Network Design Training Course

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

Itarun Pitimon Ph.D.
ipv9@duck.com

https://ipv9.me/JEw

My profile

- Chief Technical Advisor: Somapa Information Technology PCL.
- Advisory of ARIT, RMUTP
- Assistant Professor: Computer Engineering Dept., RMUTT. (Retire)

https://youtube.com/@ipv9
https://github.com/pitimon

https://ipv9.me/JEw

Agenda

https://ipv9.me/JEw

1st Day:

- แนะนำระบบเครือข่าย (Introduction to Networking)
- OSI and TCP/IP Protocol Fundamental
- Switch Architecture, Operation, Configure and Management
- Lab:
  - Ethernet Switch basic configure
  - Allied Telesis switch configure

2nd Day:

- Ethernet Frame Format
- Configuring VLANs and Trunking
- Spanning Tree Protocol (STP), Link Aggregation Control Protocol (LACP) and switch Security
- การบรรยายเทคโนโลยีภาพรวมผลิตภัณฑ์และโซลูชันของ Allied Telesis
- Lab:
  - Vlan and Trunking , Port Security
  - AMF for Allied Telesis

Introduction to Networking

Session I

Network Components

Host Roles

Every computer on a network is called a host or end device.

Servers are computers that provide information to end devices:

- email servers
- web servers
- file server

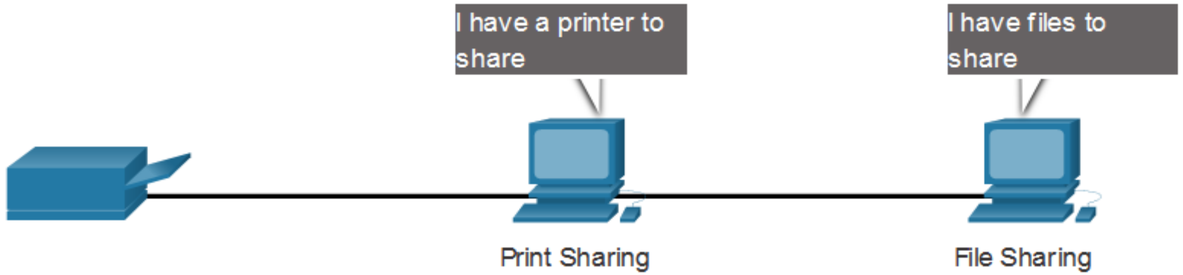
Clients are computers that send requests to the servers to retrieve information:

- web page from a web server
- email from an email server

Server Type	Description
Email	Email server runs email server software. Clients use client software to access email.
Web	Web server runs web server software. Clients use browser software to access web pages.
File	File server stores corporate and user files. The client devices access these files.

Peer-to-Peer

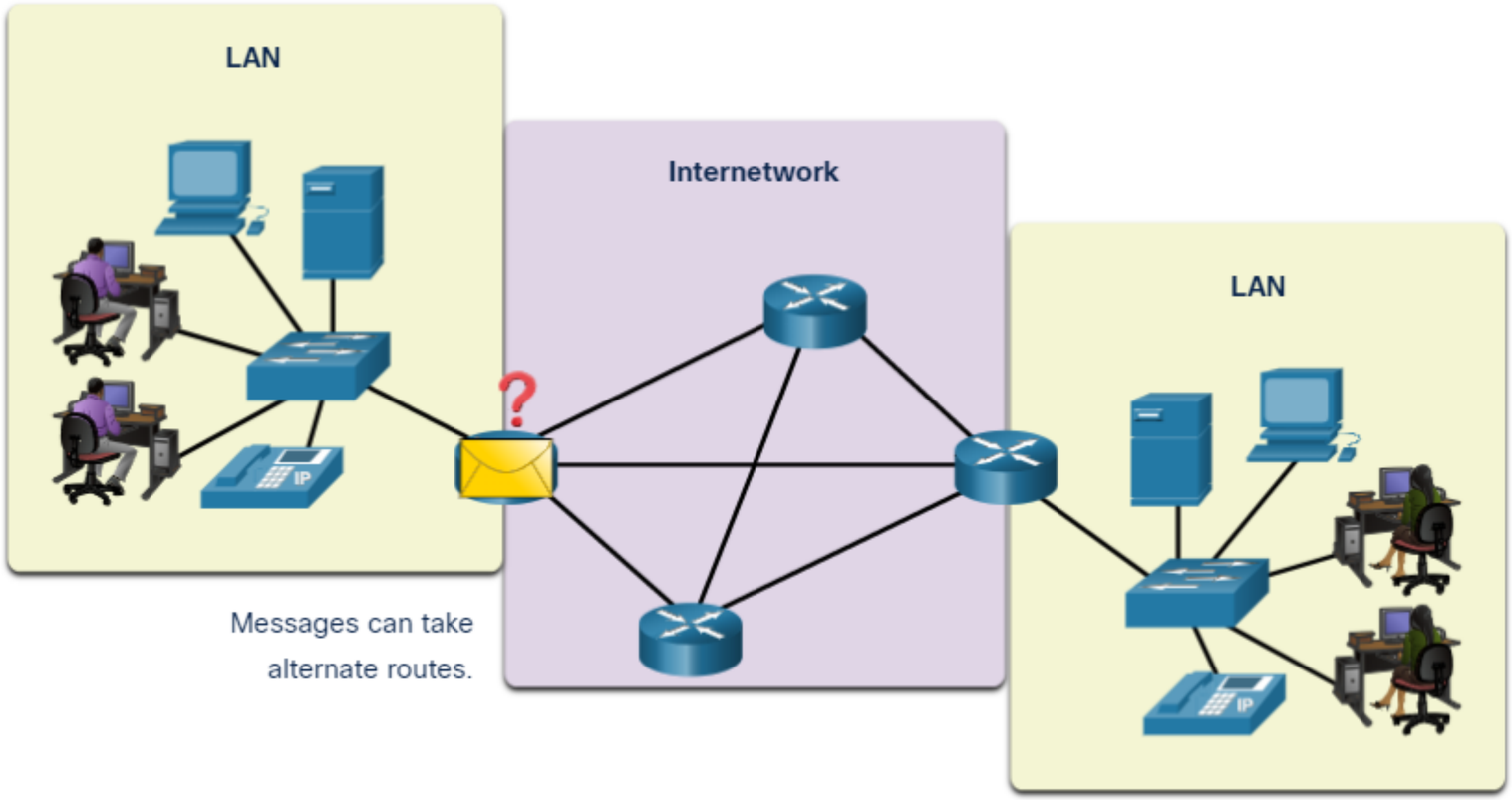
It is possible to have a device be a client and a server in a Peer-to-Peer Network. This type of network design is only recommended for very small networks.



Advantages	Disadvantages
Easy to set up	No centralized administration
Less complex	Not as secure
Lower cost	Not scalable
Used for simple tasks: transferring files and sharing printers	Slower performance

Network Components
End Devices

An end device is where a message originates from or where it is received. Data originates with an end device, flows through the network, and arrives at an end device.

