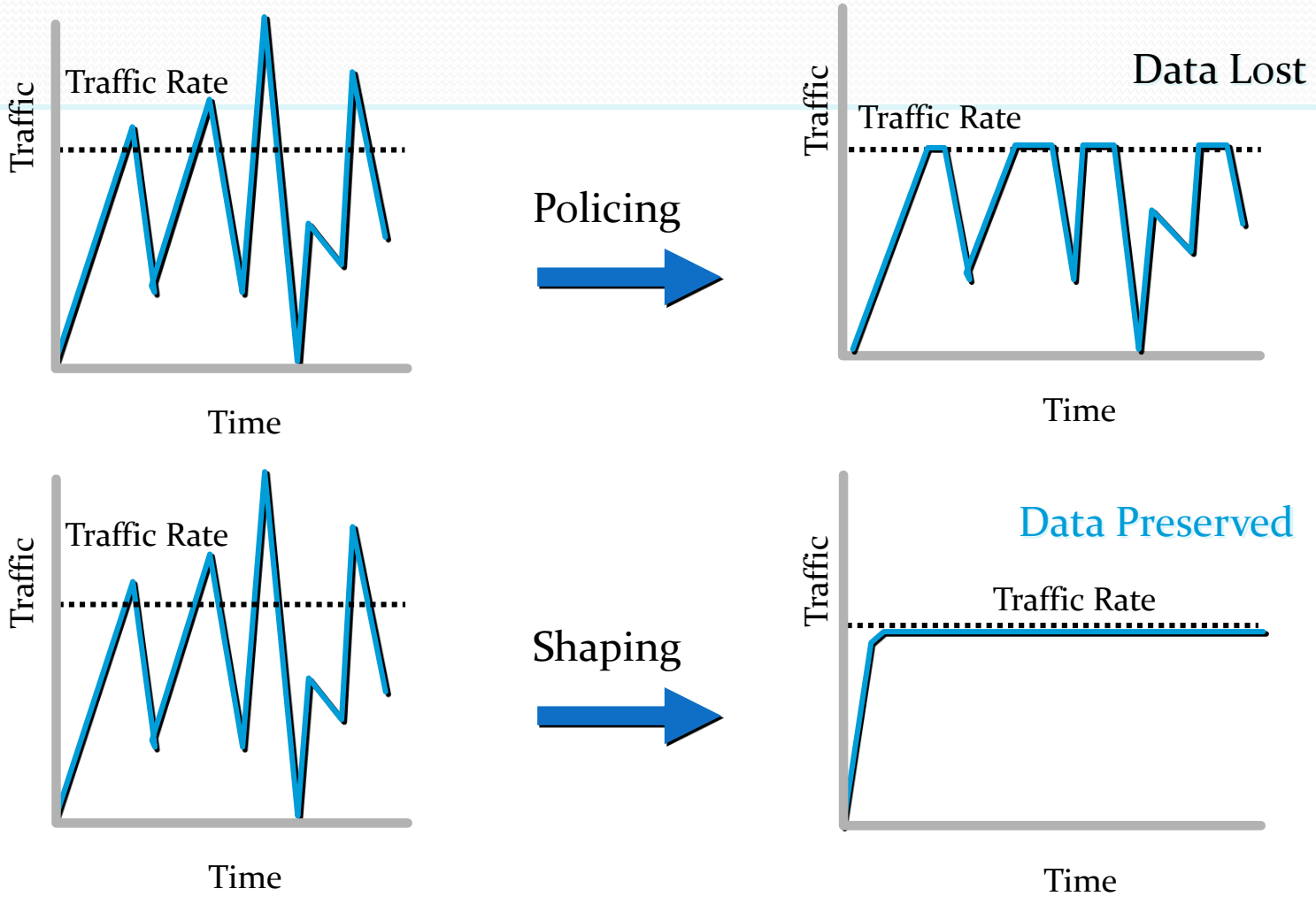
- Associates a Class with a particular function or policy
- For Catalyst 4500 IOS Supervisor, a policy is used to trust traffic, mark traffic, or police traffic
- Applies the service policy to a particular interface
- Effectively “commits” the policy to the hardware

Modular QoS Configuration Example

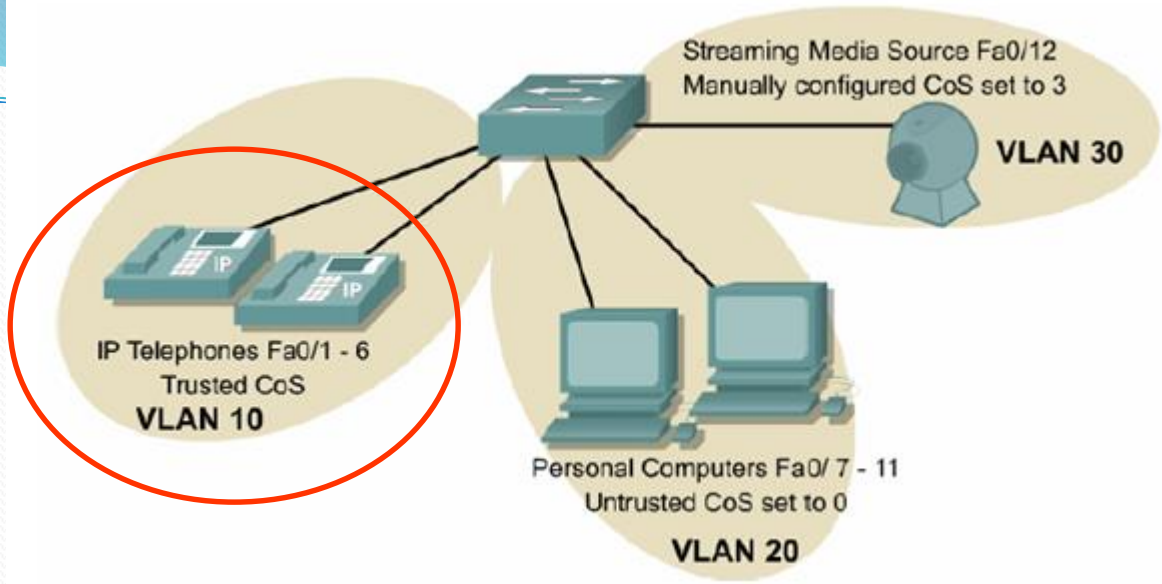
- Match all video on Gig2/1
- Set its DSCP to 5
- Police it to 100mbps and 15 kb burst
- Markdown traffic exceeding policed rate

```
access-list 101 udp permit
  any any range 19000 19010
class-map video
   match access-group 101
policy-map vid-server
   class video
   set ip precedence 5
   police 100m 15K
      exceed-action
      policed-dscp-transmit
interface Gig2/1
   service-policy input vid-
server
```

QoS Policing vs. Shaping



Assigning CoS on a per-port basis



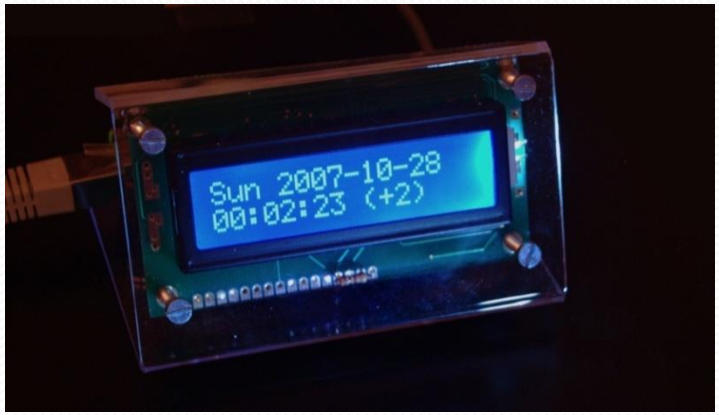

```
switch(config-if)# mls qos trust cos
switch(config-if)# mls qos cos default-cos
```

- If the incoming frame **has a CoS, maintain the same CoS.**
- If the incoming frame has **no CoS (0), apply the default CoS.**

NTP

Using NTP

- Uses
- Timekeeping
- Features/Functions



Uses

- Clocks on hosts and network devices must be maintained and synchronized to ensure that log messages are synchronized with one another
- The date and time settings of the router can be set using one of two methods:
  - Manually edit the date and time
  - Configure Network Time Protocol

Timekeeping

- Pulling the clock time from the Internet means that unsecured packets are allowed through the firewall
- Many NTP servers on the Internet do not require any authentication of peers
- Devices are given the IP address of NTP masters. In an NTP configured network, one or more routers are designated as the master clock keeper (known as an NTP Master) using the **`ntp master`** global configuration command.
- NTP clients either contact the master or listen for messages from the master to synchronize their clocks. To contact the server, use the **`ntp server`** *`ntp-server-address`* command.
- In a LAN environment, NTP can be configured to use IP broadcast messages instead, by using the **ntp broadcast client** command.

Features/Functions

- There are two security mechanisms available:
  - An ACL-based restriction scheme
  - An encrypted authentication mechanism such as offered by NTP version 3 or higher
- Implement NTP version 3 or higher. Use the following commands on both NTP Master and the NTP client.
  - **ntp authenticate**
  - **ntp authentication** *key* **md5** *value*
  - **ntp trusted-key** *key-value*

SYSLOG

Using Syslog

- Implementing Router Logging
- Syslog
- Configuring System Logging

Implementing Router Logging

Configure the router to send log messages to:

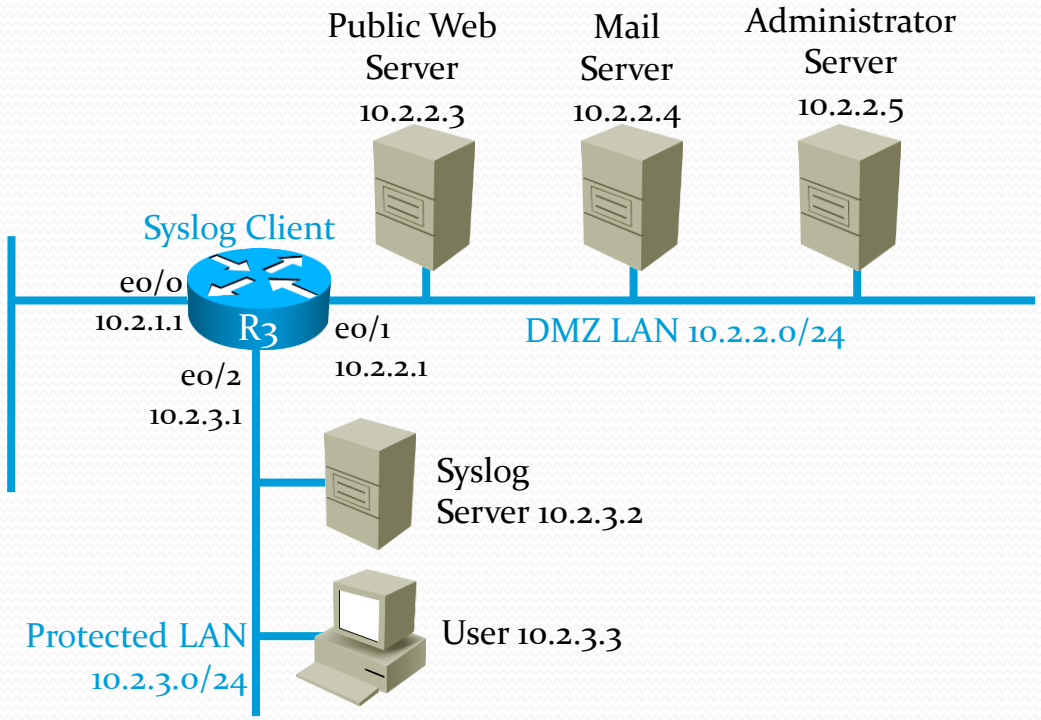
- Console: Console logging is used when modifying or testing the router while it is connected to the console. Messages sent to the console are not stored by the router and, therefore, are not very valuable as security events.
- Terminal lines: Configure enabled EXEC sessions to receive log messages on any terminal lines. Similar to console logging, this type of logging is not stored by the router and, therefore, is only valuable to the user on that line.

Implementing Router Logging

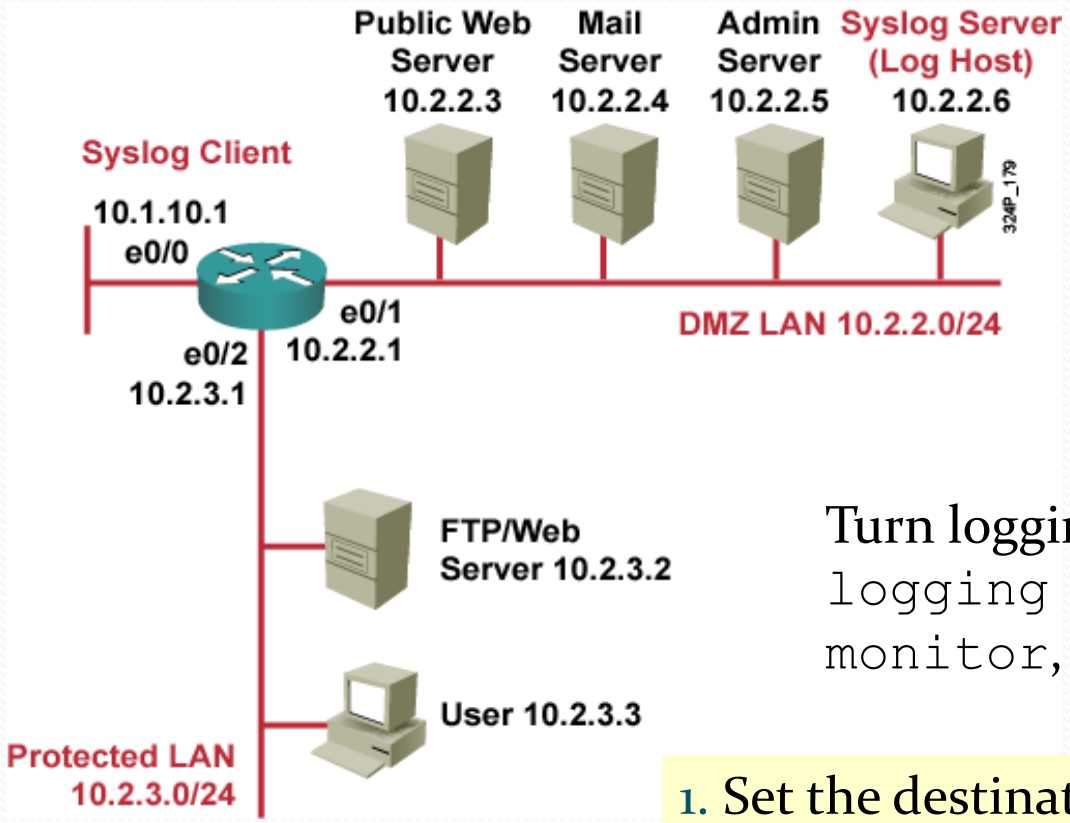
- Buffered logging: Store log messages in router memory. Log messages are stored for a time, but events are cleared whenever the router is rebooted.
- SNMP traps: Certain thresholds can be preconfigured. Events can be processed by the router and forwarded as SNMP traps to an external SNMP server. Requires the configuration and maintenance of an SNMP system.
- Syslog: Configure routers to forward log messages to an external syslog service. This service can reside on any number of servers, including Microsoft Windows and UNIX-based systems, or the Cisco Security MARS appliance.

Syslog

- Syslog servers: Known as log hosts, these systems accept and process log messages from syslog clients.
- Syslog clients: Routers or other types of equipment that generate and forward log messages to syslog servers.



Configuring System Logging



Turn logging on and off using the `logging buffered`, `logging monitor`, and `logging` commands

1. Set the destination logging host

```
R3(config)# logging 10.2.2.6
R3(config)# logging trap informational
R3(config)# logging source-interface loopback 0
R3(config)# logging on
```

2. Set the log severity (trap) level

3. Set the source interface

4. Enable logging

Syslog Severity Levels

- 0 Emergency
- 1 Alert
- 2 Critical
- 3 Error
- 4 Warning
- 5 Notice
- 6 Informational
- 7 Debugging

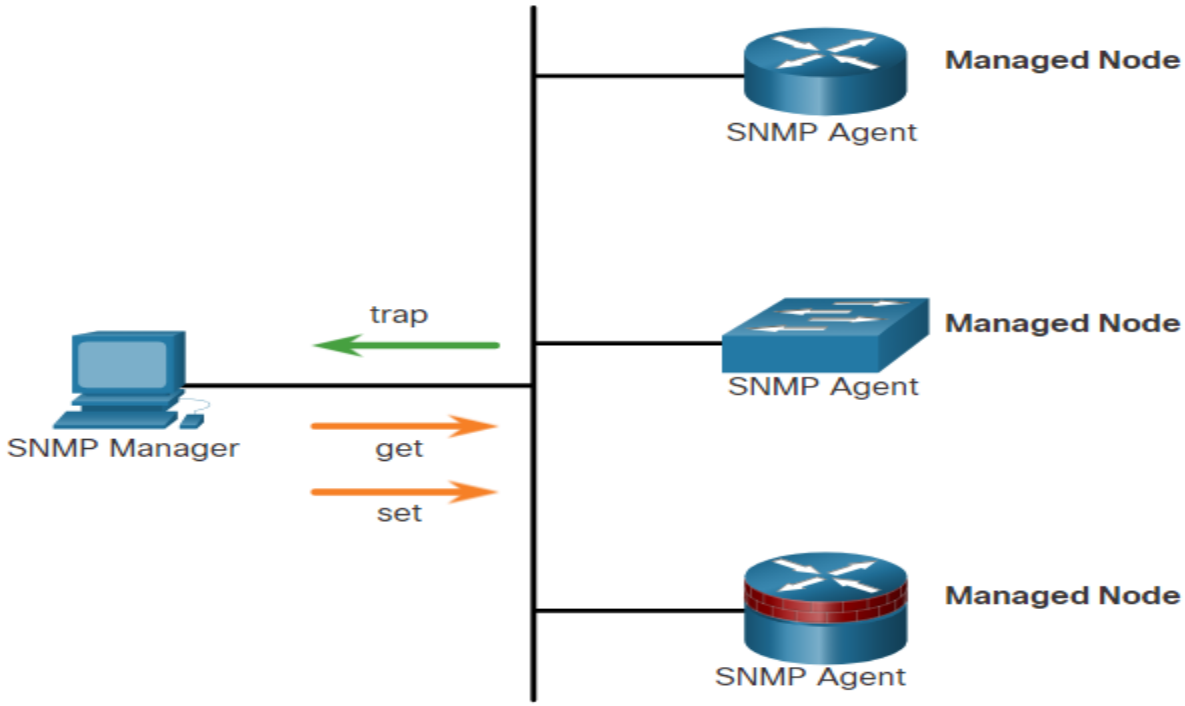
SNMP

- SNMP was developed to allow administrators to manage nodes such as servers, workstations, routers, switches, and security appliances, on an IP network

- SNMP is an application layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of three elements:

- SNMP manager
- SNMP agents (managed node)
- Management Information Base (MIB)

- the SNMP manager can collect information from an SNMP agent by using the “get” action and can change configurations on an agent by using the “set” action. In addition, SNMP agents can forward information directly to a network manager by using “traps”.



- MIBs store data about the device and operational statistics and are meant to be available to authenticated remote users. The SNMP agent is responsible for providing access to the local MIB.

- The SNMP manager polls the agents and queries the MIB for SNMP agents on UDP port 161. SNMP agents send any SNMP traps to the SNMP manager on UDP port 162

SNMP Operation

Operation	Description
`get-request`	Retrieves a value from a specific variable.
`get-next-request`	Retrieves a value from a variable within a table; the SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.
`get-bulk-request`	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data. (Only works with SNMPv2 or later.)
`get-response`	Replies to a **get-request**, **get-next-request**, and **set-request** sent by an NMS.
`set-request`	Stores a value in a specific variable.

Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

SNMP Configuration

!R1

Snmp-server community cisco ro

Snmp-server enable traps → Optional

Snmp-server host 10.0.0.2 cisco → Optional

Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

Similarities between SNMP versions

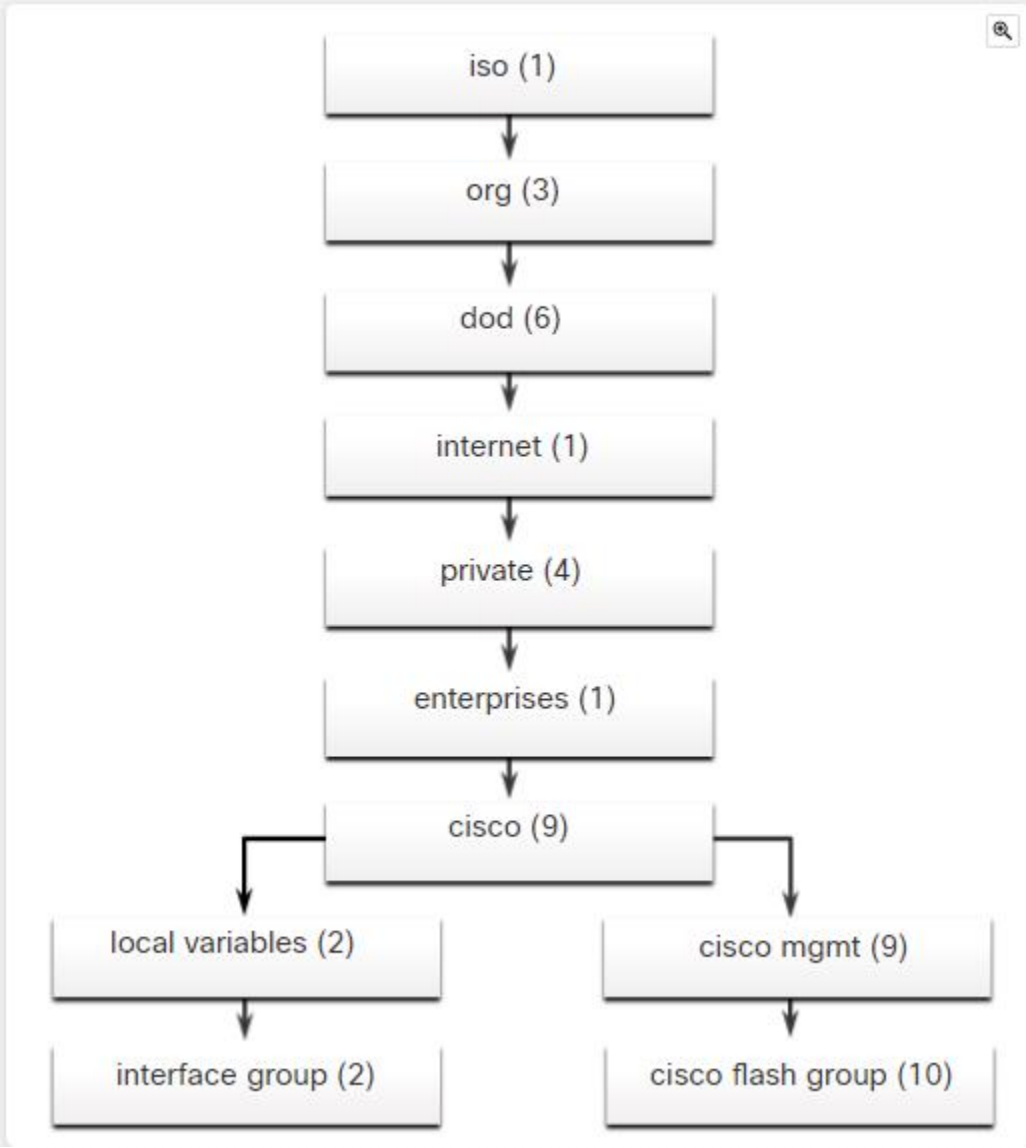
SNMP Version	Description
1	Uses SMIv1, simple authentication with communities, but used MIB-I originally.
2	Uses SMIv2, removed requirement for communities, added GetBulk and Inform messages, but began with MIB-II originally.
2c	Pseudo-release (RFC 1905) that allowed SNMPv1-style communities with SNMPv2; otherwise, equivalent to SNMPv2.
3	Mostly identical to SNMPv2, but adds significantly better security, although it supports communities for backward compatibility. Uses MIB-II.

SNMP Security

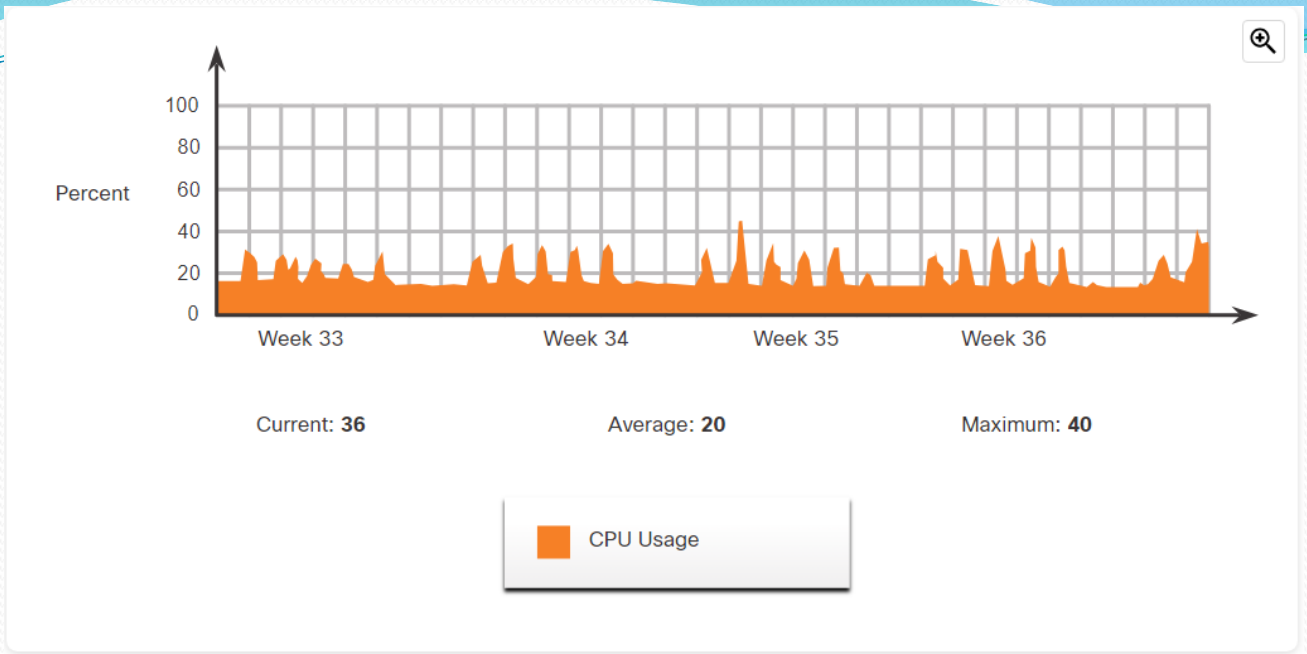
- SNMP version 3 uses MD5 & SHA for data integrity
- SNMP version 3 uses 3DES as a method of Encryption.

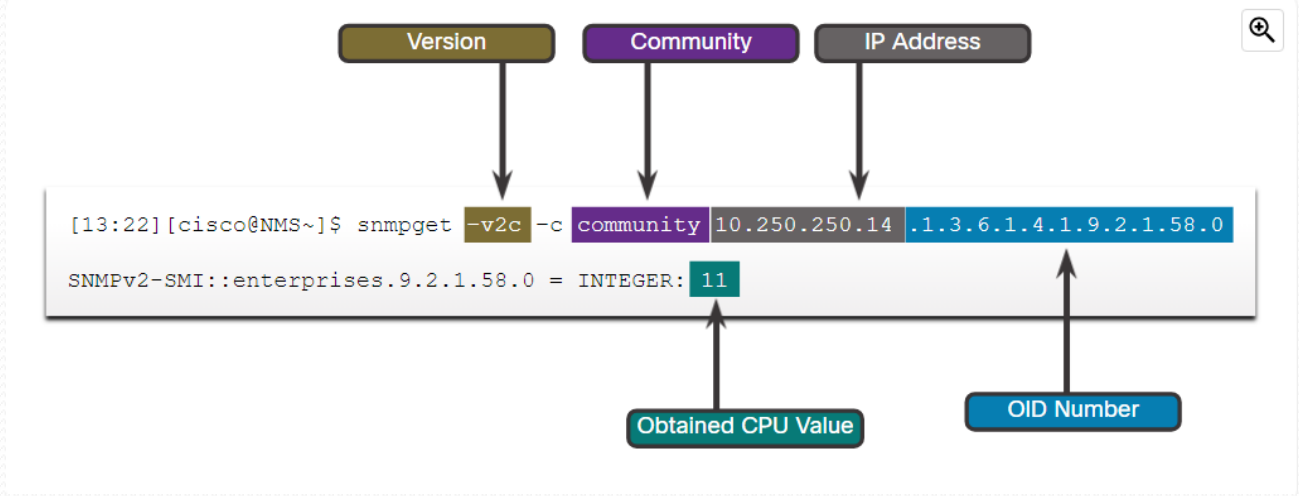
Management Information Base (OIDs)

- The MIB organizes variables hierarchically. The MIB defines each variable as an object ID (OID). OIDs uniquely identify managed objects in the MIB hierarchy.OIDs belonging to Cisco, are numbered as follows: .iso (1).org (3).dod (6).internet (1).private (4).enterprises (1).cisco (9). Therefore, the OID is 1.3.6.1.4.1.9.



Prepared By:Waleed Adlan-CCIE41999 - waleed_hashim@hotmail.com





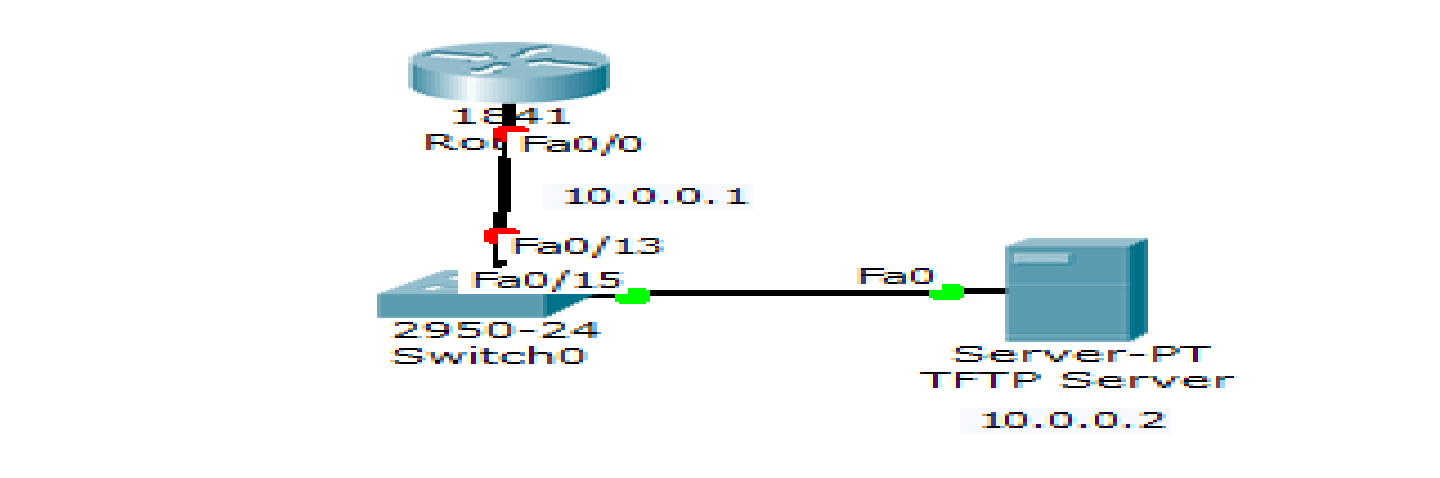
Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

FTP & TFTP

FTP & TFTP Protocols

- **FTP:** FTP is a network protocol used to transfer files from one computer to another over a TCP network. Like Telnet, it uses a client-network architecture, which means that a user has to have an FTP client installed to access the FTP server running on a remote machine. After establishing the FTP connection, the user can download or upload files to and from the FTP server.
- FTP requires authentication for transferring files. Examples of FTP Server is FileZela
- **TFTP:**is a network protocol used to transfer files between remote machines. It is a simple version of FTP, lacking some of the more advanced features FTP offers, but requiring less resources than FTP

Router Files Backup & Upgrade



Transferring File From Router to The server (Backup)

- Connect the network as shown in the Figure
- Make Sure the ping is working between the Server and the Router
- Open the tftp server program
- Then in the router enable mode issue the following commands:

- !R1
- Show flash: (and copy the name of the IOS)
- Copy flash: tftp:

Transferring File From Server to The Router (Upgrade)

- Do all the previous steps, but then issue the following command instead:
- !R1
- Copy tftp: flash:

Transferring Files Using FTP from/to Cisco Router

- You can configure the username and password in the cisco router that matches the FTP server
- **ip ftp username cisco**
- **ip ftp password cisco**

- **Then:**
- **copy ftp flash** or **copy flash ftp**

- **Or**
- copy ftp://username:password@ftpserverip/file flash

Network Security Fundamentals

What is Network Security?

National Security Telecommunications and Information Systems Security Committee (NSTISSC)

Network security is the protection of information and systems and hardware that use, store, and transmit that information.

Network security encompasses those steps that are taken to ensure the confidentiality, integrity, and availability of data or resources.

Rationale for Network Security

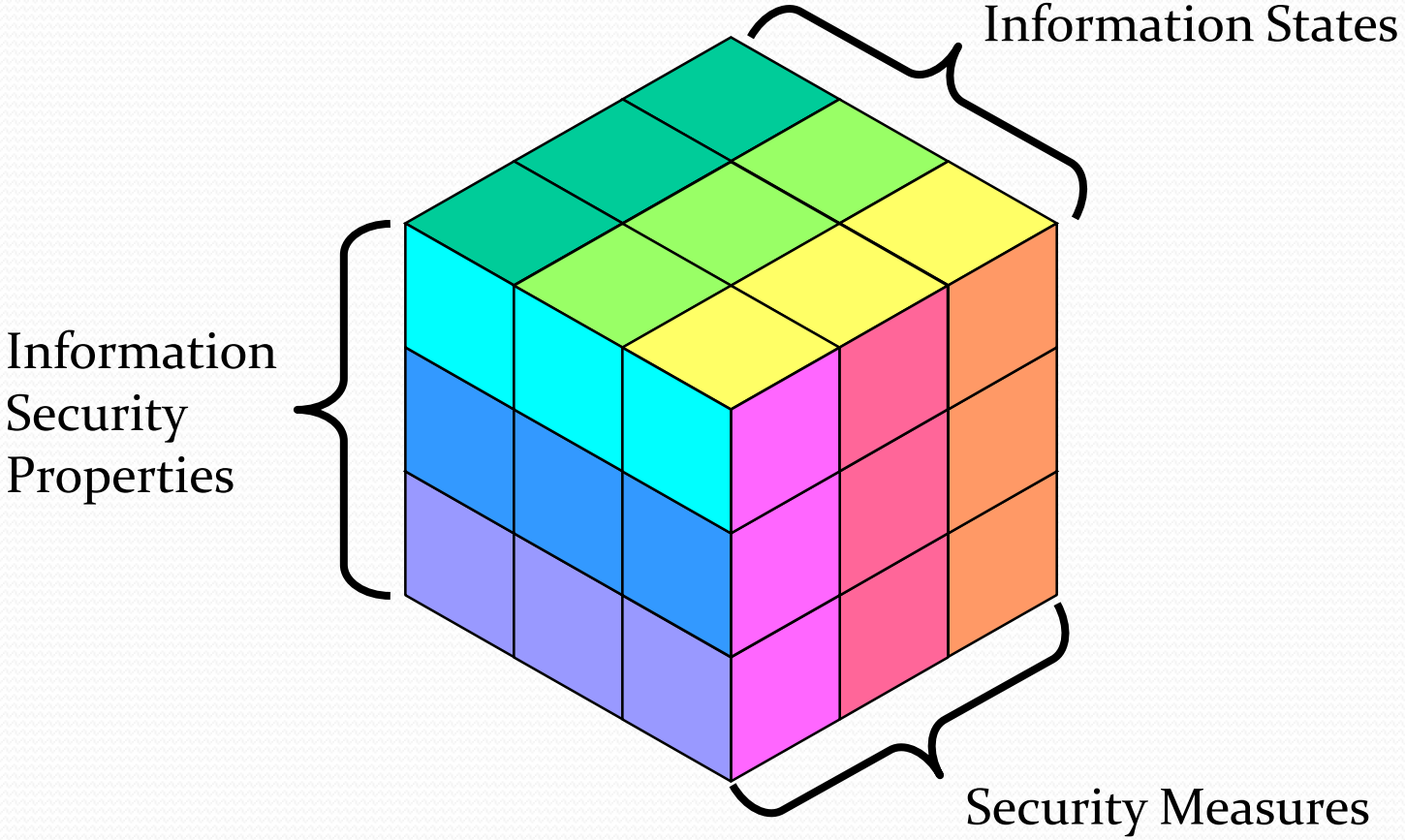
Network security initiatives and network security specialists can be found in private and public, large and small companies and organizations. The need for network security and its growth are driven by many factors:

1. Internet connectivity is 24/7 and is worldwide
2. Increase in cyber crime
3. Impact on business and individuals
4. Legislation & liabilities
5. Proliferation of threats
6. Sophistication of threats

Goals of an Information Security Program

- Confidentiality
  - Prevent the disclosure of sensitive information from unauthorized people, resources, and processes
- Integrity
  - The protection of system information or processes from intentional or accidental modification
- Availability
  - The assurance that systems and data are accessible by authorized users when needed

Information Security Model



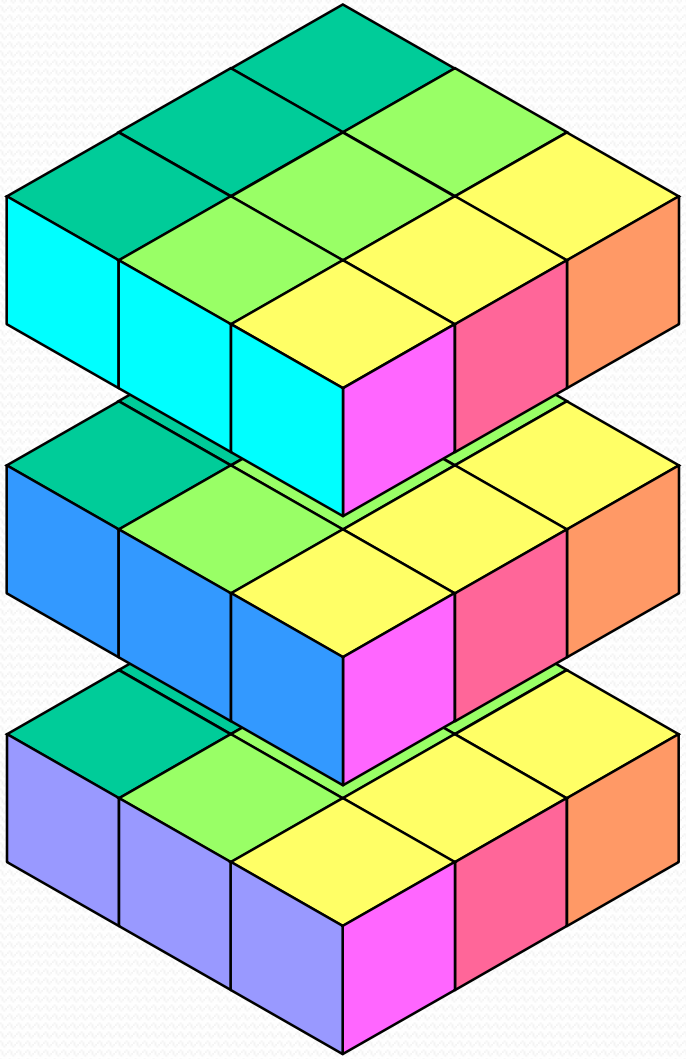
NSTISSI 4011: National Training Standard for Information Systems Security Professionals, 1994

Information Security Properties

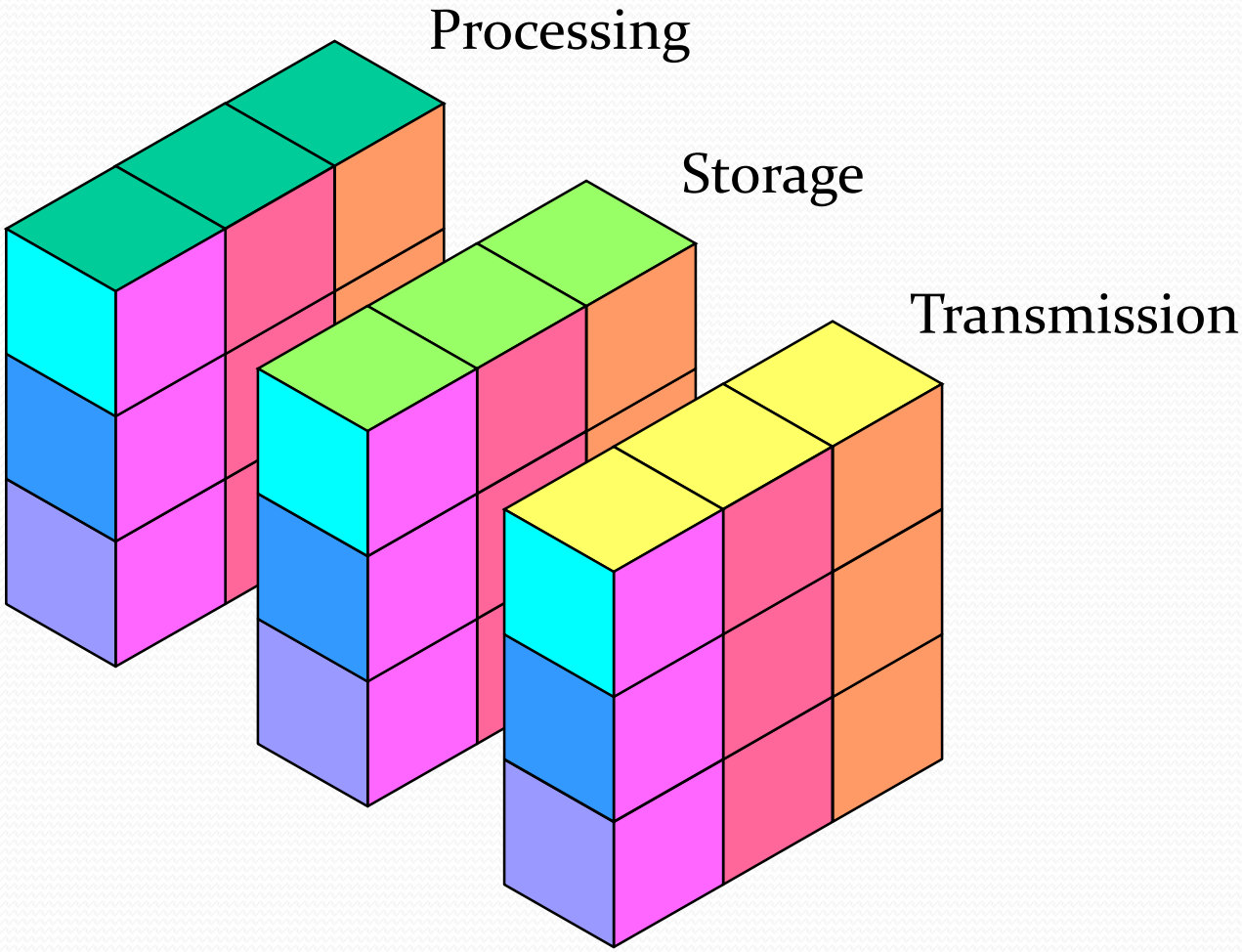
Confidentiality

Integrity

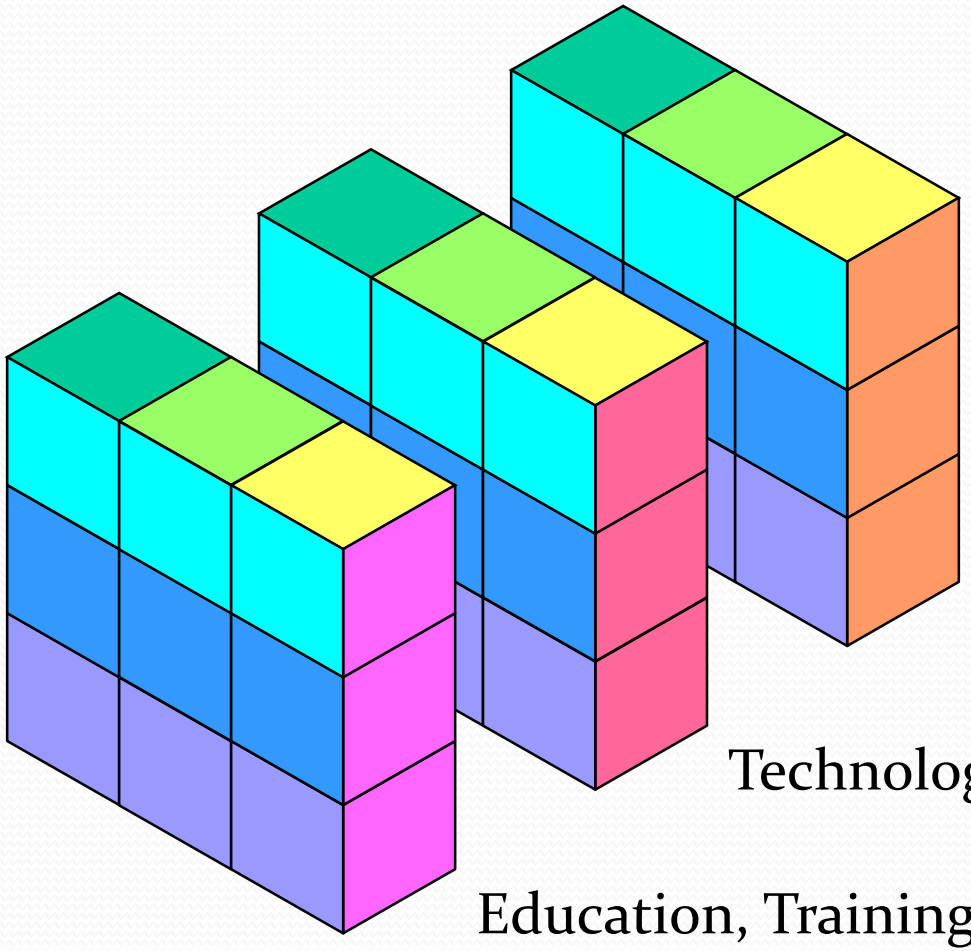
Availability



Information States



Security Measures



Policy and Procedures

Technology

Education, Training, and Awareness

Risk Management

- Risk Analysis
- Threats
- Vulnerabilities
- Countermeasures

Risk Management

Patches and Updates

Control physical access

Password protection

Anti-Virus

Firewall

Develop a Security Policy

- The process of assessing and quantifying risk and establishing an acceptable level of risk for the organization
- Risk can be mitigated, but cannot be eliminated

Risk Assessment

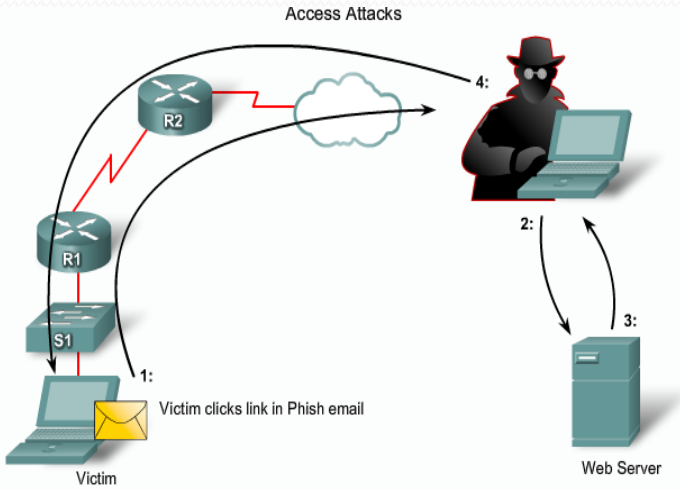
- Risk assessment involves determining the likelihood that the vulnerability is a risk to the organization
- Each vulnerability can be ranked by the scale
- Sometimes calculating anticipated losses can be helpful in determining the impact of a vulnerability

Asset Identification

- Categories of assets
  - Information Assets (people, hardware, software, systems)
  - Supporting Assets (facilities, utilities, services)
  - Critical Assets (can be either of those listed above)
- Attributes of the assets need to be compiled
- Determine each item's relative value
  - How much revenue/profit does it generate?
  - What is the cost to replace it?
  - How difficult would it be to replace?
  - How quickly can it be replaced?