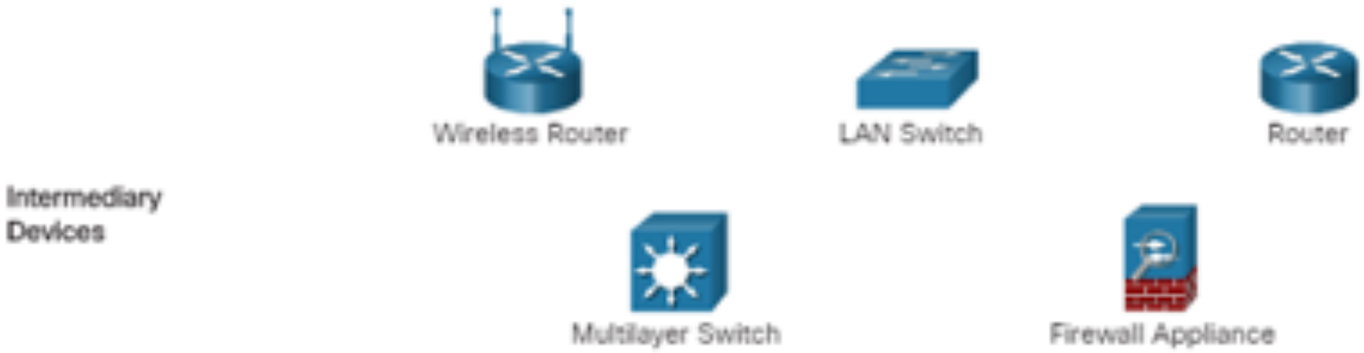


Intermediary Network Devices

An intermediary device interconnects end devices. Examples include switches, wireless access points, routers, and firewalls.

Management of data as it flows through a network is also the role of an intermediary device, including:

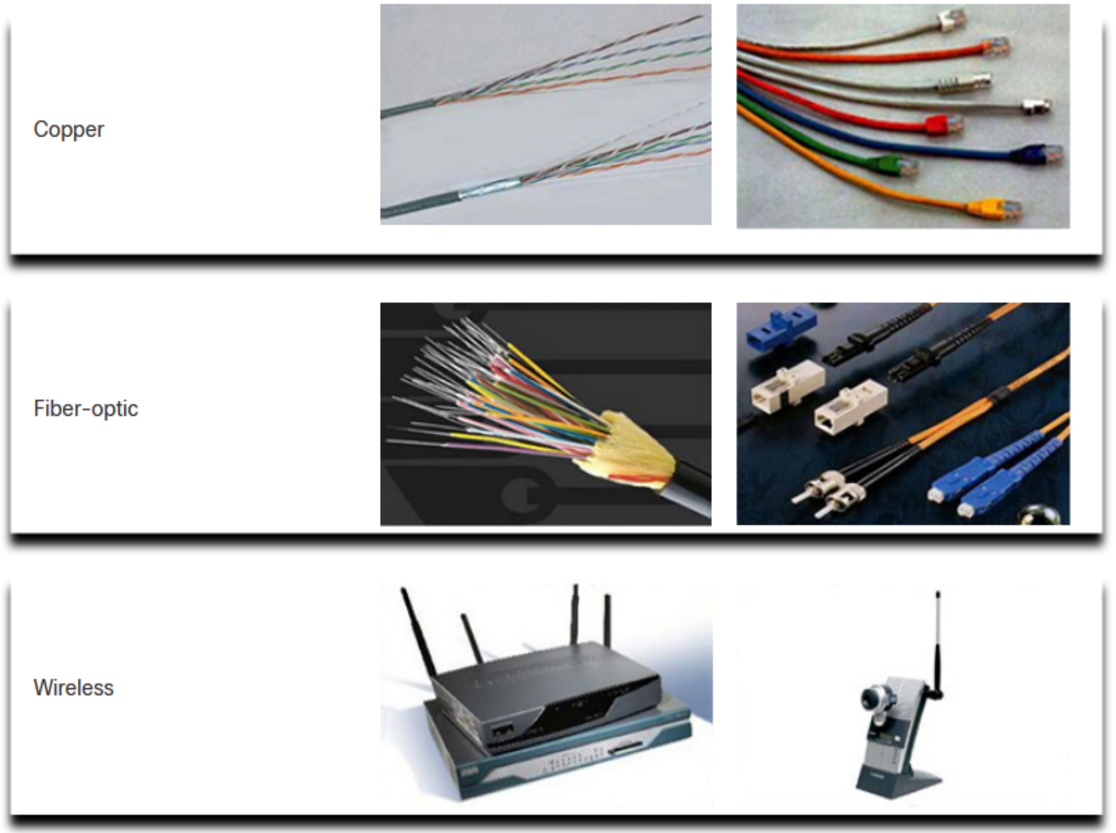
- Regenerate and retransmit data signals.
- Maintain information about what pathways exist in the network.
- Notify other devices of errors and communication failures.



Network Media

Communication across a network is carried through a medium which allows a message to travel from source to destination.

Media Types	Description
Metal wires within cables	Uses electrical impulses
Glass or plastic fibers within cables (fiber-optic cable)	Uses pulses of light.
Wireless transmission	Uses modulation of specific frequencies of electromagnetic waves.



Network Representations and Topologies

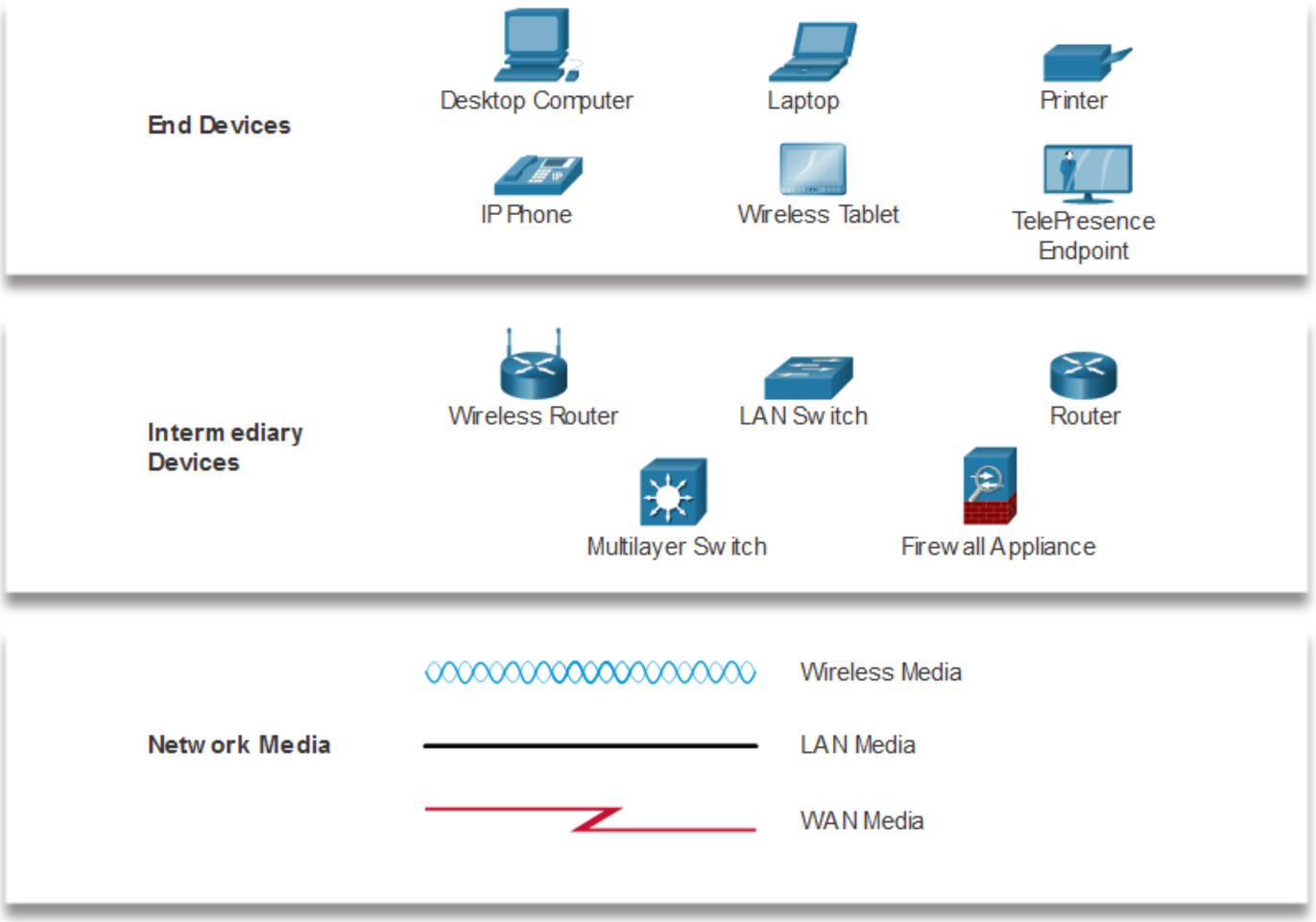
Network Representations

Network diagrams, often called topology diagrams, use symbols to represent devices within the network.

Important terms to know include:

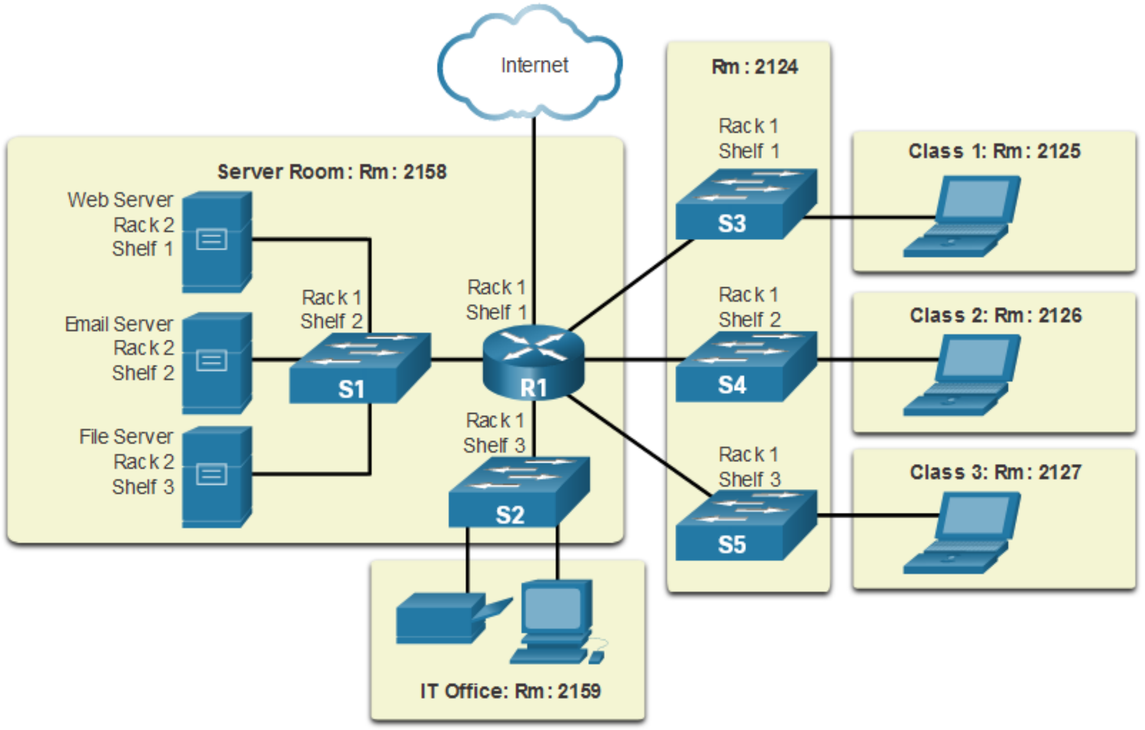
- Network Interface Card (NIC)
- Physical Port
- Interface

Note: Often, the terms port and interface are used interchangeably

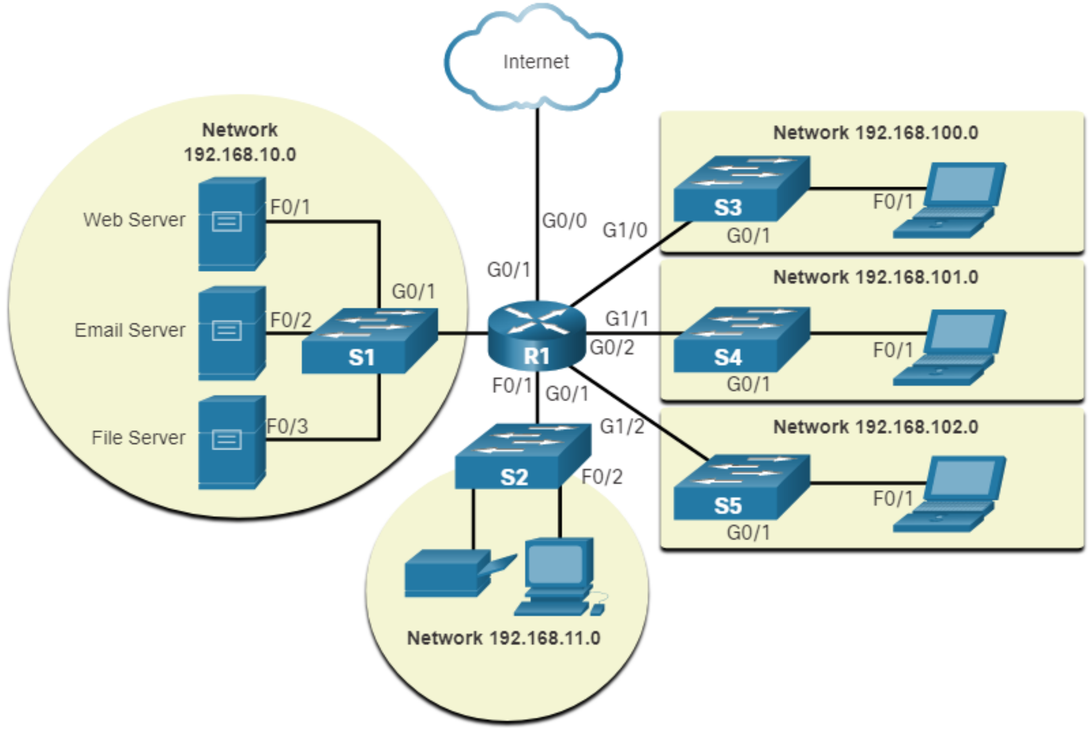


Topology Diagrams

Physical topology diagrams illustrate the physical location of intermediary devices and cable installation.