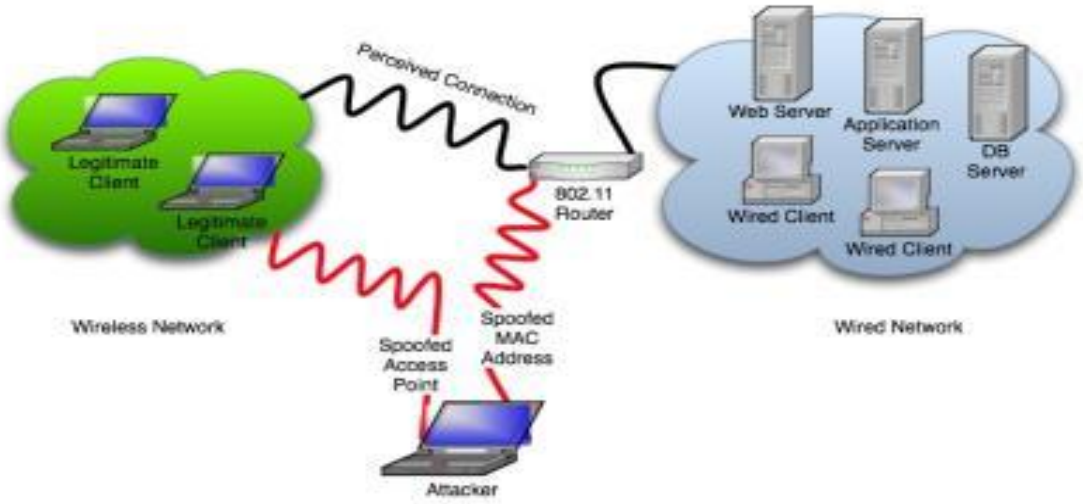
Network Security "Threat"

- A potential danger to information or a system
- An example: the ability to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network
- There may be weaknesses that greatly increase the likelihood of a threat manifesting
- Threats may include equipment failure, structured attacks, natural disasters, physical attacks, theft, viruses and many other potential events causing danger or damage



Types of Network Threats

- Impersonation
- Eavesdropping
- Denial-of-service
- Packet replay
- Man-in-the-middle
- Packet modification



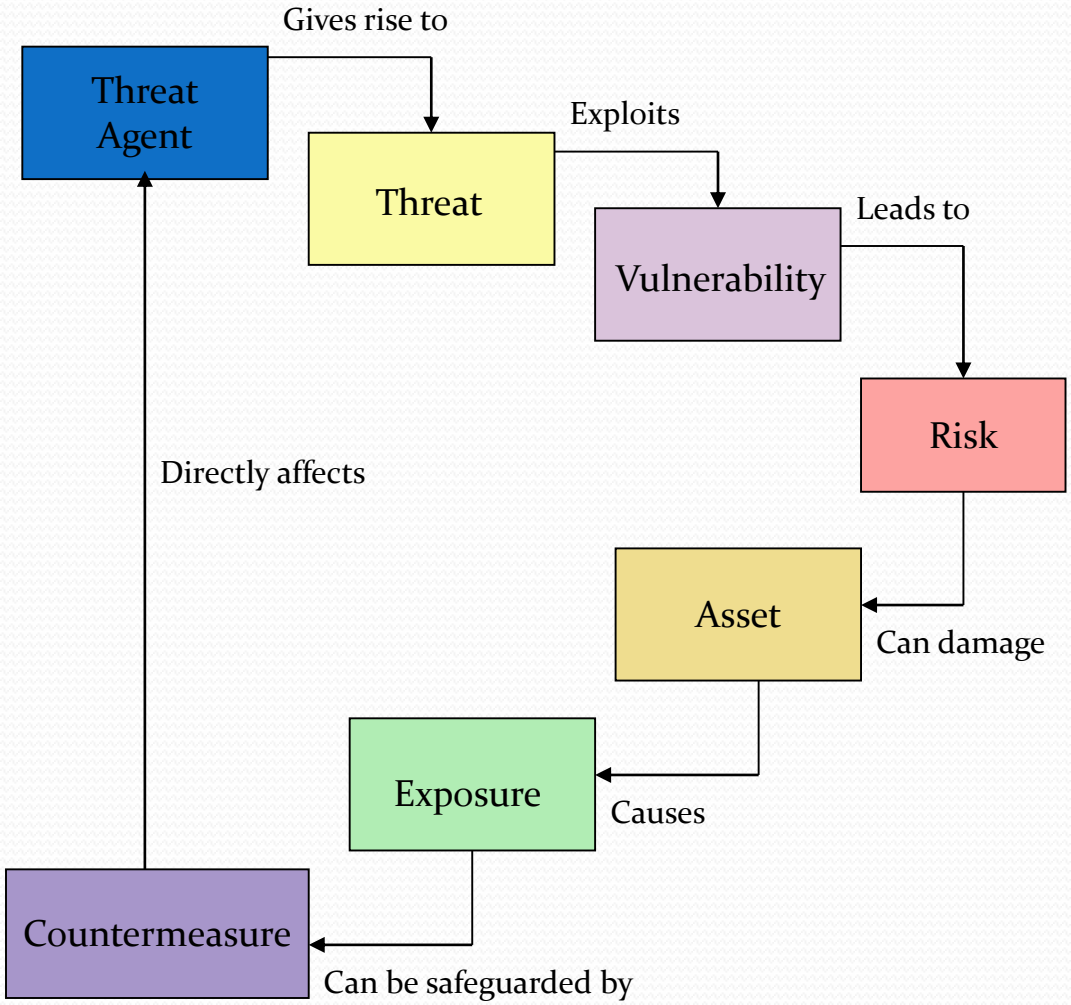
Vulnerability

- A network vulnerability is a weakness in a system, technology, product or policy
- In today's environment, several organizations track, organize and test these vulnerabilities
- The US government has a contract with an organization to track and publish network vulnerabilities
- Each vulnerability is given an ID and can be reviewed by network security professionals over the Internet.
- The common vulnerability exposure (CVE) list also publishes ways to prevent the vulnerability from being attacked

Risk Management Terms

- Vulnerability – a system, network or device weakness
- Threat – potential danger posed by a vulnerability
- Threat agent – the entity that indentifies a vulnerability and uses it to attack the victim
- Risk – likelihood of a threat agent taking advantage of a vulnerability and the corresponding business impact
- Exposure – potential to experience losses from a threat agent
- Countermeasure – put into place to mitigate the potential risk

Understanding Risk



Types of Attacks

Structured attack

Come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

Unstructured attack

Consists of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company.

Types of Attacks

External attacks

Initiated by individuals or groups working outside of a company. They do not have authorized access to the computer systems or network. They gather information in order to work their way into a network mainly from the Internet or dialup access servers.

Internal attacks

More common and dangerous. Internal attacks are initiated by someone who has authorized access to the network. According to the FBI, internal access and misuse account for 60 to 80 percent of reported incidents. These attacks often are traced to disgruntled employees.

Types of Attacks

- Passive Attack
  - Listen to system passwords
  - Release of message content
  - Traffic analysis
  - Data capturing
- Active Attack
  - Attempt to log into someone else's account
  - Wire taps
  - Denial of services
  - Masquerading
  - Message modifications

Specific Network Attacks

- ARP Attack
- Brute Force Attack
- Worms
- Flooding
- Sniffers
- Spoofing
- Redirected Attacks
- Tunneling Attack
- Covert Channels

Internet queries

Ping sweeps

Port scans

Stages of an Attack

- Today's attackers have a abundance of targets. In fact their greatest challenge is to select the most vulnerable victims. This has resulted in very well- planned and structured attacks. These attacks have common logistical and strategic stages. These stages include;
  - Reconnaissance
  - Scanning (addresses, ports, vulnerabilities)
  - Gaining access
  - Maintaining Access
  - Covering Tracks

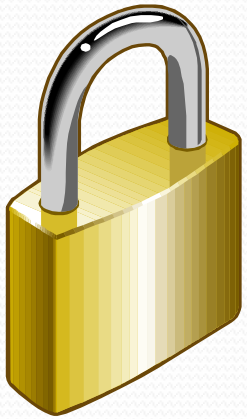
Countermeasures

- DMZ/NAT
- IDS/IPS
- Next Generation Firewalls
- NAC (Network Access Control) Devices
- Authentication/Authorization/Accounting
- Self-defending networks
- Policies, procedures, standards guidelines
- Training and awareness

Securing Network Devices

Areas of Router Security

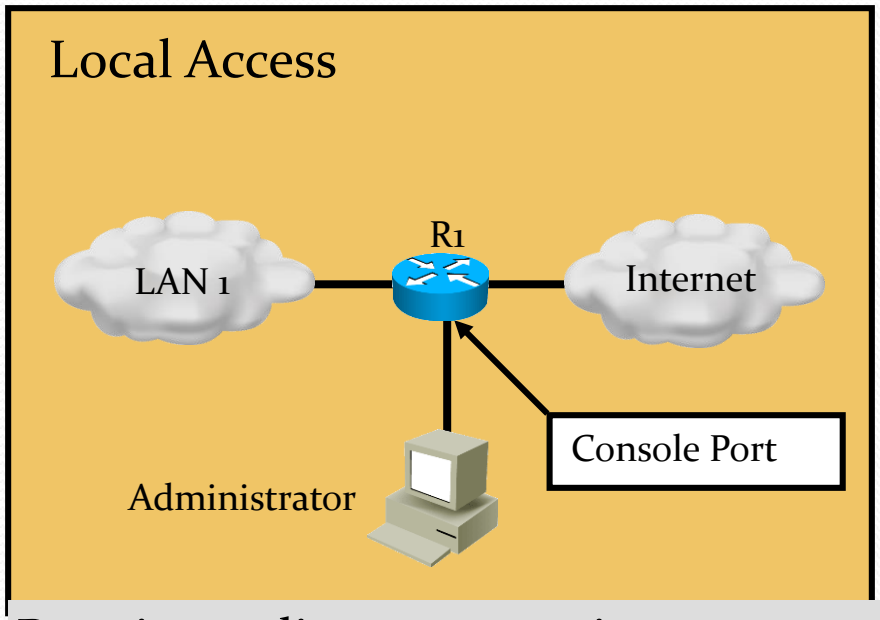
- Physical Security
  - Place router in a secured, locked room
  - Install an uninterruptible power supply
- Operating System Security
  - Use the latest stable version that meets network requirements
  - Keep a copy of the O/S and configuration file as a backup
- Router Hardening
  - Secure administrative control
  - Disable unused ports and interfaces
  - Disable unnecessary services



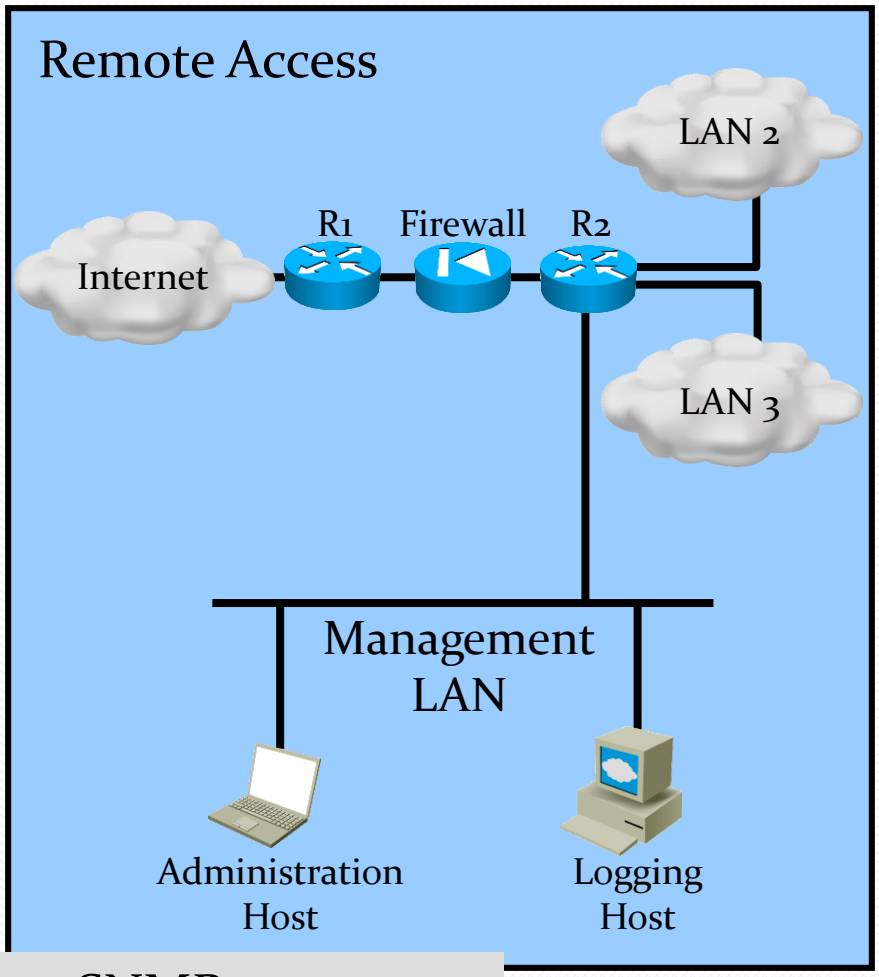
Securing Administrative Access

- Restrict Device Accessibility - Limit the accessible ports, restrict the permitted communicators and restrict the permitted methods of access.
- Log and Account for all Access - Record anyone who accesses a device.
  - Authenticate Access: Ensure access is only granted to authenticated users, groups, and services.
  - Authorize Actions: Restrict the actions and views permitted by any particular user, group, or service.
- Present Legal Notification - Display legal notice for interactive sessions.
- Ensure the Confidentiality of Data - Protect locally stored sensitive data from viewing and copying.

Local Versus Remote Access



Requires a direct connection to a console port using a computer running terminal emulation software



Uses Telnet, SSH HTTP or SNMP connections to the router from a computer

Secure Administrative Access

- Passwords
- Access Port Passwords
- Password Security
- Creating Users

Access Port Passwords

```
R1(config)# enable secret cisco
```

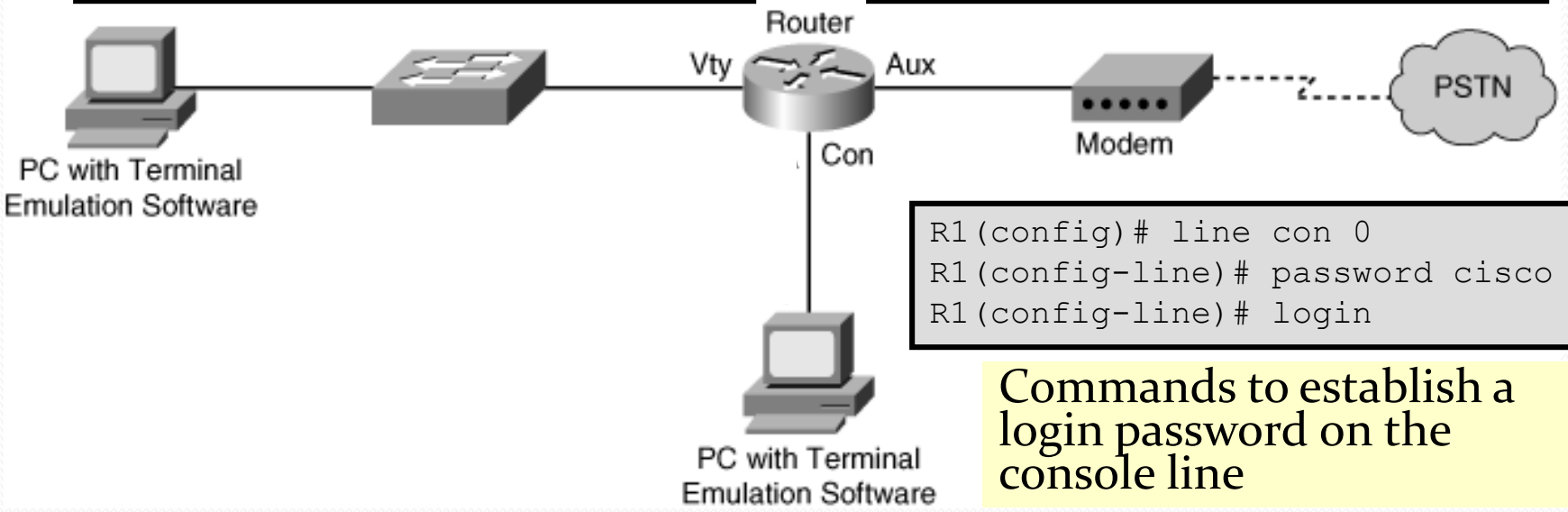
Command to restrict access to privileged EXEC mode

Commands to establish a login password on incoming Telnet sessions

```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

Commands to establish a login password for dial-up modem connections

```
R1(config)# line aux 0
R1(config-line)# password cisco
R1(config-line)# login
```




```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

Commands to establish a login password on the console line

Password Security

To increase the security of passwords, use additional configuration parameters:

- Minimum password lengths should be enforced
- Unattended connections should be disabled
- All passwords in the configuration file should be encrypted

```
R1(config)# service password-encryption
R1(config)# exit
R1# show running-config
line con 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
line aux 0
 exec-timeout 3 30
 password 7 094F471A1A0A
 login
```

Creating Users

```
username name secret {[0]password|5encrypted-secret}
```

Parameter	Description
name	This parameter specifies the username.
0	(Optional) This option indicates that the plaintext password is to be hashed by the router using MD5.
password	This parameter is the plaintext password to be hashed using MD5.
5	This parameter indicates that the encrypted-secret password was hashed using MD5.
encrypted-secret	This parameter is the MD5 encrypted-secret password that is stored as the encrypted user password.

SSH

version 1, 2

- Configuring Router
- SSH Commands
- Connecting to Router

Preliminary Steps

Complete the following prior to configuring routers for the SSH protocol:

1. Ensure that the target routers are running a Cisco IOS Release 12.1(1)T image or later to support SSH.
2. Ensure that each of the target routers has a unique hostname.
3. Ensure that each of the target routers is using the correct domain name of the network.
4. Ensure that the target routers are configured for local authentication, or for authentication, authorization, and accounting (AAA) services for username or password authentication, or both. This is mandatory for a router-to-router SSH connection.

Configuring the Router for SSH

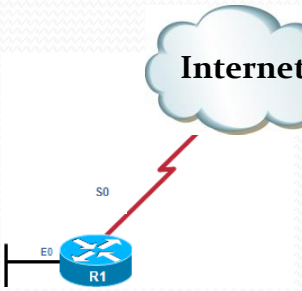
```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys
modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has
been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

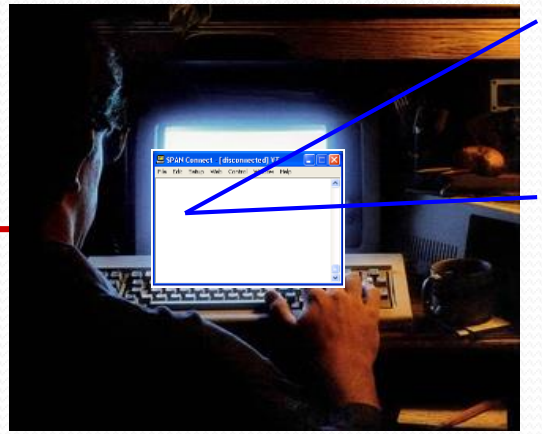
1. Configure the IP domain name of the network
2. Generate one way secret key
3. Verify or create a local database entry
4. Enable VTY inbound SSH sessions

Authentication, Authorization and Accounting

Authentication – Password-Only

Password-Only Method





User Access Verification

Password: *cisco*
Password: *cisco1*
Password: *cisco12*
% Bad passwords

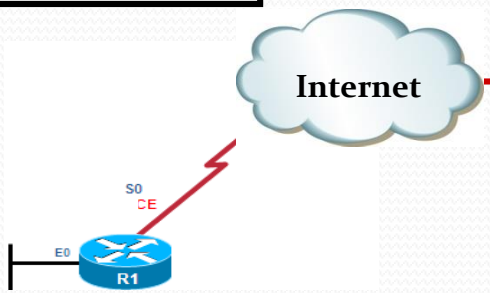
```
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
```

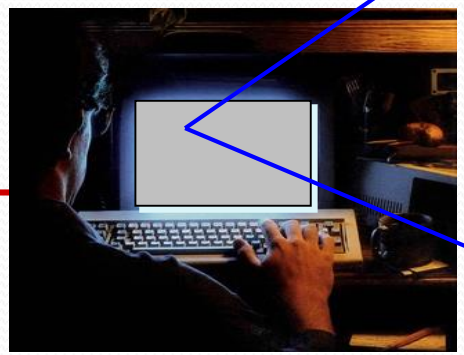
- Uses a login and password combination on access lines
- Easiest to implement, but most unsecure method
- Vulnerable to brute-force attacks
- Provides no accountability

Authentication – Local Database

- Creates individual user account/password on each device
- Provides accountability
- User accounts must be configured locally on each device
- Provides no fallback authentication method

```
R1(config)# username Admin secret
Str0ng5rPa55w0rd
R1(config)# line vty 0 4
R1(config-line)# login local
```





User Access Verification

Username: *Admin*
Password: *cisco1*
% Login invalid

Username: *Admin*
Password: *cisco12*
% Login invalid

Local Database Method

AAA Access Security

Authentication
Who are you?

Authorization
which resources the user is allowed to access and which operations the user is allowed to perform?

Accounting
What did you spend it on?

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO:
EA BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

A72919345 00178255000000003

Detach here and return upper portion with check or money order. Do not staple or fold.

Statement of Personal Credit Card Account

Retain this portion for your files.

EA BANK

Cardmember Name	Account Number	Statement Closing Date
JOE EMPLOYEE	1234-456-890	01-31-01

Statement Date:	02-01-01	Payment Due Date:	03-01-01
Closing Date:	01-31-01		
Credit Limit	$1,500.00	Credit Available:	$1221.50
New Balance:	$278.50	Minimum Payment Due:	$20.00

Account Summary

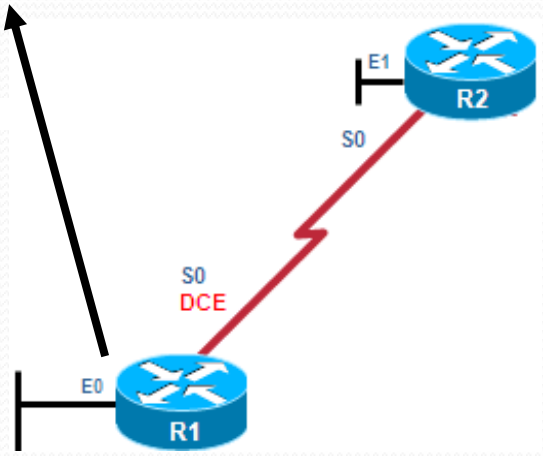
Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	$278.50

Reference Number	Sold	Posted	Activity Since Last Statement		Amount
43210987	01-03	01-13	Payment, Thank You		-$74.25
01234567	01-12	01-13	Wings 'N' Things	Anytown, USA	$25.25
78901234	01-14	01-17	Record Release	Anytown, USA	$40.00
45678901	01-14	01-17	Sports Stadium	Anytown, USA	$75.25
3210987	01-22	01-23	Tie Tack	Anytown, USA	$20.75
76543210	01-29	01-30	Electronic World	Anytown, USA	$89.25
23455678		01-30	Transaction Fees		$3.00
34567890		01-01	Annual Fee		$25.00

PAGE 1 OF 1

Local AAA Authentication Commands

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```



To authenticate administrator access (character mode access)

1. Add usernames and passwords to the local router database
2. Enable AAA globally
3. Configure AAA parameters on the router
4. Confirm and troubleshoot the AAA configuration

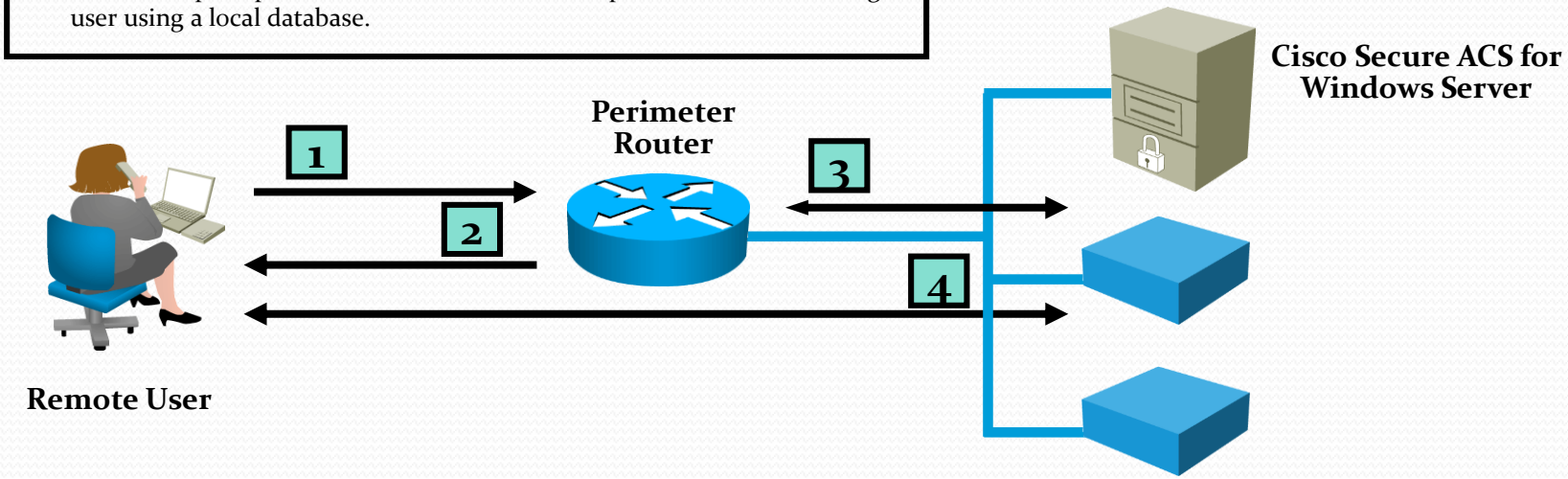
Server-Based AAA

- Comparing Local versus Server-Based AAA
- Overview of TACACS+ and RADIUS
- TACACS (Terminal Access Controller Access-Control System)
- RADIUS (Remote Authentication Dial-In User Service)

Local Versus Server-Based Authentication

Local Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password authenticating the user using a local database.

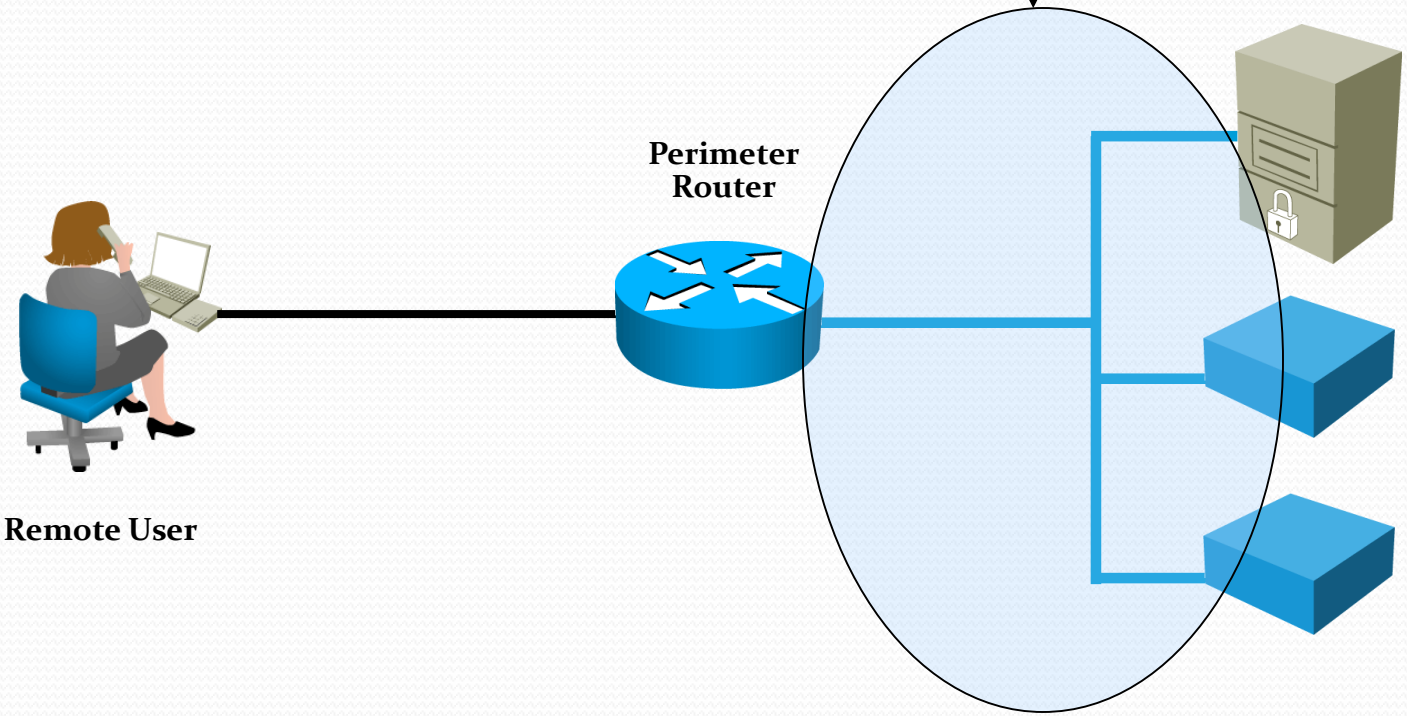


Server-Based Authentication

1. The user establishes a connection with the router.
2. The router prompts the user for a username and password.
3. The router passes the username and password to the Cisco Secure ACS (server or engine).
4. The Cisco Secure ACS authenticates the user. The user is authorized to access the router (administrative access) or the network based on information found in the Cisco Secure ACS database.

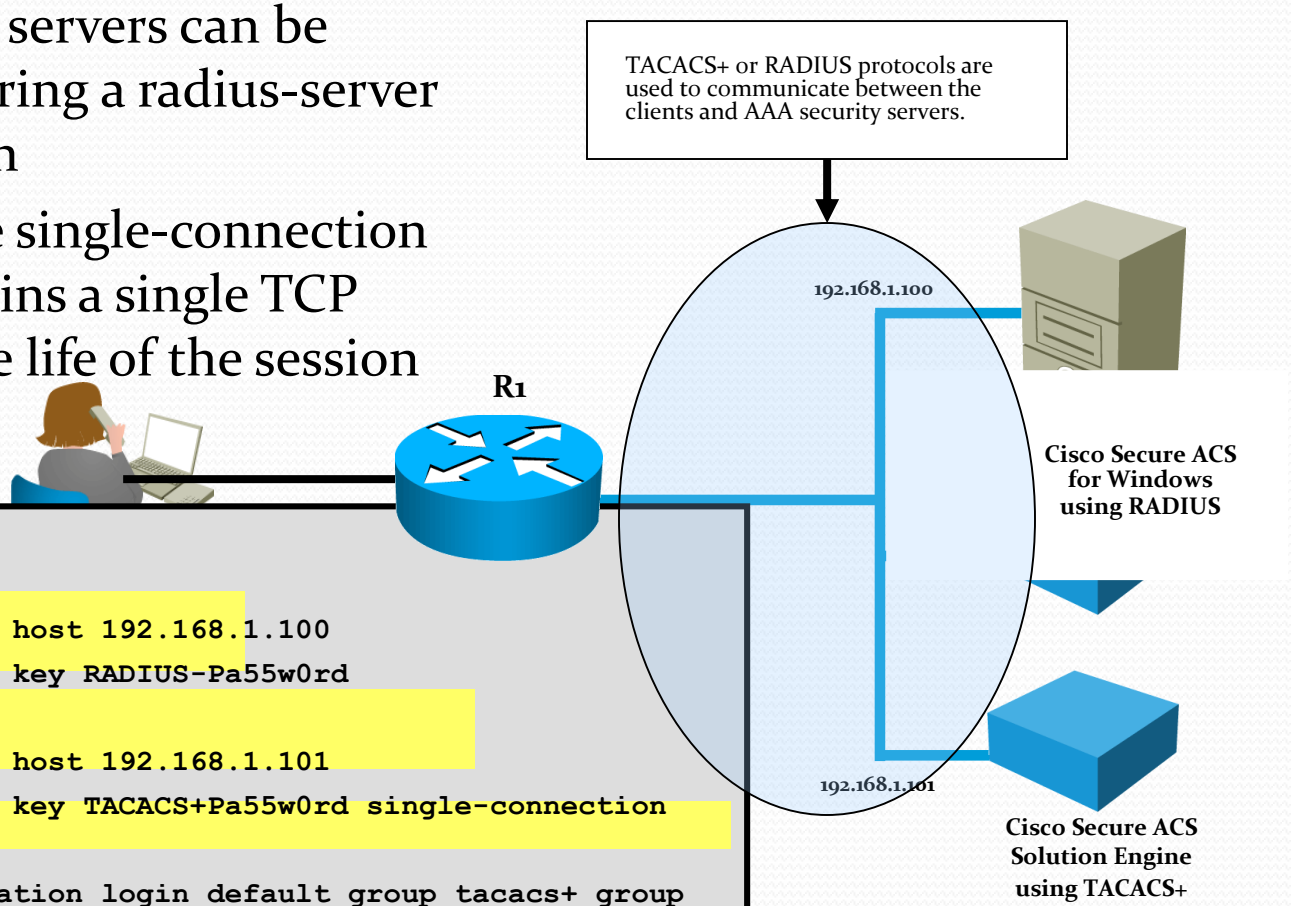
Overview of TACACS+ and RADIUS

TACACS+ or RADIUS protocols are used to communicate between the clients and AAA security servers.



Sample Configuration

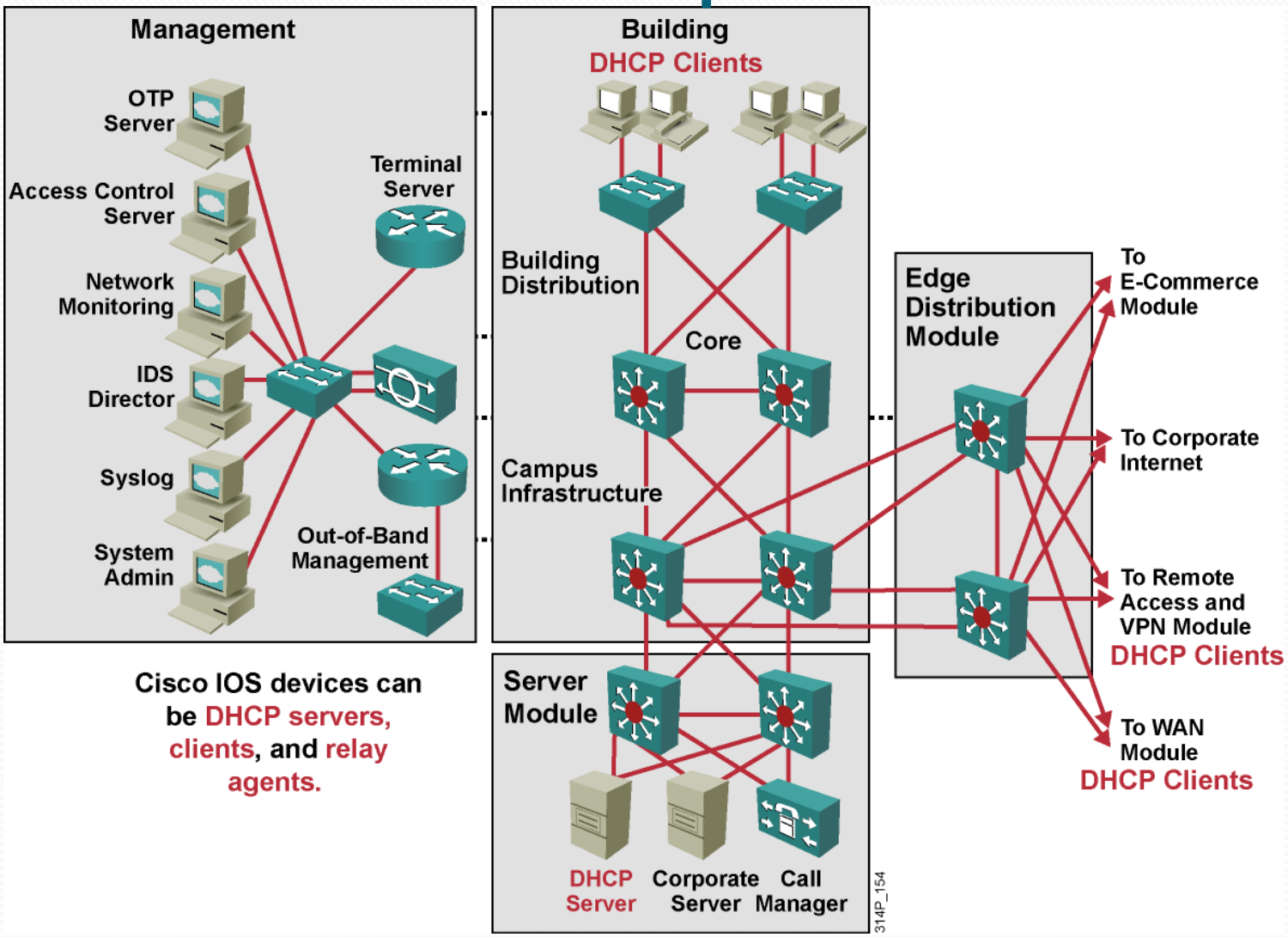
- Multiple RADIUS servers can be identified by entering a radius-server command for each
- For TACACS+, the single-connection command maintains a single TCP connection for the life of the session



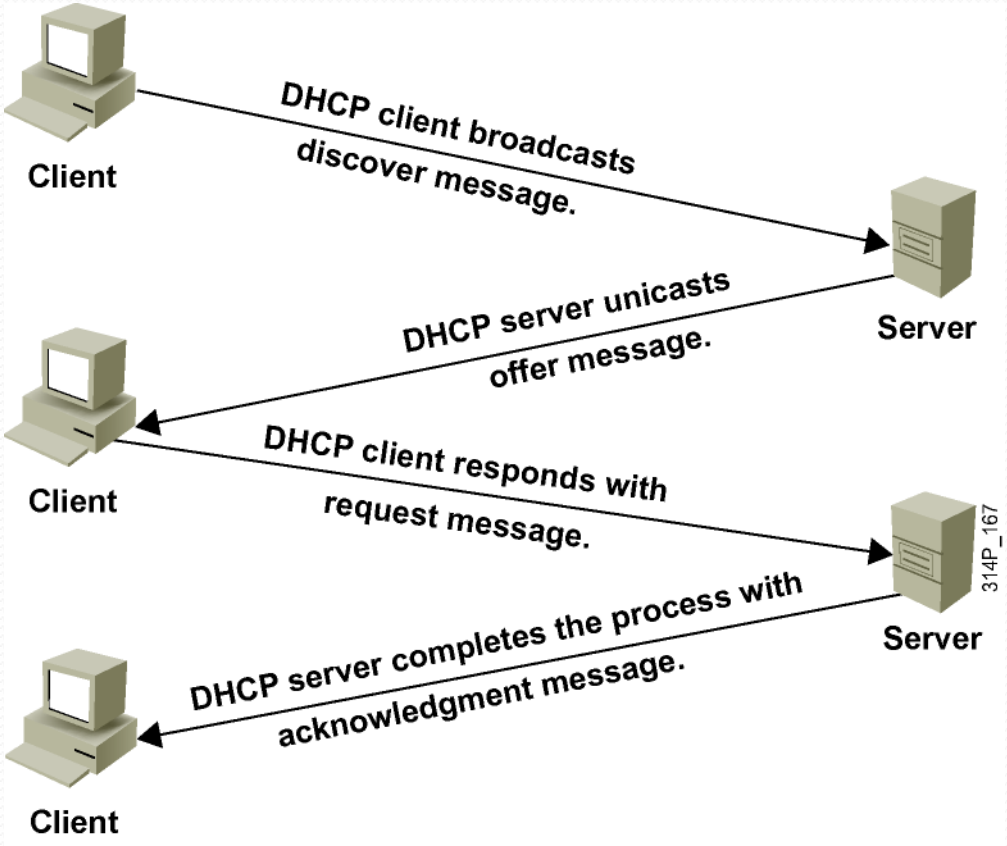