Logical topology diagrams illustrate devices, ports, and the addressing scheme of the network.



Common Types of Networks

Networks of Many Sizes

Small Home

SOHO

Medium/Large

World Wide

- Small Home Networks – connect a few computers to each other and the Internet
- Small Office/Home Office – enables computer within a home or remote office to connect to a corporate network
- Medium to Large Networks – many locations with hundreds or thousands of interconnected computers
- World Wide Networks – connects hundreds of millions of computers world-wide – such as the internet

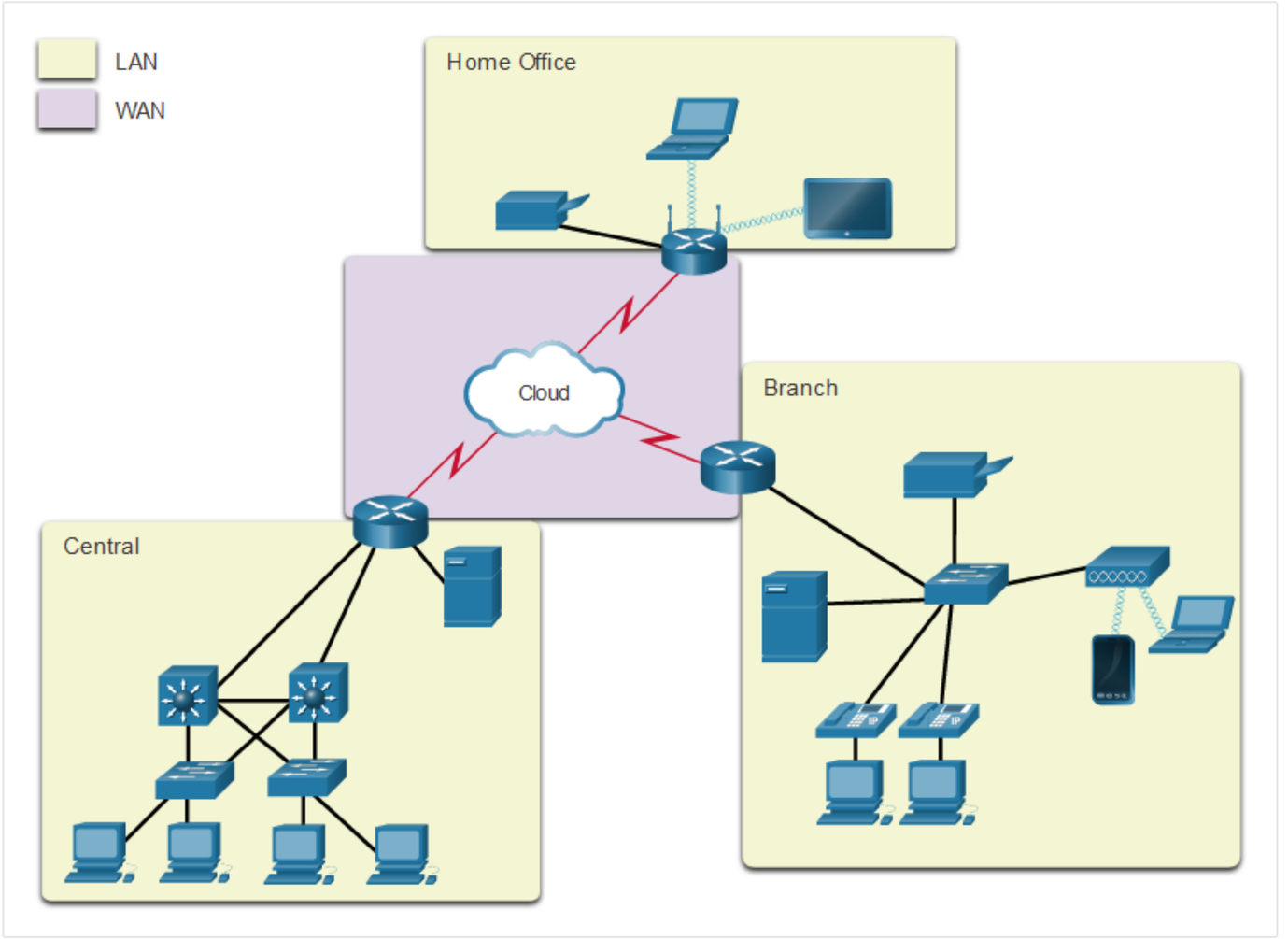
LANs and WANs

Network infrastructures vary greatly in terms of:

- Size of the area covered
- Number of users connected
- Number and types of services available
- Area of responsibility

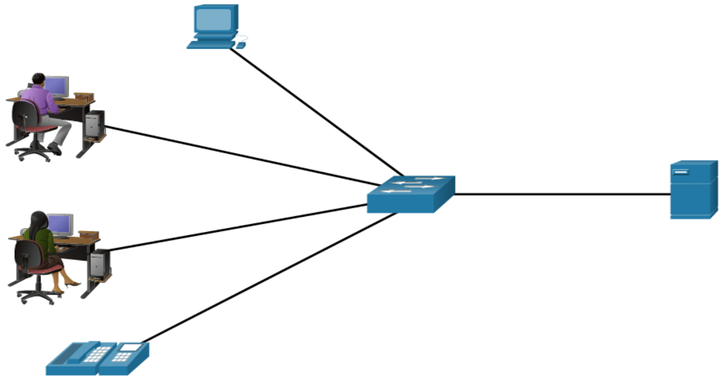
Two most common types of networks:

- Local Area Network (LAN)
- Wide Area Network (WAN).

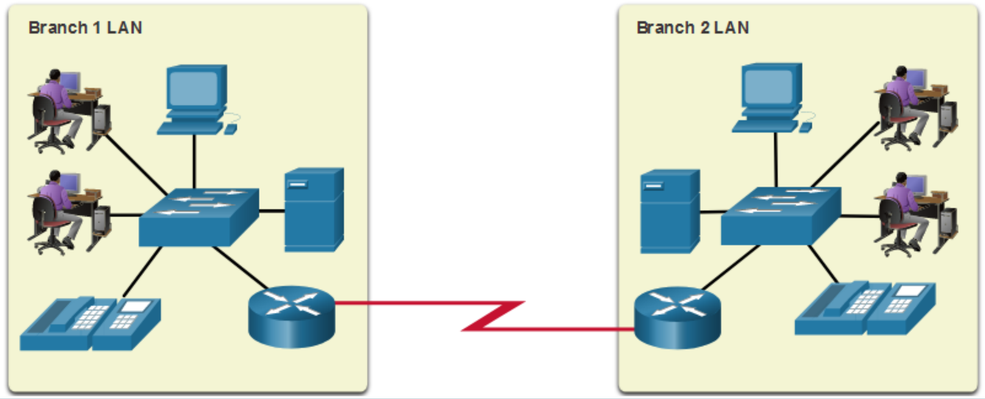


LANs and WANs (cont.)

A LAN is a network infrastructure that spans a small geographical area.



A WAN is a network infrastructure that spans a wide geographical area.



LAN	WAN
Interconnect end devices in a limited area.	Interconnect LANs over wide geographical areas.
Administered by a single organization or individual.	Typically administered by one or more service providers.
Provide high-speed bandwidth to internal devices.	Typically provide slower speed links between LANs.

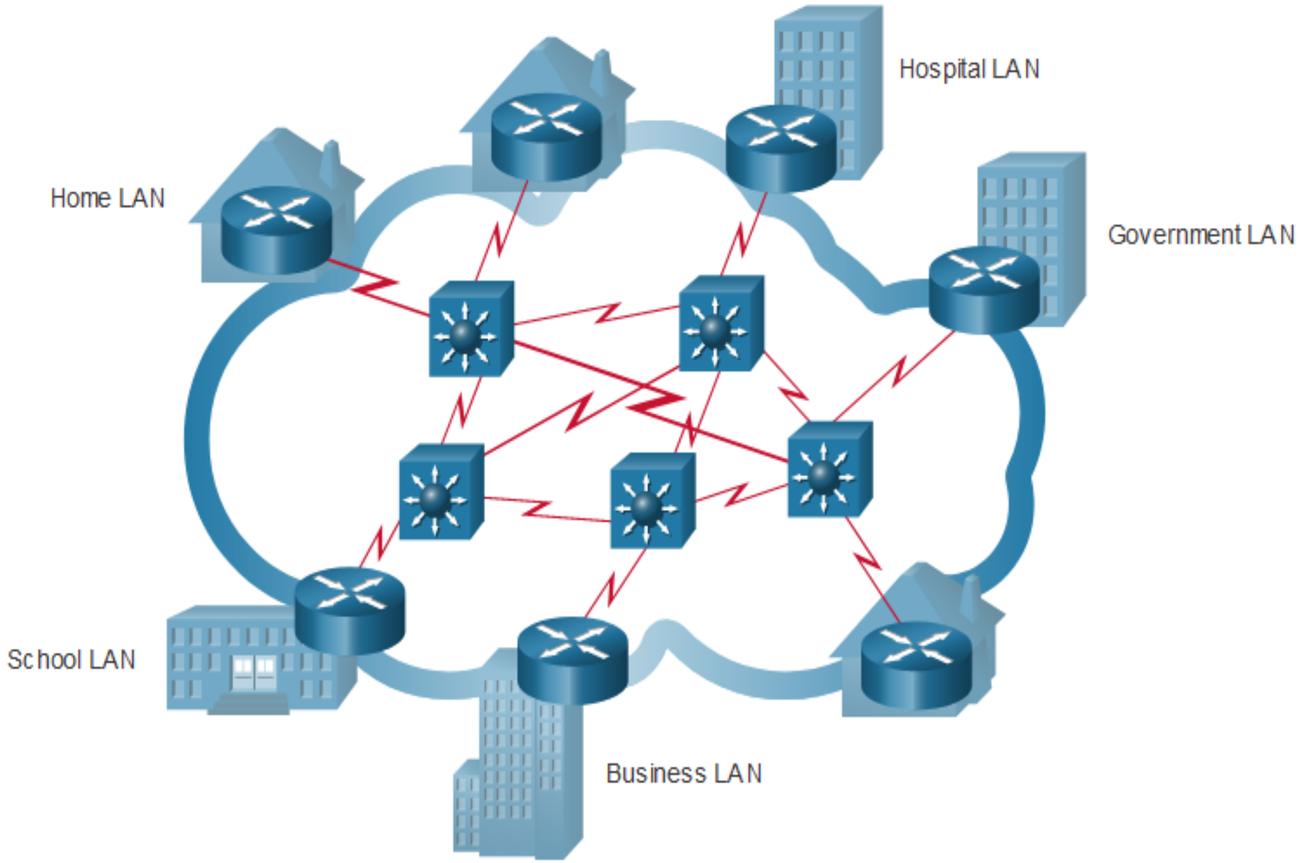
The Internet

The internet is a worldwide collection of interconnected LANs and WANs.

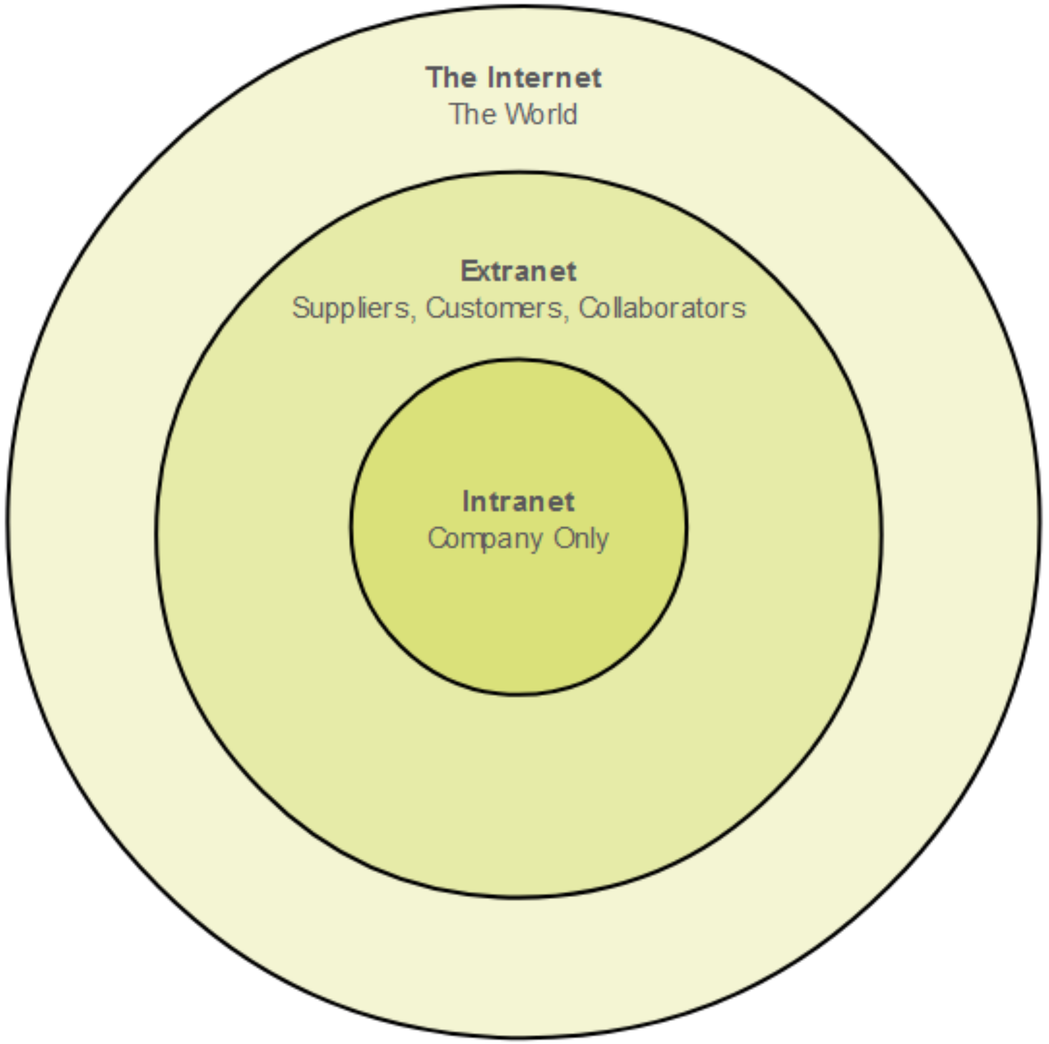
- LANs are connected to each other using WANs.
- WANs may use copper wires, fiber optic cables, and wireless transmissions.