```
R1(config)# aaa new-model
R1(config)#
R1(config)# radius-server host 192.168.1.100
R1(config)# radius-server key RADIUS-Pa55w0rd
R1(config)#
R1(config)# tacacs-server host 192.168.1.101
R1(config)# tacacs-server key TACACS+Pa55w0rd single-connection
R1(config)#
R1(config)# aaa authentication login default group tacacs+ group
radius local-case
R1(config)#
```

DHCP

DHCP in an Enterprise Network



Dynamic Host Configuration Protocol



Configuring a DHCP Server

```
Router(config)#ip dhcp pool [pool name]
```

- Enables a DHCP pool for use by hosts

```
Router(config-dhcp)#import all
```

- Imports DNS and WINS information from IPCP

```
Router(config-dhcp)#network [network address][subnet mask]
```

- Specifies the network and subnet mask of the pool

```
Router(config-dhcp)#default-router [host address]
```

- Specifies the default router for the pool to use

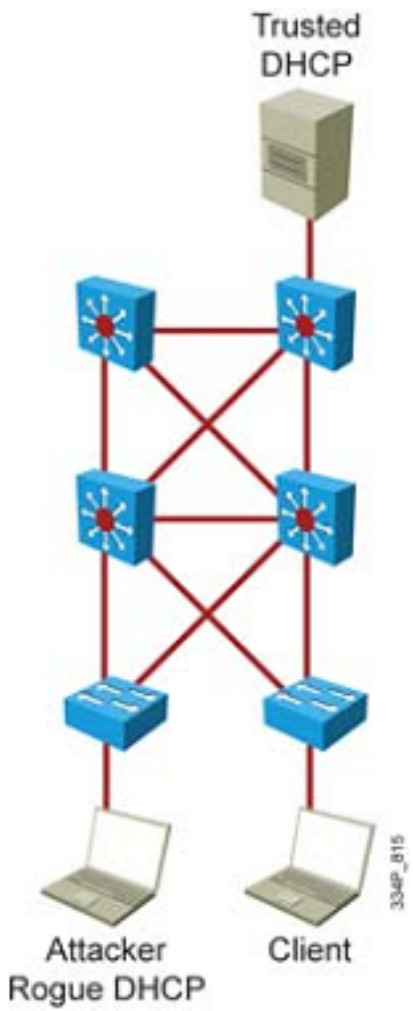
DHCP Server Configuration Example

```
ip dhcp excluded-address 172.16.1.100 172.16.1.103

ip dhcp excluded-address 172.16.2.100 172.16.2.103

ip dhcp pool 0

  network 172.16.0.0/16

  domain-name global.com

  dns-server 172.16.1.102 172.16.2.102

  default-router 172.16.1.100
```

DHCP Spoofing Attacks

DHCP Spoofing Attacks

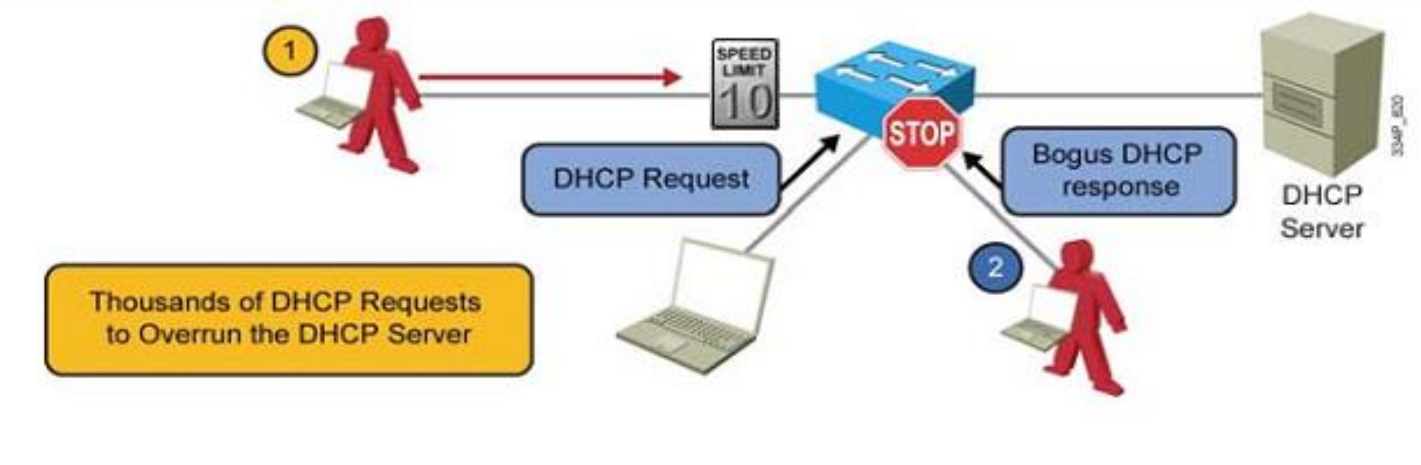
- An attacker activates a DHCP server on the VLAN.
- An attacker replies to a valid client DHCP request.
- An attacker assigns IP configuration information that establishes a rogue device as client default gateway.
- An attacker floods the DHCP server with requests.



DHCP Snooping

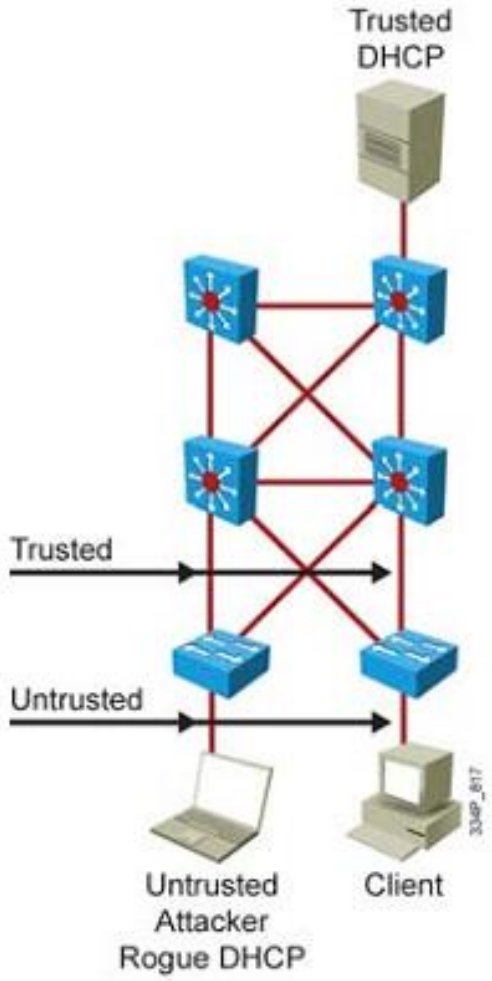
DHCP Snooping Protects Against Rogue and Malicious DHCP Servers

- DHCP requests (discover) and responses (offer) are tracked
- Rate-limiting requests on untrusted interfaces limit DoS attacks on DHCP servers
- Deny responses (offers) on untrusted interfaces to stop malicious or errant DHCP servers.



DHCP Snooping

- DHCP snooping allows the configuration of ports as trusted or untrusted.
- Untrusted ports cannot forward DHCP replies.
- Configure DHCP trust on the uplinks to a DHCP server.
- Do not configure DHCP trust on client ports.



Configuring DHCP Snooping

Configuring DHCP Snooping

- Enable DHCP snooping globally.
- Enable DHCP snooping on selected VLANs.
- Configure trusted interfaces (untrusted is default).
- Configure DHCP rate limit on untrusted interfaces.

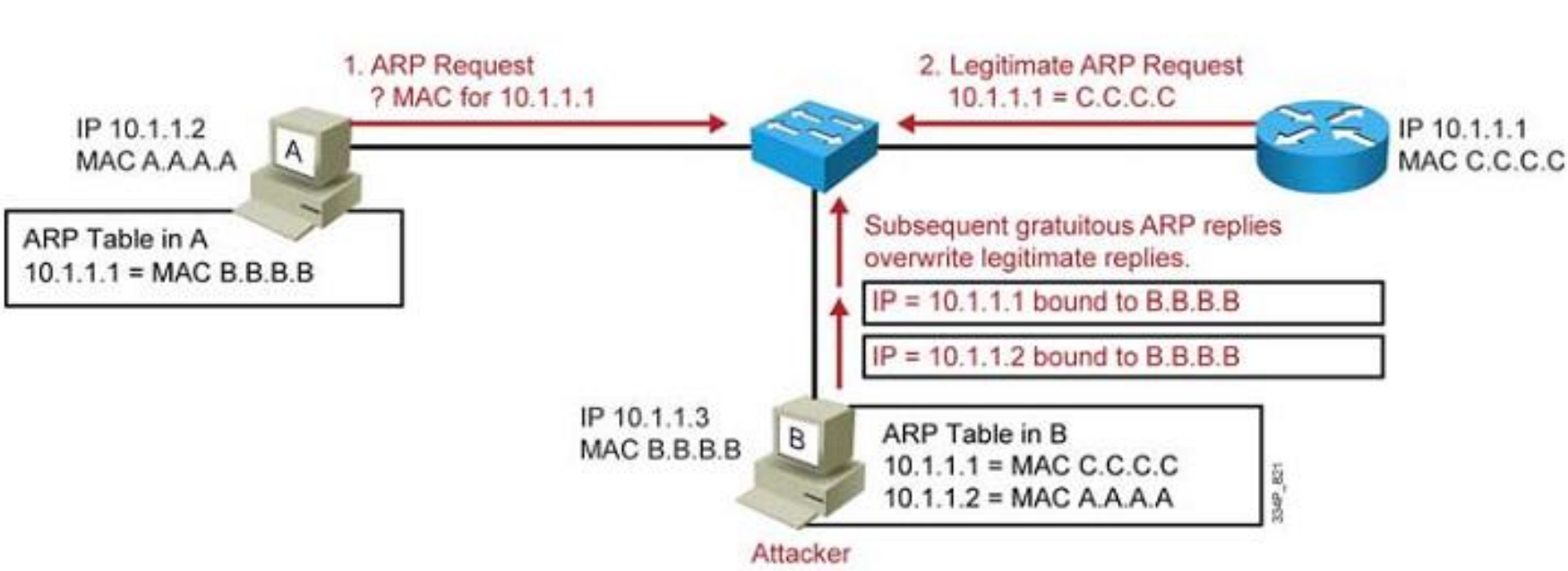
```
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping information option
switch(config)# ip dhcp snooping vlan 10,20
switch(config)# interface fastethernet 0/1
switch(config-if)# description Access Port
switch(config-if)# ip dhcp limit rate 50
switch(config)# interface fastethernet 0/24
switch(config-if)# description Uplink
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10,20
switch(config-if)# ip dhcp snooping trust
```

Verifying DHCP Snooping

```
switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20
DHCP snooping is operational on following VLANs:
10,20
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 001a.e372.ab00 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            no         no              50
FastEthernet0/24           yes        yes             unlimited
```

ARP Poisoning

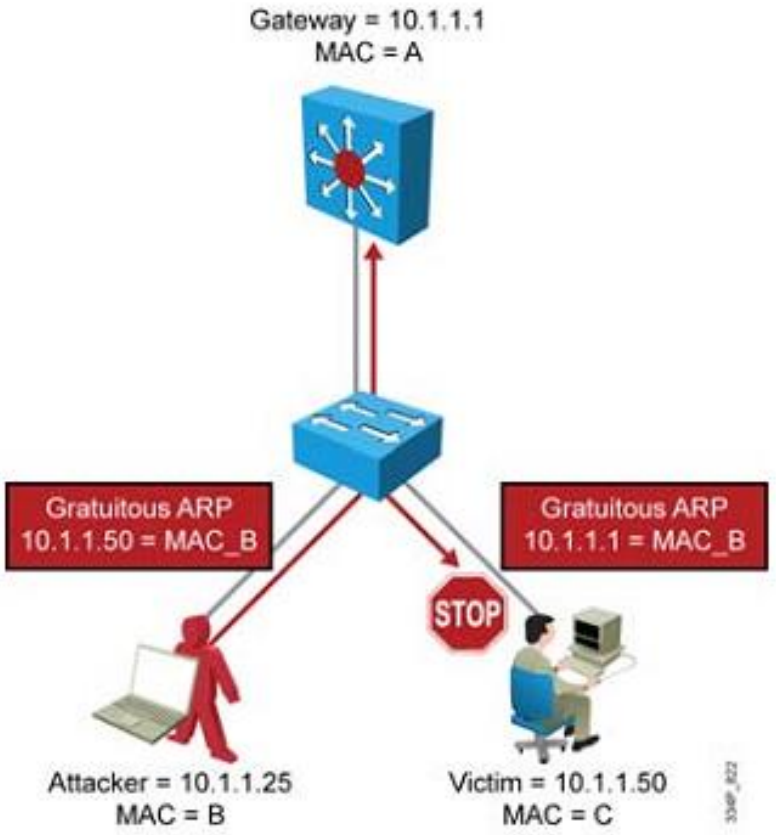
ARP Poisoning



Dynamic ARP Inspection

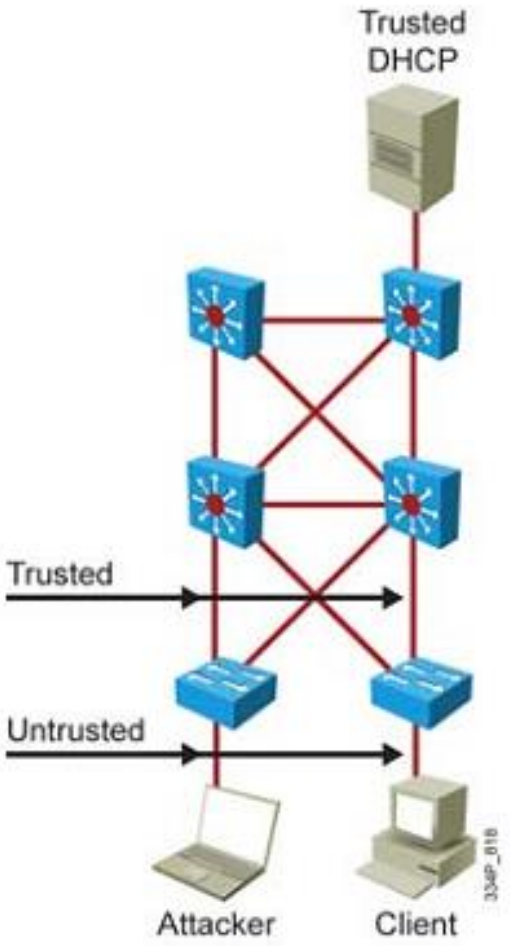
DAI Protection Against ARP Poisoning

- Protects against ARP poisoning (ettercap, dsniff, or arpspoof)
- Uses the DHCP snooping binding table
- Tracks IP-to-MAC bindings from DHCP transactions
- Drops gratuitous ARPs
- Stops ARP poisoning and man-in-the-middle attacks
- Rate-limits ARP requests from client ports; stops port scanning



About DAI

- DAI associates each interface with a trusted state or an untrusted state.
- Trusted interfaces bypass DAI.
- Untrusted interfaces undergo DAI validation.
- DHCP snooping is required to build a table with MAC-to-IP bindings for DAI validation.



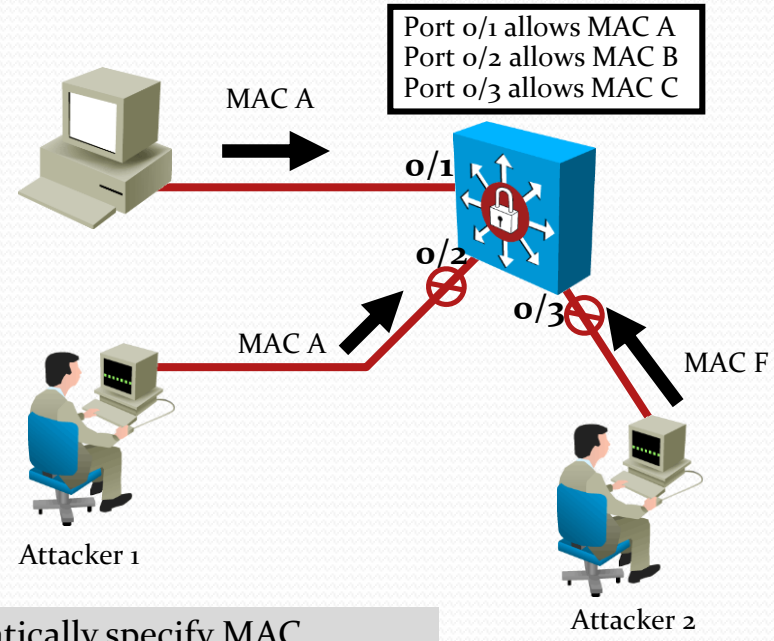
Configuring DAI

- Enable DHCP snooping globally.
- Enable DHCP snooping on selected VLANs.
- Enable ARP inspection on selected VLANs.
- Configure trusted interfaces (untrusted is default).

```
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 10,20
switch(config)# ip arp inspection vlan 10,20
switch(config)# interface fastethernet 0/1
switch(config-if)# ip dhcp limit rate 50
switch(config)# interface fastethernet 0/24
switch(config-if)# description Uplink
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10,20
switch(config-if)# ip dhcp snooping trust
switch(config-if)# ip arp inspection trust
```

Port Security

Port Security Overview



Allows an administrator to statically specify MAC Addresses for a port or to permit the switch to dynamically learn a limited number of MAC addresses

CLI Commands

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

- Sets the interface mode as access

```
Switch(config-if)#
switchport port-security
```

- Enables port security on the interface

```
Switch(config-if)#
switchport port-security maximum value
```

- Sets the maximum number of secure MAC addresses for the interface (optional)

Port Security Violation Configuration

```
Switch(config-if)#
```

```
switchport port-security violation {protect
| restrict | shutdown}
```

- Sets the violation mode (optional)

```
switchport port-security mac-address mac-
address
```

- Enters a static secure MAC address for the interface (optional)

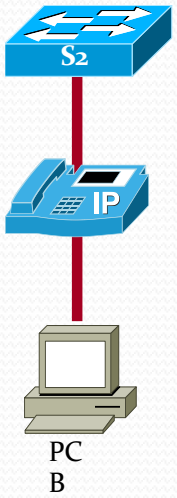
```
switchport port-security mac-address sticky
```

- Enables sticky learning on the interface (optional)

Switchport Port-Security Violation Parameters

Parameter	Description
protect	(Optional) Set the security violation protect mode. When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.
restrict	(Optional) Set the security violation restrict mode. When the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. In this mode, you are notified that a security violation has occurred.
shutdown	(Optional) Set the security violation shutdown mode. In this mode, a port security violation causes the interface to immediately become error-disabled and turns off the port LED. It also sends an SNMP trap, logs a syslog message, and increments the violation counter. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Typical Configuration




```
Switch(config-if)#
```

```
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
switchport port-security aging time 120
```

CLI Commands

```
sw-class# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
             (Count)        (Count)      (Count)
---------------------------------------------------------------------------
  Fa0/12          2             0            0          Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
sw-class# show port-security interface f0/12
Port Security                : Enabled
Port status                  : Secure-down
Violation mode               : Shutdown
Maximum MAC Addresses        : 2
Total MAC Addresses          : 1
Configured MAC Addresses     : 0
Aging time                   : 120 mins
Aging type                   : Absolute
SecureStatic address aging   : Disabled
Security Violation Count     : 0
```

View Secure MAC Addresses

```
sw-class# show port-security address

Secure Mac Address Table
------------------------------------------------------------------------
   --
Vlan    Mac Address       Type                      Ports    Remaining
   Age                                                          (mins)
----    -----------       ----                      -----    -----------
   --
   1    0000.ffff.aaaa    SecureConfigured          Fa0/12         -
------------------------------------------------------------------------
   --
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Wireless LANs

Introducing Wireless LANs

- How do various wireless LAN technologies function, and what wireless standards are in common use?
- What are some of the most important WLAN design considerations?
- What WLAN security risks exist, and how can those risks be mitigated?

WLAN Basic Concepts and Components

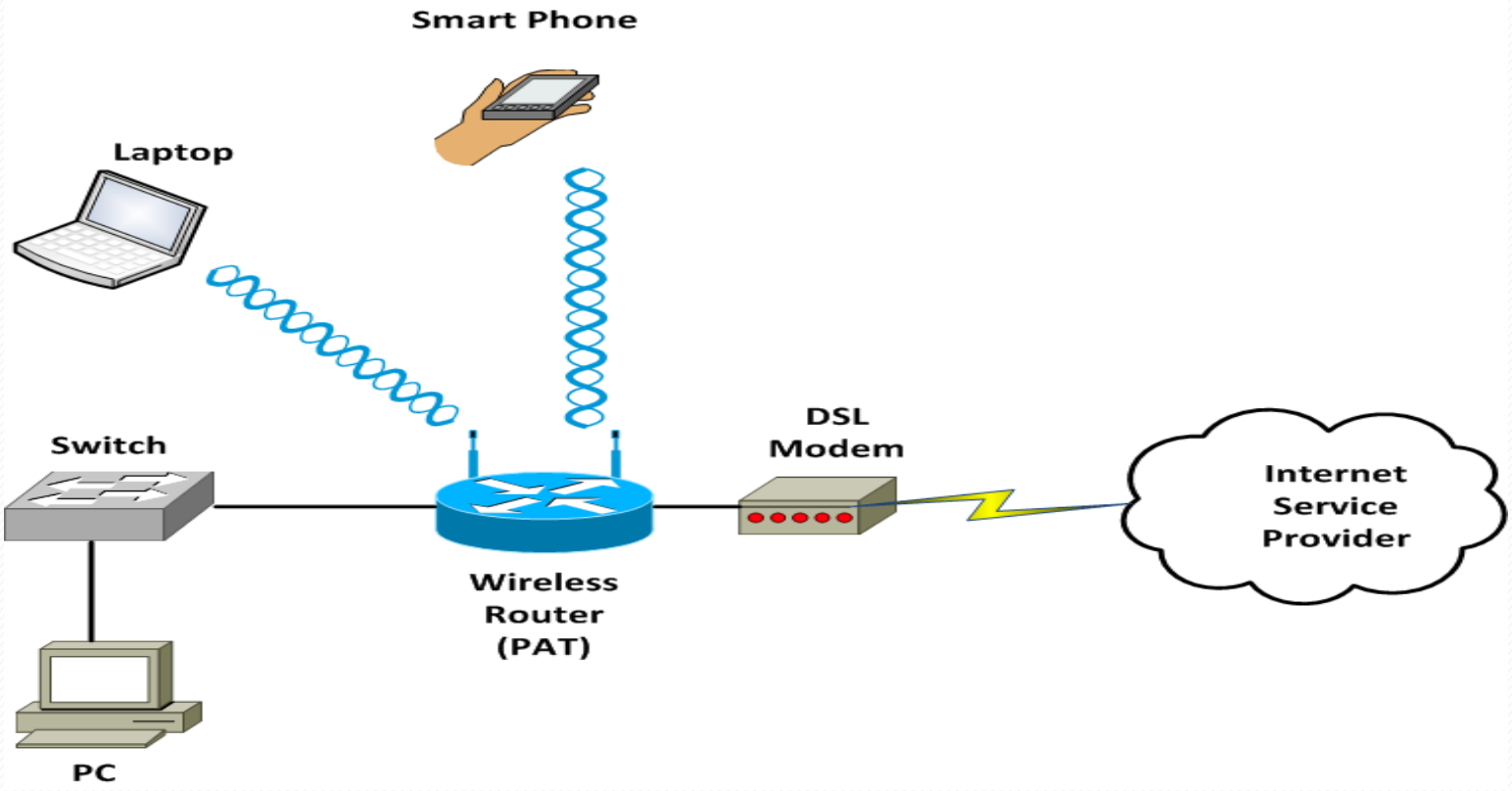
- Two general categories of *wireless LANs* (WLANs):
- Ad hoc WLANs: Wireless devices communicate directly with each other.
- Infrastructure WLANs: Wireless devices communicate with other wireless or wired devices through a wireless router or wireless access point.

Infrastructure: WLAN, Wireless Routers

- Homes and small businesses use a wireless router to provide the following services:
- As a centralized connection station providing
  - Wireless access point (AP) for wireless Ethernet
  - Physical Switch for wired Ethernet
  - A default gateway connection to the Internet for both wired and wireless devices.
  - DHCP Service for automated IP addressing
  - Network Address Translation Service
  - Firewall (usually a basic rule set)
- Cable or DSL modem
  - Providers often provide this device.
  - Sometimes it is an all-in-one appliance

Basic WLAN Topology

The switch, Wireless Router, and the DSL Modem could potentially all run on the same appliance.



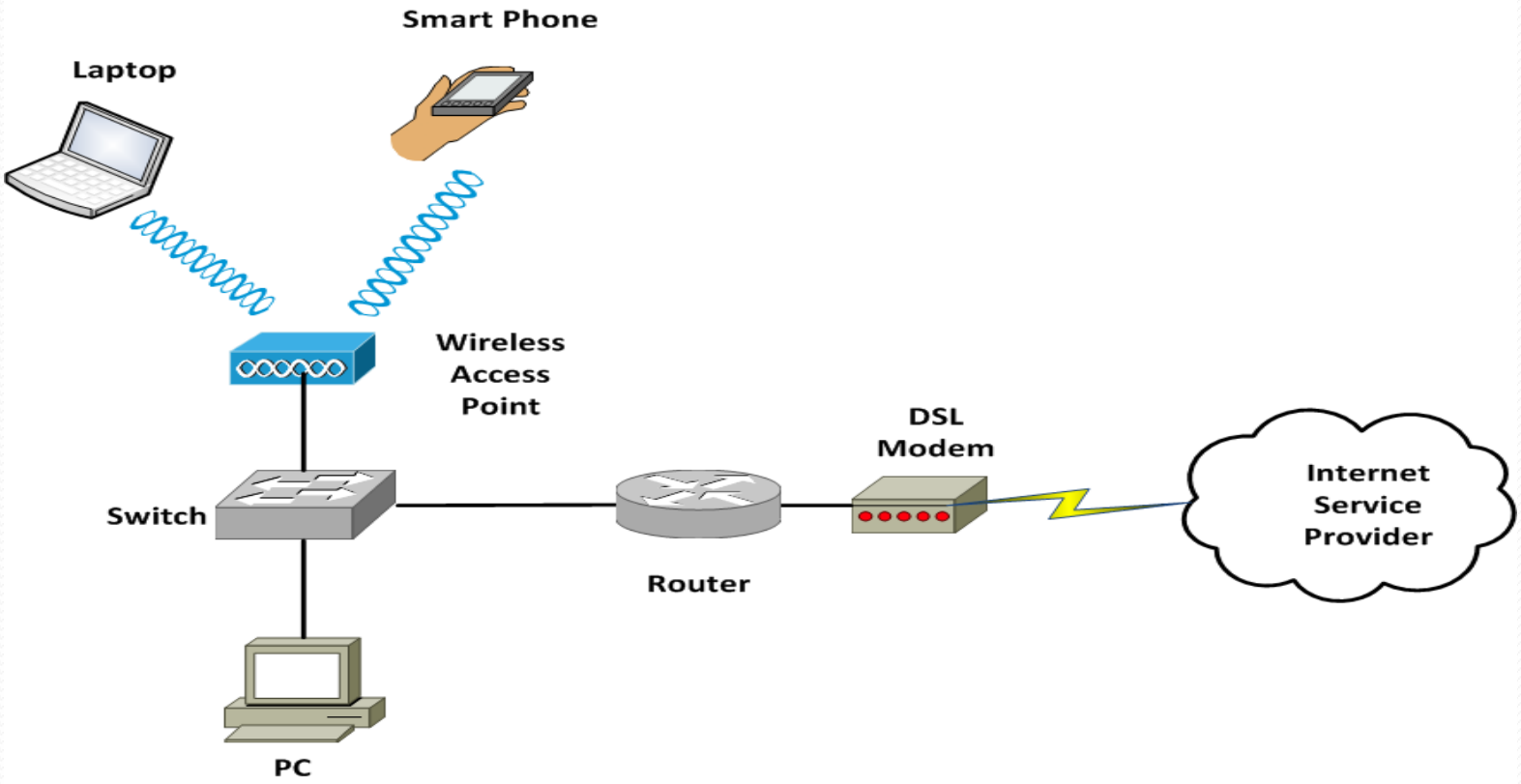
Wireless Access Point

- A wireless *access point* (AP) interconnects a wired LAN with a WLAN. It does not interconnect two different networks. It is a physical bridge between two signal types using the same broadcast domain.

- The wireless AP connects to the wired LAN, and the wireless devices that connect to the wired LAN via the AP are in the same broadcast domain/subnet as the AP.

Wireless Access Point

Note that the Wireless AP is extending the same physical network that the switch is on to be able to receive wireless signals. This makes the Wireless AP act as a wireless bridge.
This would also be known as a mixed media broadcast domain.



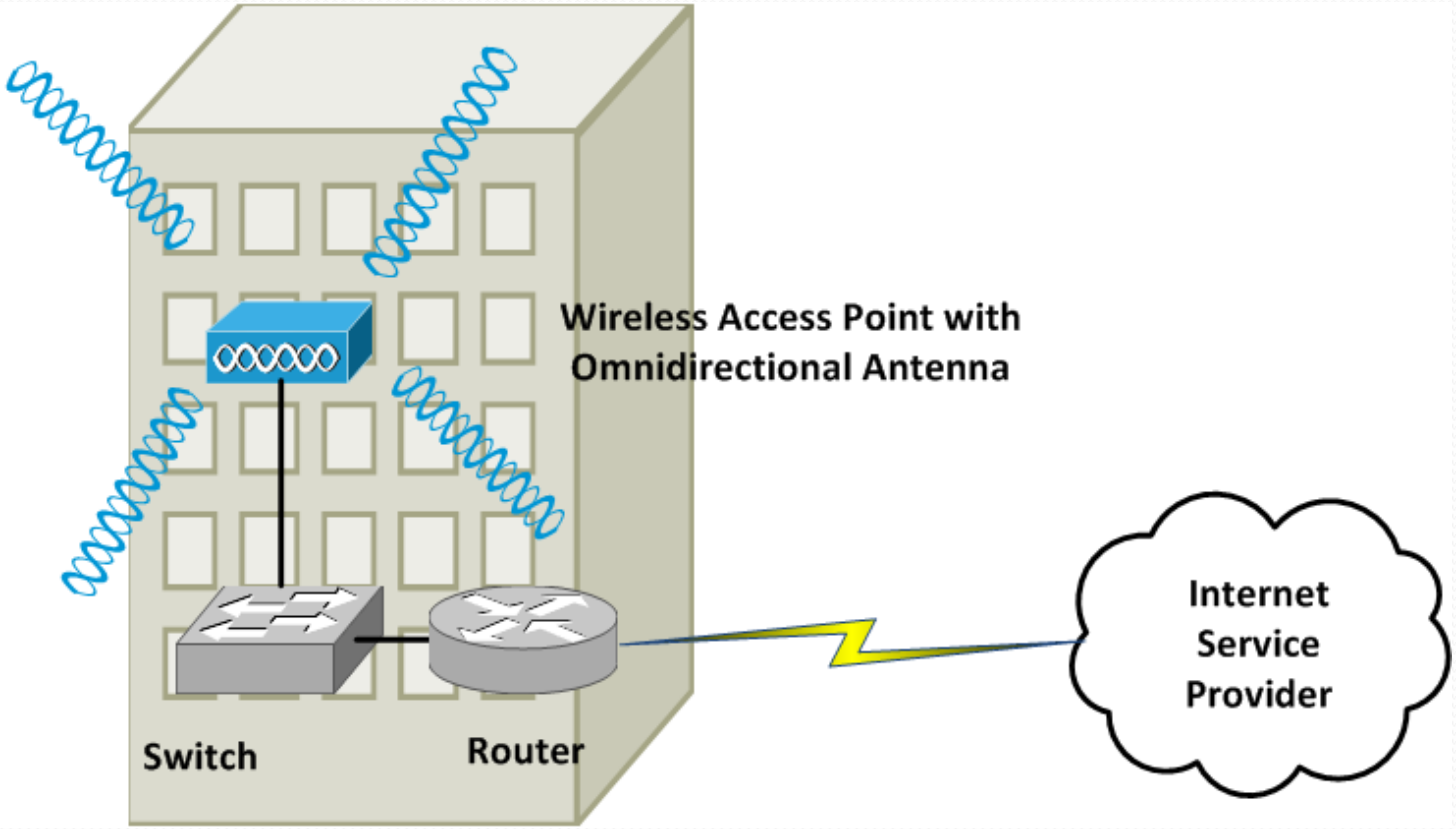
Antennas (signal extenders)

- Antennas extend the coverage area of a wireless AP.
- Coverage varies based on:
  - The transmission power from the source
  - Type of antenna
    - Most home and small business wireless APs have omni-directional antennas
    - Enterprise-class APs support different antenna types.
  - Distance to the target
  - Antenna specific coverage pattern (signal dispersion)
  - Environmental barriers: indoor and outdoor
  - Interference with other AP signals in the same frequency range

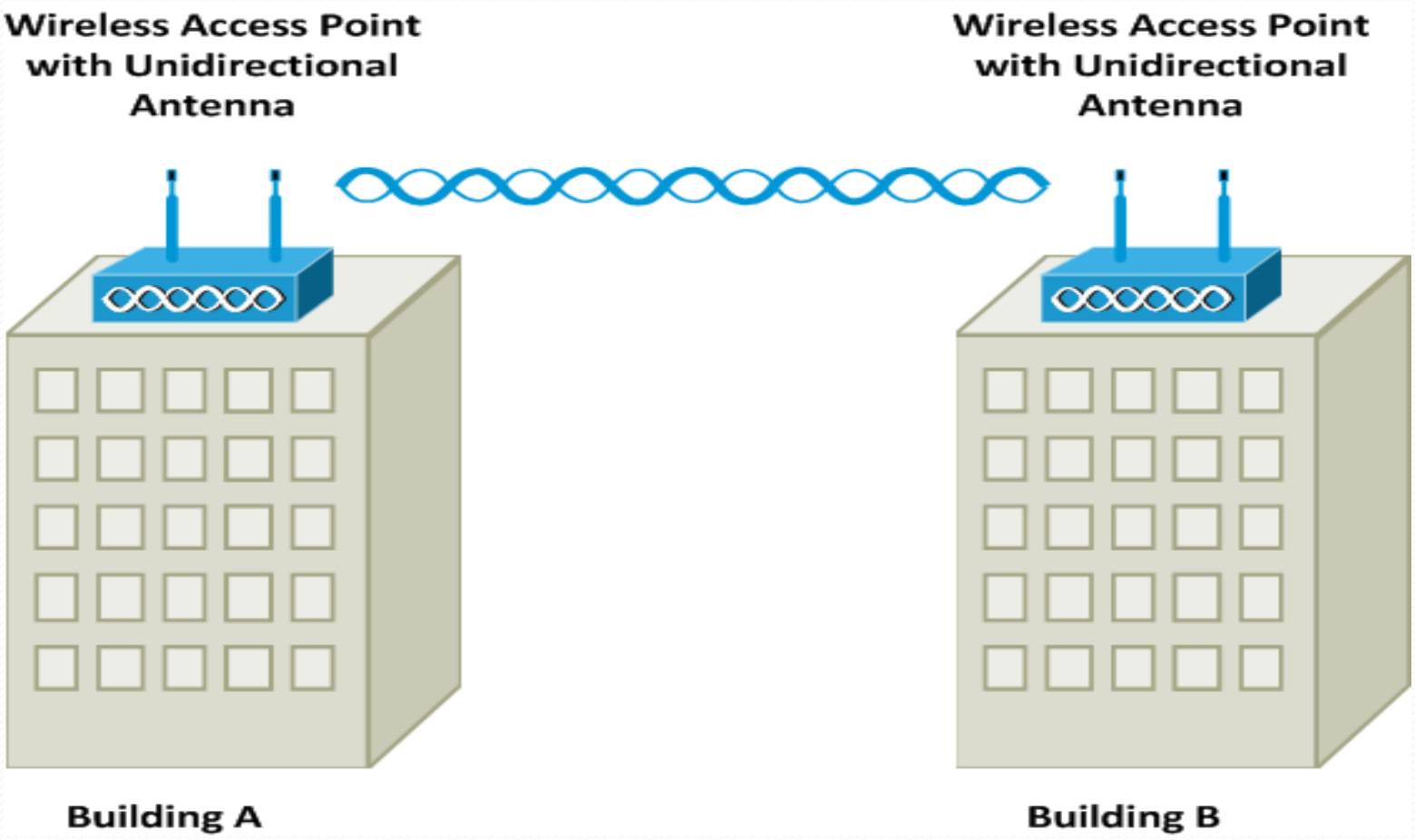
Antennas

- There are two general categories of antenna types:
- Omnidirectional: Omnidirectional antennas radiate power at relatively equal power levels in all directions.
- Unidirectional: Unidirectional antennas focus power.

Omnidirectional Antenna Coverage



Unidirectional Antenna Coverage



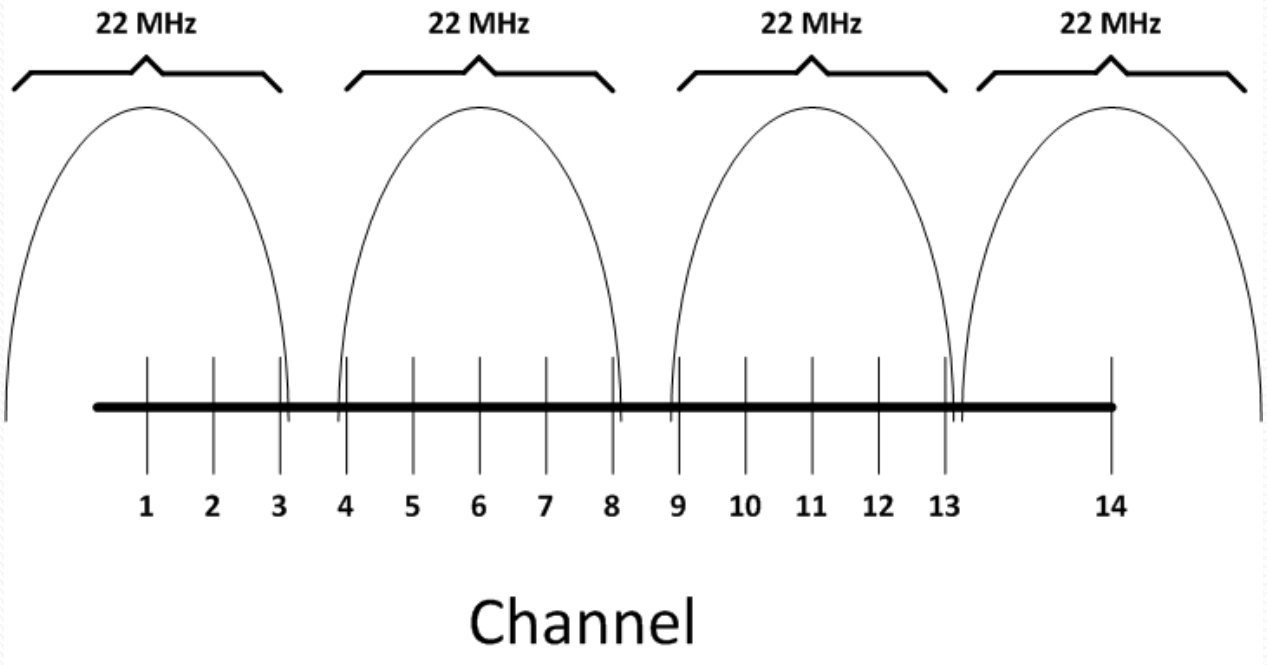
Frequencies and Channels

- *IEEE 802.11* standard defines a large number of wireless standards. One of the characteristics that differentiates the standards is the frequency range (or frequency band).

- Two of these bands are commonly used for WLANs:
  - 2.4-GHz to 2.5-GHz range or *2.4-GHz band*
  - 5.75-GHz to 5.875-GHz range or *5-GHz band*

- Within each band are specific frequencies (or *channels*) at which devices operate.

Frequencies and Channels



The 22 MHz width of the band means that a channel can overlap with another channel if in close proximity. This generates sub-optimal signals.

Channel Frequencies in the 2.4-GHz Band

Channel	Frequency	Nonoverlapping Channel
1	**2.412**	**Yes**
2	2.417	No
3	2.422	No
4	2.427	No
5	2.432	No
6	**2.437**	**Yes**
7	2.442	No
8	2.447	No
9	2.452	No
10	2.457	No
11	**2.462**	**Yes**
12	2.467	No
13	2.472	No
14	2.484	Yes (not supported in the United States)

Notice that channels 1, 6, and 11 are non-overlapping.
You could also use 2, 7, and 12 and achieve the same result.
Minimal channel separation of at least 5 is generally enough.

Channel Frequencies in 5 Ghz Band

- The 5 GHz Wi-Fi band (5150 MHz – 5850 MHz) is divided into four Unlicensed National Information Infrastructure (U-NII) sections, each with different usage rules. Some channels are free for Wi-Fi, while others are shared with radar systems (like weather & military radars).

U-NII Band	Channels	Channel Widths	DFS Required?	Common Usage
U-NII-1	36, 40, 44, 48	20 / 40 / 80 MHz	✗ No	Home & office Wi-Fi, best for stability
U-NII-2A	52, 56, 60, 64	20 / 40 / 80 MHz	✓ Yes	DFS required (shared with radar)
U-NII-2B	100–144	20 / 40 / 80 / 160 MHz	✓ Yes	DFS required (weather & military radar)
U-NII-3	149, 153, 157, 161, 165	20 / 40 / 80 MHz	✗ No	Often used for outdoor Wi-Fi, less crowded

DFS (Dynamic Frequency Selection) channels are shared with radar systems. If radar is detected, your router must automatically switch to another channel, which can cause brief disconnections. These include:
DFS Channels:
52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144

So 5 Ghz gives a total of 25 non overlapping channels

Channel Frequencies in the 6Ghz band

- Wi-Fi 6E and Wi-Fi 7 introduce the 6 GHz band, which provides faster speeds, lower latency, and less interference compared to 2.4 GHz and 5 GHz.
- Covers the 5925 MHz – 7125 MHz frequency range (in most regions).

Channel Width	Number of Non-Overlapping Channels
20 MHz	59 channels (Channels 1–59)
40 MHz	29 channels (Channels 1–59)
80 MHz	14 channels
160 MHz	7 channels
320 MHz (Wi-Fi 7)	3 channels

CSMA/CD *vs* CSMA/CA

- Wired Ethernet uses CSMA/CD to control access to the medium. (Contention based, collisions possible)

- WLANs uses *Carrier Sense Multiple Access/Collision Avoidance* (CSMA/CA).
- The common element is that both rely on client machines to listen for break in the traffic before sending a signal.

- Collision Detection allows the client to determine if the line is clear and when to start transmitting. That is not the case in Collision Avoidance.