The internet is not owned by any individual or group. The following groups were developed to help maintain structure on the internet:

- IETF
- ICANN
- IAB



Intranets and Extranets



An intranet is a private collection of LANs and WANs internal to an organization that is meant to be accessible only to the organizations members or others with authorization.

An organization might use an extranet to provide secure access to their network for individuals who work for a different organization that need access to their data on their network.

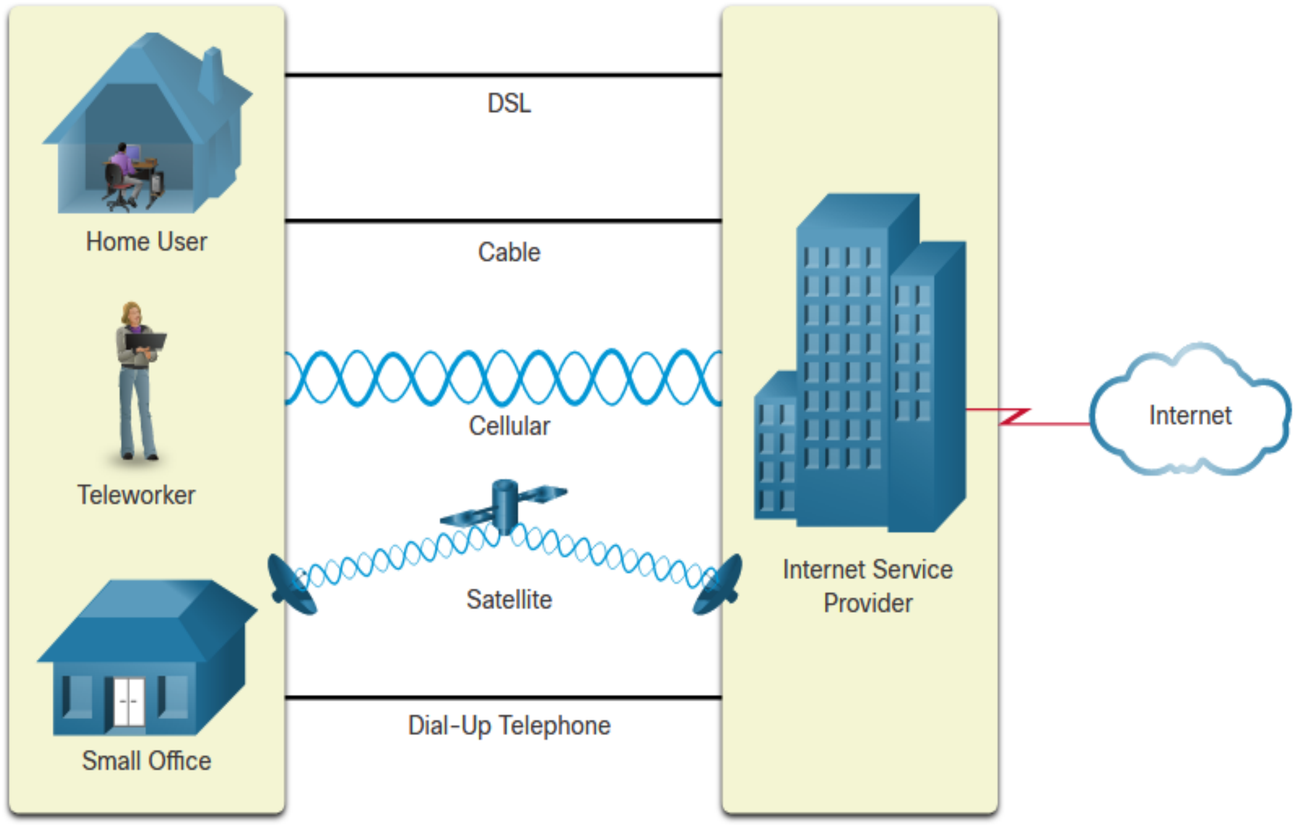
Internet Connections

Internet Access Technologies

There are many ways to connect users and organizations to the internet:

- Popular services for home users and small offices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.
- Organizations need faster connections to support IP phones, video conferencing and data center storage.
- Business-class interconnections are usually provided by service providers (SP) and may include: business DSL, leased lines, and Metro Ethernet.

Home and Small Office Internet Connections

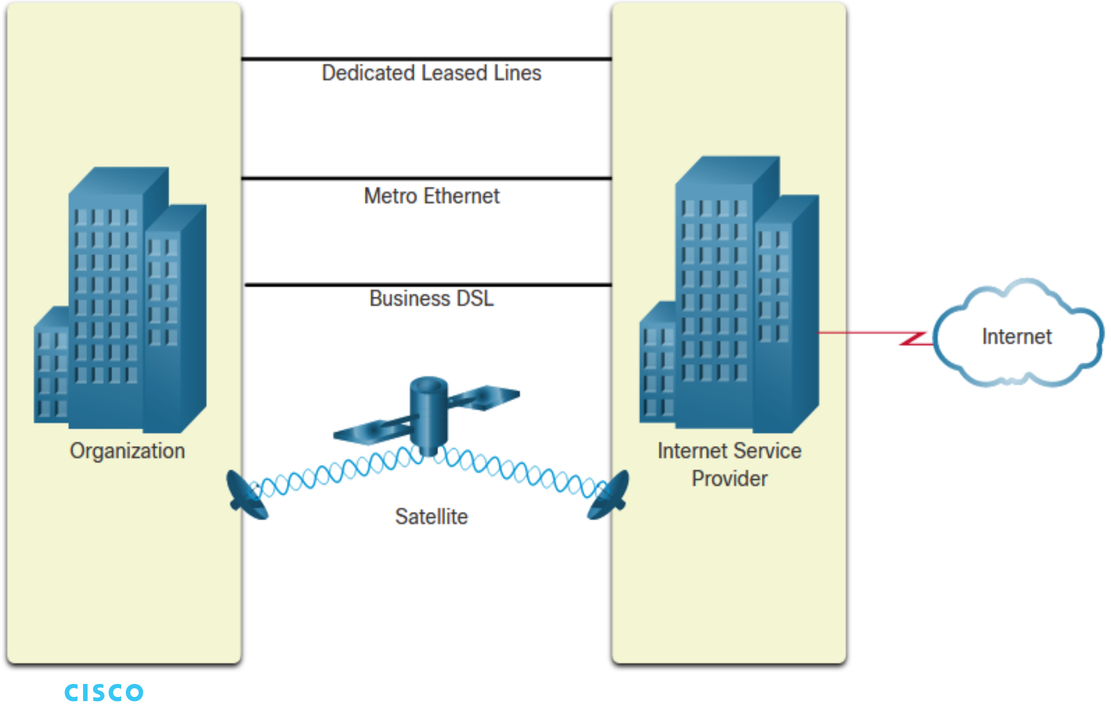


Connection	Description
Cable	high bandwidth, always on, internet offered by cable television service providers.
DSL	high bandwidth, always on, internet connection that runs over a telephone line.
Cellular	uses a cell phone network to connect to the internet.
Satellite	major benefit to rural areas without Internet Service Providers.
Dial-up telephone	an inexpensive, low bandwidth option using a modem.

Businesses Internet Connections

Corporate business connections may require:

- higher bandwidth
- dedicated connections
- managed services

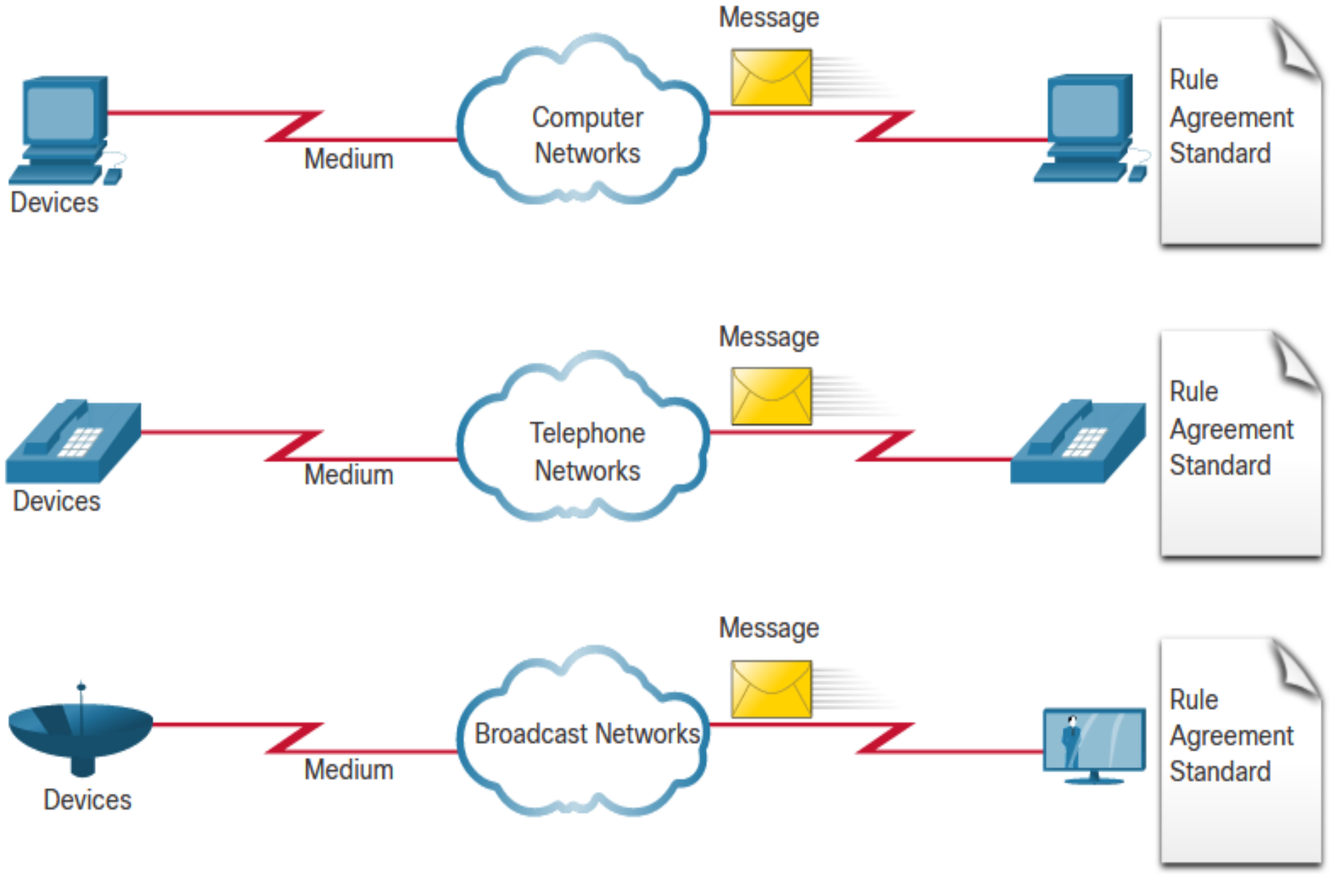


Type of Connection	Description
Dedicated Leased Line	These are reserved circuits within the service provider's network that connect distant offices with private voice and/or data networking.
Ethernet WAN	This extends LAN access technology into the WAN.
DSL	Business DSL is available in various formats including Symmetric Digital Subscriber Lines (SDSL).
Satellite	This can provide a connection when a wired solution is not available.

The Converging Network

Before converged networks, an organization would have been separately cabled for telephone, video, and data. Each of these networks would use different technologies to carry the signal.

Each of these technologies would use a different set of rules and standards.