CSMA/CA

- The *collision avoidance* (CA) mechanism differs from collision detection by the use of RTS/CTS signals
  - In Wireless CSMA/CA, an AP device listens for a transmission from a client on a wireless channel. The client sends a "Request to Send" (RTS) signal at its earliest opportunity.
  - The AP is monitoring the activity of other devices in the wireless frequency channel.
  - If there is live traffic, it will delay sending a 'Clear to Send' (CTS) signal to the newly requesting client
  - After the AP provides a "Clear to Send" message, the new client can start the transmission of its packets.
  - This signal control method avoids collisions between packets
  - Some Wireless Aps use a 'round robin' method of contacting each device separately to see if they need to use the frequency
  - *Disadvantage: this method can be a limiting factor on the number of wireless devices using the same channel*

WLAN Standards

Wi-Fi Standard	IEEE Name	Max Speed	Frequency Bands	Channel Width	Key Features
Wi-Fi 1	802.11b (1999)	11 Mbps	2.4 GHz	20 MHz	First widely used Wi-Fi standard, very slow by today's standards
Wi-Fi 2	802.11a (1999)	54 Mbps	5 GHz	20 MHz	Faster than 802.11b, but shorter range
Wi-Fi 3	802.11g (2003)	54 Mbps	2.4 GHz	20 MHz	Improved version of 802.11b with backward compatibility
Wi-Fi 4	802.11n (2009)	600 Mbps	2.4 GHz & 5 GHz	20/40 MHz	First Wi-Fi to support MIMO (multiple antennas)
Wi-Fi 5	802.11ac (2013)	6.9 Gbps	5 GHz	20/40/80/160 MHz	Introduced MU-MIMO, Beamforming for better speed
Wi-Fi 6	802.11ax (2019)	9.6 Gbps	2.4 GHz & 5 GHz	20/40/80/160 MHz	OFDMA for better efficiency, lower latency, improved MU-MIMO
Wi-Fi 6E	802.11ax (6 GHz) (2020)	9.6 Gbps	2.4 GHz, 5 GHz, & 6 GHz	20/40/80/160 MHz	Added 6 GHz band for less congestion and faster speeds
Wi-Fi 7	802.11be (2024)	46 Gbps	2.4 GHz, 5 GHz, & 6 GHz	20/40/80/160/320 MHz	320 MHz channels, 4096-QAM, Multi-Link Operation (MLO)

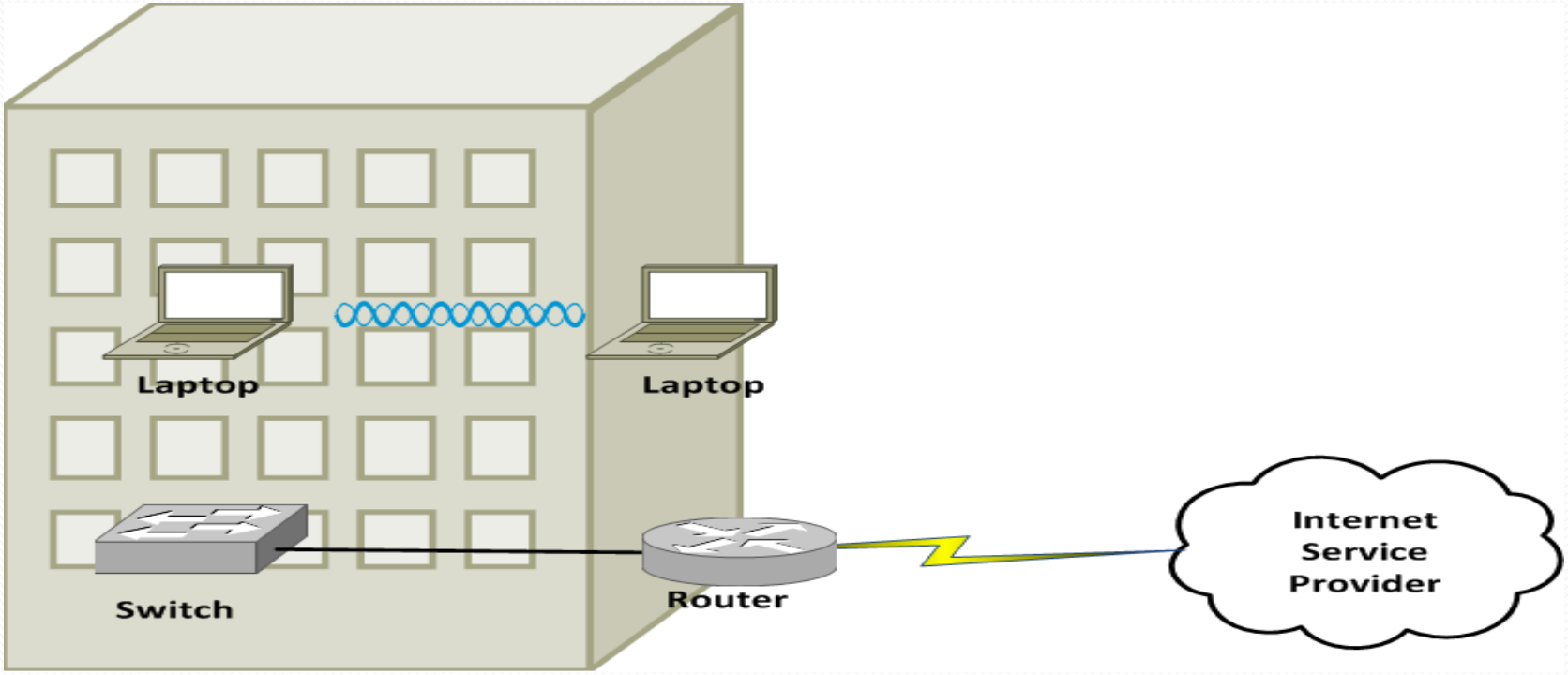
Deploying Wireless LANs

- The three main categories of WLANs are as follows:
- Ad Hoc Mode
- IBSS – Independent Basic Service Set
  - Also known as an ad hoc WLAN. Contains no access points, just wireless devices.
- Infrastructure Mode
- BSS – Basic Service Set
  - Typical WLAN with one AP connected to the network.

- ESS – Extended Service Set
  - Contains more than one AP working together to provide more coverage than a single AP.
  - Extends the range of the broadcast network

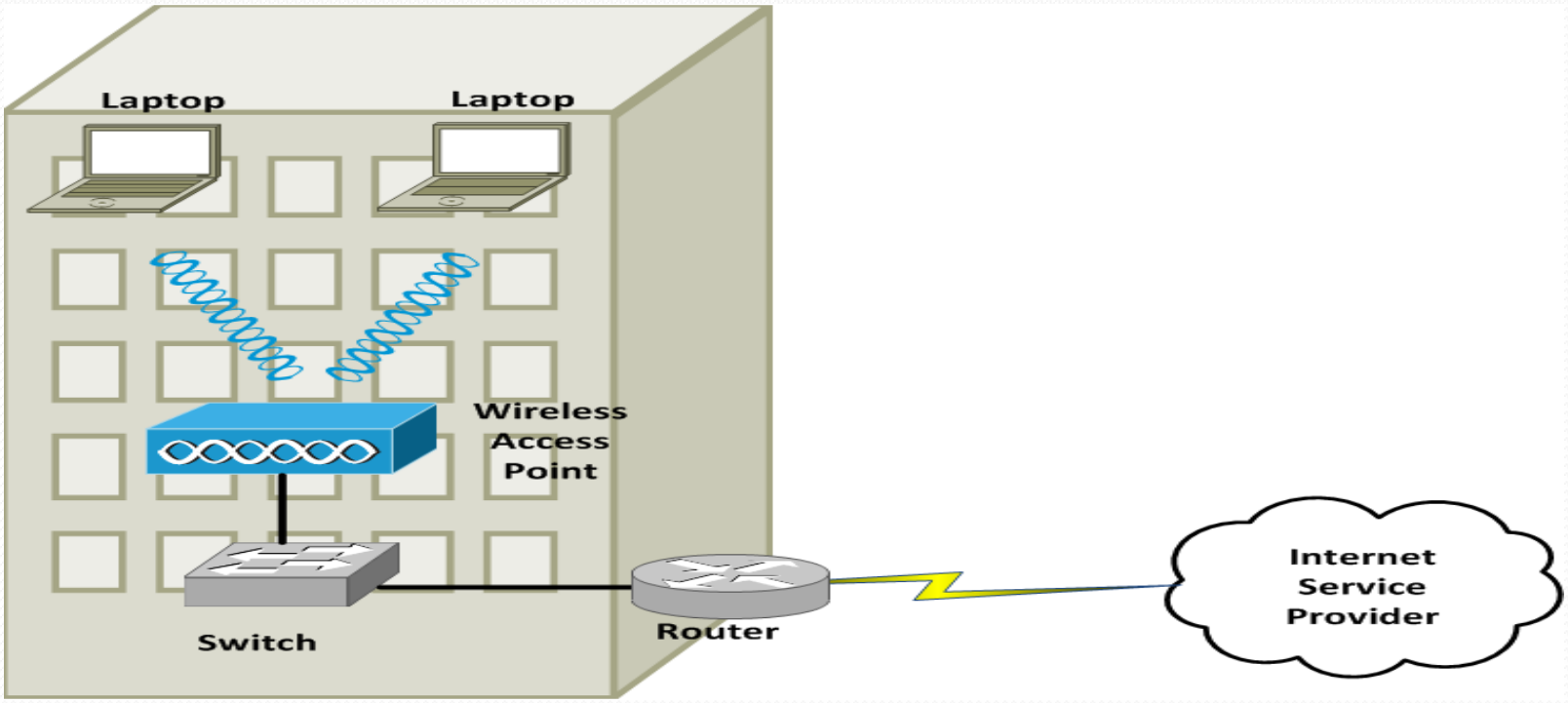
Independent Basic Service Set (IBSS) WLAN

IBSS is not often used for creating wireless networks. However, you might consider what happens when you use your phone to pay for groceries. The "Near Field Communication" that happens between your phone and the cash register is a type of Ad-Hoc technology.

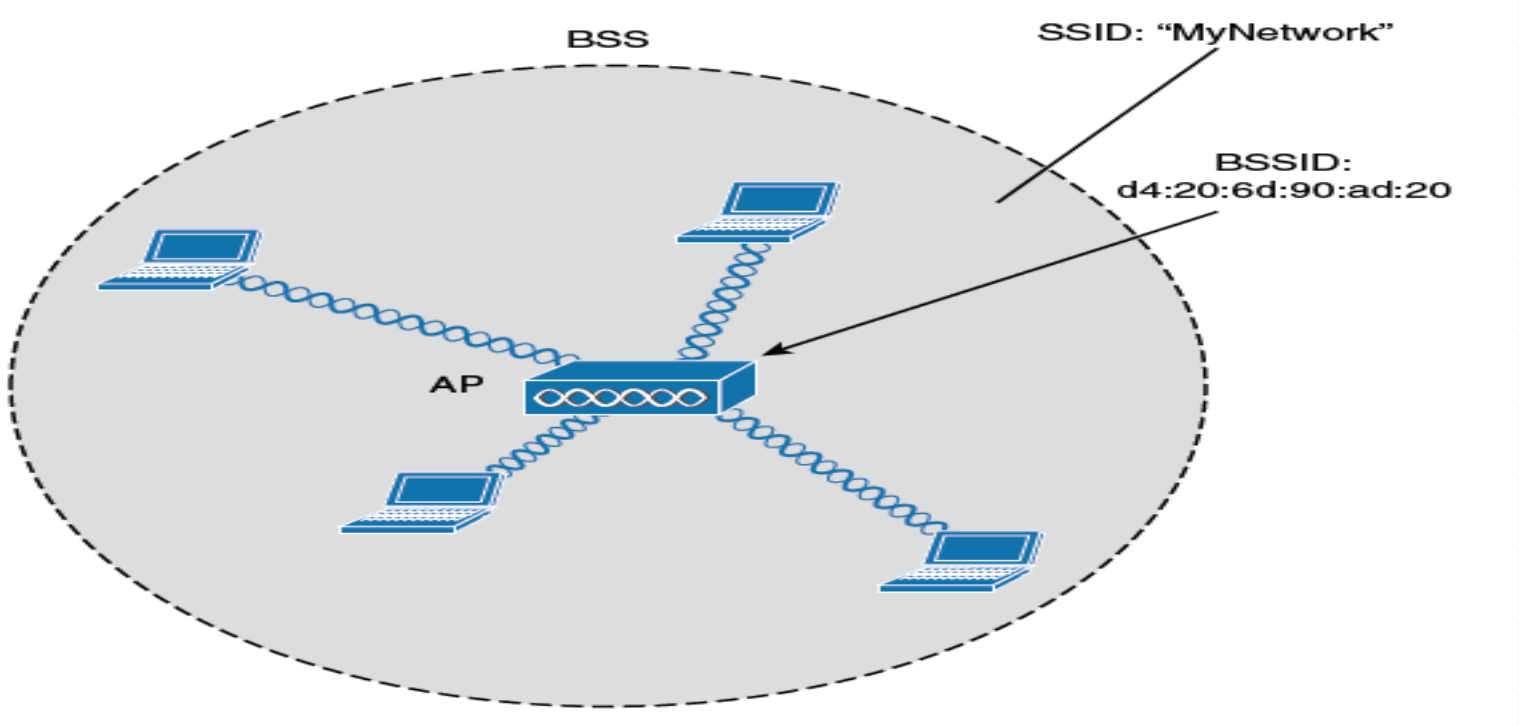


Basic Service Set (BSS) WLAN

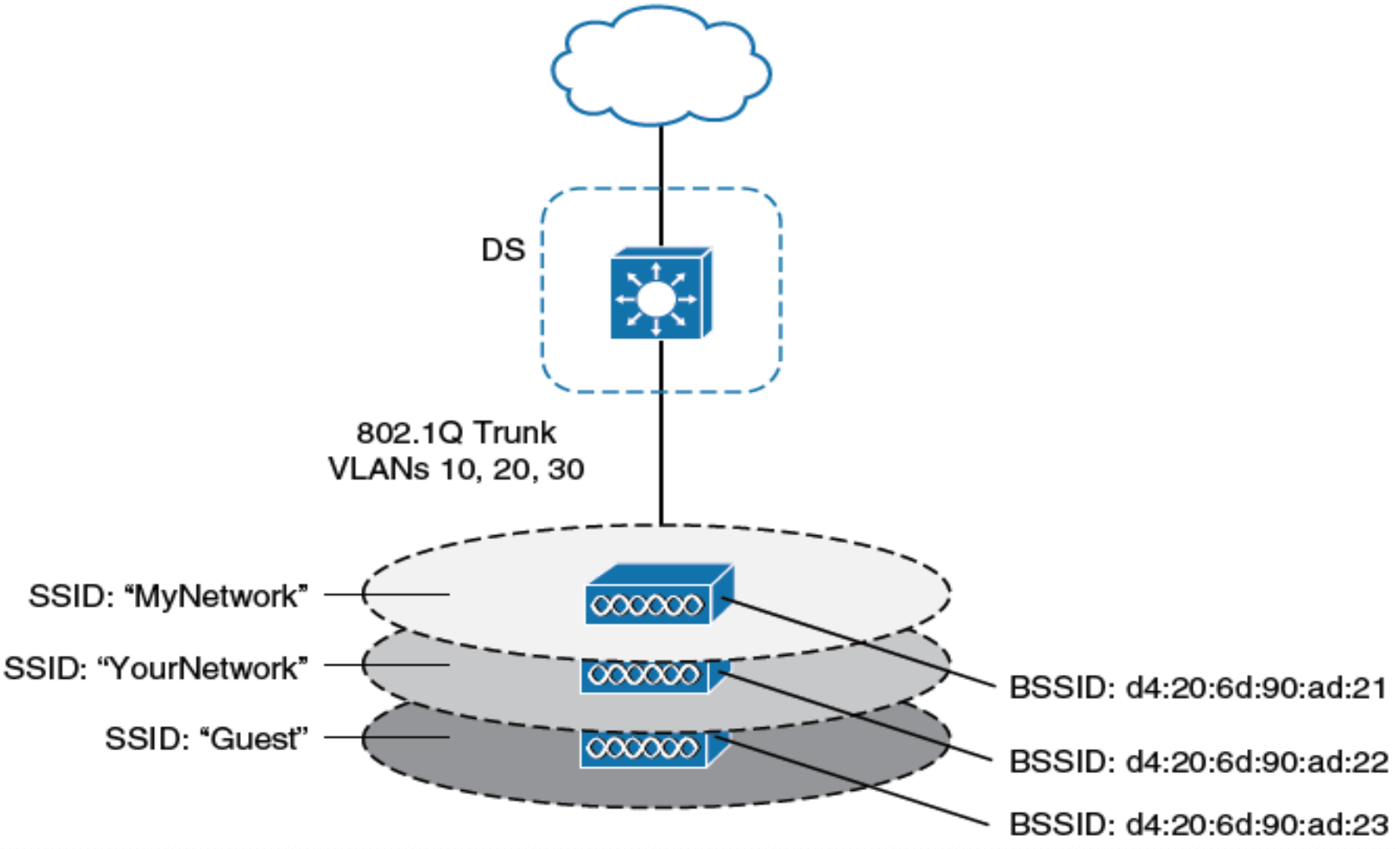
This is more likely to be seen in a residence or apartment that is not more than 80 feet wide or three stories tall.
Bigger than this causes problems with the signals passing through multiple walls.
In such cases, a range extender can maintain the structure of the BSS. It is also possible to change an extra Wireless Router to 'Transparent Bridge' mode to achieve the same effect.



- BSS: Is the set of wireless devices and wireless AP belonging to the same connection
- BSSID (BSS Identifier): Is the Aps radio mac address
- SSID (Service Set Identifier): Is the logical name used by humans to describe the wireless network

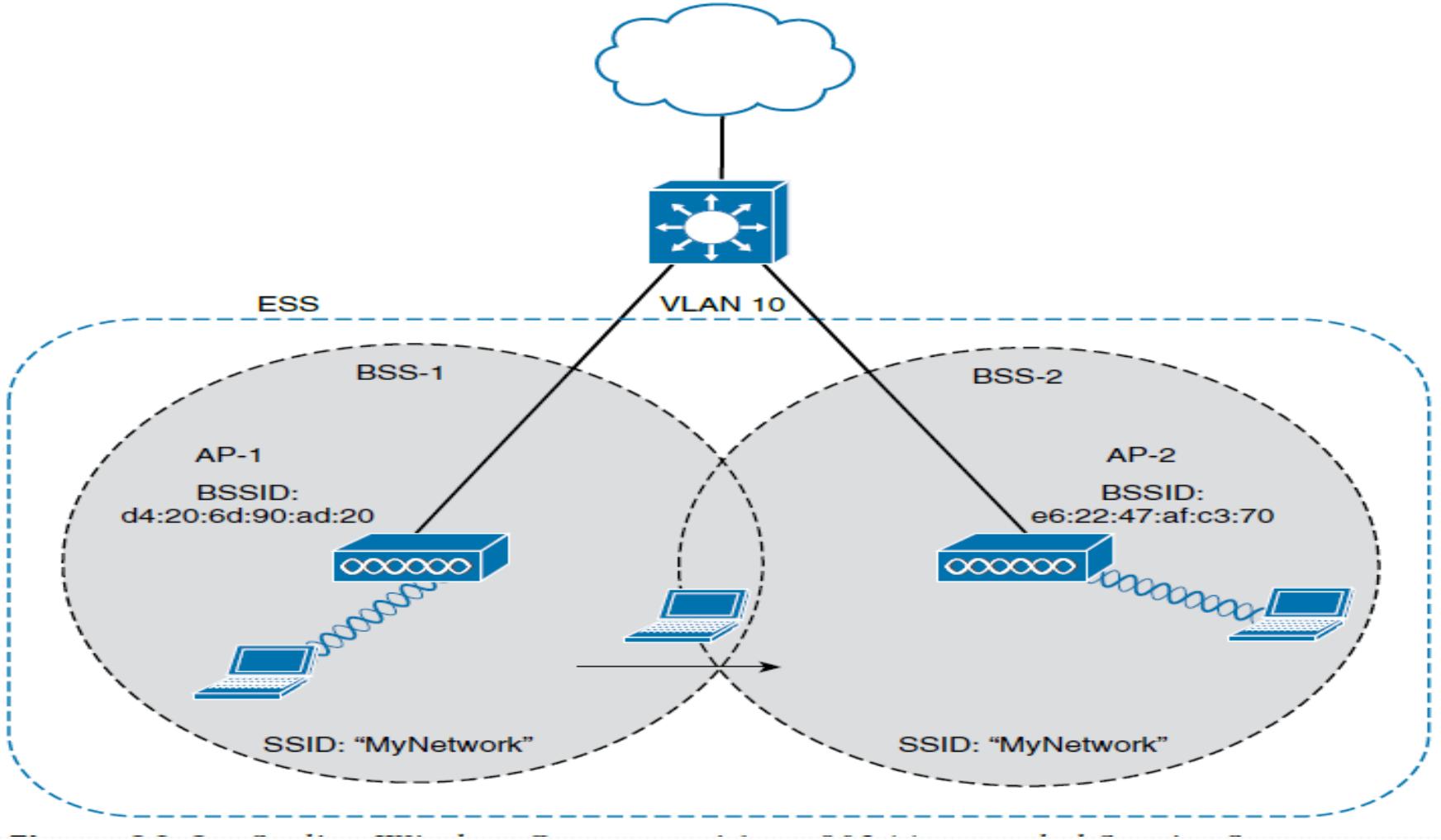


Mapping Multiple SSID to Multiple Vlans



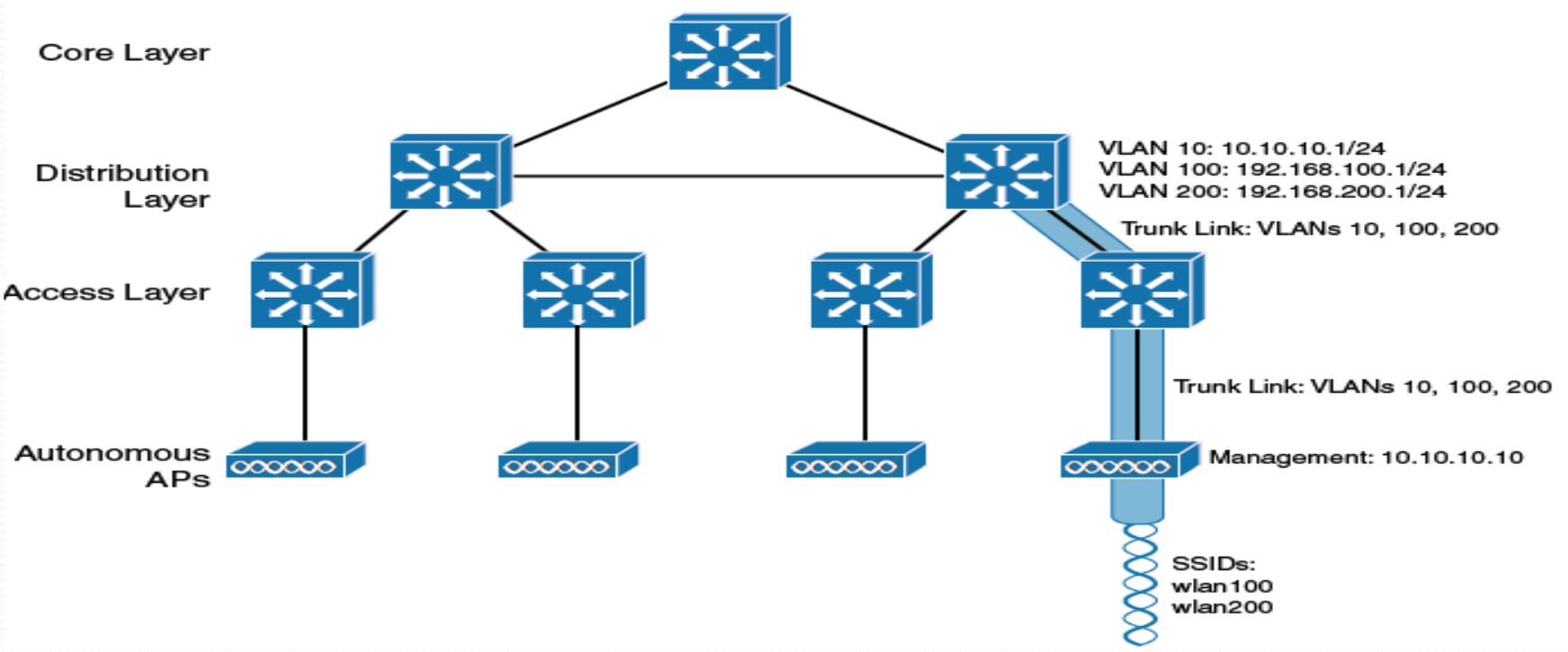
Extended Service Set (ESS) WLAN

Two Access points can use the same SSID, but different BSSID



Autonomous AP

- Autonomous APs offer one or more fully functional, standalone basic service sets (BSSs).
- They are also a natural extension of a switched network, connecting wireless service set identifiers (SSIDs) to wired virtual LANs (VLANs) at the access layer.



On Premises Centeralized Management

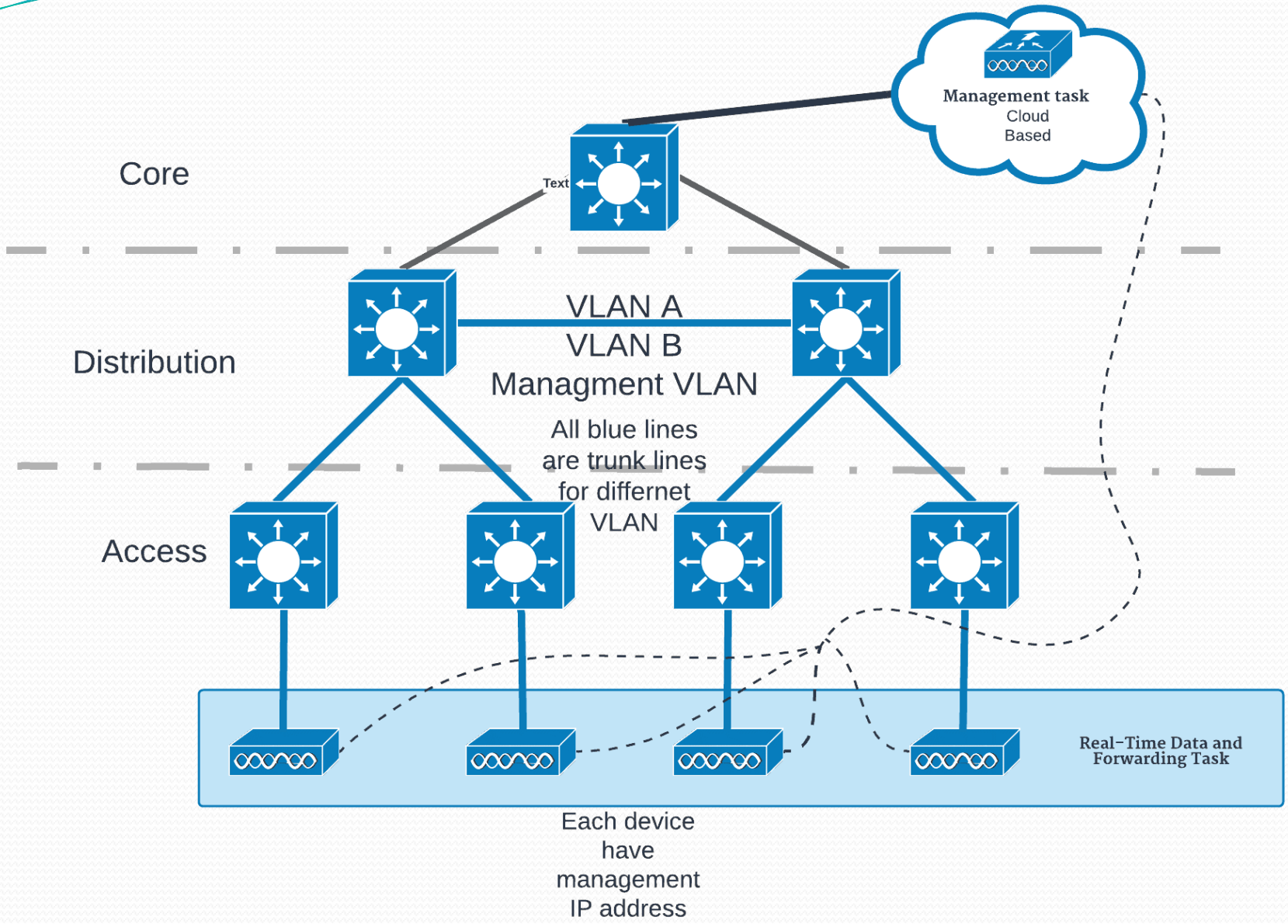
- AP management becomes complex because of the tedious task of logging in individually on every AP. To make it easier, Cisco introduced centralized management software solutions, such as:

- Cisco DNA (Digital Network Architecture) Center
- Cisco Prime Infrastructure

Cloud Based Architecture

- Network scalability is one of the biggest concerns for wireless architecture when a company is growing. As for the Autonomous AP architecture, scaling is possible, although it is more complicated. Cisco saw this issue and now introduced a cloud-based wireless architecture called the Cisco Meraki, a Cisco unified wireless network solution. Here are the key characteristics of a Cloud-based AP architecture:

- The software is not on the premise but in the server farms of the provider
- Management task of the AP is moved to the Cloud
- Only real-time data forwarding tasks are done by the AP

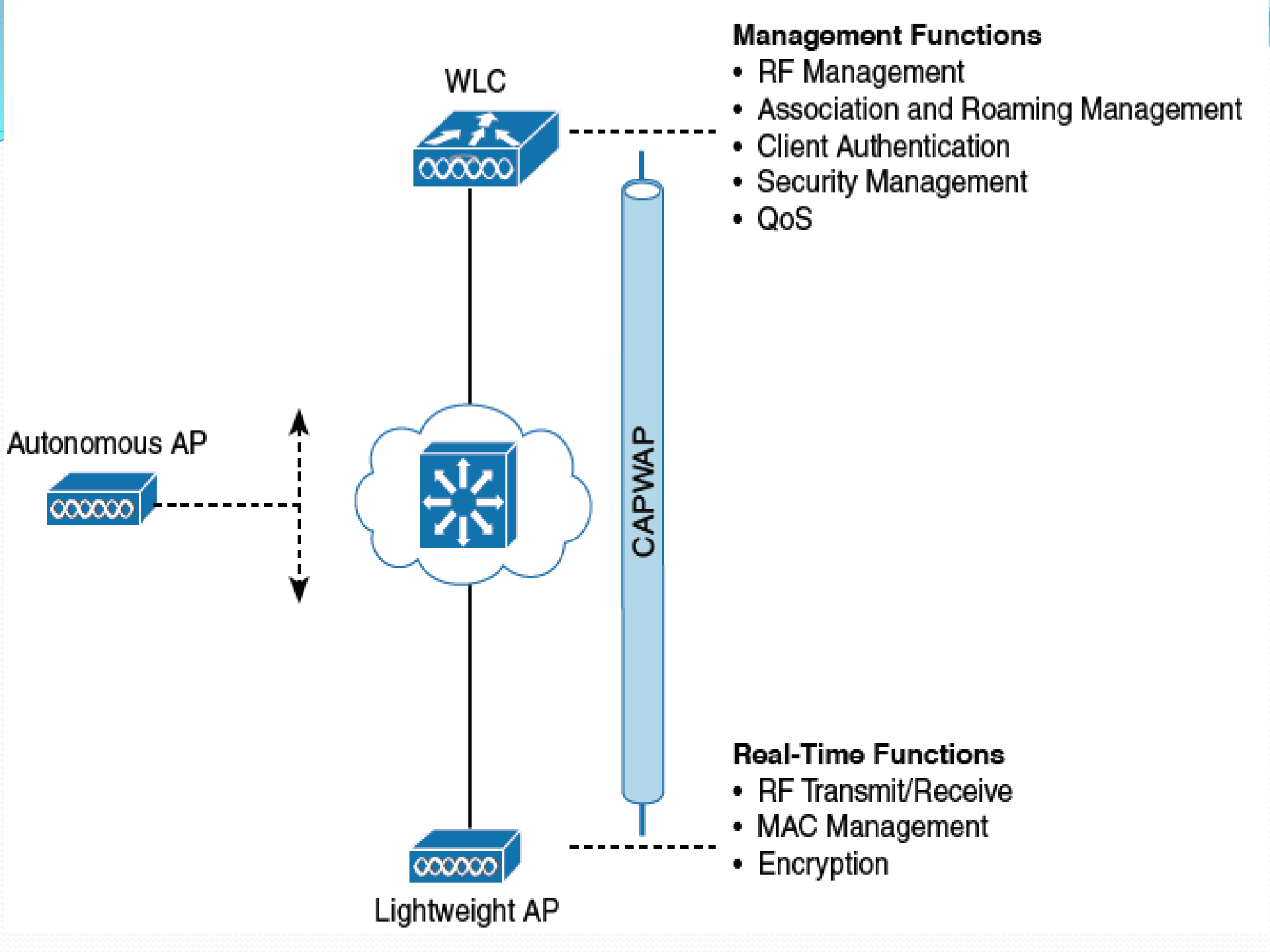

Management task
Cloud
Based
Core
Text
Distribution
VLAN A
VLAN B
Managment VLAN
All blue lines
are trunk lines
for differnet
VLAN
Access
Real-Time Data and
Forwarding Task
Each device
have
management
IP address

Wireless Controller (WLC)

- Because autonomous APs are…well, autonomous, managing their RF operation can be quite difficult.
- As a network administrator, you are in charge of selecting and configuring the channel used by each AP and detecting and dealing with any rogue APs that might be interfering.
- You must also manage things such as the transmit power level to make sure that the wireless coverage is sufficient, it does not overlap too much, and there aren't any coverage holes—even when an AP's radio fails.

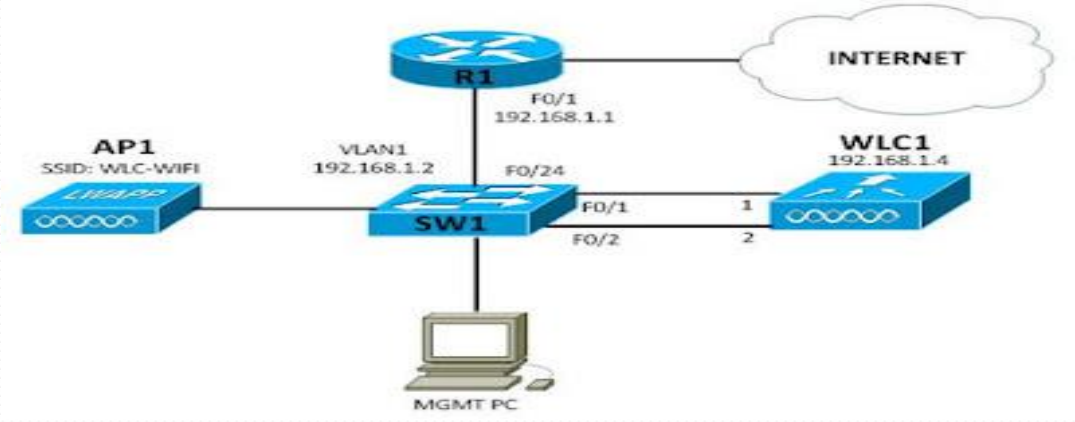
Wireless Controller (WLC)

- Managing wireless network security can also be difficult. Each autonomous AP handles its own security policies, with no central point of entry between the wireless and wired networks.
- That means there is no convenient place to monitor traffic for things such as intrusion detection and prevention, quality of service, bandwidth policing, and so on.
- To overcome the limitations of distributed autonomous APs, many of the functions found within autonomous APs have to be shifted toward some central location which is the WLC


WLC
Management Functions
• RF Management
• Association and Roaming Management
• Client Authentication
• Security Management
• QoS
Autonomous AP
CAPWAP
Real-Time Functions
• RF Transmit/Receive
• MAC Management
• Encryption
Lightweight AP

Cisco LAG in WLC

- Cisco WLAN LAG (Link Aggregation Group) is a networking feature used in Cisco Wireless LAN Controllers (WLCs) to combine multiple physical Ethernet links into a single logical link. This provides increased bandwidth, redundancy, and fault tolerance for the connection between the WLC and the wired network infrastructure.



Cisco WLC Deployments

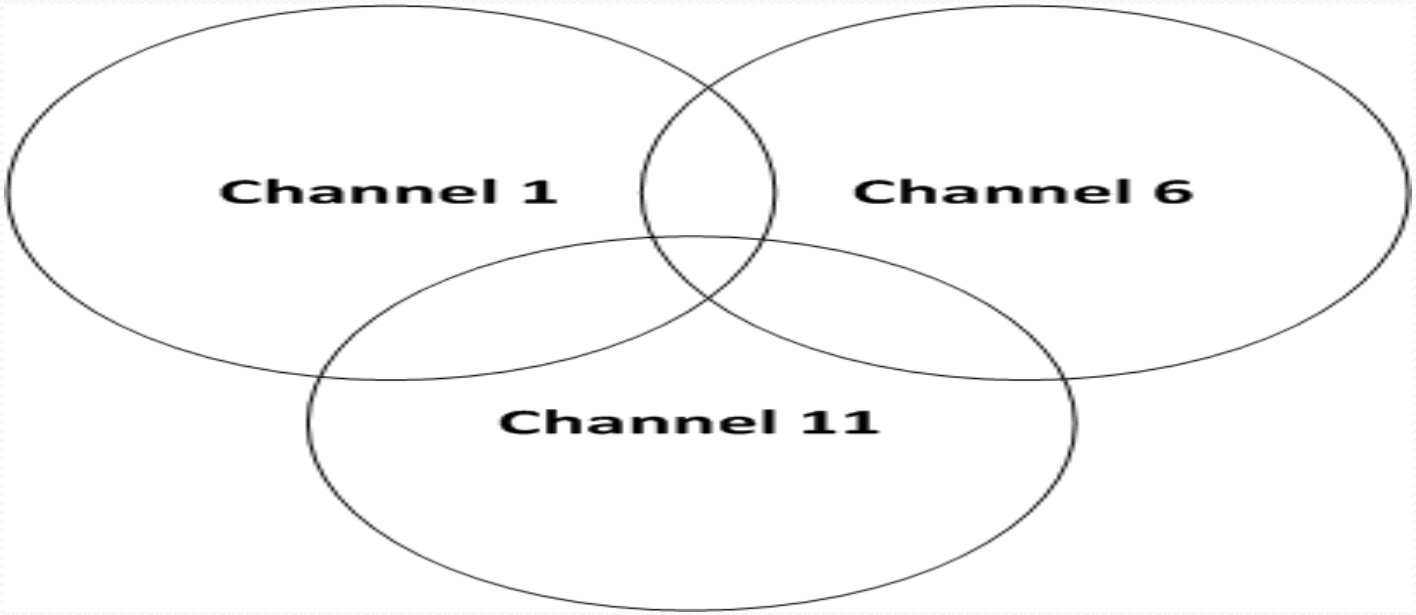
- Cisco WLC can be deployed in different modes:
- Centeralized WLAN Controller
- Cloud Based WLAN Controller
- Embeded WLAN Controller
- Mobility Express WLAN Controller

Sources of Interference

- *Radio frequency interference* (RFI) is caused by other devices using similar frequencies to the WLAN clients or existing AP devices. Common sources of interference include the following:
  - Second or Third wireless AP
  - Cordless phones / baby monitors
  - Microwave ovens
  - Wireless security systems
  - Physical obstacles
  - Signal strength

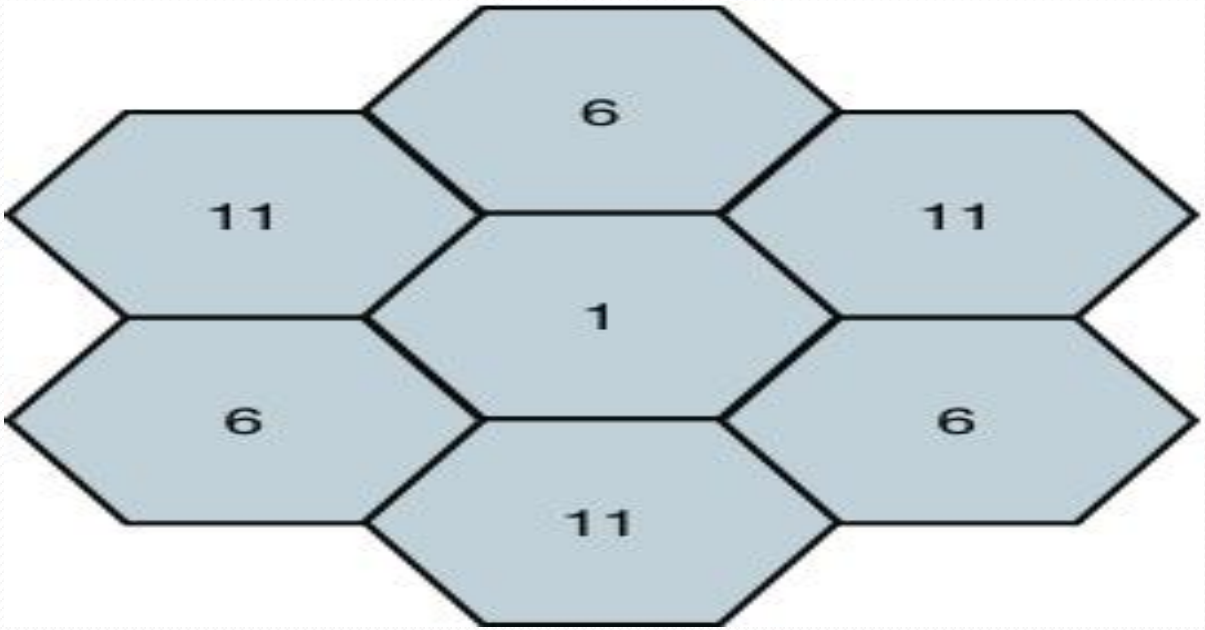
Wireless AP Placement

- Allow 10% to 15 % coverage overlap in coverage area for non-overlapping channels
- This makes it easier for a roaming laptop or smartphone to move from one wireless transmitter to the next one without interruption.



Wireless AP Placement

Nonoverlapping coverage cells for the 2.4-GHz band
The separation of any overlapping channels optimizes the bandwidth distribution by limiting competing frequencies



Cisco Wireless AP Operation Modes

- Many Cisco APs can operate in autonomous or lightweight mode; this depends on the image that you run.
- Local
- Monitor
- FlexConnect
- Sniffer
- Rogue Detector
- Bridge/Mesh
- Flex Plus Bridge
- SE-Connect

Local Mode

- Default mode for CAPWAP-based APs.
- The AP establishes a tunnel to the Wireless LAN Controller (WLC) for centralized management.
- Provides client connectivity and periodically scans other channels for interference, rogue devices, and RF optimization.
- If the WLC becomes unavailable, the AP stops functioning

Monitor Mode

- Used exclusively for monitoring the wireless environment.
- Does not serve clients; instead, it continuously scans all channels for:
- Rogue APs
- RF interference
- IDS/IPS security threats
- Ideal for wireless security and performance monitoring.

FlexConnect

- Designed for remote branch offices with limited connectivity to a central WLC.
- Can operate in:
- Connected mode (when WLC is reachable) – Functions like Local mode.
- Standalone mode (when WLC is unreachable) – Switches traffic locally without needing the WLC.
- Useful for reducing WAN traffic and ensuring continued operations during WLC failure.

Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

Sniffer

- Converts the AP into a wireless packet sniffer.
- Captures all wireless traffic on a specified channel and forwards it to a network analyzer (e.g., Wireshark).
- Ideal for troubleshooting and network analysis.

Rogue Detector

- Dedicated to detecting rogue access points by monitoring wired and wireless traffic.
- Does not serve clients or perform RF scanning.
- Gathers MAC addresses from both wired and wireless networks to identify potential unauthorized devices.

Bridge/Mesh

- Enables APs to function as wireless bridges.
- Commonly used for point-to-point (PtP) or point-to-multipoint (PtMP) links.
- Can form mesh networks where APs communicate wirelessly with each other and a root AP connected to a wired network.
- Used in outdoor deployments, campus environments, or locations where wired connections are impractical.

Prepared By:Waleed Adlan-CCIE41999 - waleed_hashim@hotmail.com

Flex Plus Bridge

- An enhanced version of FlexConnect mode that supports wireless bridging.
- Allows an AP to act as both:
- A FlexConnect AP serving clients locally.
- A wireless bridge connecting remote wired devices.
- Useful for extending wired networks over wireless links in branch offices

Prepared By:Waleed Adlan-CCIE41999 - waleed_hashim@hotmail.com

SE-Connect

- Turns the AP into a dedicated spectrum analyzer.
- Provides deep RF analysis to detect:
- Interference sources (microwaves, Bluetooth, non-Wi-Fi devices).
- Channel utilization issues.
- Works with Cisco Spectrum Expert software for troubleshooting.

Securing Wireless LANs

- Improperly installed wireless APs and routers are roughly equivalent to putting an Ethernet port in a building's parking lot, where anyone can drive up and have access to the network.

- Users who want to use free Internet access perform reconnaissance, known as *war driving*, looking for unsecured WLANs.

Security Issues

- Warchalking
  - Once an open WLAN is found in a public place, a user writes a symbol on a wall to notify others.
  - This is not commonly seen since Wireless hotspots are pretty much everywhere
- WEP and WPA Security code cracking
  - Utilities can capture wireless packets and run mathematical algorithms to determine the pre-shared key. WEP is no longer considered secure.
- Rogue Access Point
  - A malicious user sets up his own Wireless AP to which legitimate users would attempt to authenticate and uses it to collect passwords

Approaches to WLAN Security

- MAC Address Filtering
  - Configures an AP with a listing of permitted MAC addresses
    - Problem: Knowledgeable users can intercept signals, decode and falsify their MAC to match an allowed MAC.
- Disabling SSID Broadcast
  - Configures the AP to not broadcast the name of the wireless LAN
    - Problem: Knowledgeable users can still find the SSID because when a new user authenticates, it must transmit the SSID in order to connect.

Approaches to WLAN Security

- Preshared Key

❑ Both the AP and wireless client need the same key.

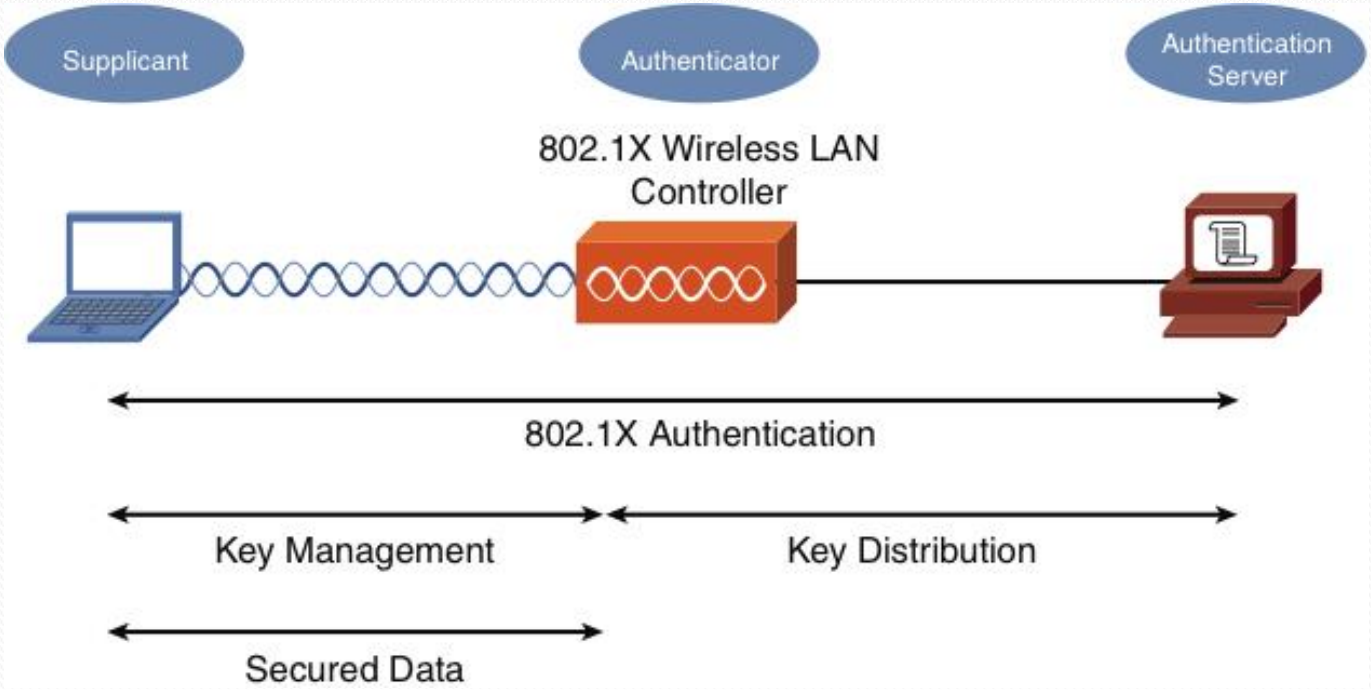
  - Problem: Scalability problems in large networks if the key is compromised.

- IEEE 802.1X

❑ Each wireless user authenticates with their own credentials.

  - Not exclusively used for wireless networks. This authentication method is used for wired networks as well.

IEEE 802.1X Security for a WLAN



Security Standards

- The most common wireless security standards are as follows:
- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access Version 2 (WPA2)
- Wi-Fi Protected Access Version 3 (WPA3)

WEP

- The original 802.11 wireless security standard.

- WEP uses RC4 (Rivest Cipher 4) for Authentication and Encryption
  - Sent in clear text

- Can Be compromised with a Brute-Force Attack
  - Multiple utilities available to crack WEP.

WPA

- Developed to address issues with WEP.

- Uses Temporal Key Integrity Protocol (TKIP)
  - Uses a 48-bit IV instead of a 24-bit IV

- Uses Message Integrity Check (MIC)
  - Confirms data was not modified in transit

- Enterprise Mode WPA
  - Users can be required to authenticate before exchanging keys.
  - Keys between client and AP are temporary.

WPA2

- WPA Version 2 implemented the requirements of the IEEE 802.11i standard.
- Uses *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* (CCMP) for integrity checking
- Uses *Advanced Encryption Standard* (AES) for encryption

WPA3

- WPA Version 2 implemented using AES protocols and GCMP Galois/Counter Mode Protocol
- GCMP is a robust authenticated encryption suite that is more secure and more efficient than CCMP.

Authentication and Encryption Feature Support	WPA	WPA2	WPA3*
Authentication with Pre-Shared Keys?	Yes	Yes	Yes
Authentication with 802.1x?	Yes	Yes	Yes
Encryption and MIC with TKIP?	Yes	No	No
Encryption and MIC with AES and CCMP?	Yes	Yes	No
Encryption and MIC with AES and GCMP?	No	No	Yes

Cloud

- Cisco has defined cloud as follows: IT resources and services that are abstracted from the underlying infrastructure and provided “on-demand” and “at scale” in a multitenant environment.

- a. “**On-demand**” means that resources can be provisioned immediately when needed, released when no longer required, and billed only when used.
- b. “**At-scale**” means the service provides the illusion of infinite resource availability in order to meet whatever demands are made of it.
- c. “**Multitenant environment**” means that the resources are provided to many consumers from a single implementation, saving the provider significant costs.

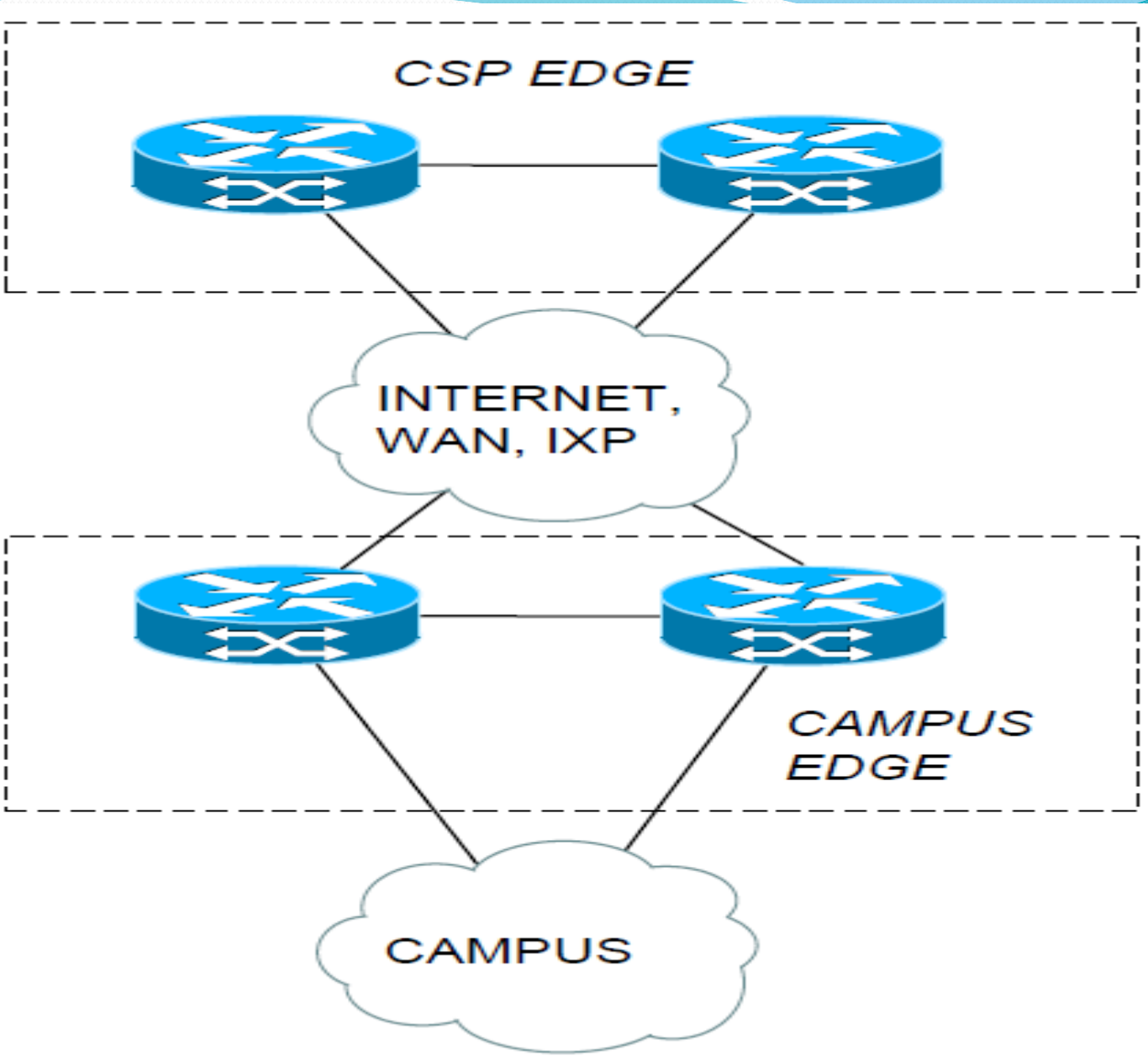
Cloud Deployment Models

- Cloud can be deployed in one of three models:
- Public
- Private
- Virtual Private or Hybrid

Public Cloud

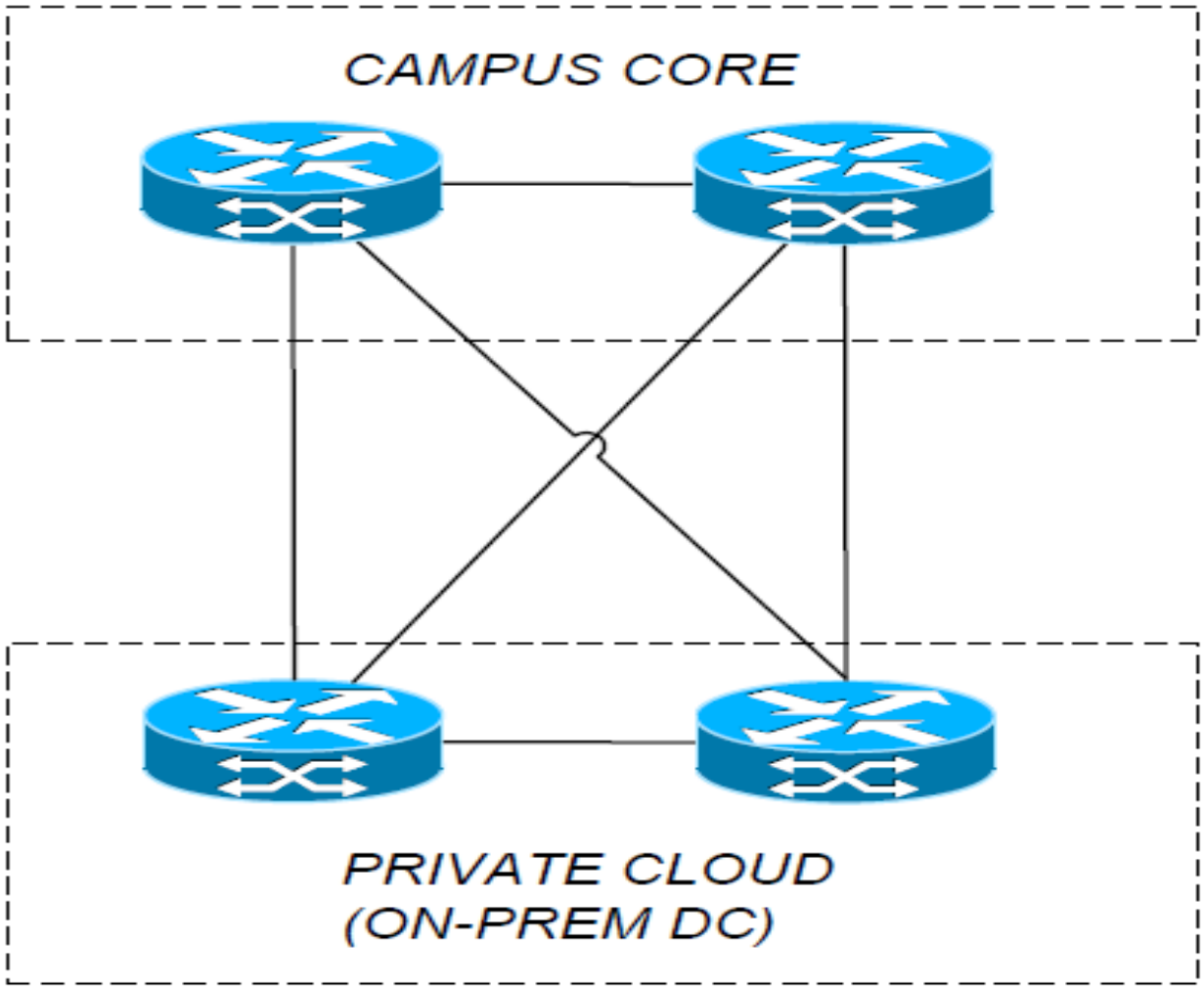
- They rely on a third party organization (off-premise) to provide infrastructure where a customer pays a subscription fee for a given amount of compute/storage, time, data transferred, or any other metric that meaningfully represents the customer's "use" of the cloud provider's shared infrastructure.

- This is viewed by many businesses as a way to reduce capital expenses (CAPEX) since purchasing new DC equipment is unnecessary. It can also reduce operating expenses (OPEX) since the cost of maintaining an on-premise DC


CSP EDGE
INTERNET,
WAN, IXP
CAMPUS
EDGE
CAMPUS

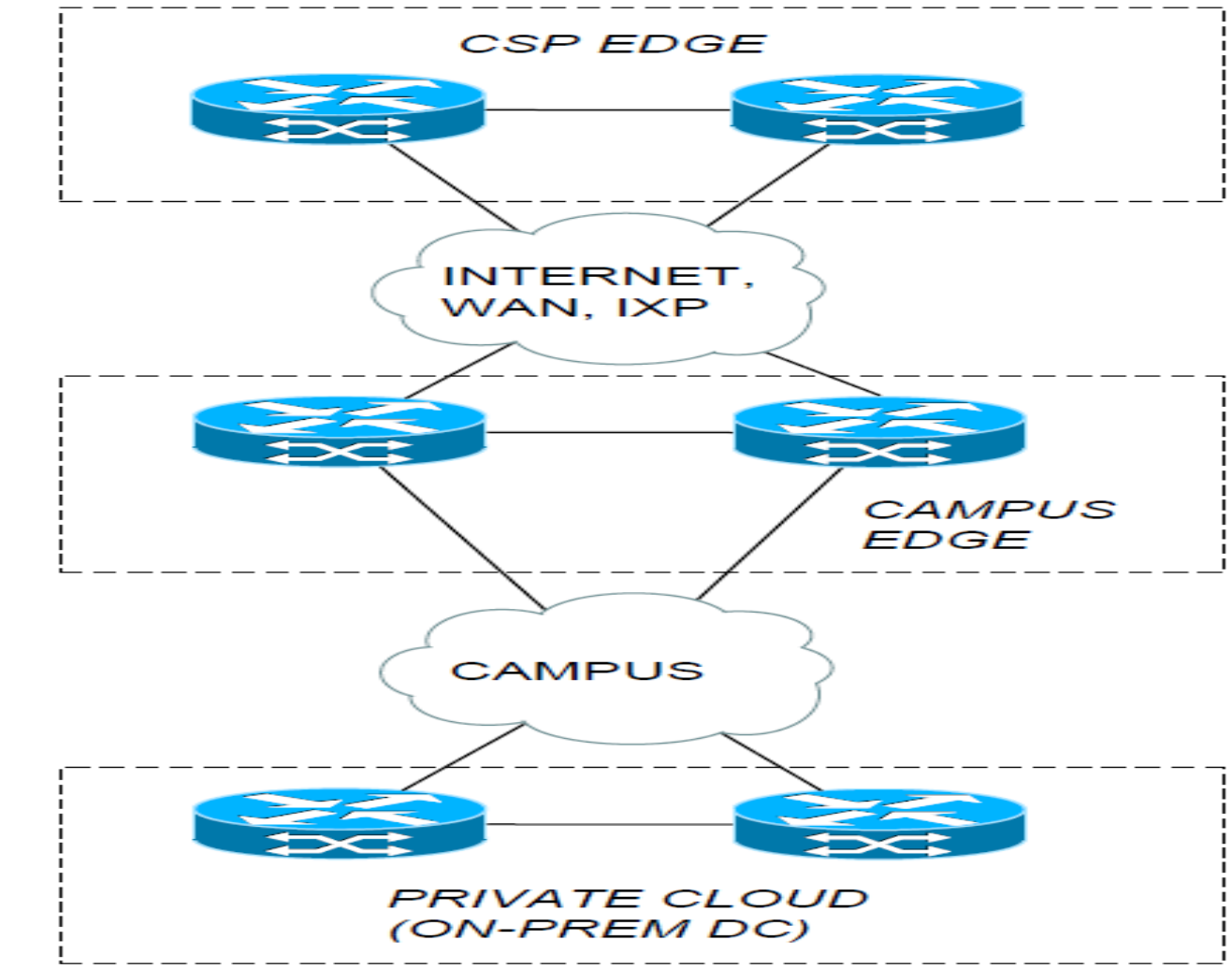
Private Cloud

- This model is like an on-premises DC except must supply the three key ingredients identified by Cisco to be considered a “private cloud”. Specifically, this implies automation/orchestration, workload mobility, and compartmentalization must all be supported in an on-premises DC to qualify


CAMPUS CORE
PRIVATE CLOUD
(ON-PREM DC)

Virtual Private Cloud/Hybrid

- A virtual private cloud is a combination of public and private clouds. An organization may decide to use this to offload some (but not all) of its DC resources into the public cloud, while retaining some things in-house.


CSP EDGE
INTERNET,
WAN, IXP
CAMPUS
EDGE
CAMPUS
PRIVATE CLOUD
(ON-PREM DC)

Infrastructure, Platform and Software Services (XAAS)

- There are three service layers of Cloud Computing:
- **Software as a Service (SaaS):** is where application services are delivered over the network on a subscription and on-demand basis. A simple example would be to create a document but not installing the appropriate text editor on a user's personal computer.
- Another example of Well-known SaaS are: Google Apps, Microsoft 365,Amazon Webservices

- **Platform as a Service (Paas):** consists of run-time environments and software development frameworks and components delivered over the network on a pay-as-you-go basis. PaaS offerings are typically presented as API to consumers
- Examples:AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos.
- **Infrastructure as a Service (IaaS):** is where compute, network, and storage are delivered over the network on a pay-as-you-go basis. The approach that Cisco is taking is to enable service providers to move into this area. This is likely the first thing that comes to mind when individuals think of “cloud”
- Examples:Amazon EC2, Windows Azure, Rackspace, Google Compute Engine.

OpenStack

- OpenStack is a cloud operating system that controls large pools of compute, storage and networking resources throughout a datacenter, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface.

Virtualization

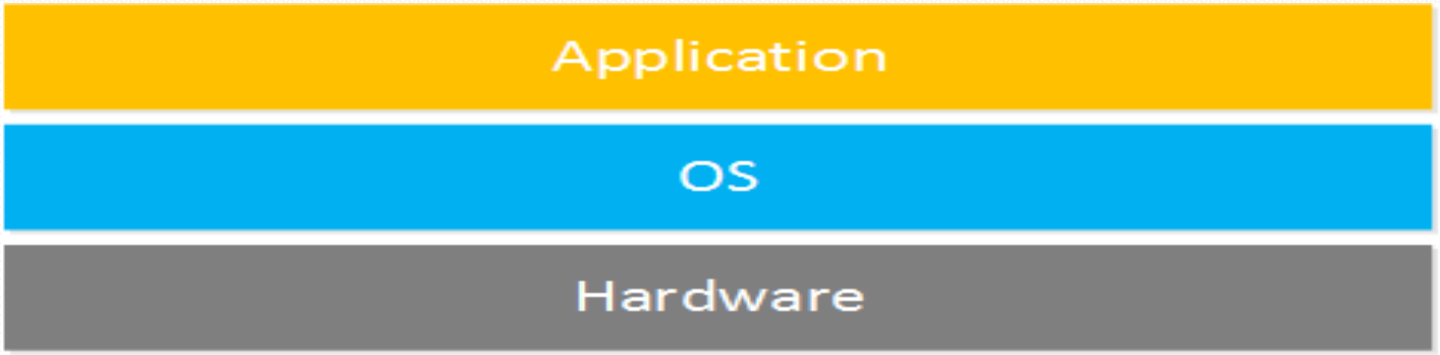
Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

Virtual Machines and Containers

Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

Virtual Machines

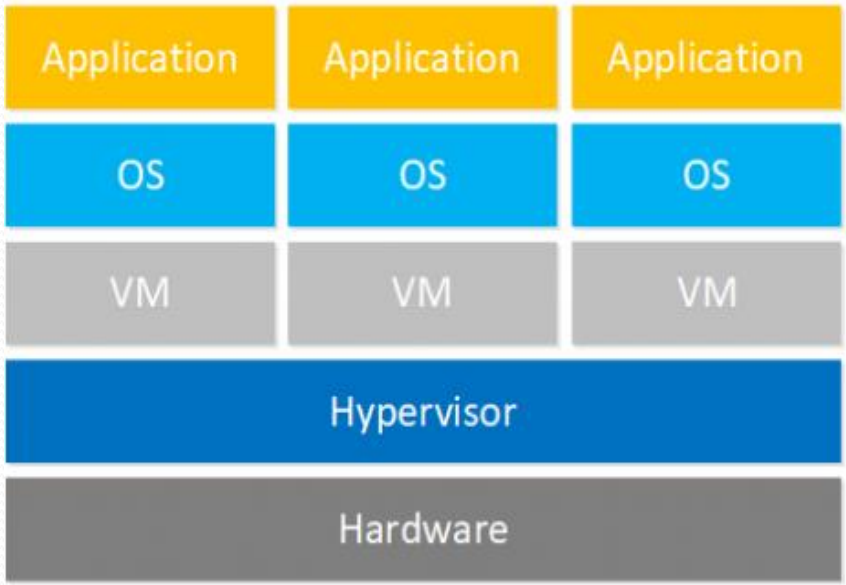
- Back in the days, a physical server would only run a single operating system with one or a few applications. We started with CPUs with a single core, then hyperthreading, and then multiple cores.
- The amount of memory in a single physical server also increased and became more affordable



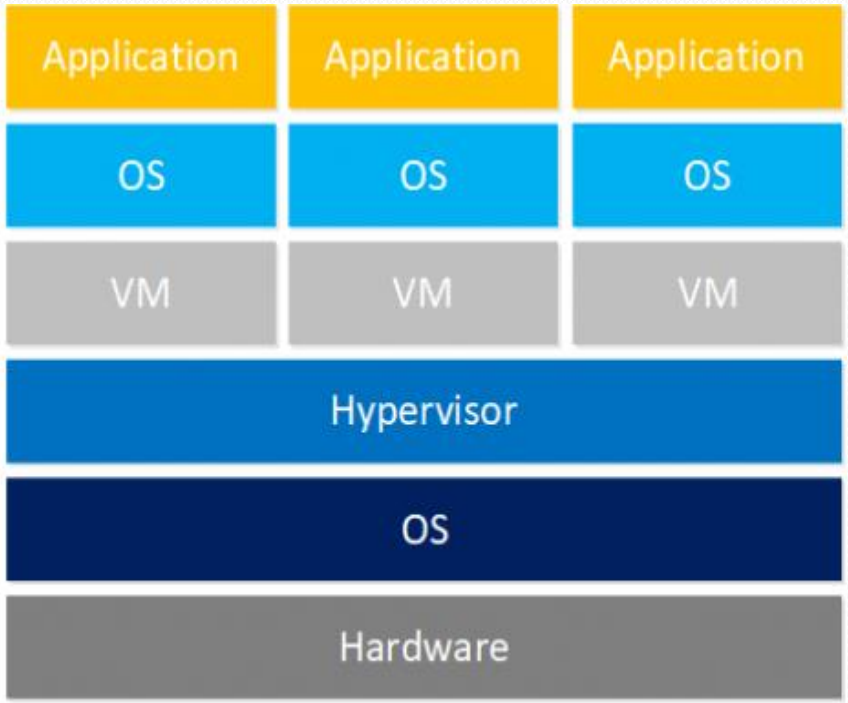
Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

- One of the reasons virtualization is now so popular is that servers were under-utilized.
- We can easily run multiple operating systems and multiple applications on a single physical server.
- A virtual machine is pretty identical to a physical server except it's virtual. We have virtual hardware (CPUs, memory, storage, etc.) which runs on a **hypervisor**

- There are two hypervisor types:
- **Type 1:** this hypervisor runs directly on hardware, which means you can assign more resources to virtual machines. Examples are VMware ESXi, Citrix Xen, KVM, and Microsoft Hyper-V.
- **Type 2**: this hypervisor runs on top of an operating system like Microsoft Windows, Apple MacOS, or Linux. We usually use a type 2 hypervisor on desktops or laptops. Two popular hypervisors are Oracle VM Virtualbox and VMWare Workstation. If you have never played with virtual machines before, give Virtualbox a try. You can download it for free.



Type 1

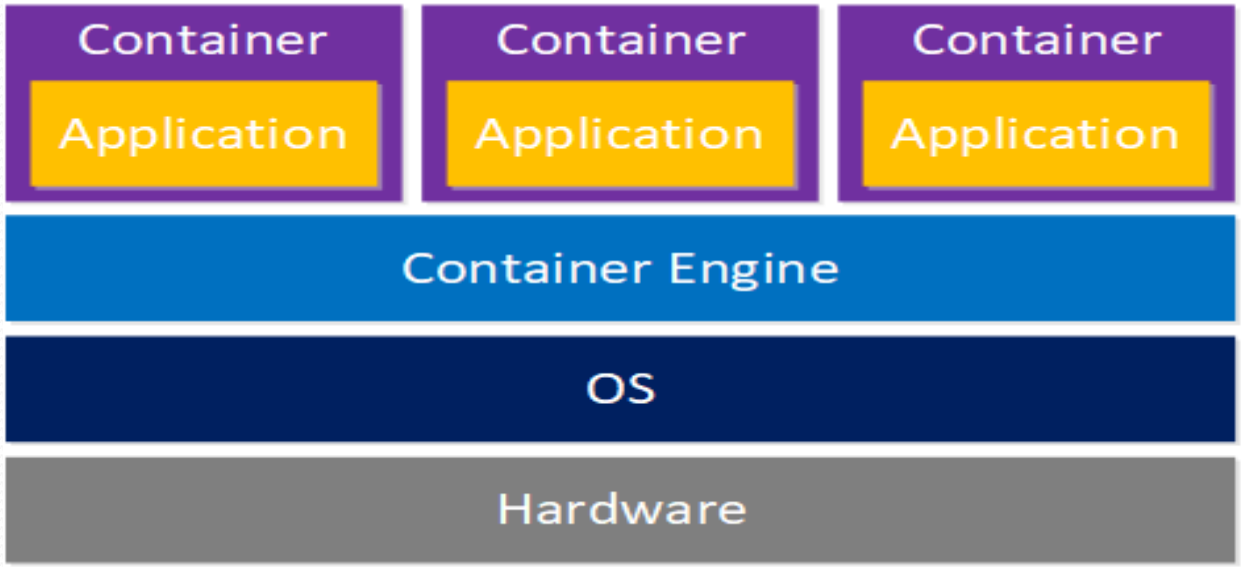


Type 2

Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

Containers

- Containers are sometimes called *light-weight virtual machines*, but they are nothing like virtual machines.
- A container is a “package” that only contains an application and its dependencies, nothing more. This package is stored as a container image. Containers run on top of a **container engine**, which runs on top of an operating system. Starting a container is very quick since the operating system is already running. Containers are isolated from each other by the container engine.



Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

Network Function Virtualization (NFV)

Prepared By:Waleed Adlan-CCIE41999 - waleed_hashim@hotmail.com

Network Function (NF)

- **A network function (NF)** is a function that is performed by a physical appliance like a router, switch, firewall, load balancer, IDS, WAN optimizer, etc. Most vendors have proprietary solutions in which hardware and software are tightly coupled. Cisco is a good example.
- They sell their routers and switches as appliances. You need the hardware and software.
- You cannot run Cisco IOS (officially) without the hardware and you can't run anything else besides Cisco IOS on a router or switch

Virtual Network Function (VNF)

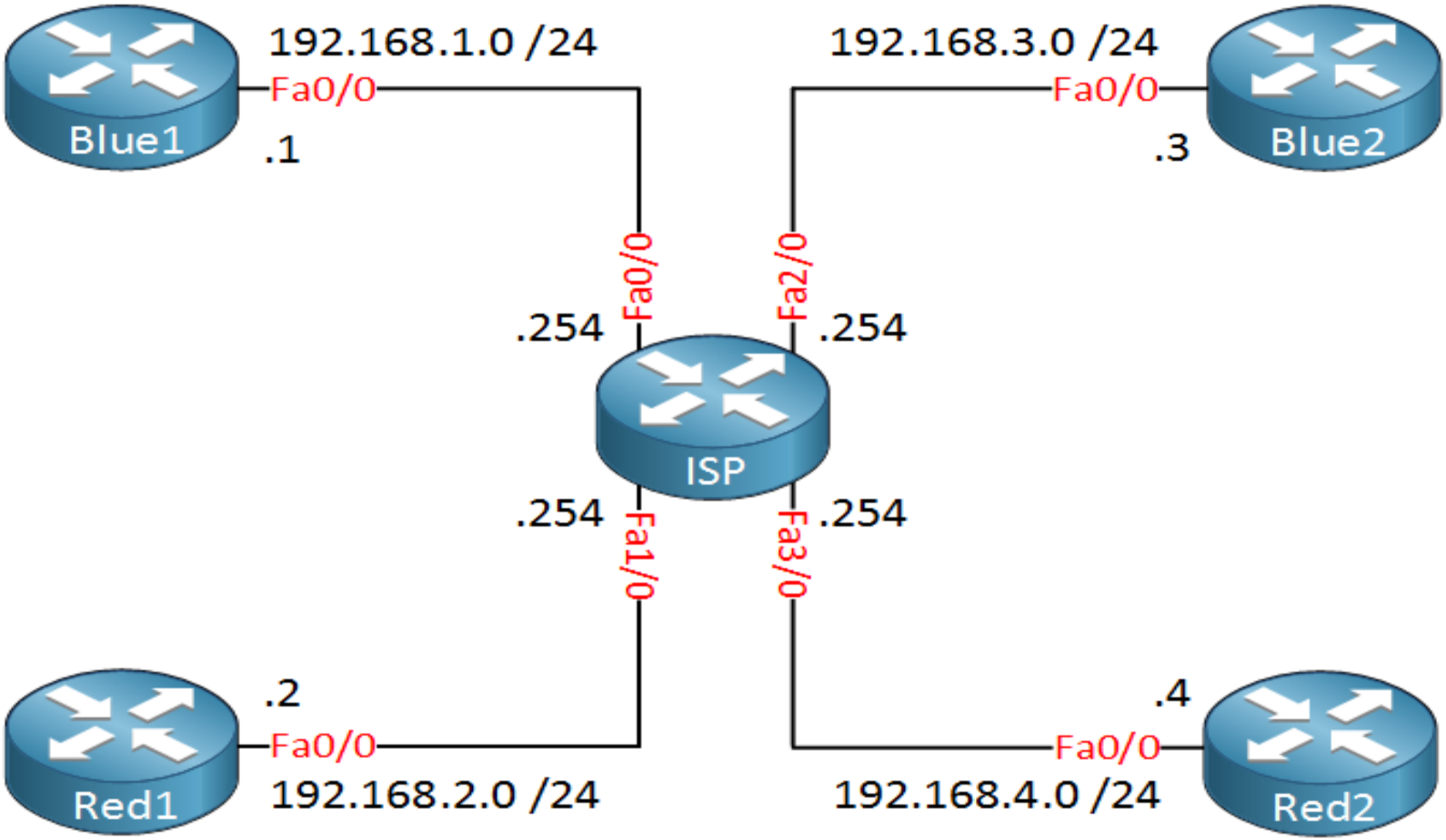
- Nowadays, we can also use virtual solutions. A **virtual network function (VNF)** is the virtual version of a hardware device's network function. VNFs are available as virtual machines or containers.
- Here are examples of Cisco VNFs:
- vEdge Cloud
- CSR1000v
- ASAV
- Cloud Services Platform (CSP) 2100
- XRv 9000
- Firepower NGFWv
- Web Security Virtual Appliance (WSAv)
- Email Security Virtual Appliance (ESAv)
- Advanced Malware Protection Virtual (AMPv)

VRF Lite

Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

- VRFs are like VLANs for routers, instead of using a single global routing table we can use multiple virtual routing tables.
- Each interface of the router is assigned to a different VRF.
- VRFs are commonly used for MPLS deployments, when we use VRFs without MPLS then we call it **VRF lite**.

VRF Lite Example



Prepared By:Waleed Adlan-CCIE41999 -
waleed_hashim@hotmail.com

VRF Configuration

- VRF Creation:

```
ISP(config)#ip vrf Red
ISP(config-vrf)#exit
ISP(config)#ip vrf Blue
ISP(config-vrf)#exit
```

VRF Interface Assignment:

- ISP(config)#interface FastEthernet 0/0
- ISP(config-if)#ip vrf forwarding Blue
- % Interface FastEthernet0/0 IP address 192.168.1.254 removed due to enabling VRF Blue
- ISP(config-if)#ip address 192.168.1.254 255.255.255.0
- ISP(config)#interface FastEthernet 1/0
- ISP(config-if)#ip vrf forwarding Red
- ISP(config-if)#ip address 192.168.2.254 255.255.255.0
- ISP(config)#interface FastEthernet 2/0
- ISP(config-if)#ip vrf forwarding Blue
- ISP(config-if)#ip address 192.168.3.254 255.255.255.0
- ISP(config)#interface FastEthernet 3/0
- ISP(config-if)#ip vrf forwarding Red
- ISP(config-if)#ip address 192.168.4.254 255.255.255.0

VRF Verification

ISP#**show ip vrf**

Name	Default RD	Interfaces
Blue		Fa0/0 Fa2/0
Red		Fa1/0 Fa3/0

ISP#**show ip route vrf Blue connected**

C 192.168.1.0/24 is directly connected, FastEthernet0/0

C 192.168.3.0/24 is directly connected, FastEthernet2/0

ISP#**show ip route vrf Red connected**

C 192.168.4.0/24 is directly connected, FastEthernet3/0

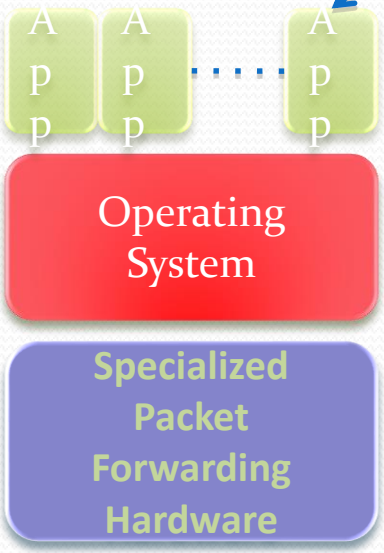
C 192.168.2.0/24 is directly connected, FastEthernet1/0

Prepared By:Waleed Adlan-CCIE41999 - waleed_hashim@hotmail.com

Software Defined Networks (SDN)

The Networking Industry (2007)

Routing, management, mobility management, access control, VPNs, …



Million of lines of source code

Manage by 5400 RFCs

500M gates
10Gbytes RAM

Power Hungry

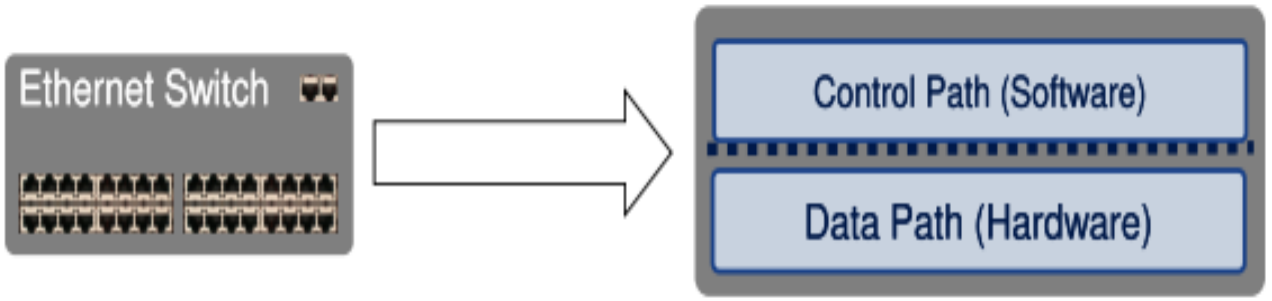
Many complex functions baked into the infrastructure

OSPF, BGP, multicast, differentiated services, Traffic Engineering, NAT, firewalls, MPLS, redundant layers, …

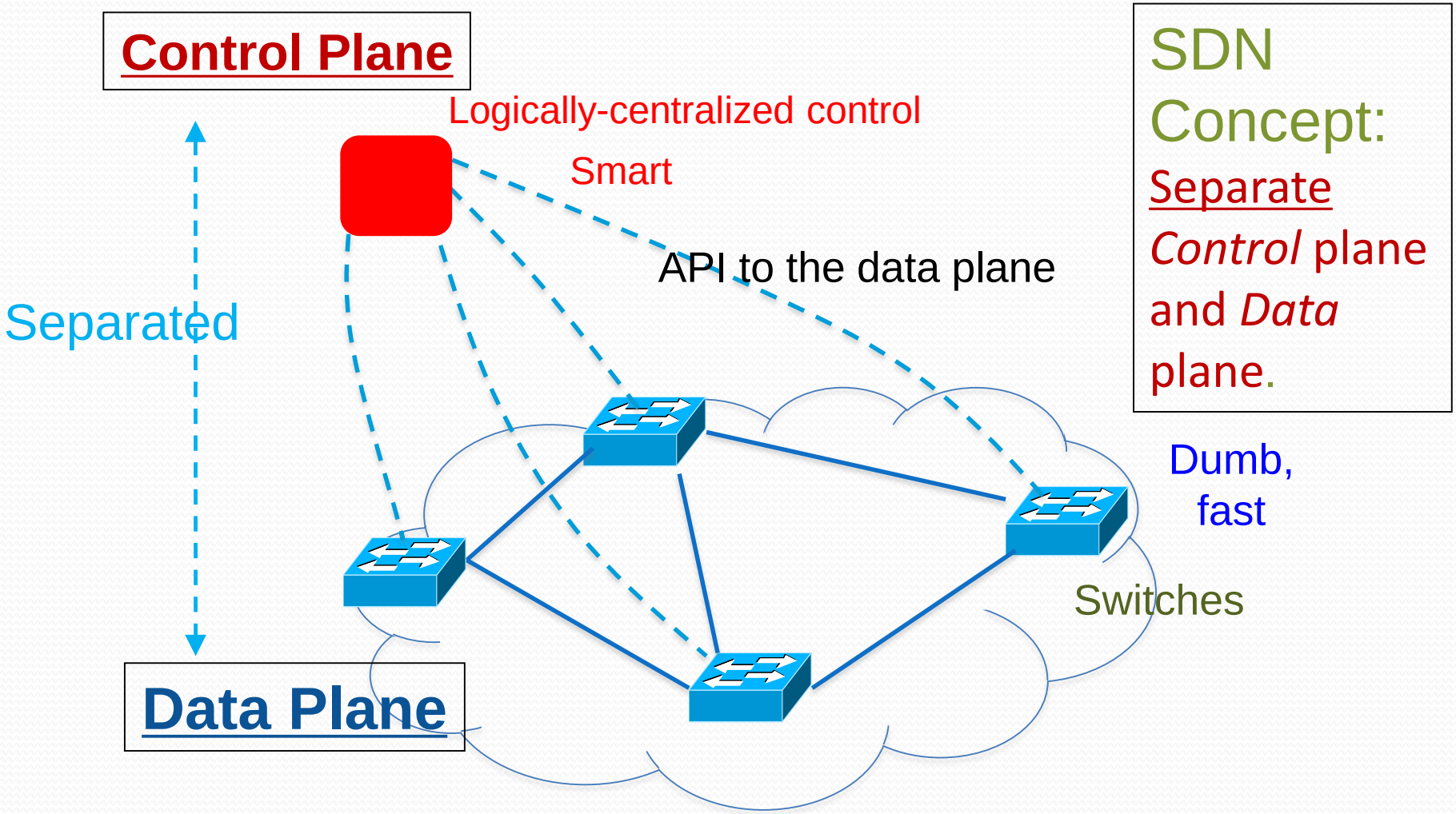
An industry with a “mainframe-mentality”

Traditional network Router In Summary

- Typical Networking Software
  - Management plane
  - Control Plane – The brain/decision maker
  - Data Plane – Packet forwarder

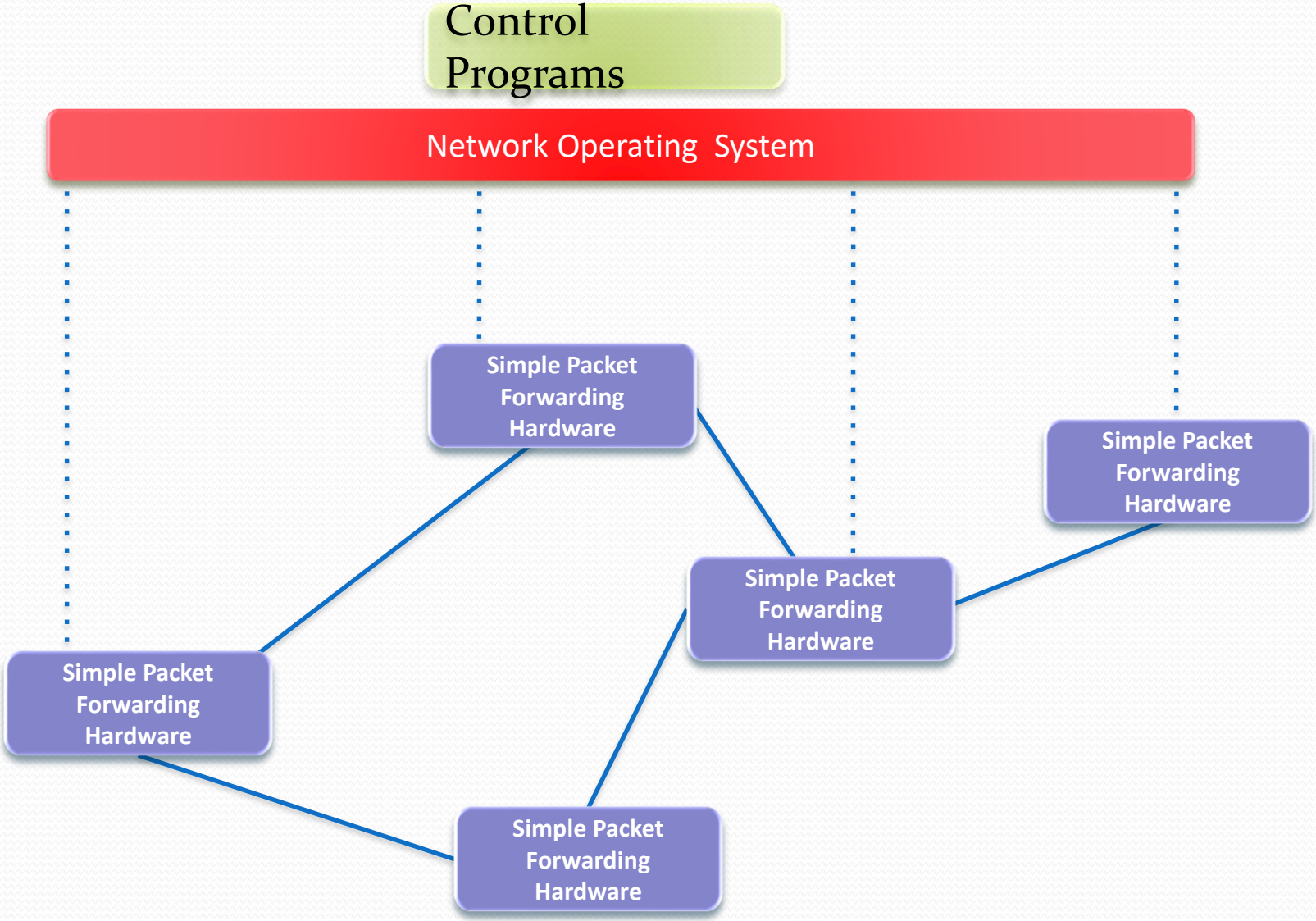


Imagine **IF** The Network is……!!!



SDN Concept: Separate *Control* plane and *Data* plane.

Idea: An OS for Networks



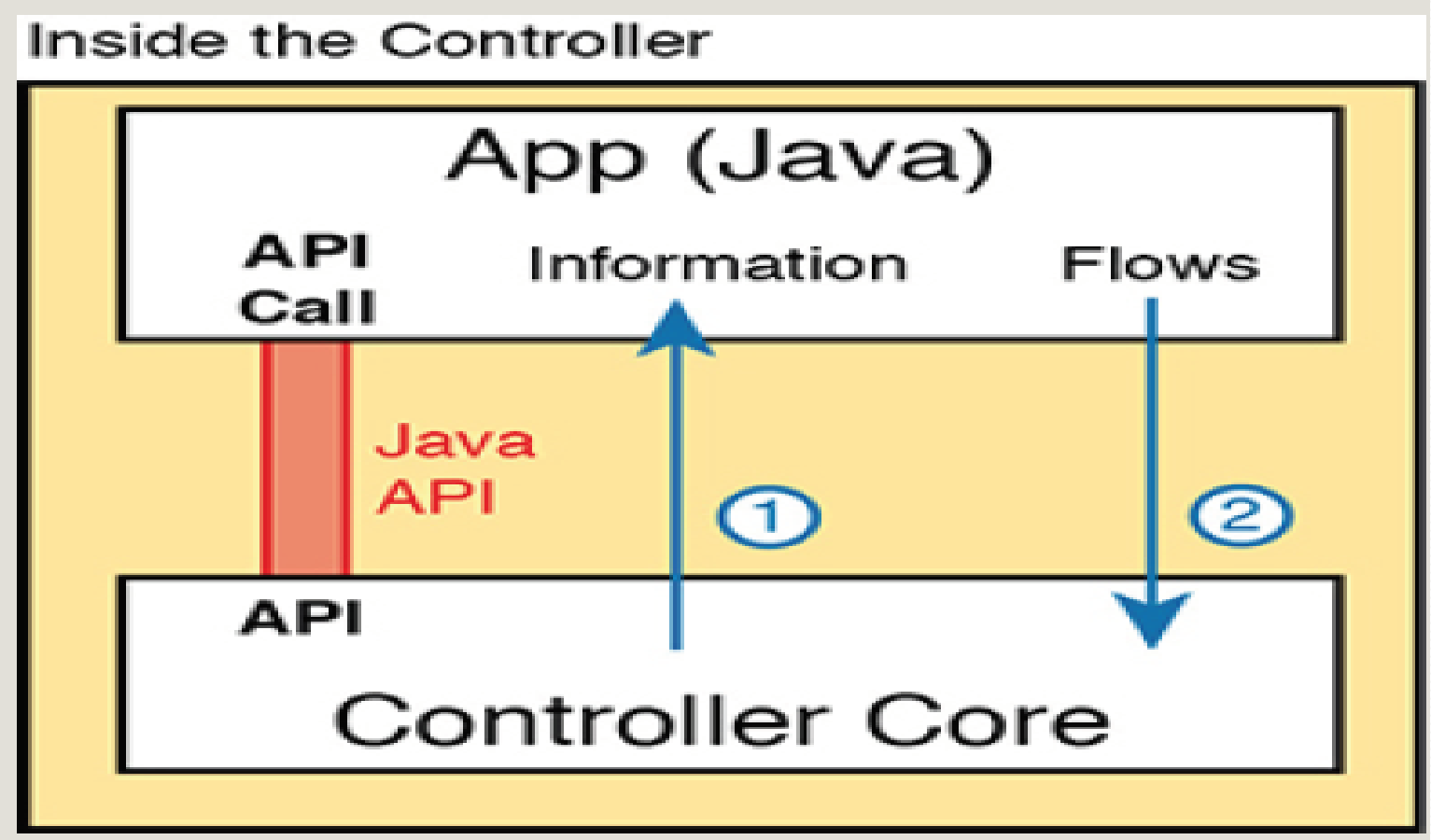
Northbound & Southbound Protocols

- **The northbound interfaces** are considered APIs which are interfaces to existing business applications. This is generally used so that applications can make requests of the network, which could include specific performance requirements (bandwidth, latency, etc).
- **The southbound interfaces** include the control-plane protocol between the centralized controller and the network forwarding hardware.

Examples of Southbound Interfaces

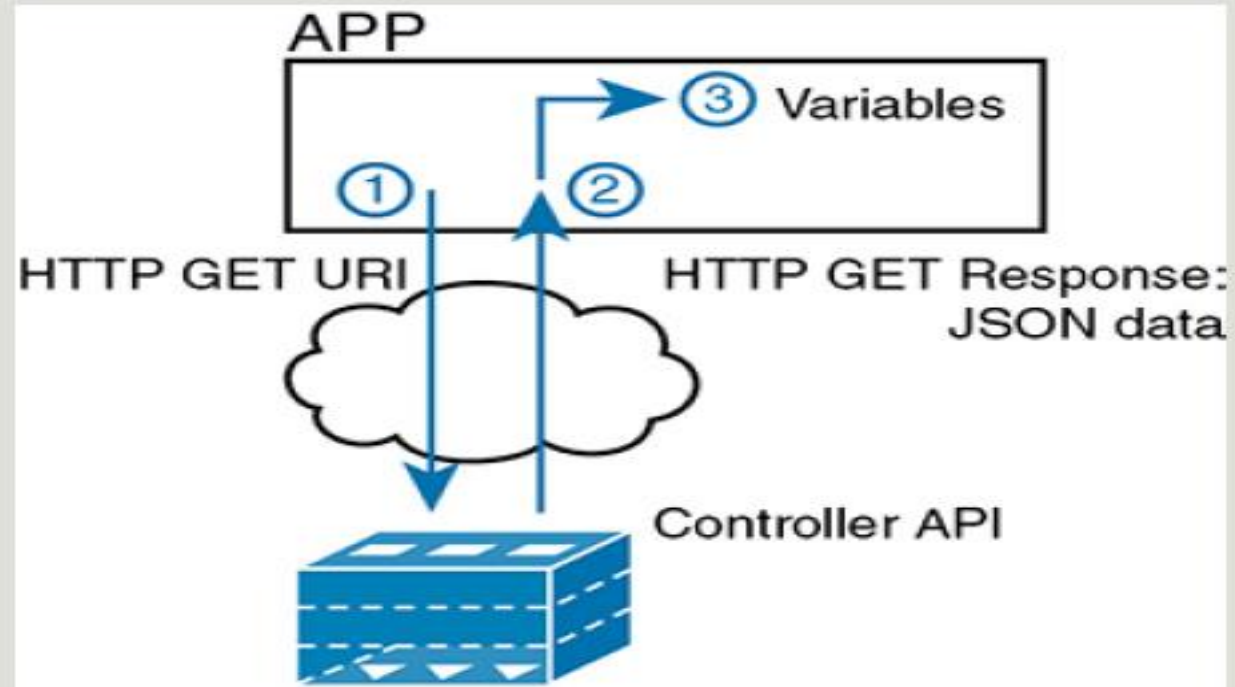
- OpenFlow (from the ONF; www.opennetworking.org)
- OpFlex (from Cisco; used with ACI)
- CLI (Telnet/SSH) and SNMP (used with Cisco APIC-EM)
- CLI (Telnet/SSH) and SNMP, and NETCONF (used with Cisco Software-Defined Access)

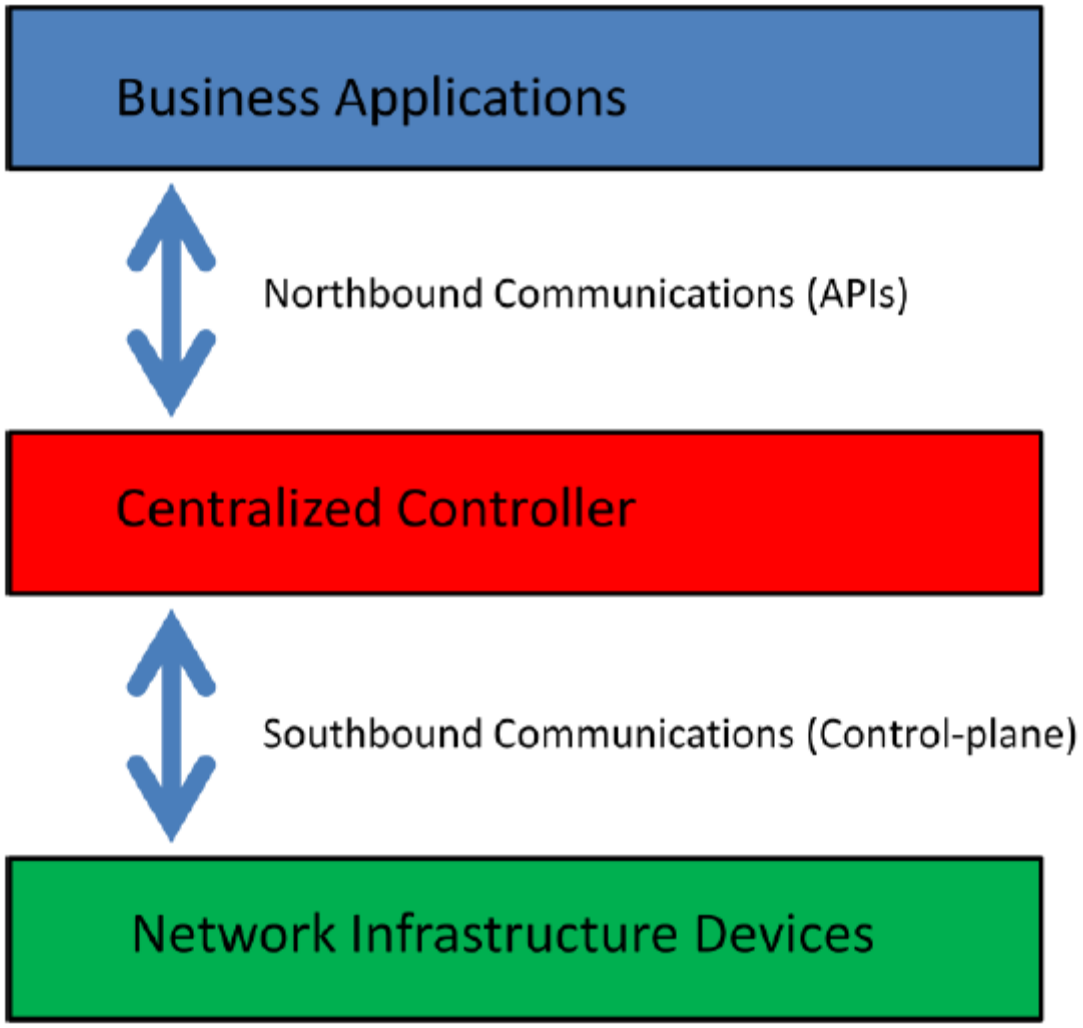
Northbound Interface



Examples of Northbound Interfaces

- Restful API (Representational State Transfer) : Used when the machine is hosting the application is not the same machine that is hosting the controller. So they normally use http messages to communicate



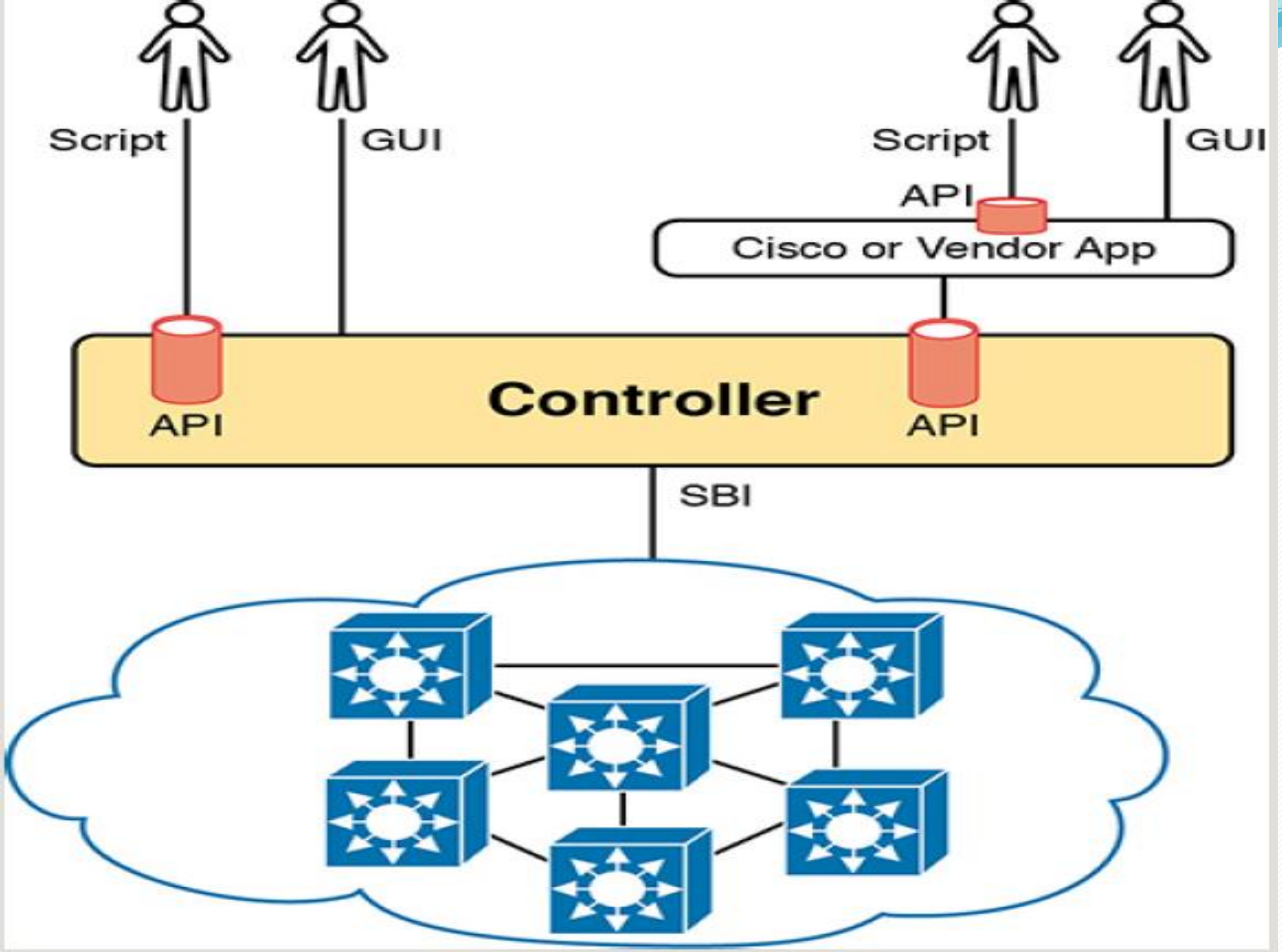

Business Applications
Northbound Communications (APIs)
Centralized Controller
Southbound Communications (Control-plane)
Network Infrastructure Devices

Examples of SDN Controllers

- OpenDaylight (ODL) Controller
- Cisco DNAC (Digital Network Architecture Center)
- Cisco vManage, vSmart and vBond
- Cisco APIC (Application Policy Infrastructure Controller)

Cisco Software Defined Access (SDA)

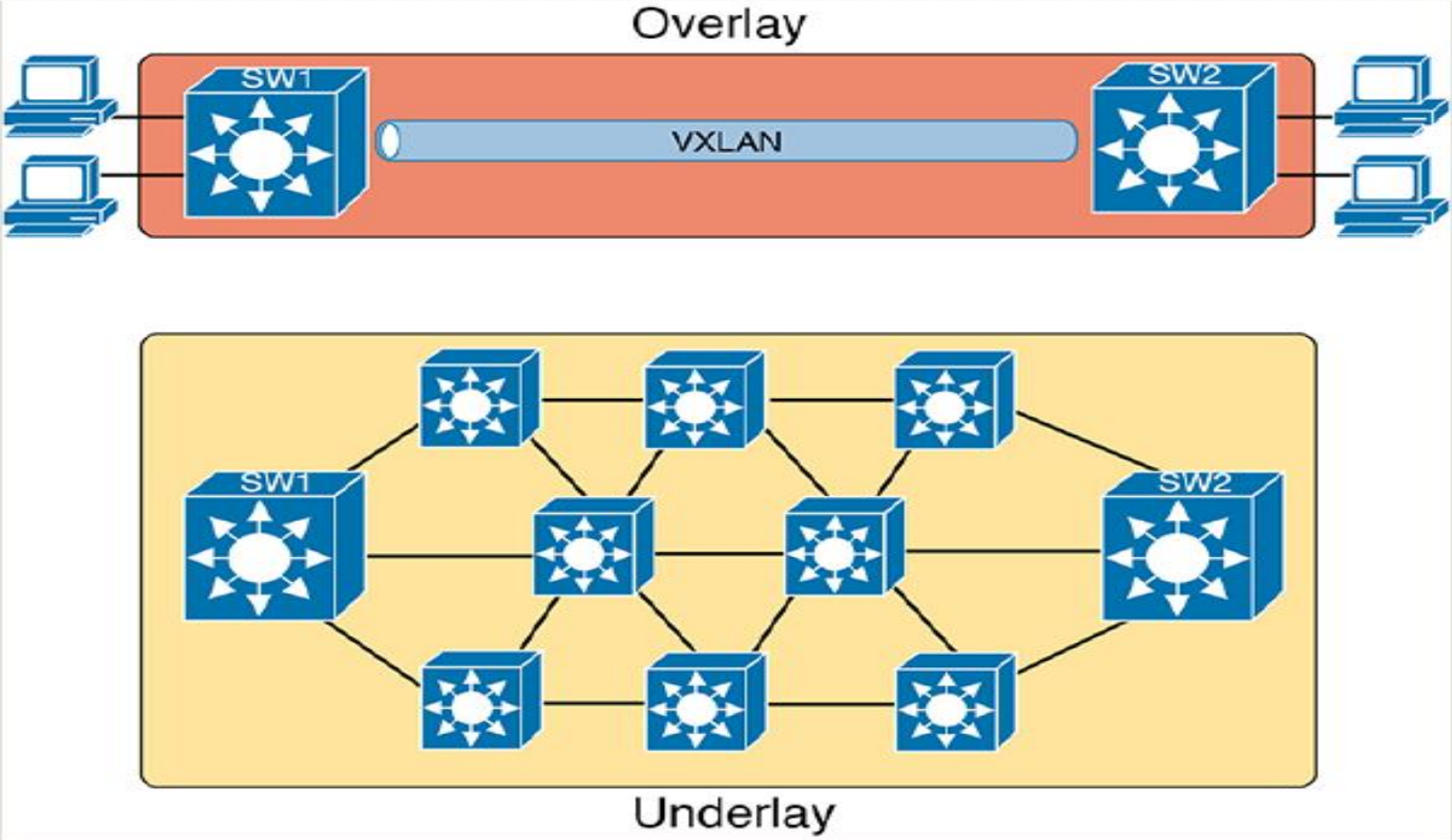
- Cisco Software-Defined Access (SDA) creates an entirely new way to build campus LANs.
- SDA uses the software-defined architectural model with a controller and various APIs
- It still uses a physical network with switches and routers, cables, and various endpoints. At the center sits the Digital Network Architecture (DNA) Center controller with human users making use of a graphical user interface (GUI) and automation using APIs


Script
GUI
Script
GUI
API
Cisco or Vendor App
API
Controller
API
SBI

Software Defined Access (SDA)

- Architecturally, the southbound side of the controller contains the fabric, underlay, and overlay. By design in SDN implementations, most of the interesting new capabilities occur on the northbound side
- **Overlay:** The mechanisms to create VXLAN tunnels between SDA switches, which are then used to transport traffic from one fabric endpoint to another over the fabric.
- **Underlay:** The network of devices and connections (cables and wireless) to provide IP connectivity to all nodes in the fabric, with a goal to support the dynamic discovery of all SDA devices and endpoints as a part of the process to create overlay VXLAN tunnels.

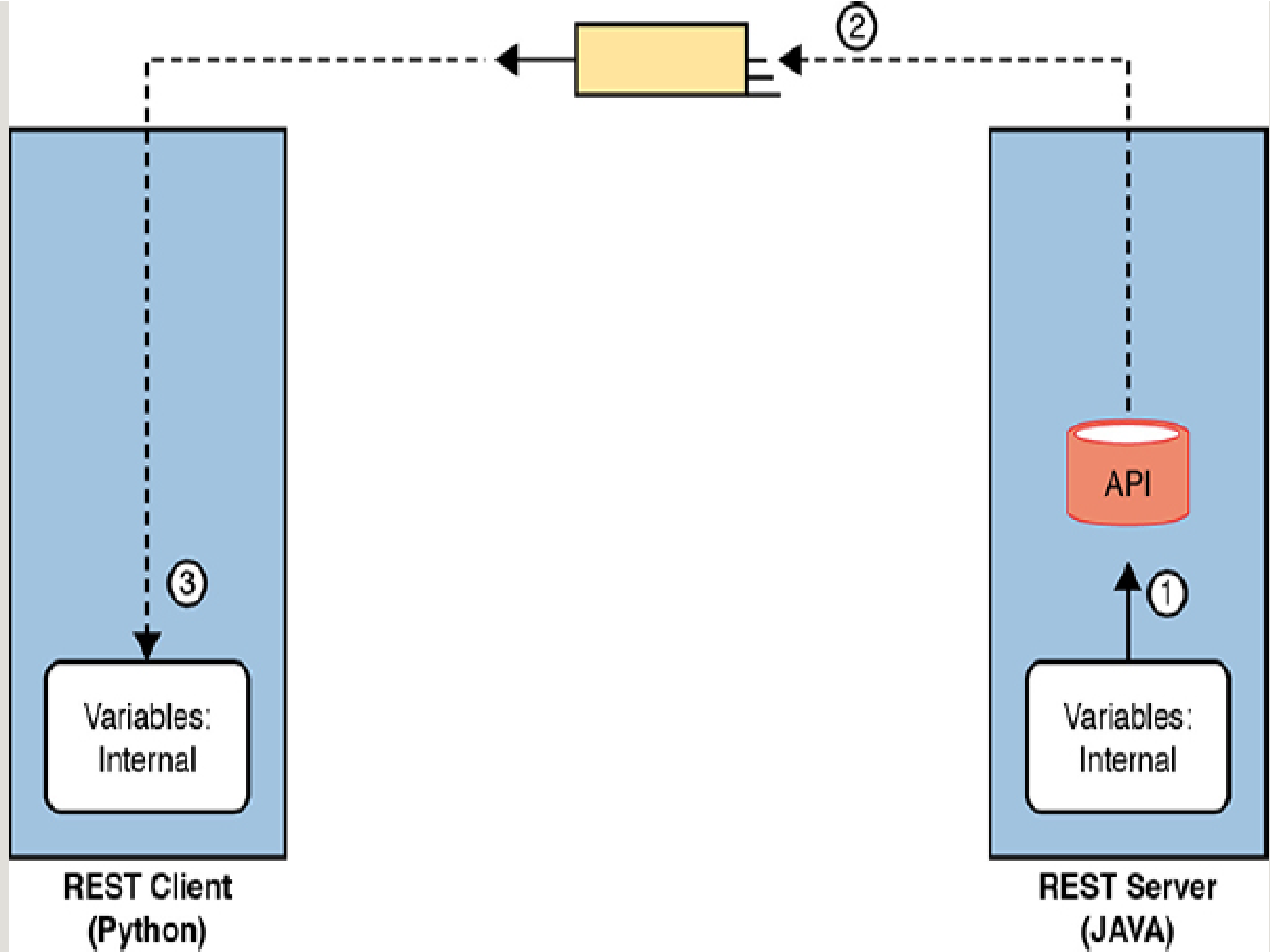
- **Fabric:** The combination of overlay and underlay, which together provide all features to deliver data across the network with the desired features and attributes.



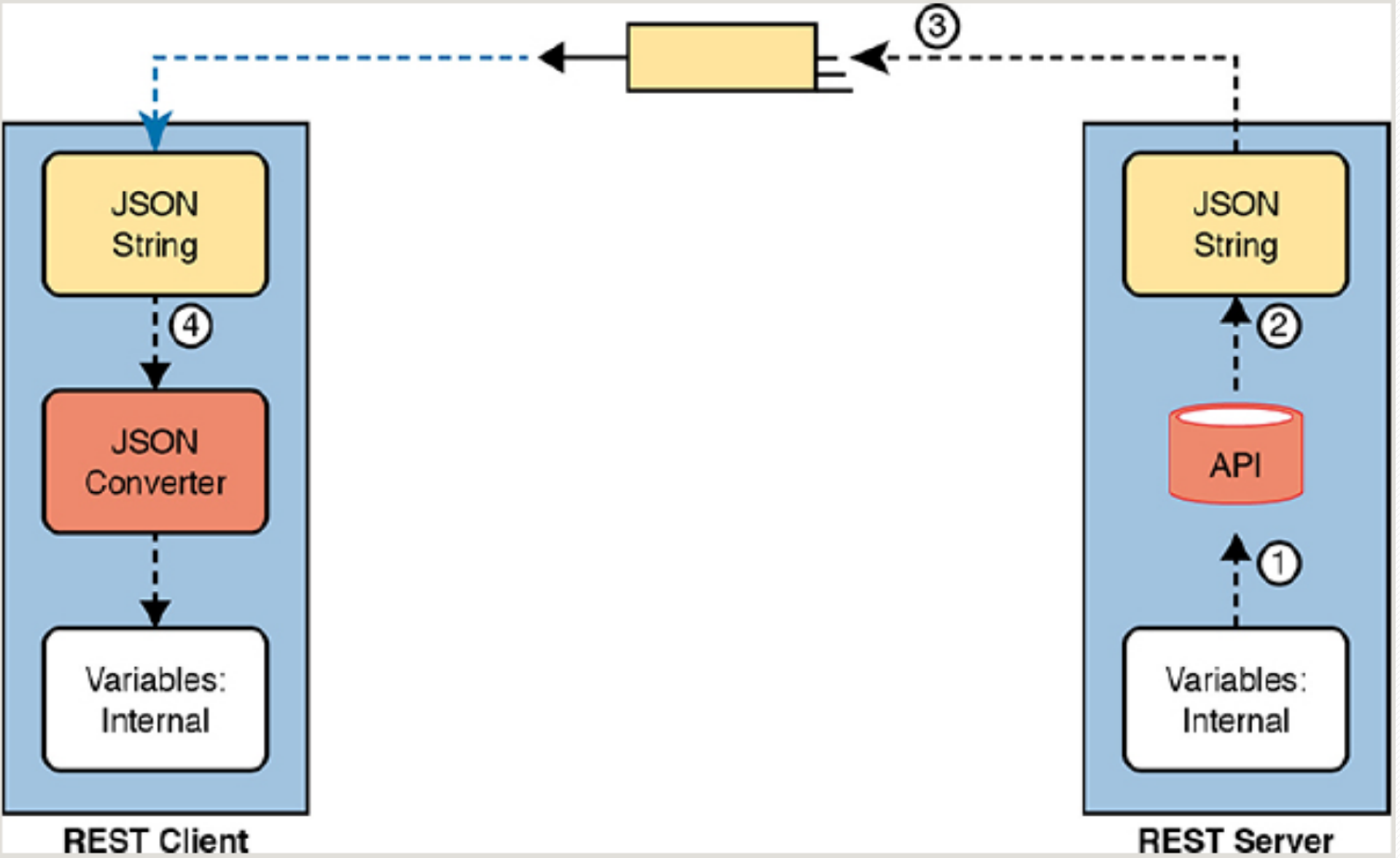
Data Format

Data Format

- Each data serialization language or Data Format provides methods of using text to describe variables, with a goal of being able to send that text over a network or to store that text in a file.
- Examples of Data Serialization Languages are:
- XML
- JSON
- YAML


②
API
①
Variables:
Internal
③
Variables:
Internal
REST Client
(Python)
REST Server
(JAVA)

After Using JSON (JavaScript Object Notation)



Common Elements on Data Format

- Format Syntax
- Objects Representation
- Key / Value Notation
- Values can be objects, lists, strings, numbers, boolean
- Arrays or List Notation

Common Elements on Data Format

"Key" : "Value"

- "Key" identifies/labels a set of data
- Left side of the colon
- Inside of "quotes"

- "Value" is the Data
- Right side of colon
- Canbe:String,Integer,Array/ List,Boolean,Object

```
{
   "name": "GigabitEthernet2",
   "description": "Wide Area Network”,
   "enabled": true
}
```

XML-eXtensible Markup Language

- A human readable data structure
- that applications use to
- store, transfer, and read data.

- <?xml version="1.0" encoding="UTF-8" ?>
- <interface xmlns="ietf-interfaces">
- <name>GigabitEthernet2</name>
- <description>
- Wide Area Network
- </description>
- <enabled>true</enabled>
- <ipv4>
- <address>
- <ip>172.16.0.2</ip>
- <netmask>255.255.255.0</netmask>
- </address>
- </ipv4>
- </interface>

XML-eXtensible Markup Language

- Designed for the Internet
- <tags></tags> surround
- elements for structure and
- layout
- Key/Value representation
- <key>value</key>
- Whitespace not significant

- <?xml version="1.0" encoding="UTF-8" ?>
- <interface xmlns="ietf-interfaces">
- <name>GigabitEthernet2</name>
- <description>
- Wide Area Network
- </description>
- <enabled>true</enabled>
- <ipv4>
- <address>
- <ip>172.16.0.2</ip>
- <netmask>255.255.255.0</netmask>
- </address>
- </ipv4>
- </interface>

XML Object

- A related set of data surrounded by <tags></tags>
- An object can contain other objects or data entries
- <key>value</key> contained within the object tags

- <?xml version="1.0" encoding="UTF-8" ?>
- <interface xmlns="ietf-interfaces">
- <name>GigabitEthernet2</name>
- <description>
- Wide Area Network
- </description>
- <enabled>true</enabled>
- <ipv4>
- <address>
- <ip>172.16.0.2</ip>
- <netmask>255.255.255.0</netmask>
- </address>
- </ipv4>
- </interface>

XML List

- List of data
- Can be composed of XML objects
- Repeated instances of <tags></tags> for each element

- <?xml version="1.0" encoding="UTF-8" ?>
- <addresses>
- <ip>172.16.0.2</ip>
- <netmask>255.255.255.0</netmask>
- </addresses>
- <addresses>
- <ip>172.16.0.3</ip>
- <netmask>255.255.255.0</netmask>
- </addresses>
- <addresses>
- <ip>172.16.0.4</ip>
- <netmask>255.255.255.0</netmask>

JSON-Java Script Object Notation

- A human readable data structure that applications use to store, transfer, and read data.

```
{
  "ietf-interfaces:interface": {
    "name": "GigabitEthernet2",
    "description": "Wide Area Network",
    "enabled": true,
    "ietf-ip:ipv4": {
      "address": [
        {
          "ip": "172.16.0.2",
          "netmask": "255.255.255.0"
        }
      ]
    }
  }
}
```

JSON

- A data-interchange text format
- Notated with {} for objects, [] for arrays
- Key/Value representation
- "key": value
- Whitespace not significant

```
{
  "ietf-interfaces:interface": {
    "name": "GigabitEthernet2",
    "description": "Wide Area Network",
    "enabled": true,
    "ietf-ip:ipv4": {
      "address": [
        {
          "ip": "172.16.0.2",
          "netmask": "255.255.255.0"
        }
      ]
    }
  }
}
```

JSON Object

- Data surrounded by { }
- An object can contain other objects or data entries
- Key/Value set separated by comma
- No comma at the end!

```
{
  "ietf-interfaces:interface": {
    "name": "GigabitEthernet2",
    "description": "Wide Area Network",
    "enabled": true,
    "ietf-ip:ipv4": {
      "address": [
        {
          "ip": "172.16.0.2",
          "netmask": "255.255.255.0"
        }
      ]
    }
  }
}
```

JSON List

- List of data
- Can be composed of JSON objects
- Notated with brackets
- Comma Separated

```
{
  "addresses": [
    {
      "ip": "172.16.0.2",
      "netmask": "255.255.255.0"
    },
    {
      "ip": "172.16.0.3",
      "netmask": "255.255.255.0"
    },
    {
      "ip": "172.16.0.4",
      "netmask": "255.255.255.0"
    }
  ]
}
```

YAML-YAML Ain't Markup Language

- A human readable data structure that applications use to store, transfer, and read data.

```
---
ietf-interfaces:interface:
  name: GigabitEthernet2
  description: Wide Area Network
  enabled: true
  ietf-ip:ipv4:
    address:
    - ip: 172.16.0.2
      netmask: 255.255.255.0
```

YAML

- Minimalist format commonly used for configuration files
- Whitespace indentation defines structure
- No commas
- Key/Value representation
- key: value

```
---
ietf-interfaces:interface:
  name: GigabitEthernet2
  description: Wide Area Network
  enabled: true
  ietf-ip:ipv4:
    address:
    - ip: 172.16.0.2
      netmask: 255.255.255.0
```

YAML Object

- Related set of data at the common indentation level under name
- An object can contain other objects or data entries
- key: value pairs left aligned

```
---
ietf-interfaces:interface:
  name: GigabitEthernet2
  description: Wide Area Network
  enabled: true
  ietf-ip:ipv4:
    address:
    - ip: 172.16.0.2
      netmask: 255.255.255.0
```

YAML List

- List of data Can be composed of YAML objects
- Uses “-” character to indicate a list element

```
---
addresses:
- ip: 172.16.0.2
  netmask: 255.255.255.0
- ip: 172.16.0.3
  netmask: 255.255.255.0
- ip: 172.16.0.4
  netmask: 255.255.255.0
```

Data Modeling

YANG

- **YANG** stands for **Y**et **A**nother **N**ext **G**eneration. It is a data modeling language used to describe the structure of data for network configuration and management.

- In short:

- YANG defines how data is structured in a network device.
- It works with NETCONF, RESTCONF, and other network management protocols.
- It makes automating network devices easier and more standardized.

Where is YANG Used?

- NETCONF and RESTCONF both use YANG to define the data that can be configured or monitored.
- YANG models describe:
- Interfaces
- Routing protocols
- Access control lists (ACLs)
- System services
- And much more…

How YANG Works?

- Think of YANG as a blueprint for network data.
- It defines:
- Data types (strings, integers, etc.)
- Hierarchies (how data is structured)
- Constraints (rules for data)
- Operations (like create, read, update, delete)

Example of YANG Model

```
module example-interface {
  namespace "urn:example:interface";
  prefix "iface";

  container interfaces {
    list interface {
      key "name";
      leaf name {
        type string;
      }
      leaf enabled {
        type boolean;
        default "true";
      }
      leaf ip-address {
        type string;
      }
    }
  }
}
```

Protocols Using YANG

- **NETCONF:** Uses YANG to exchange XML data for configuration and monitoring.
- **RESTCONF:** Uses YANG with HTTP/HTTPS (like REST APIs) to interact with network devices.

Benefits of YANG

- **Standardization:** All vendors (Cisco, Juniper, etc.) can use the same models.
- **Automation-friendly:** Works well with tools like Ansible, Cisco NSO, and others.
- **Extensibility:** You can extend existing YANG models or create your own.
- **Readable and Structured:** Human-readable with clear data structure.

What is API?

”It’s a way for two pieces of software to talk to each other”

Application Programming Interface (API)

For a long time.. Humans were the only users

Software displays results in User Interface (UI)

User asks for data or takes action by interacting with UI

The API is the User Interface for software systems

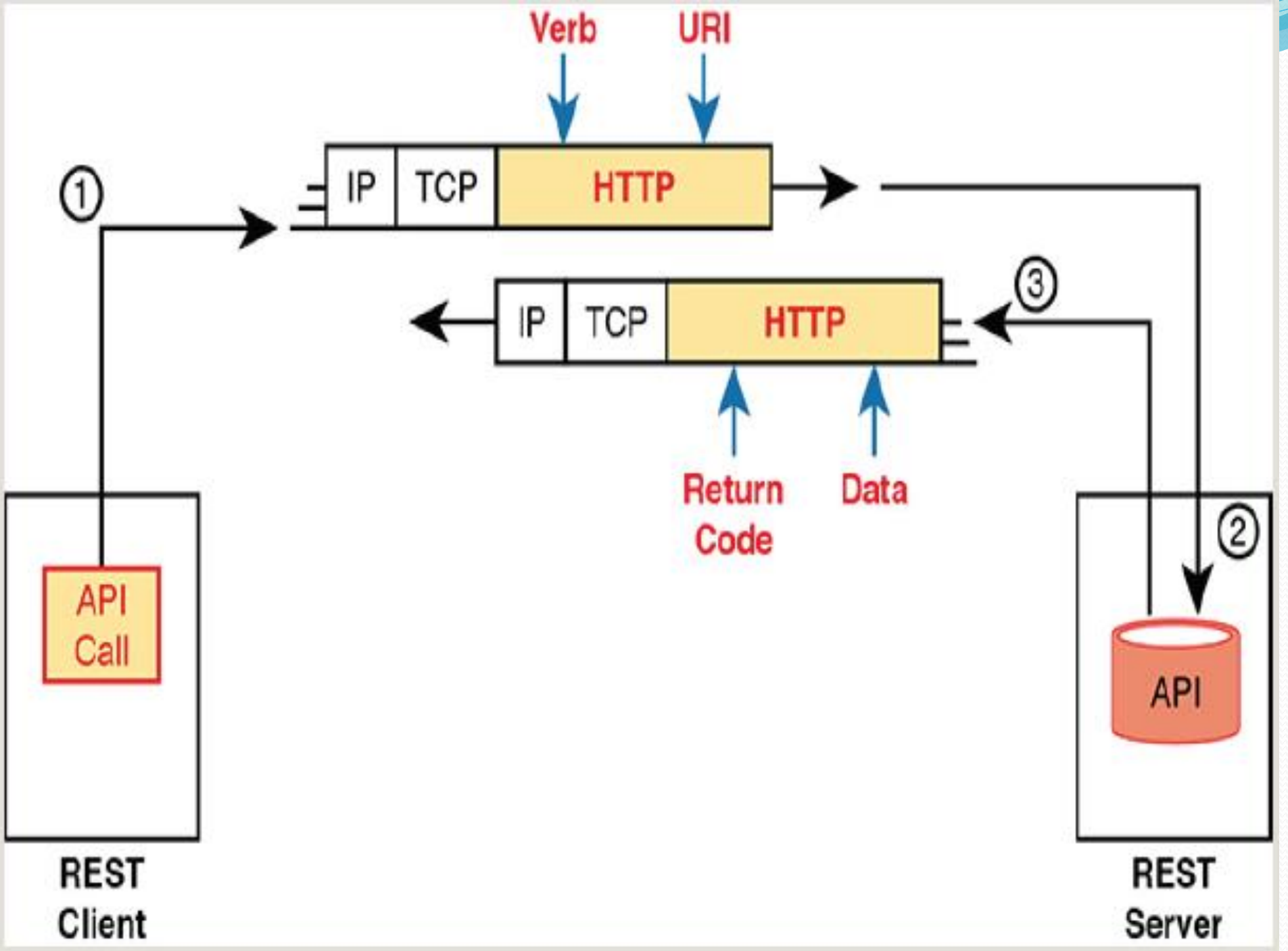
Examples of APIs

- SNMP
- SOAP
- REST
- XML-RPC
- JSON-RPC
- NETCONF
- RESTCONF

REST
(REpresentational State Transfer)

REST Based (RESTful) APIs

- REST APIs follow a set of foundational rules about what makes a REST API and what does not
- REST APIs include the six attributes:
- Client/server architecture
- Stateless operation
- Clear statement of cacheable/uncacheable
- Uniform interface
- Layered
- Code-on-demand

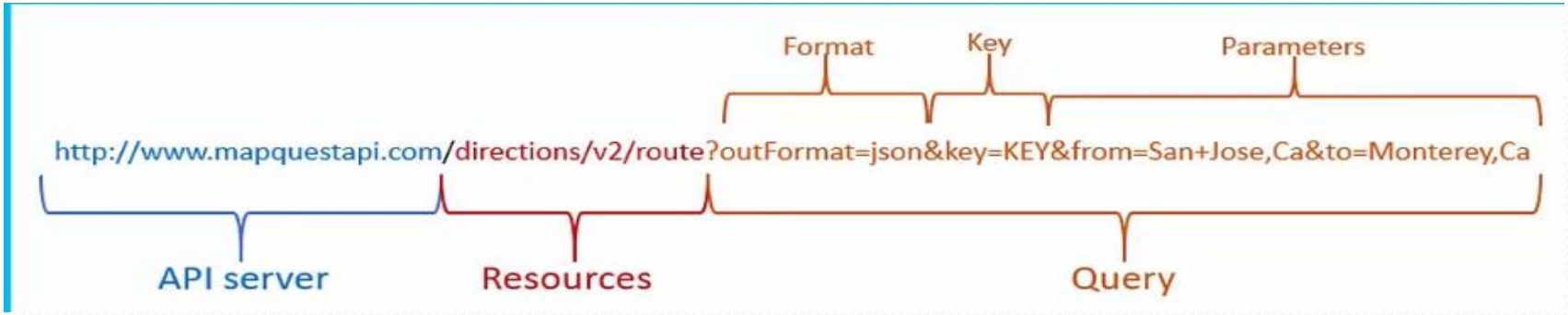

Verb
URI
IP
TCP
HTTP
1
IP
TCP
HTTP
3
Return Code
Data
2
API Call
API
REST Client
REST Server

CRUD Acronym

- The software industry uses a memorable acronym—*CRUD*—for the four primary actions performed by an application
- **Create:** Allows the client to create some new instances of variables and data structures at the server and initialize their values as kept at the server
- **Read:** Allows the client to retrieve (read) the current value of variables that exist at the server, storing a copy of the variables, structures, and values at the client
- **Update:** Allows the client to change (update) the value of variables that exist at the server
- **Delete:** Allows the client to delete from the server different instances of data variables

- REST API when ueses HTTP, HTTP got four messages which equivalent to CRUD actions:
- POST
- GET
- PATCH/PUT
- DELETE

URI(Universal Resource Identifier)



HTTP Methods

HTTP Verb	Typical Purpose (CRUD)	Description
POST	Create	Used to create a new object, or resource. *Example: Add new book to library*
GET	Read	Retrieve resource details from the system. *Example: Get list of books from the library*
PUT	Update	Typically used to replace or update a resource. Can be used to modify or create. *Example: Update the borrower details for a book*
PATCH	Update	Used to modify some details about a resource. *Example: Change the author of a book*
DELETE	Delete	Remove a resource from the system. *Example: Delete a book from the library.*

Status Response Code

Status Code	Status Message	Meaning
200	OK	All looks good
201	Created	New resource created
400	Bad Request	Request was invalid
401	Unauthorized	Authentication missing or incorrect
403	Forbidden	Request was understood, but not allowed
404	Not Found	Resource not found
500	Internal Server Error	Something wrong with the server
503	Service Unavailable	Server is unable to complete request

Headers

Header	Example Value	Purpose
Content-Type	application/json	Specify the format of the data in the body
Accept	application/json	Specify the requested format for returned data
Authorization	Basic dmFncmFudDp2YWdyYW50	Provide credentials to authorize a request
Date	Tue, 25 Jul 2017 19:26:00 GMT	Date and time of the message

Many Options for Working with REST APIs

- **Web Browser**
- Use Http protocol as if accessing website
- **curl**
- Linux command line application
- **Postman**
- Chrome browser plugin and application
- **Requests**
- Python library for scripting

API Calls Examples

- **Use Web:**
- https://ipinfo.io/72.163.4.185/json
- **Curl Command:**
- curl -k https://ipinfo.io/72.163.4.185/json (-k for bypassing the ssl certificate)
- **Postman**
- **Python**

Python Script Example

```
import requests

url = "https://ipinfo.io/72.163.4.185/json"

try:
    # Send a GET request to the API
    response = requests.get(url)

    # Check if the request was successful (HTTP 200)
    if response.status_code == 200:
        data = response.json()
        print("IP Information:")
        for key, value in data.items():
            print(f"{key}: {value}")
    else:
        print(f"Failed to retrieve data. Status code: {response.status_code}")

except requests.exceptions.RequestException as e:
    print(f"An error occurred: {e}")
```

Rest Based API Authentication

- **None:** the Web API resource is public, anybody can place call.
- **Basic Authentication**
- **Access or Bearer Token Authentication**
- **API Key Authentication**
- **OAuth Authentication**

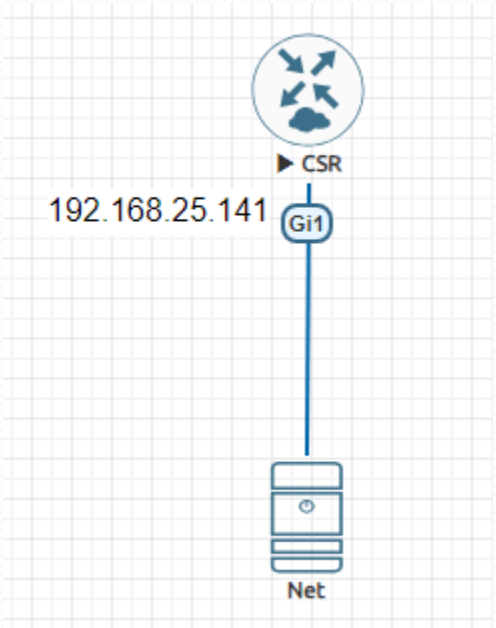
Basic Authentication

- Basic authentication is a straightforward method for securing RESTful APIs. In this approach, the client sends HTTP requests with an Authorization header that contains a username and password.

- Example:
- Use Postman to GET request to a basic-auth protected endpoint at “https://postman-echo.com/basic-auth”. This endpoint is provided by Postman to simulate a basic-auth protected endpoint. The endpoint accepts a username:postman and password:password and returns a status code of 200 ok if the credentials are correct. Otherwise, it returns status code 401 unauthorized

Router Basic Authentication Example

```
!CSR
interface G1
no shutdown
ip address 192.168.25.141 255.255.255.0
exit
!
username admin privilege 15 password cisco
!
ip http server
ip http secure-server
ip http authentication local
!
restconf
!(Optional)
netconf-yang
```



- **Linux Machine Terminal Command to get all interfaces**
- curl -k -u admin:cisco \
- https://192.168.25.141/restconf/data/ietf-interfaces:interfaces

- **Windows Machine Terminal Command to get all interfaces**
- curl -k -u admin:cisco https://192.168.25.141/restconf/data/ietf-interfaces:interfaces
- or
- curl -u admin:cisco -k -X GET "https://192.168.25.141/restconf/data/Cisco-IOS-XE-native:native/interface" -H "Accept: application/yang-data+json"

Access Token Authentication

- Access token authentication is a robust and flexible method used to secure RESTful APIs by issuing tokens to clients upon successful authentication.
- **Advantages of Access Tokens Over Basic Authentication**
- **Security:** Tokens reduce the risk of exposing credentials (like username and password) in every request. They can be scoped to limit access and can be revoked if compromised.
- **Convenience:** Once you generate a token, it can be used for multiple API calls without having to authenticate each time.
- **Control:** Multiple tokens can be generated for different purposes or applications, each with its own set of permissions.

API Key Authentication

- API key authentication is a simple and effective method for securing RESTful APIs. In this approach, a unique identifier known as an API key is issued to a client. This key acts as a secret token that identifies the client making the request, allowing the server to determine if the request is authorized. The API key is used in headers, query parameters, or the body of HTTP requests to authenticate access to the API.
- API key authentication is popular because it is straightforward to implement and manage. It is often used in public APIs and services where simplicity and ease of integration are prioritized. API keys are unique identifiers used to authenticate API requests.

API Key VS Token

- API keys and bearer (access) tokens both authenticate and authorize API access, but they differ in usage and security.

- **API Keys:**
- Usage: Simple, static identifiers included in request headers or query parameters to authenticate clients.
- Example: Used with OpenWeather.
- Management: Easy to manage but less secure due to their static nature and lack of expiration.
- Security: Less secure; some providers may enforce usage limits and allow expiration dates.

- **Bearer Tokens:**
- Usage: Require users to log into their account to generate a token, which grants short-lived, scoped access to resources. Included in the Authorization header.
- Example: Used with GitHub.
- Security: Offer more security, providing granular control over access and permissions. Suitable for user-specific authentication and secure service-to-service communication.

Choosing between API Keys and Access Token

- **API Keys:** Best for simple applications where ease of implementation and management is a priority, and high security is not a critical requirement.
- **Bearer Tokens:** Ideal for applications needing higher security, user-specific authentication, and detailed control over permissions and access.

OAuth Authentication

- OAuth 2.0 is a framework that allows one app (called **the Client**) to access resources from another app (called the **Resource Server**) on behalf of the user, without sharing the user's password.
- **Key Players in OAuth 2.0:**
- Resource Owner: The user who owns the data.
- Client: The application that wants to access the user's data (e.g., a third-party app).
- Authorization Server: The server that authenticates the user and issues tokens (e.g., Google, Facebook).
- Resource Server: The server that holds the user's data and requires a token for access (e.g., Google API).

Example of OAuth

- **Authorization Request:**
- User clicks "Log in with Google" on the music platform.
- The music platform redirects the user to Google's login page, requesting access to their Gmail profile and email.
- **Authorization Grant:**
- User logs into Gmail and grants permission.
- **Access Token Request:**
- The music platform sends the authorization code and its own credentials to Google to request an access token.
- **Access Token:**
- Google verifies the code and the music platform's identity.
- Google issues an access token to the music platform.
- **Resource Request:**
- The music platform uses the access token to request the user's profile and email from Google.
- **Protected Resource:**
- If the access token is valid, Google provides the requested information to the music platform.

Why Use OAuth 2.0?

- Secure: No need to share passwords.
- Limited Access: Apps can access only what you allow.
- Token-based: Tokens can be revoked anytime.
- Standardized: Widely supported by APIs (Google, GitHub, Facebook, etc.).

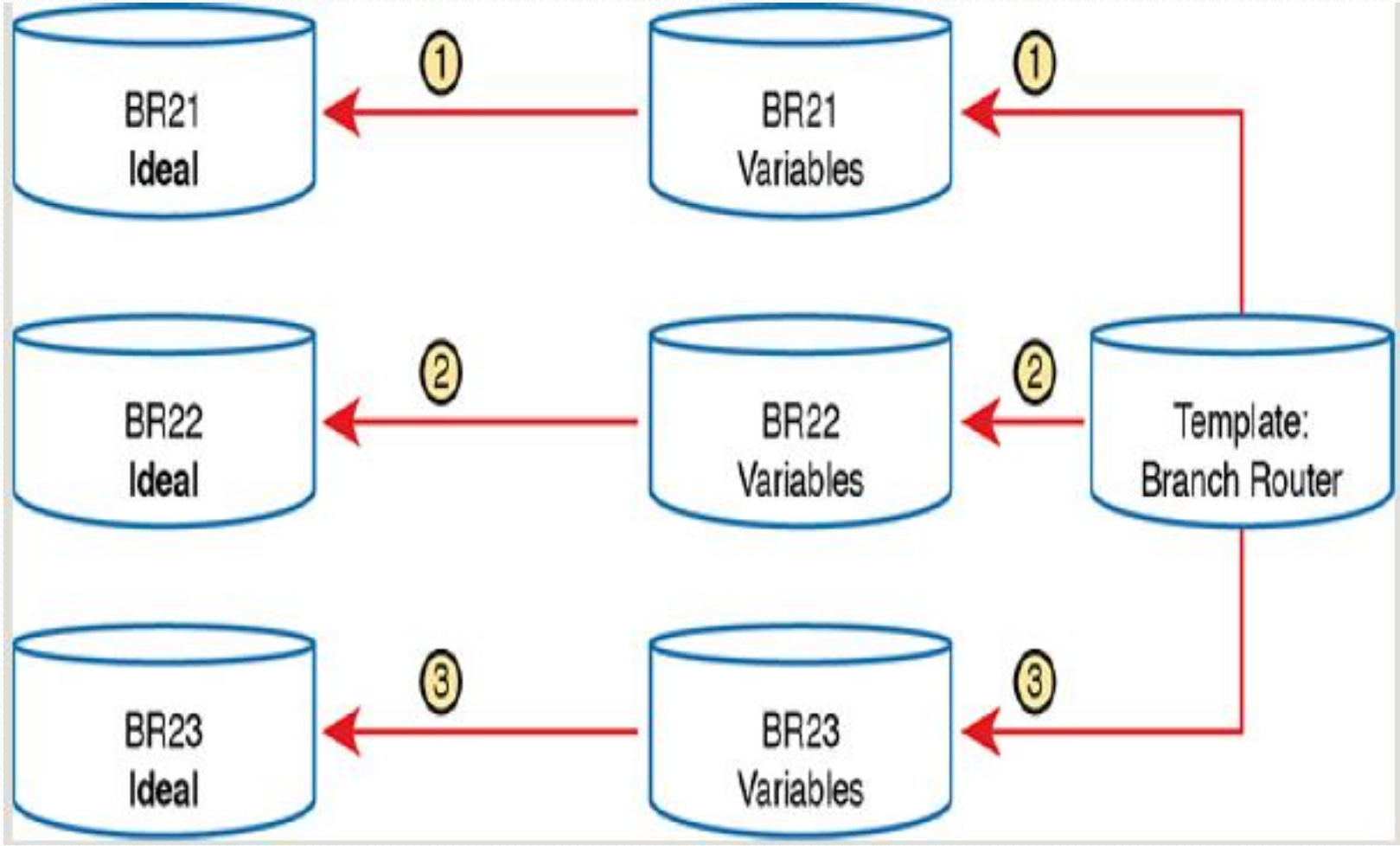
Network Automation

Why Network Automation

- Network automation is the process of automating the provisioning, orchestration, and management of network and their services.
- **Benefits of Network Automation:**
- It allows network operations to be automated, which reduces human-to-machine interaction
- It greatly reduces the chance of human error such as typos
- It can also save time and manual labor because it provides Zero Touch Provisioning (ZTP) that configures network devices automatically
- It does reduce the operational expenditures, especially for service providers and enterprises.
- It guarantees consistency in your configurations
- Next is a simple example of the templates concept in automation

```
hostname BR1
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip ospf 1 area 11
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/1/0
 ip address 10.1.12.1 255.255.255.0
 ip ospf 1 area 11
!
router ospf 1
 router-id 1.1.1.1
```

- Configuration management tools can separate the components of a configuration into the parts in common to all devices in that role (the template) versus the parts unique to any one device (the variables)



Example of Template File

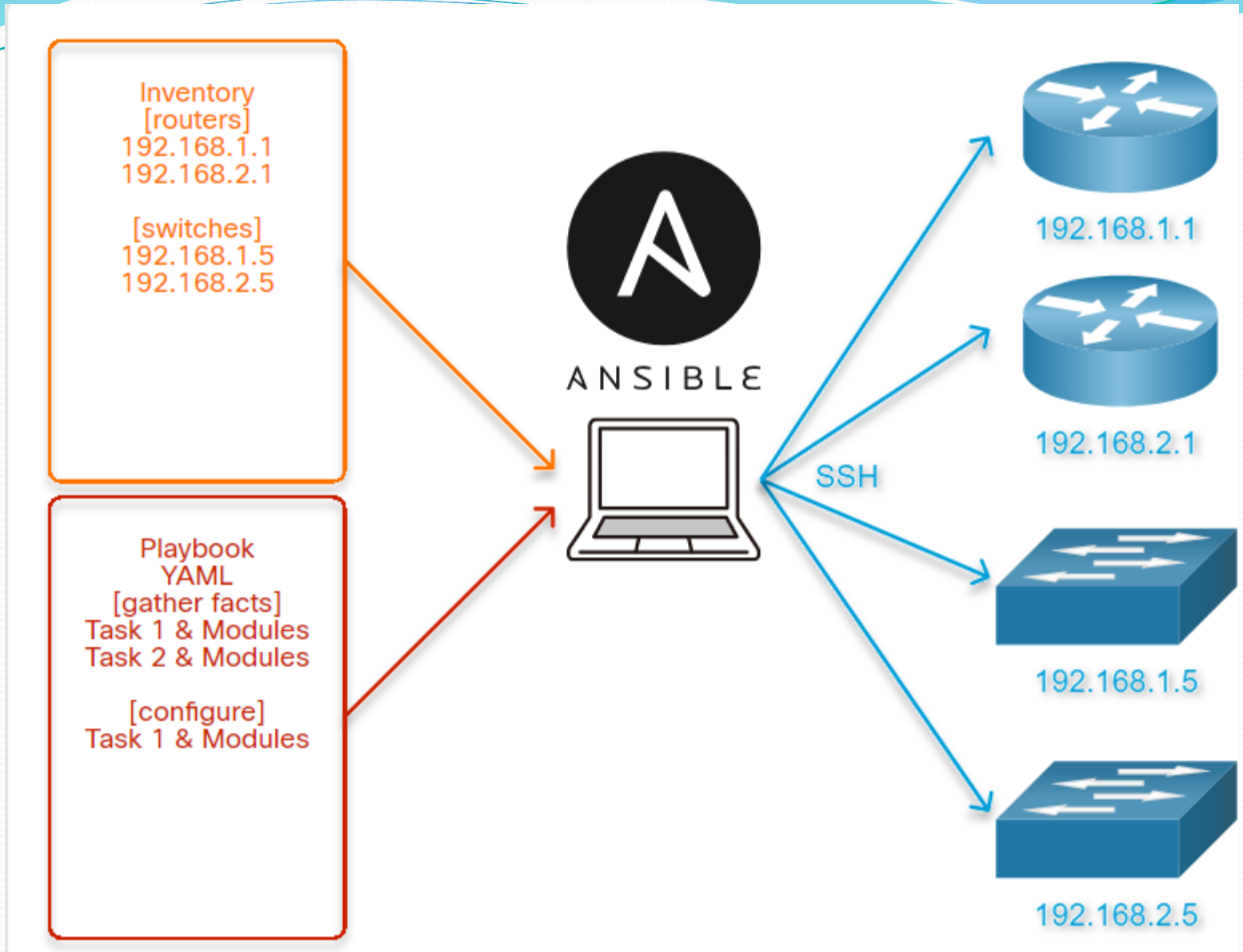
```
hostname {{hostname}}
!
interface GigabitEthernet0/0
 ip address {{address1}} {{mask1}}
 ip ospf {{OSPF_PID}} area {{area}}
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/1/0
 ip address {{address2}} {{mask2}}
 ip ospf {{OSPF_PID}} area {{area}}
!
router ospf {{OSPF_PID}}
 router-id {{RID}}
```

Network Automation Tools

- Multiple methods can be used to automate network
- Python scripts
- SDN Controllers
- Ansible
- Puppet
- Chef
- Terraform

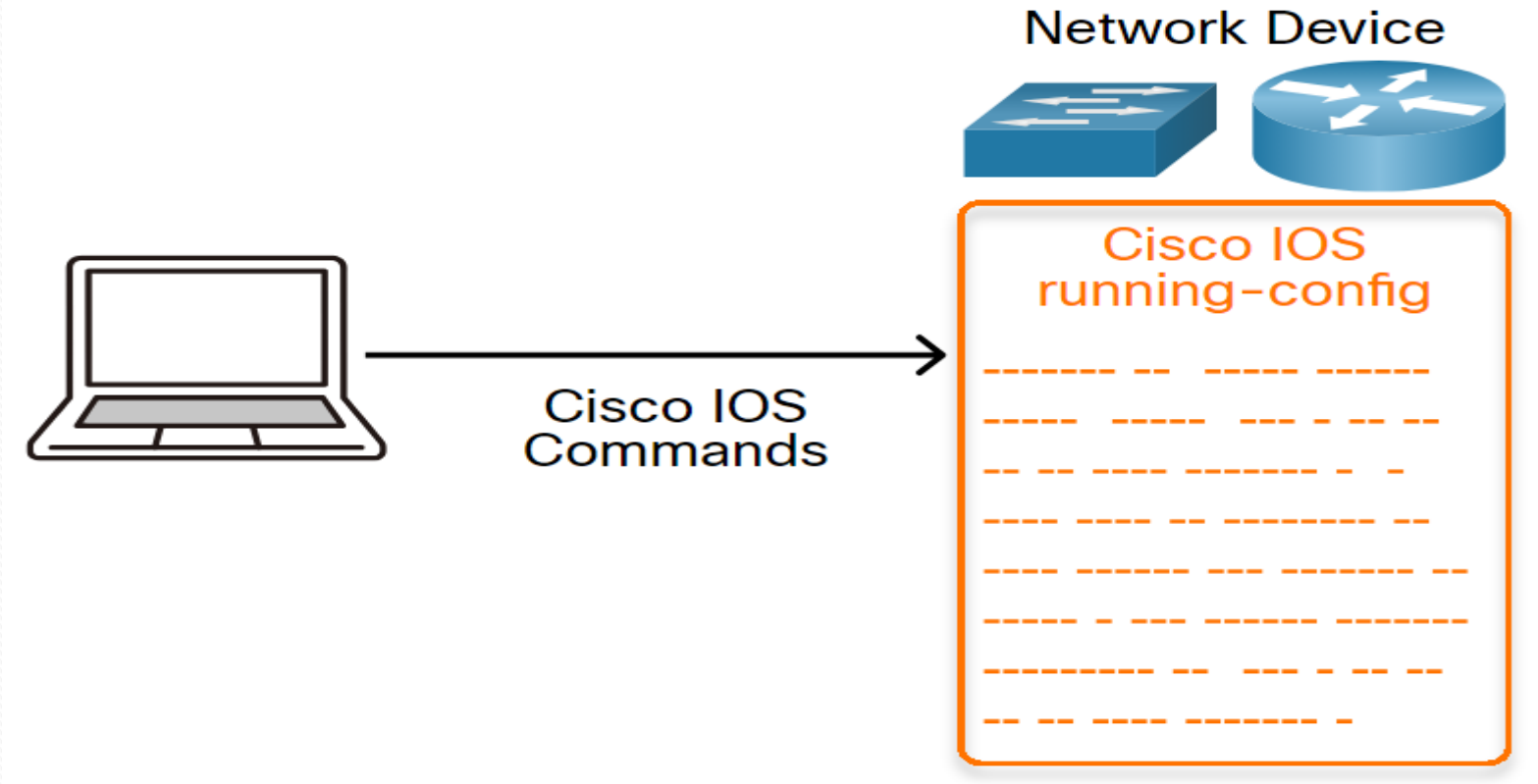
Ansible

- Ansible is considered a tool for Infrastructure as Code (IaC).
- IaC is a concept in modern IT that involves managing and provisioning infrastructure through machine-readable definition files, rather than physical hardware configuration or interactive configuration commands or tools.
- Ansible allows you to define and manage your network and IT infrastructure through code, using simple, human-readable playbooks.
- Ansible is an open-source automation tool that uses a simple, human-readable language called YAML to describe automation tasks.
- Ansible operates in an agentless manner, which means it does not require any specialized software installed on the managed devices.
- This allows Ansible to operate through standard protocols like SSH.

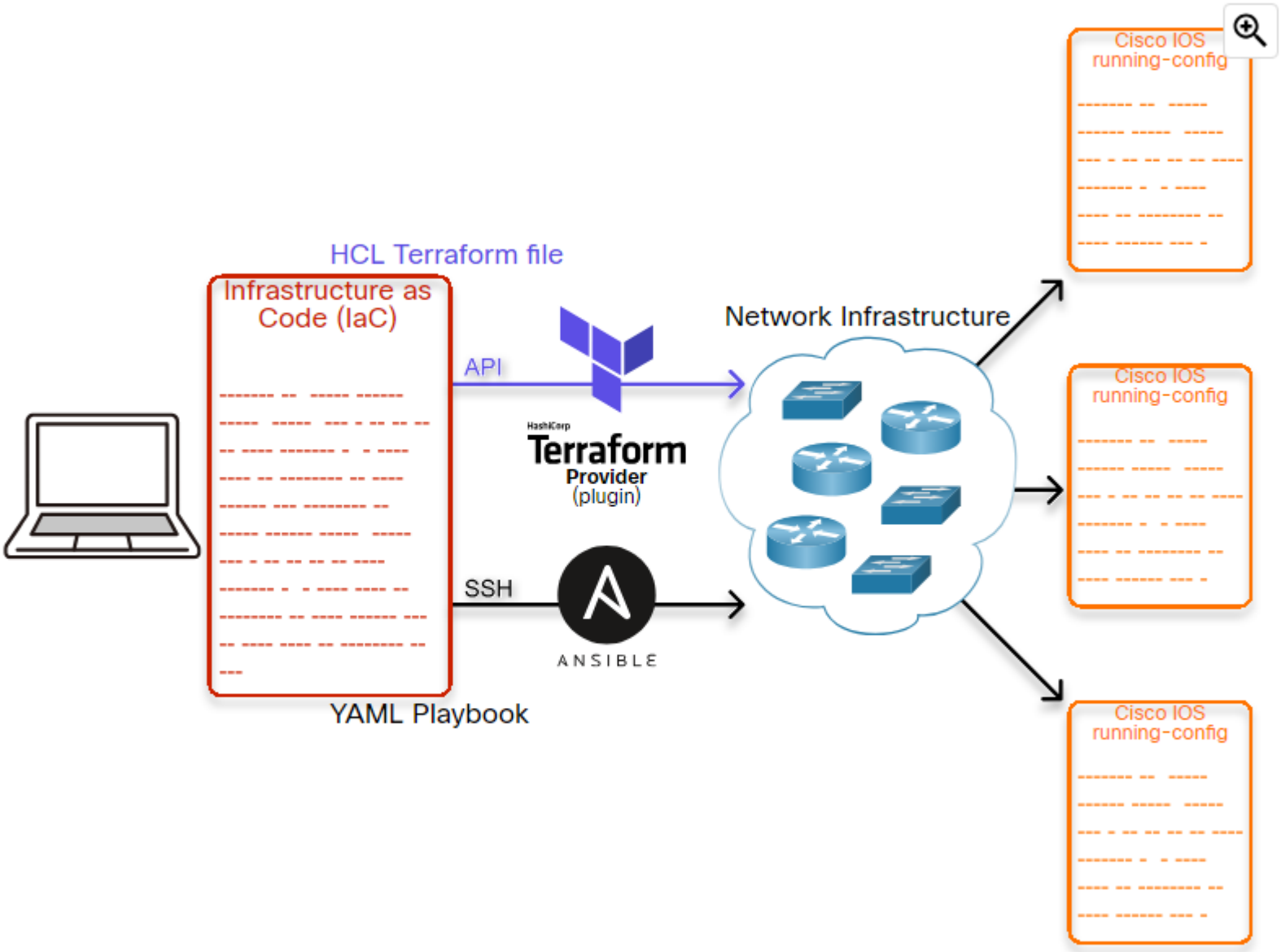

Inventory
[routers]
192.168.1.1
192.168.2.1
[switches]
192.168.1.5
192.168.2.5
Playbook
YAML
[gather facts]
Task 1 & Modules
Task 2 & Modules
[configure]
Task 1 & Modules
ANSIBLE
SSH
192.168.1.1
192.168.2.1
192.168.1.5
192.168.2.5

Infrastructure as a Code (IaC)

- Traditionally, network administrators have used CLI (command line interface) commands to configure Cisco IOS devices. These commands are added to the running-configuration file of the network device, as shown in the figure.

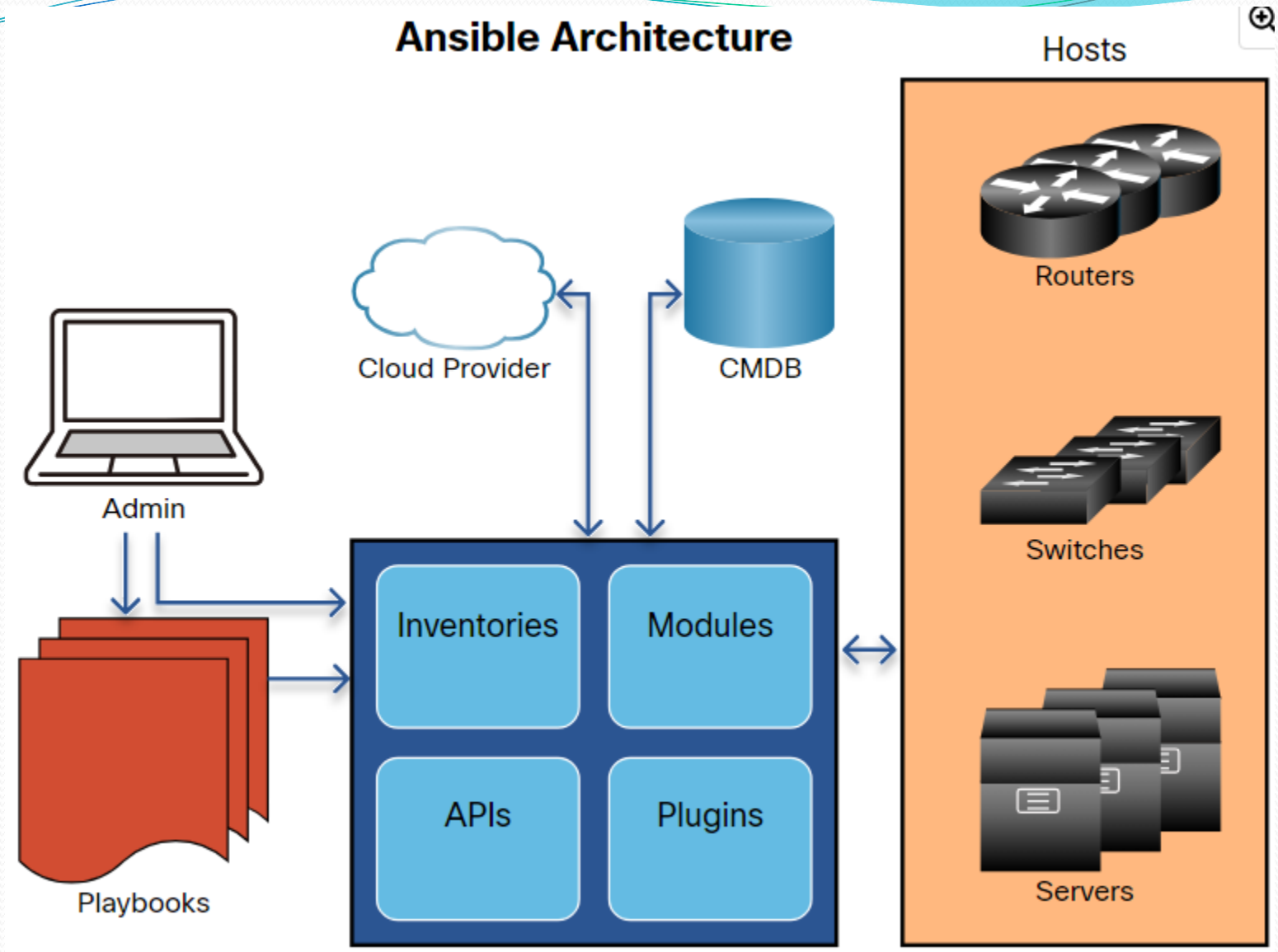


- Now, imagine being able to create a similar configuration file that can also be used to automatically set up, modify, and manage not just one device, but an entire network infrastructure including servers, routers, switches, and even cloud resources.
- Infrastructure as Code (IaC) enables administrators to do so.
- IaC uses machine-readable definition files to automatically provision and manage all the components of an infrastructure across multiple environments
- **Ansible** uses **YAML** for its playbook format, which is very human-readable and easy to understand, organizing tasks in a simple list format.
- **Terraform** uses its own **HashiCorp Configuration Language (HCL)**, which is also designed to be human-readable. However, it is specifically structured to provision infrastructure components.


HCL Terraform file
Infrastructure as Code (IaC)
API
HashiCorp
Terraform
Provider
(plugin)
Network Infrastructure
Cisco IOS running-config
Cisco IOS running-config
Cisco IOS running-config
SSH
ANSIBLE
YAML Playbook

Ansible Architecture

- Ansible main components are:
- **Playbook:** written in YAML, the playbook defines a series of tasks to automate, such as configuring a network device. It includes Plays, which contain the variables, roles and an ordered lists of tasks.
- **Modules:** These are the building blocks of tasks included in the playbook, providing specific functions like executing commands or configuring interfaces on Cisco IOS devices.
- **Inventories:** These files list the devices you want to manage, including their IP addresses and connection details.


Ansible Architecture
Hosts
Routers
Switches
Servers
Cloud Provider
CMDB
Admin
Inventories
Modules
APIs
Plugins
Playbooks

Ansible Playbook Example in a file (display_ipv4_addresses.yml)

```
- name: Show IP Interface Brief on Cisco IOS routers
  hosts: switches
  gather_facts: no
  tasks:
    - name: Run 'show ip interface brief' command
      ios_command:
        commands:
          - show ip interface brief
      register: output

    - name: Display command output
      debug:
        var: output.stdout
```

- In the previous example ios_command and debug are examples of **modules.**
- **ios_command:** executes single or multiple ios show commands
- **debug:** display variable output

Inventory file named hosts

- [cisco_routers]
- 192.168.25.151 ansible_connection=network_cli ansible_network_os=ios ansible_user=admin ansible_password=cisco ansible_become=yes ansible_become_method=enable ansible_become_password=cisco

- 192.168.25.152 ansible_connection=network_cli ansible_network_os=ios ansible_user=admin ansible_password=cisco ansible_become=yes ansible_become_method=enable ansible_become_password=cisco

Argument	Description	Example
ansible_connection	Specifies the type of connection Ansible should use to communicate with the devices.	Common value for networking devices using SSH: **network_cli**
ansible_network_os	Indicates the network operating system running on the devices.	Common value for Cisco IOS devices: **ios**
ansible_user	The username used to log in to the devices via SSH.	Example: **admin**
ansible_password	The password for the SSH user to log in to the devices.	Example: **C1$c0$$hp@$$w0rd**
ansible_become	Indicates whether privilege escalation is needed to perform certain tasks.	Common Value: **yes**
ansible_become_method	Specifies the method for privilege escalation	Common Value for Cisco Devices to enter privileged EXEC mode: **enable**
ansible_become_password	The password required to enter enable mode on the devices.	Example: **C1$c0pr1vp@$$w0rd**

Execute Ansible on Linux Machine

- ansible-playbook -i hosts display_ipv4_addresses.yml

- where:
- hosts is the inventory file
- display_ipv4_addresses.yml is the playbook file

Output Example

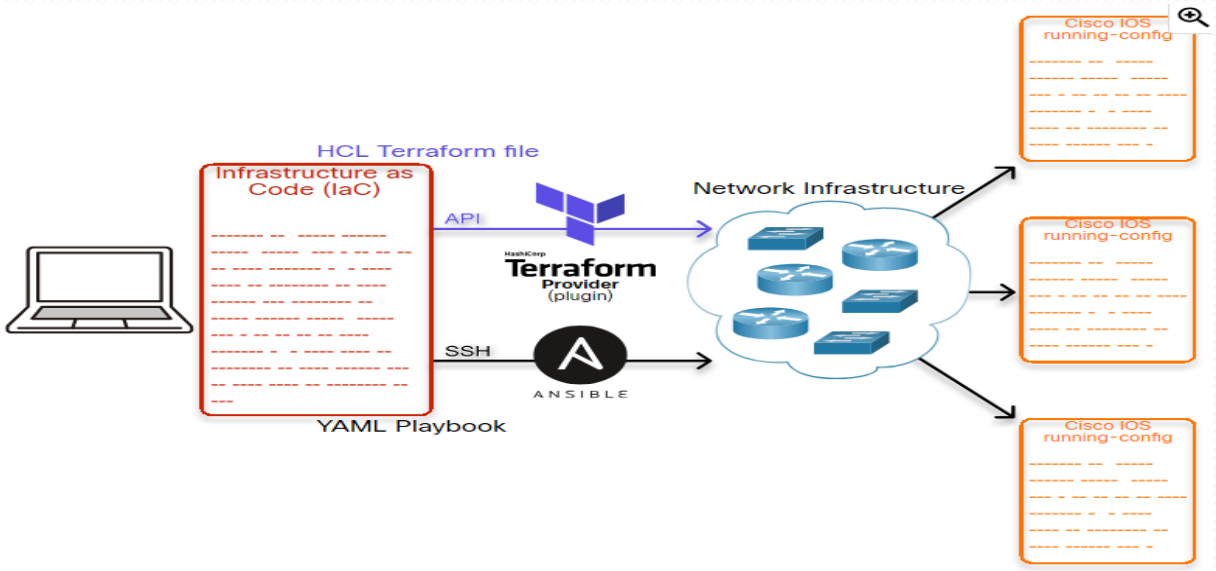
```
PLAY [Show IP Interface Brief on Cisco IOS routers] ****************************

TASK [Run 'show ip interface brief' command] ***********************************
ok: [192.168.1.1]
ok: [192.168.2.1]

TASK [Display command output] **************************************************
ok: [192.168.1.1] => {
    "output.stdout": [
        "Interface              IP-Address   OK? Method Status                Protocol",
        "GigabitEthernet0/0   192.168.1.1  YES manual up                    up",
        "GigabitEthernet0/1   unassigned   YES unset  administratively down down"
    ]
}
ok: [192.168.2.1] => {
    "output.stdout": [
        "Interface              IP-Address   OK? Method Status                Protocol",
        "GigabitEthernet0/0   192.168.2.1  YES manual up                    up",
        "GigabitEthernet0/1   192.168.1.2  YES manual up                    up"
    ]
}

PLAY RECAP *********************************************************************
192.168.1.1                : ok=2    changed=0    unreachable=0    failed=0
```

Terraform

- Terraform, like Ansible, is a tool for Infrastructure as Code (IaC).
- It automates the setup and management of networking resources, such as routers, switches, and firewalls, in both on-premises and cloud environments. Using Terraform ensures consistent and repeatable network configurations.
- This aligns with modern DevOps practices, which emphasize automation and monitoring in software and infrastructure management.
- Terraform Uses HCL (HashiCorp Configuration Language) compared to Ansible that uses YAML.

Terraform Architecutre

- Ansible and Terraform are both IaC with different methods for managing infrastructure, as shown in the figure. Ansible uses SSH to directly access devices. In contrast, Terraform uses providers, which are plugins that interact with devices through APIs like RESTCONF or NETCONF.



- A Terraform provider is essentially a plugin that allows Terraform to interact with different technologies. For example, Cisco offers several Terraform providers to configure devices.
- Like a plugin, a Terraform provider is software that adds specific features to an existing computer program, enhancing its capabilities without modifying the core application.
- The Terraform provider enables Terraform to communicate with and manage technologies through their specific APIs.
- The Terraform provider translates Terraform configurations written in HashCorp Configuration Language (HCL) into commands that specific technologies, like a Cisco router or a cloud service, can understand and execute

Terraform Example

```
# Assuming there is a provider that supports Cisco IOS XE RESTCONF
provider "cisco_ios_xe" {
  host     = "192.168.10.1"
  username = "admin"
  password = "adminpass"
  secure   = true  # Assuming secure implies HTTPS/RESTCONF is being used securely
}

# Resource configuration for an interface
resource "cisco_ios_xe_interface" "gigabit1" {
  name        = "GigabitEthernet1"
  description = "Uplink Interface"
  enabled     = true
}

# Output the operational status of the interface
output "interface_status" {
  value = cisco_ios_xe_interface.gigabit1.operational_status
  description = "Operational status of the GigabitEthernet1 interface."
}
```

Expected Output

- interface_status = "up"
- or
- interface_status = "down"

HCL Compared to JSON & XML

- **Human Readability:** JSON and XML are machine-friendly but can be verbose and hard for humans to write and read. HCL uses a more relaxed syntax, making it easier to write and understand. For instance, HCL does not require quotes around keys and allows comments making it easier to document the code.
- **Structure and Syntax:** HCL resembles JSON in its use of curly braces { } to define objects and square brackets [ ] for lists. However, HCL introduces resource blocks and attribute assignments, which are more straightforward than the tag-based approach of XML or the strictly quoted keys in JSON.

Configuration on the Cisco Device

- Router1> enable
- Router1# configure terminal
- Router1(config)# restconf
- Router1(config)# netconf-yang
- Router1(config)# end
- Router1# write memory

Terraform on Machine

- First Install Terraform on PC
- terraform -v
- (To check the version of the terraform)
- The project should include:
- network_automation_project/
- ├── main.tf
- ├── terraform.tfstate
- └── .terraform/
- .main.tf --> this is the main hcl code
- terraform.tfstate --> this is tracks the state of the code execution
- .terraform --> this is where plugin, module cache are stored

Terraform Run Commands

- **terraform init**
- The terraform init command initializes the Terraform working directory. It downloads the necessary provider plugins specified in the file, as shown in the example.

- **terraform plan**
- The terraform plan command creates an execution plan specifying what actions Terraform will take to achieve the desired state defined in the configuration file.

- **terraform apply**
- The terraform apply command applies the changes required to reach the desired state of the configuration. As shown in the example, It will prompt for a yes to confirm before making any changes. For automated runs, you can use the

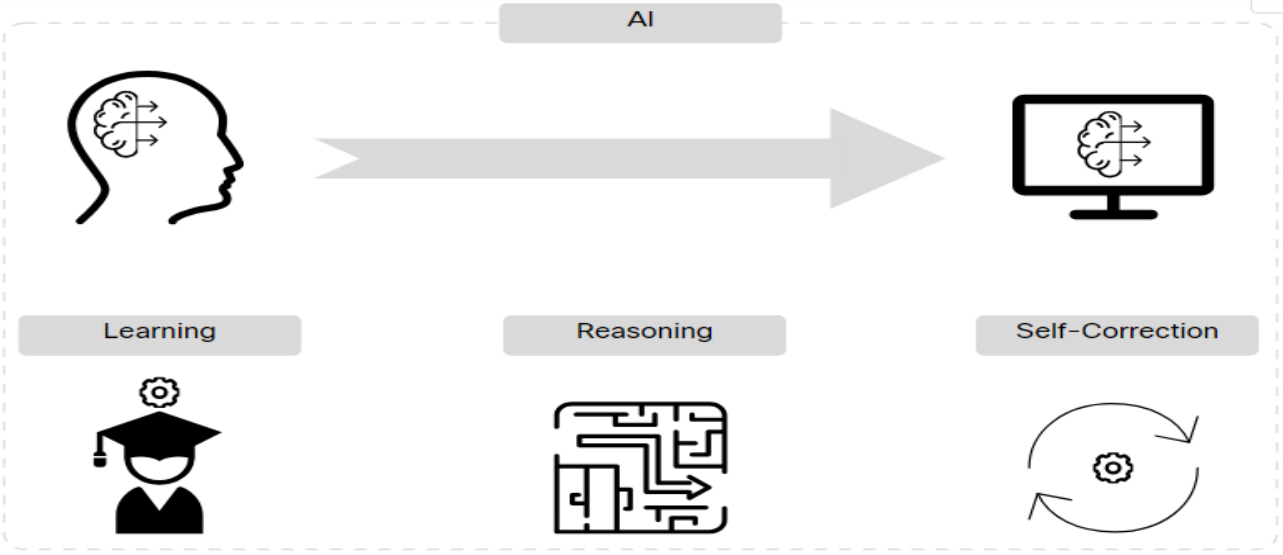
AI & ML

Introduction

- Imagine a future where machines not only assist us in mundane tasks but also engage in creative processes, predict outcomes with remarkable accuracy, and understand human language as we do. From providing recommendations on your favorite streaming service to the sophisticated chatbots that provide customer support, artificial intelligence (AI) and machine learning (ML) are transforming our world in ways we never thought possible.

Difference Between AI & Machine Learning

- Artificial Intelligence (AI) is an umbrella term that can be explained as the simulation of human intelligence by computer systems. This includes understanding language, recognizing patterns, solving complex problems, and learning from experience. These processes include learning, reasoning, and self-correction, are shown in the figure.



- **Machine Learning (ML)** is a subset of AI. ML enables machines to mimic intelligent human behavior by learning from data without being explicitly programmed. This method allows computer systems to self-improve their performance over time through data analysis and pattern recognition without explicit programming or human intervention.
- **Key Difference**
- AI without ML → Follows strict, predefined rules and logic. (Rule Based Chatbot, Medical Diagnosis Systems)
- AI with ML → Learns patterns and improves over time from data. (Spam Fliters, Fraud Detection)

The Evolution of AI

- **The Era of Rule Based AI**
- AI in strategy games like chess was dominated by rule-based systems such as IBM's Deep Blue and the open-source chess engine, Stockfish. These systems operated on hardcoded rules and decision trees, meticulously crafted from existing chess knowledge and strategies, to evaluate positions and calculate the best moves during gameplay

- **The Deep Blue Milestone**
- In 1997, Deep Blue's victory over world chess champion Garry Kasparov was a milestone for AI. It showcased a machine's ability to surpass human expertise in a highly strategic domain. Deep Blue was programmed using an immense library of chess openings, strategies, and endings, along with a brute-force algorithm to evaluate millions of positions. However, its operation was fundamentally based on human-prepared rules and decision trees. It didn't "learn" from its games but executed programmed strategies very efficiently.

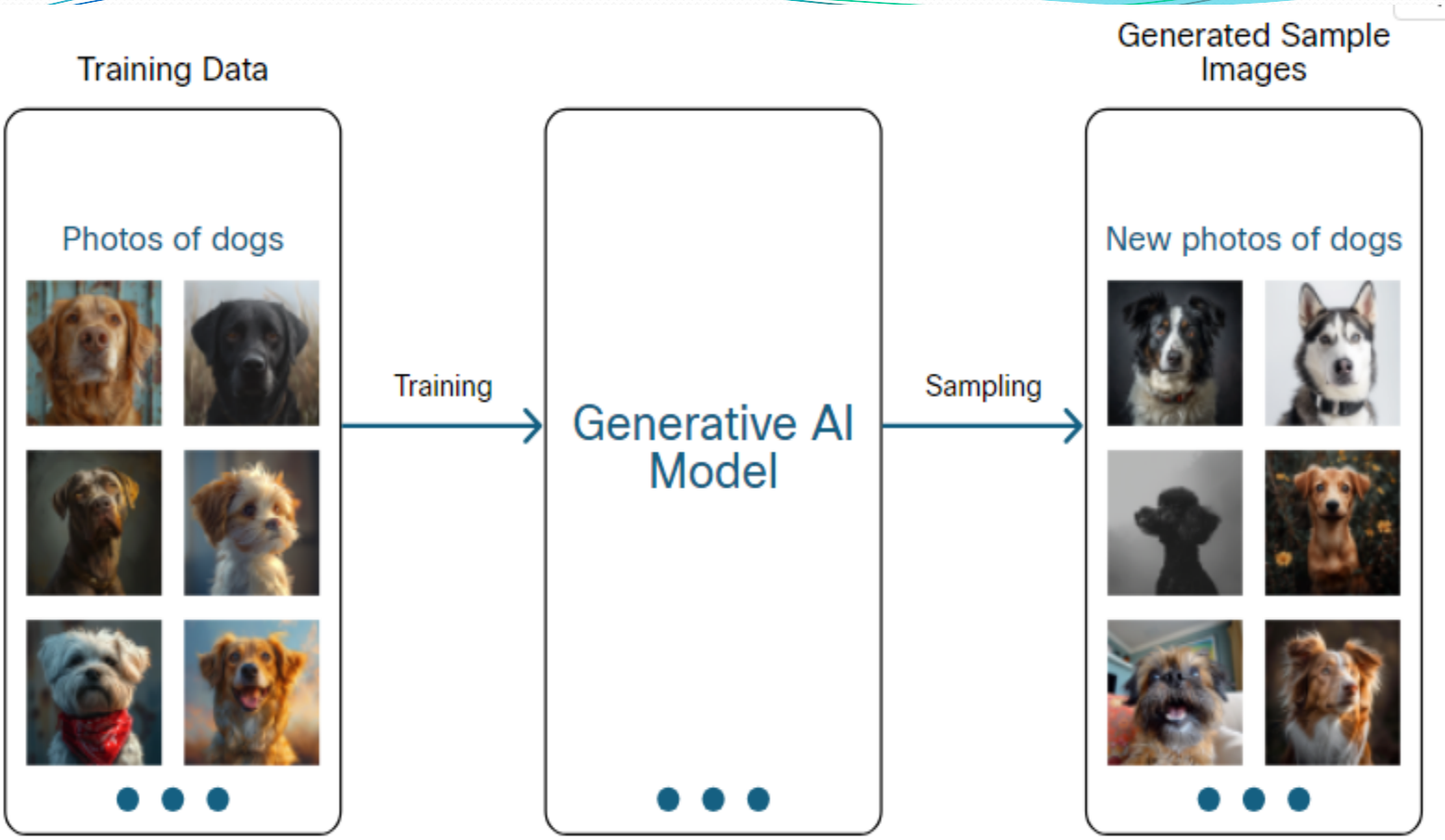
- **The Leap to Machine Learning with Alphazero**
- In 2017, Google DeepMind's AlphaZero signified a quantum leap in AI capabilities.it learned to play chess simply by playing against itself, using a reinforcement learning algorithm coupled with neural networks to recognize patterns and learn from data. This approach enabled AlphaZero to develop its own understanding of chess from scratch, free from the conventional wisdom that typically guides human and computer strategies alike.
- During its training phase, AlphaZero played millions of games against itself in a matter of hours, continuously learning and evolving its strategies

- **The match between Alphazero and Stockfish**
- The culmination of this self-training was a series of matches against Stockfish, one of the world's premier chess engines known for its computational rigor and extensive use of predefined chess strategies. In these matches, AlphaZero's dynamic learning allowed it to outmaneuver Stockfish, showcasing a more intuitive style of play. Out of 100 matches, AlphaZero won 28 games, drew 72, and lost none.

- **Implications of Alphazero's Success**
- AlphaZero's dominance over Stockfish demonstrated its superior strategic understanding and marked a significant shift in how AI could develop independent problem-solving capabilities without human input. Its success illustrated a new era where AI could discover knowledge for itself, contrasting starkly with the manual and rule-based systems of the past.
- This shift has significant implications. AlphaZero's approach can be applied to problems beyond chess, particularly in fields where the rules are not well-defined and where learning and adaptation are key.

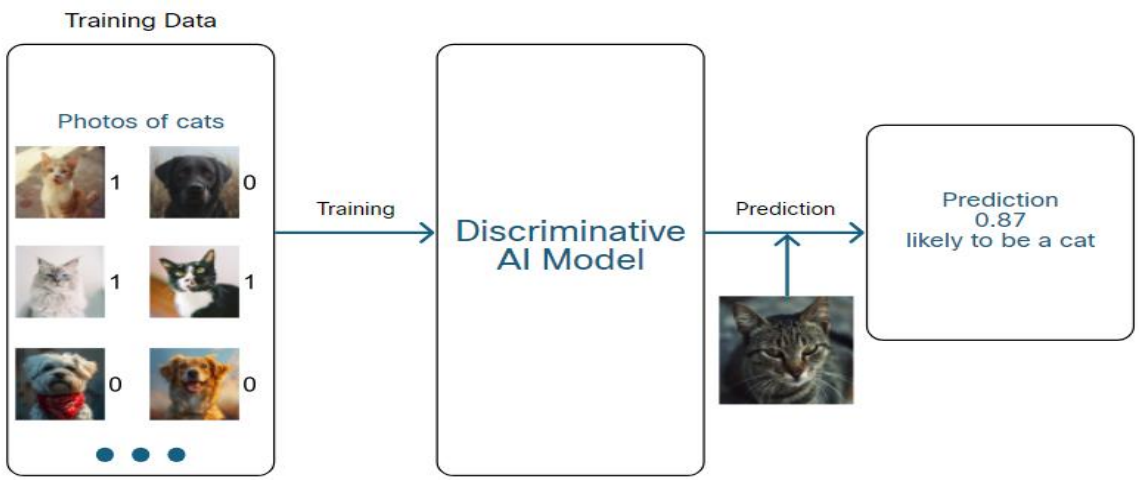
Types of AI

- **Narrow AI**
- Stockfish, Deep Blue, and AlphaZero are all examples of Narrow AI. Narrow AI focuses on executing particular tasks with high proficiency, such as winning at chess. Other examples include:
- Google Translator
- Netflix History Analysis for recommending new movies
- **Generative AI**
- Refers to artificial intelligence systems that create new content, such as text, images, music, or code, based on patterns and knowledge learned from large datasets. For example, a generative AI model trained on photos of dogs learns patterns and features from these photos. Once trained, it can generate new, realistic images of dogs, called generated sample images, as shown in the figure.

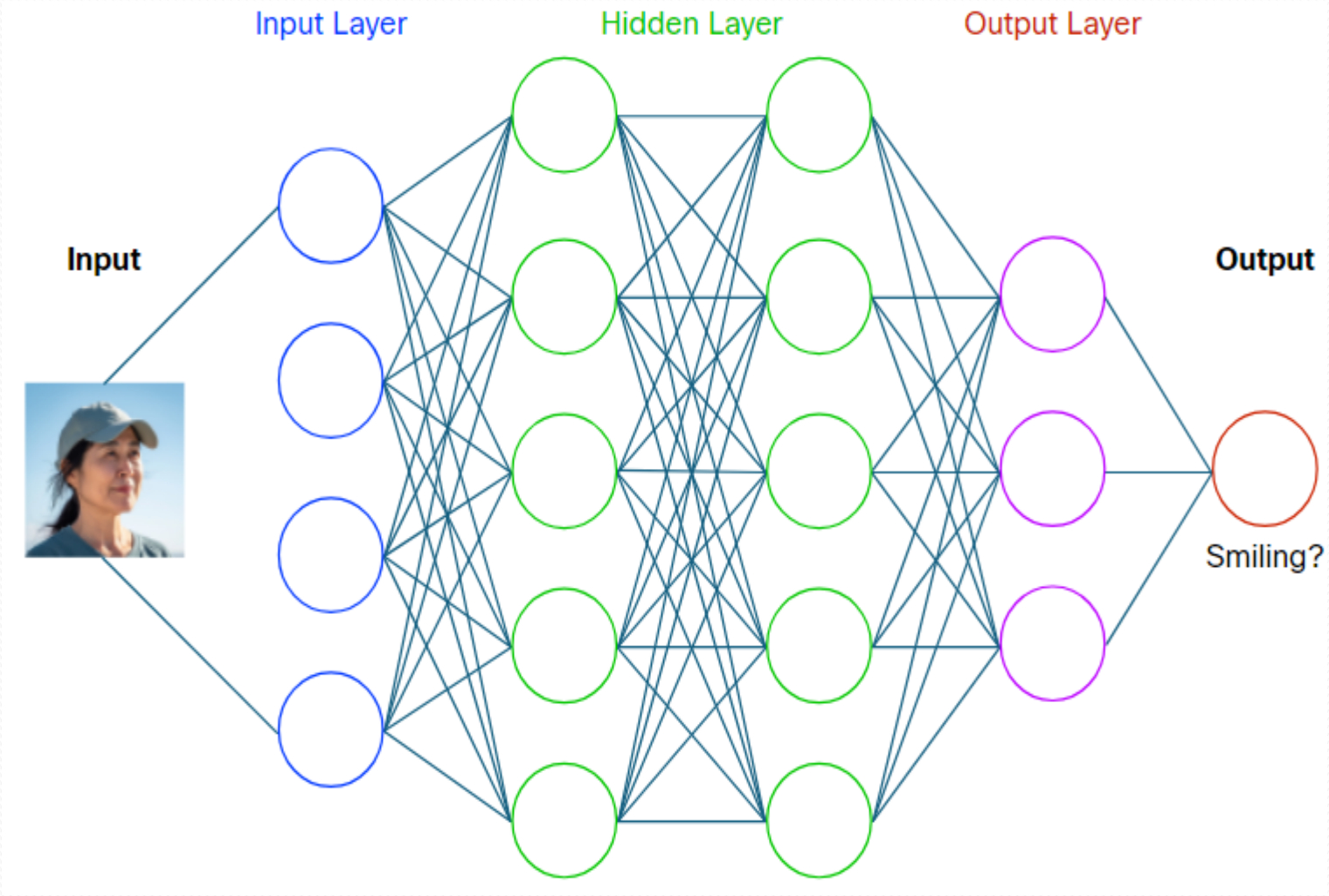

Training Data
Photos of dogs
Training
Generative AI Model
Sampling
Generated Sample Images
New photos of dogs

Discriminative AI

- On the other hand, determines the probability that a data observation belongs to a given label. It predicts how closely an observation (e.g., an image or text) matches its label based on its features. For instance, a discriminative AI model trained on labeled photos of animals uses binary classification labels (0 for not a dog and 1 for a cat). This labeled data trains the model to recognize and classify new photos accurately. When given a new photo, it predicts the probability that the photo is of a dog, such as an 87% likelihood shown in the figure.



- Generative AI creates new, original outputs similar to the original data, while discriminative AI classifies data into predefined categories. Machine learning allows these models to learn from data and improve over time without explicit programming.
- **Neural networks**, inspired by the human brain, consist of interconnected layers of nodes. The figure shows a basic neural network architecture with three types of layers: the input layer, hidden layers, and the output layer. The input layer receives the initial data, which is processed through one or more hidden layers where the network learns to detect patterns and features. The output layer then produces the final prediction or classification
- Neural networks provide the computational framework for both generative and discriminative AI models, enabling them to learn complex patterns in data for tasks ranging from data generation to classification

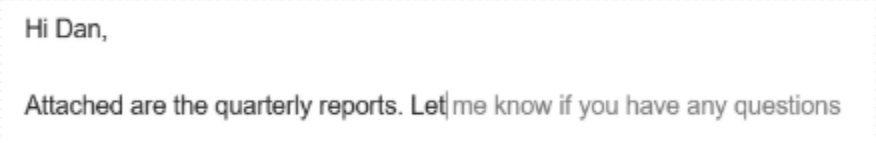

Input Layer
Hidden Layer
Output Layer
Input
Output
Smiling?

Large Language Models (LLMs)

- GPTs (Generative Pre-trained Transformers), such as ChatGPT, exemplify generative AI that uses Large Language Models (LLMs). LLMs are advanced AI systems trained on extensive text data to understand and generate human-like language. By learning language patterns, they can predict and generate coherent, contextually relevant text based on input.
- LLMs are designed to process and integrate information from multiple data types, or "modalities," such as text, images, audio, and video. By combining these data types, LLMs can perform tasks like generating images from text descriptions, interpreting visual data alongside textual information, and creating rich, contextually aware content.

Examples of LLMs Usage

- Generative AI (eg.ChatGPT)
- Gmail Smart Compose



- Smart Phone Predictive Text

- AI Generated Artwork
- Enhanced Search Capablities
- DeepFake Technology

Prompt Engineering

- An important aspect of working with generative AI today is prompt engineering. Prompt engineering involves crafting specific and strategic input prompts to optimize the AI's output.

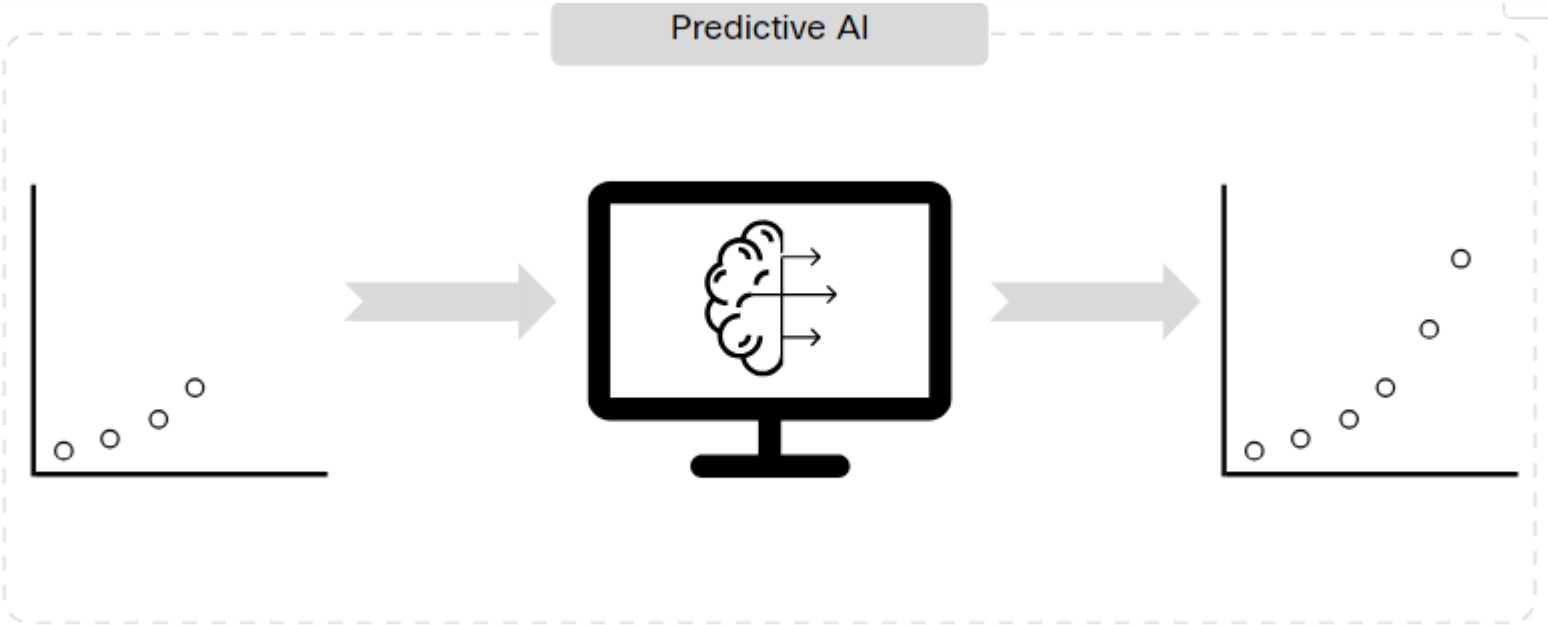
- Generic prompt: "How do I set up a trunk port?"

- Specific prompt: "Provide the Cisco IOS commands to configure a trunk port on interface GigabitEthernet1/0/48 with allowed VLANs 1, 10, 20, 30, native VLAN 888, and DTP disabled."

Descriptive and Predictive AI

- Descriptive AI and predictive AI use statistical and machine learning techniques to process and analyze data. Both aim to generate insights, but they differ in their focus on historical versus future analysis.
- **Descriptive AI:** analyzes data to describe what is happening or has happened. It focuses on understanding past and present data to provide insights and a clear picture of current or historical events. Below are examples:
- Business Intelligent Tools
- Data Analytics Tools
- Customer Relation Management (CRM) Systems
- Financial and Operational Analytics

- **Predictive AI:** refers to artificial intelligence systems designed to make predictions about future events or outcomes based on historical data. These systems use machine learning algorithms to analyze patterns and trends in data, then use this analysis to predict what will happen next. Examples of Predictive AI:
- Netflix Movies Suggestions
- Traffic Forecasting



Machine Learning

- The defining characteristic of ML is its ability to learn from data and improve performance over time without explicit programming. As a subset of AI, ML can encompass elements of narrow, descriptive, predictive, and generative AI, depending on its application.

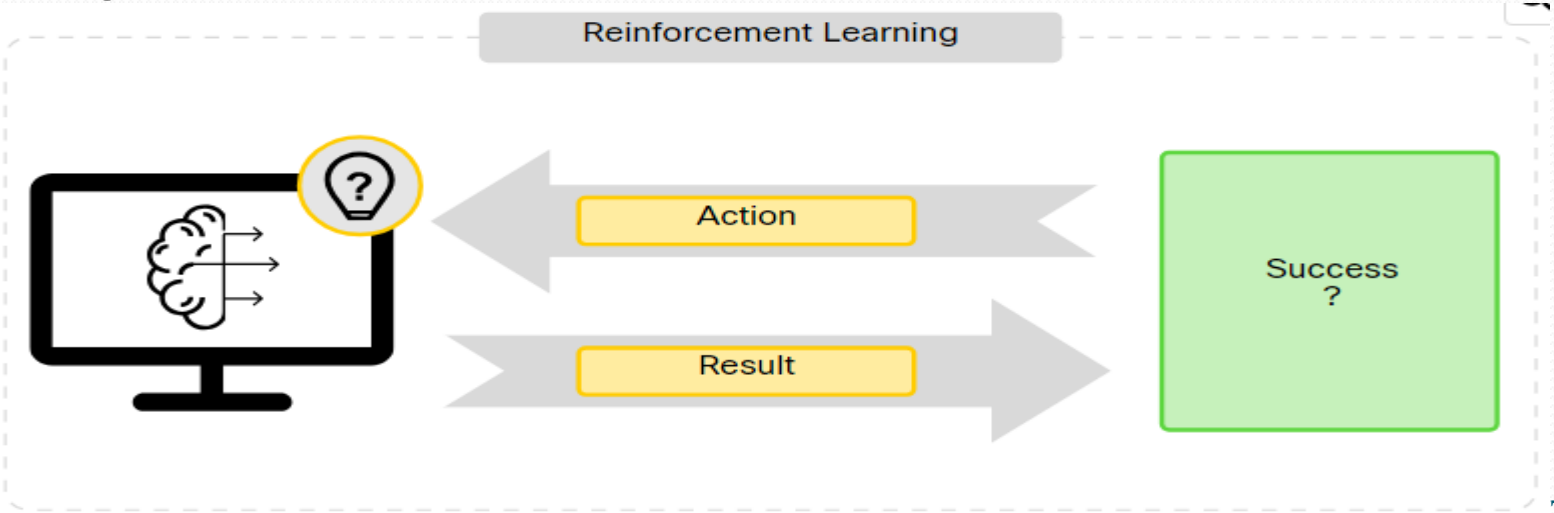
How AI Learns

- In ML, there are various approaches through which algorithms can learn and improve including **supervised**, **unsupervised**, and **reinforcement learning**. ML also uses **Retrieval-Augmented Generation (RAG)** to reduce the impact of hallucinations

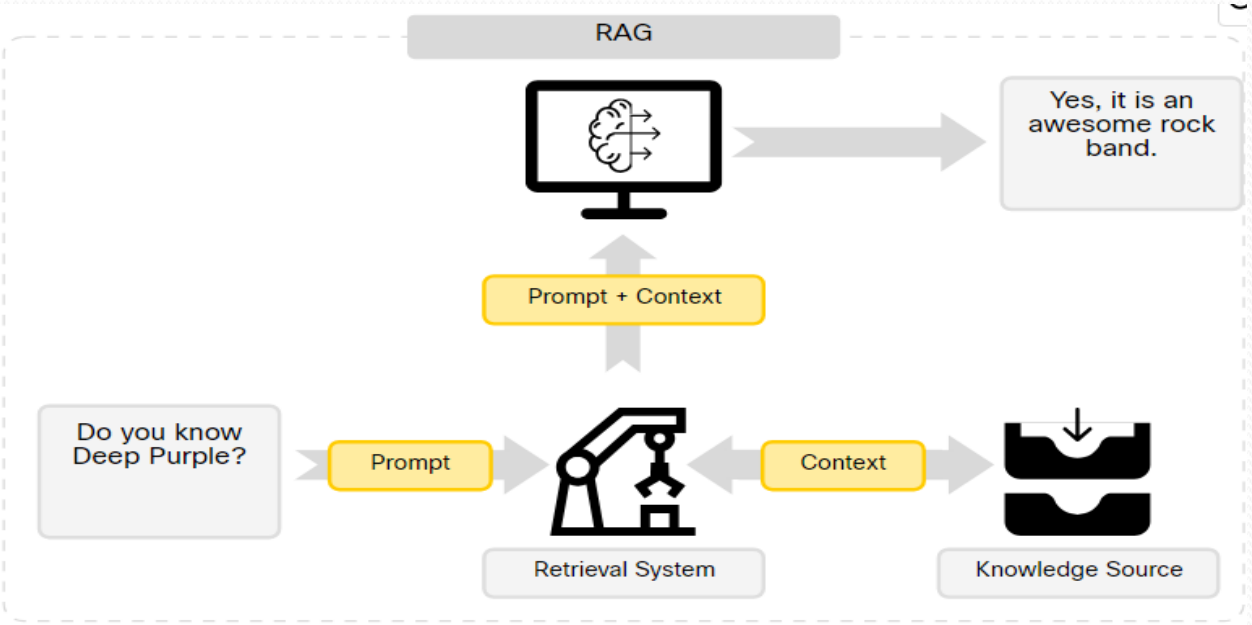
- **Supervised Leaarning:**
- For example, how do you have AI recognize a cat? One method is to teach AI to identify many different representations of its many different attributes including pointy ears, a tail, whiskers, and so one.
- To better identify an image of a cat, AI can learn by observing images labeled as cats in various situations and contexts.
- Supervised learning is a method where the AI system is trained using labeled datasets.
- In network security, supervised machine learning is utilized to categorize network traffic or predict security threats by training AI systems with datasets that have already been tagged with outcomes, such as "safe" or "malicious"

- **Unsupervised Learning:**
- Unsupervised learning does not rely on pre-labeled data. In situations where there are vast amounts of data, unsupervised learning can be used to find potentially useful insights.
- For example, video services such as Netflix capture the video habits of its large customer base. Using this information and these algorithms, it can identify customers with similar viewing habits and recommend specific movies for them to watch.
- In networking, It enables the system to spot unusual traffic patterns that deviate from what's considered normal, potentially flagging a security breach.

- **Reinforcement Learning:**
- Reinforcement learning is a type of machine learning where an agent learns to make decisions by performing actions in an environment and receiving rewards or penalties based on the outcomes. The goal is to maximize cumulative rewards over time.
- AlphaZero used reinforcement learning to teach itself chess. It played many games against itself, starting with random moves and gradually improving its strategies.Reinforcement learning is like trial-and-error learning



- **Retrieval-Augmented Generation (RAG):** is a technique that helps reduce hallucination and outdated answers in LLMs. RAG combines a retrieval system with a generative model.
- The main advantage of RAG is that it anchors the model's responses to actual content, making them more accurate and less likely to fabricate information



AI & ML Potential Issues

- Below are some of the issues associated of heavily relying on AI:
- Bias and Fairness
- Transparency and Explainability
- Data Privacy
- Dependancy and Automation Bias
- Job Displacement
- Security Risks
- Deception in AI

Security for Using GPTs

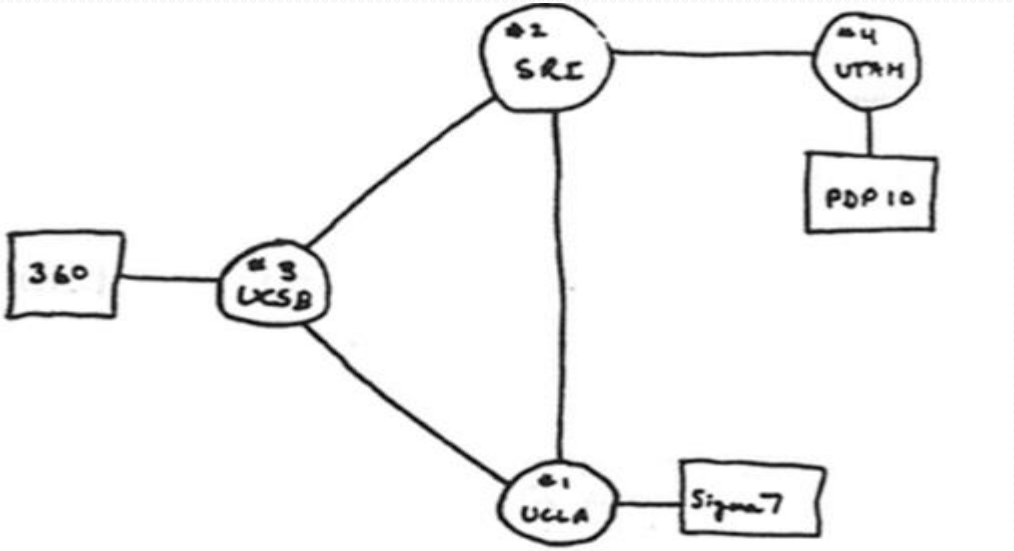
- When using a GPT, you must be vigilant about security, especially concerning the type of information shared through public and private instances of the AI. Below are common usage and practices when using GPTs:
- Public GPT Instances
- Private GPT Instances
- Be carefult with prompts found Publicly
- Strengthen GPT Security

Ethics in AI

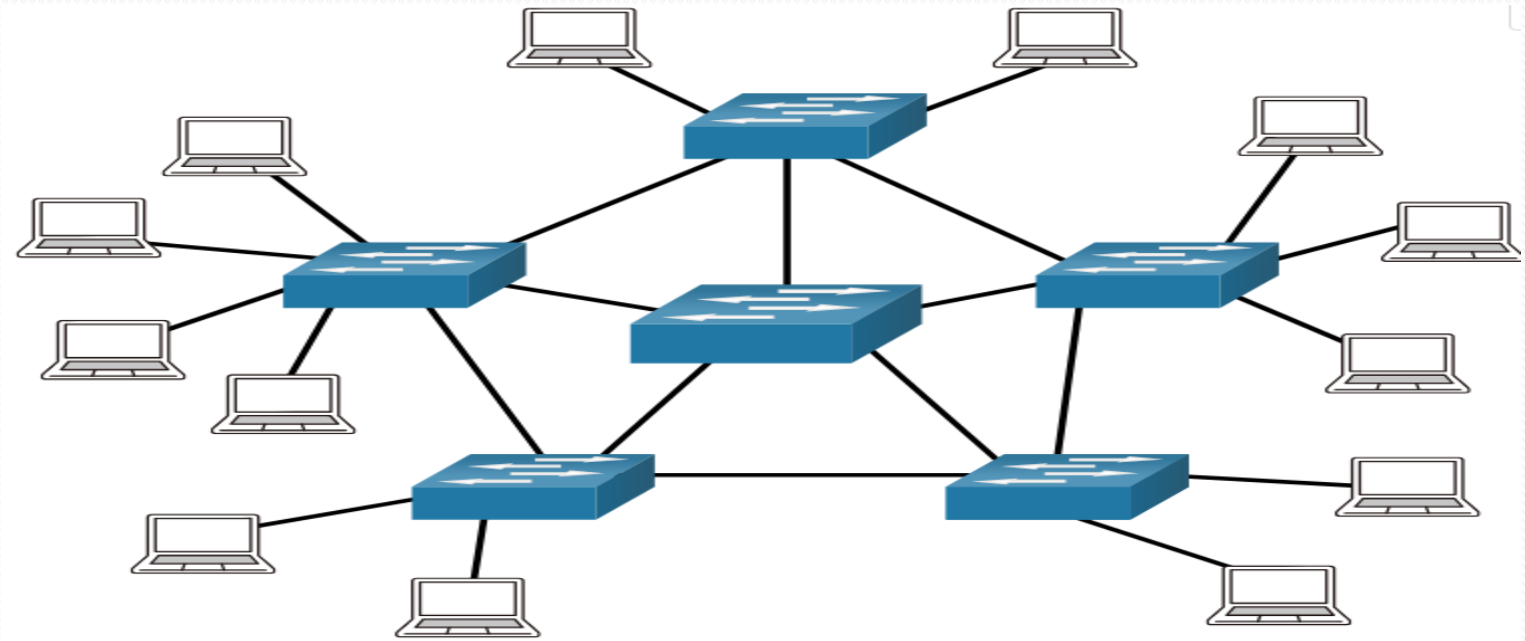
- In recent years, leading AI researchers, tech executives, and global organizations have increasingly emphasized the need for ethical frameworks and regulatory measures to manage the potential risks posed by unregulated artificial intelligence.
- In May 2023, over 350 leading AI researchers and top executives signed a 23-word Statement on AI Risk:
- **"Mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war."**
- In 2024, Cisco Systems, along with Microsoft, IBM, and other major technology companies, signed the "Rome Call for AI Ethics," facilitated by the Vatican. By endorsing this document, Cisco has committed to principles prioritizing human dignity, transparency, impartiality, and security in AI applications

Evolution of Networking

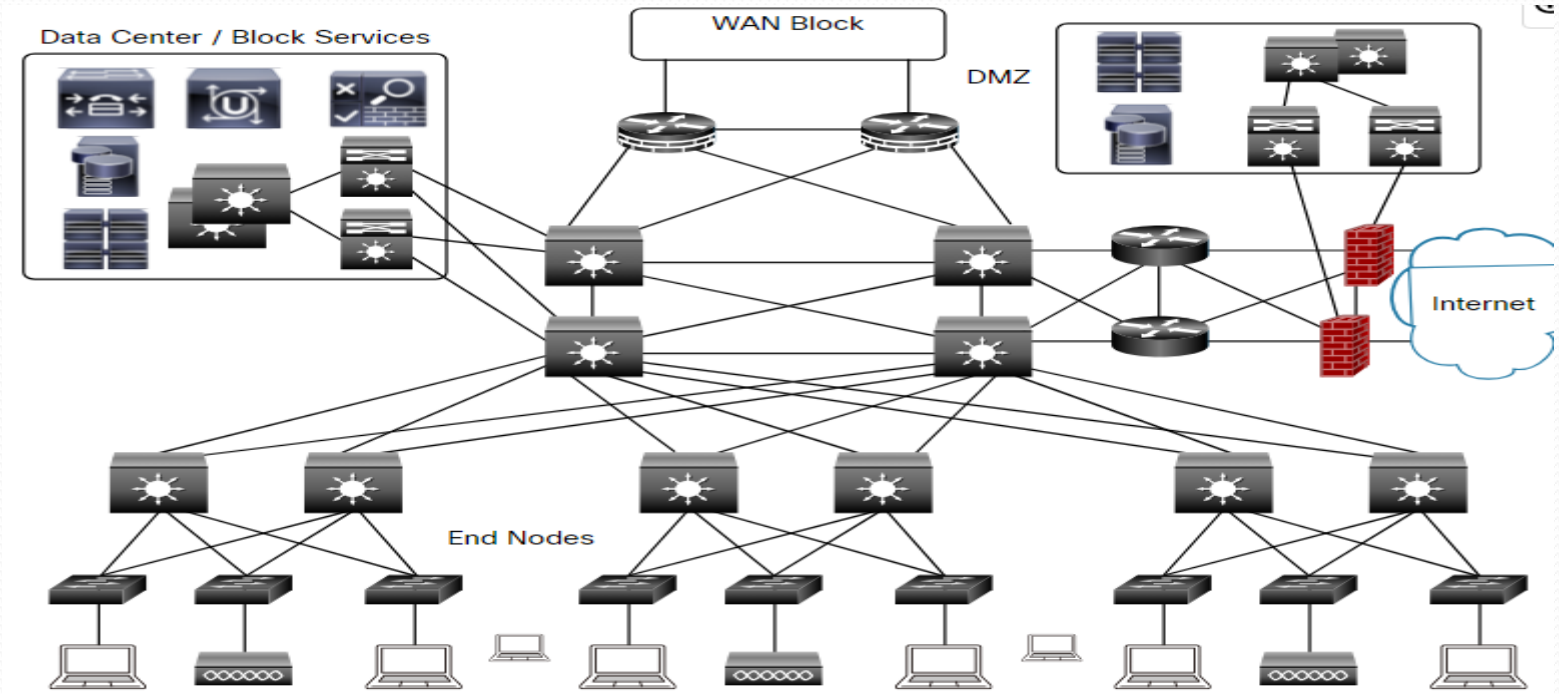
- **1950 to 1980:** The goal was to connect mainframe computers over leased telephone lines. This effort led to the creation of ARPANET, which on October 29, 1969, linked four university computers at UCLA, Stanford Research Institute (SRI), UC Santa Barbara (UCSB), and the University of Utah



- **1980 to 2000** The 1980s saw the rise of Local Area Networks (LANs), initially using coaxial cables and Ethernet hubs. These hubs broadcast data to all devices on the network, causing collisions and limited performance. The introduction of Ethernet switches, which direct data only to the intended recipient, reduced traffic and increased efficiency.

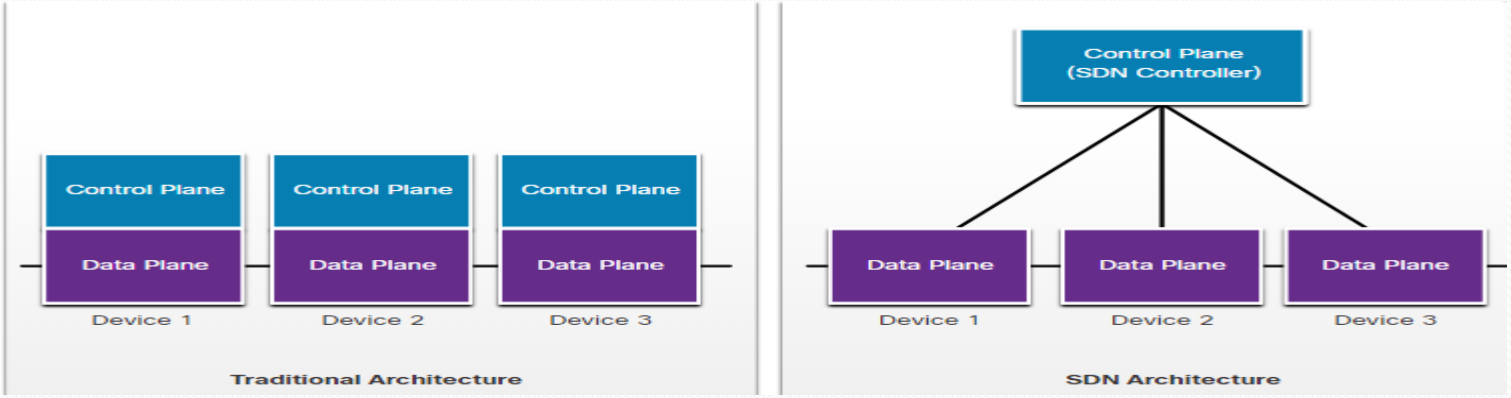


- **2000 to 2010** Networks expanded from simple connections of a few switches and routers to complex infrastructures with numerous devices and connections across multiple locations, as shown in the figure. This growth required complex routing schemes and configurations, traditionally managed manually.



The Evolution of SDN

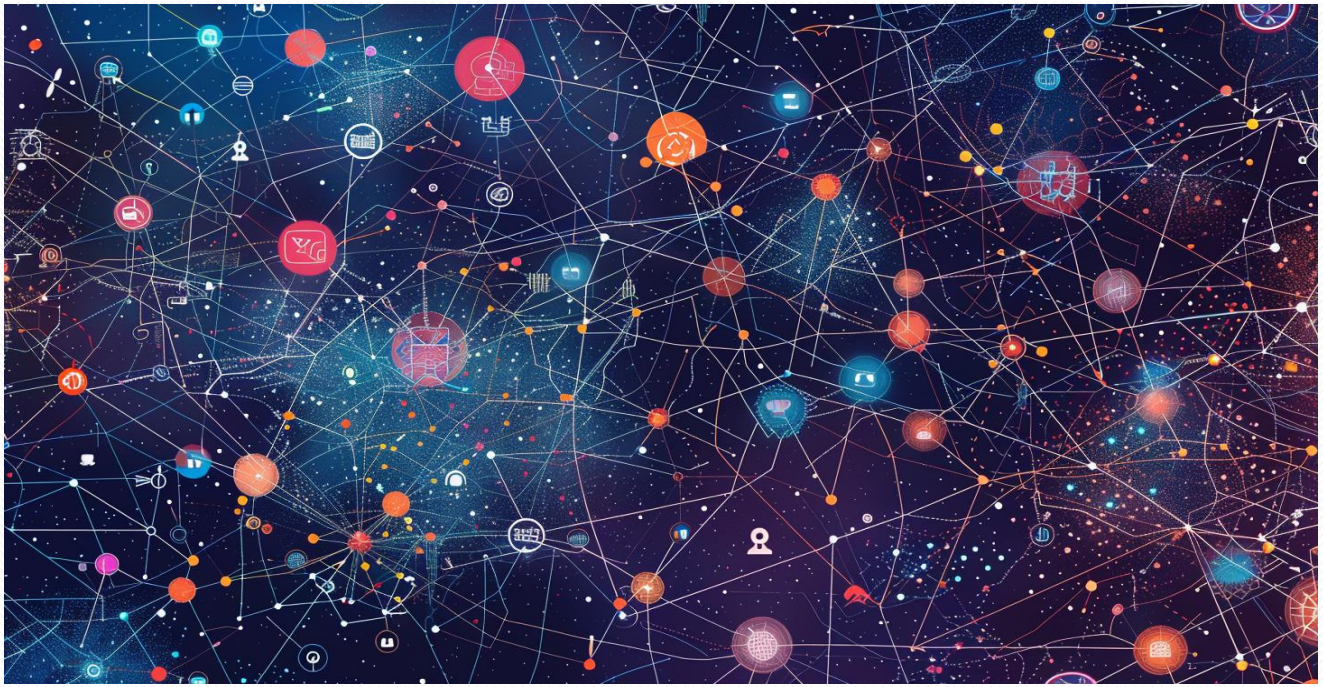
- The sheer scale of modern networks made it clear that a new approach was needed to manage and configure these vast systems more efficiently. This necessity paved the way for the development of Software-Defined Networking (SDN). Around 2010, SDN emerged as a paradigm shift, decoupling the network control (the intelligence of where to send data) from the network forwarding (the actual process of sending the data), as shown in the figure



From SDN to IBN and AI

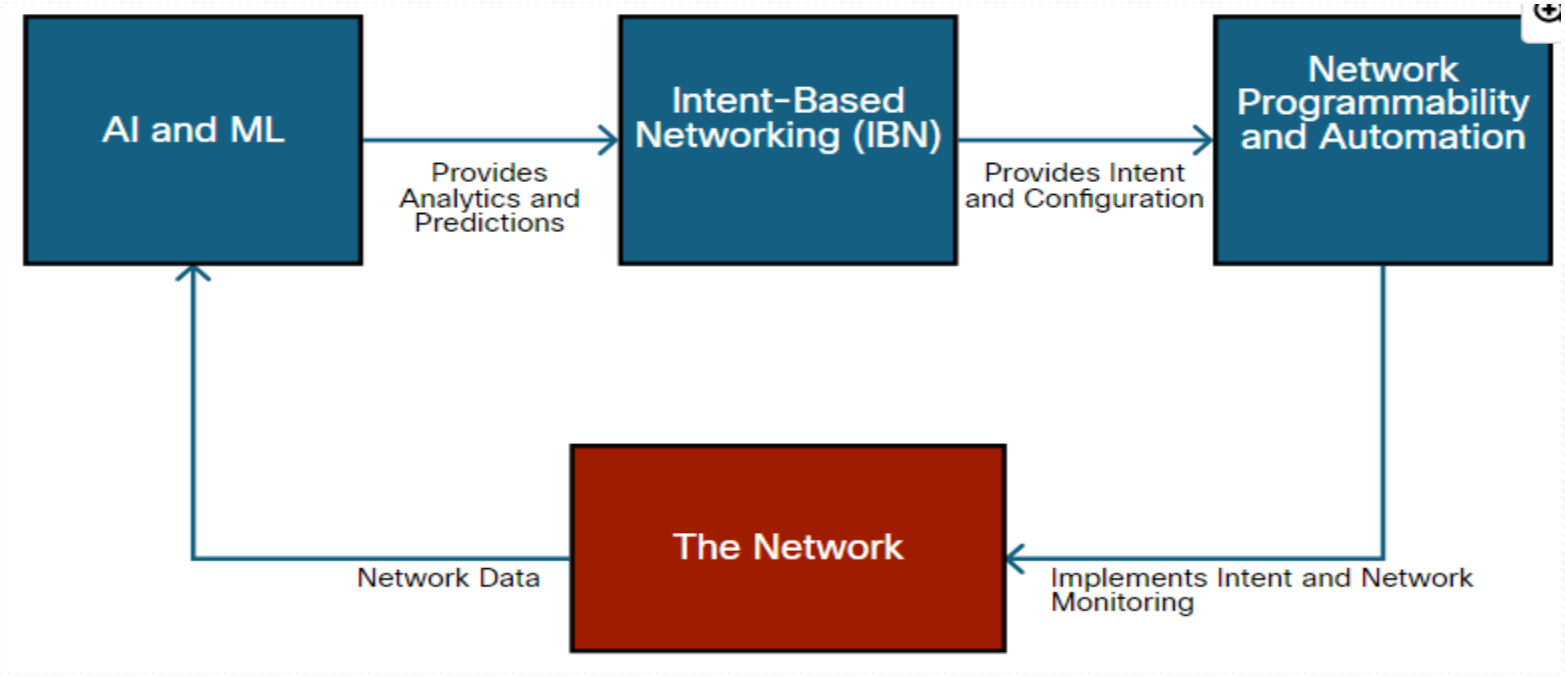
- **IBN (Intent Based Networking)** shifted the focus from managing individual network elements to expressing the desired state of the network through high-level policies and intents.
- This approach allows network engineers to define what they want the network to achieve, and the IBN system translates these intents into the necessary configurations automatically.
- IBN and AI are closely related because AI enhances the capabilities of IBN systems. AI provides the analytics and learning capabilities necessary to automate complex decision-making processes.

- For example, AI can analyze historical data to predict network behavior and adjust configurations automatically to optimize performance or prevent issues.



The Role of Network Automation and Programmability in AI

- Network automation and programmability are fundamental aspects that complement the functionalities of IBN and AI in modern networks. In the figure, the flowchart illustrates the interaction between various components in a network with AI and IBN enabled.



AI & ML in Networking

The Importance of Explainable AI

- **Black Box AI** models operate without showing their internal workings or logic to the user. AlphaZero is an example of this; it makes decisions that are not clear to the user.
- **Explainable AI (XAI)** aims to make AI processes and decisions clear and understandable to humans. It ensures transparency and trust in AI decisions, allowing professionals to understand and validate the AI's reasoning.
- Below are Fields that XAI is Crucial:
- Healthcare
- Autonomus Vehicles
- Justice Systems
- Job Application Reviews
- Networking

AI in Network Management

- AI transforms network management by automating key functions, improving efficiency, and reducing human error. Below are the functions can be managed by AI:
- Network Planning
- Automated Configuration and Management
- Predictive Maintenance
- Remedation
- Fault Monitoring and Troubleshooting
- Root Cause Analysis

AI in Network Optimization

- AI is revolutionizing network optimization by improving traffic analysis, reliability, and resource use. It analyzes traffic patterns to predict congestion, routes data to reduce latency, and identifies potential failures for continuous service. This dynamic adaptation ensures optimal performance in modern digital communications. AI will mainly help in the following:
- Traffic Analysis and Management
- Enhancing Reliability
- Maximizing Resouce Utilization

AI in Network Security

- AI plays a crucial role in network security by using advanced machine learning models to protect against cyber threats. By learning from network data and user behavior, AI can identify potential security incidents, providing a dynamic defense that adapts to evolving threats. Below are examples of Security Aspects that can use AI:
- Access Control
- Anomaly Detection and Security
- Anti-malware Systems
- Firewalls

LLMs have their limitations

- LLMs like ChatGPT are great at processing and generating text. However, they may not solve complex network problems that need real-time data analysis and predictive modeling.
- Cisco's AI/ML systems, integrated into their products, are more effective for these tasks. Cisco's AIOps solutions, designed for network engineering, offer advanced features like predictive maintenance, in-depth anomaly detection, and dynamic traffic management.