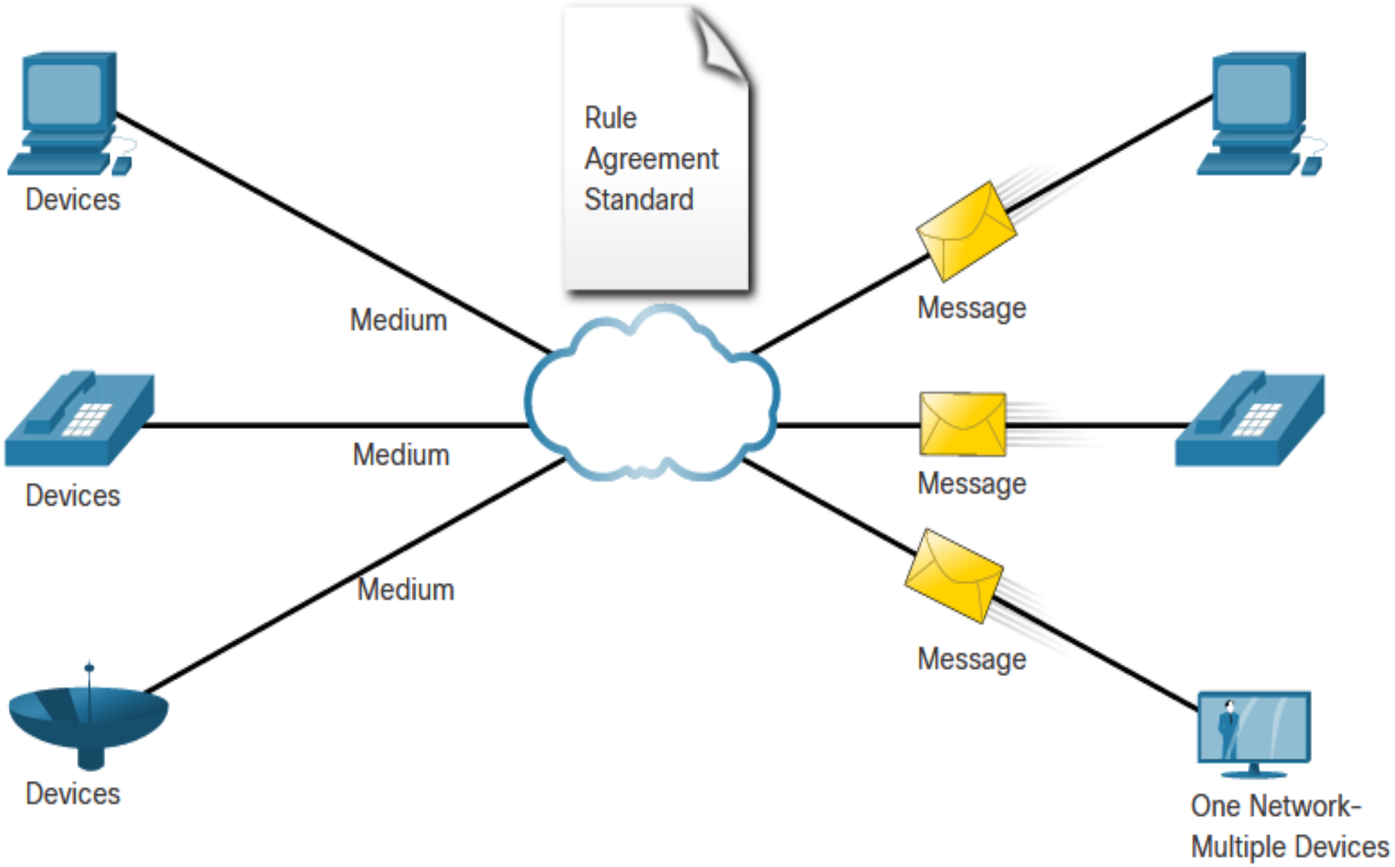


The Converging Network (Cont.)

Converged data networks carry multiple services on one link including:

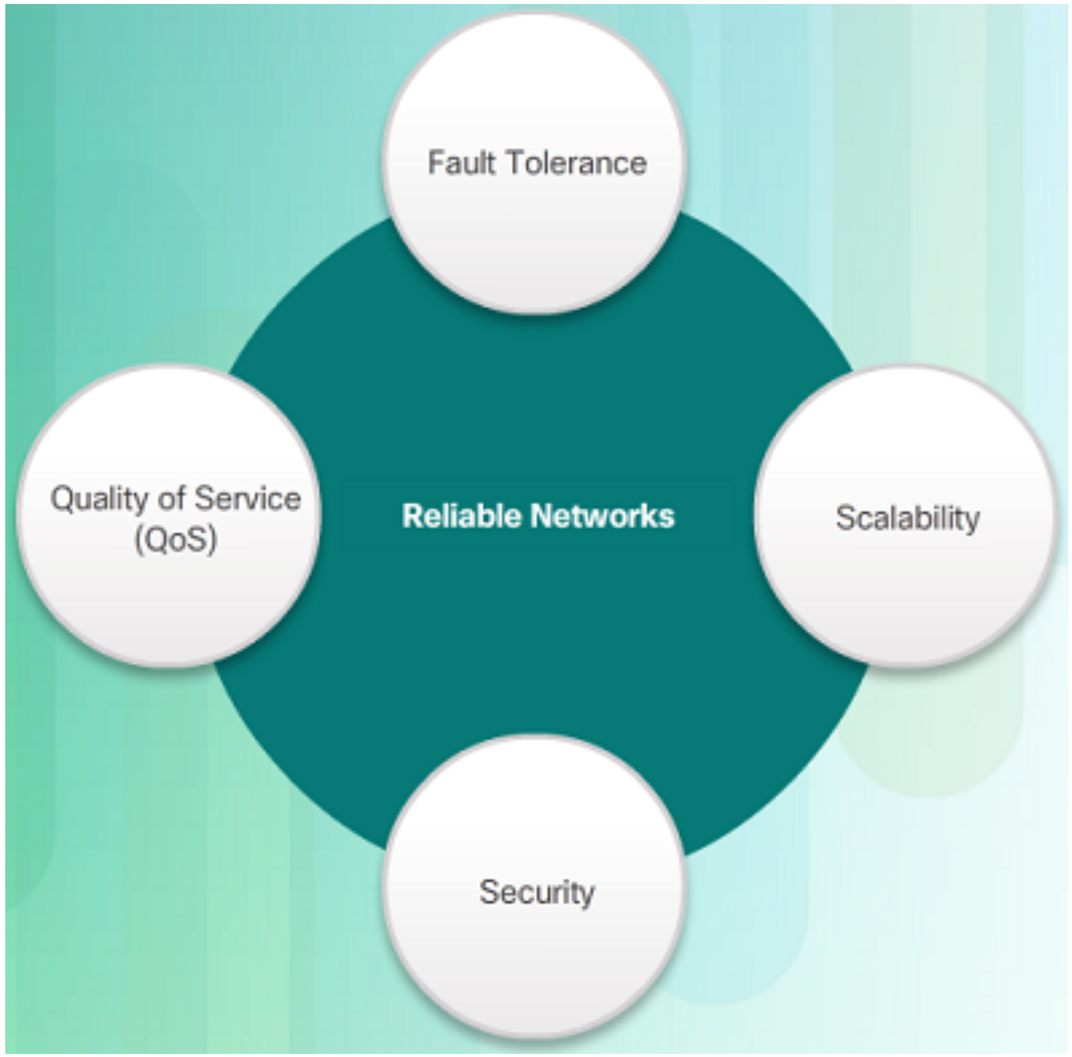
- data
- voice
- video

Converged networks can deliver data, voice, and video over the same network infrastructure. The network infrastructure uses the same set of rules and standards.



Reliable Networks

Network Architecture



Network Architecture refers to the technologies that support the infrastructure that moves data across the network.

There are four basic characteristics that the underlying architectures need to address to meet user expectations:

- Fault Tolerance
- Scalability
- Quality of Service (QoS)
- Security

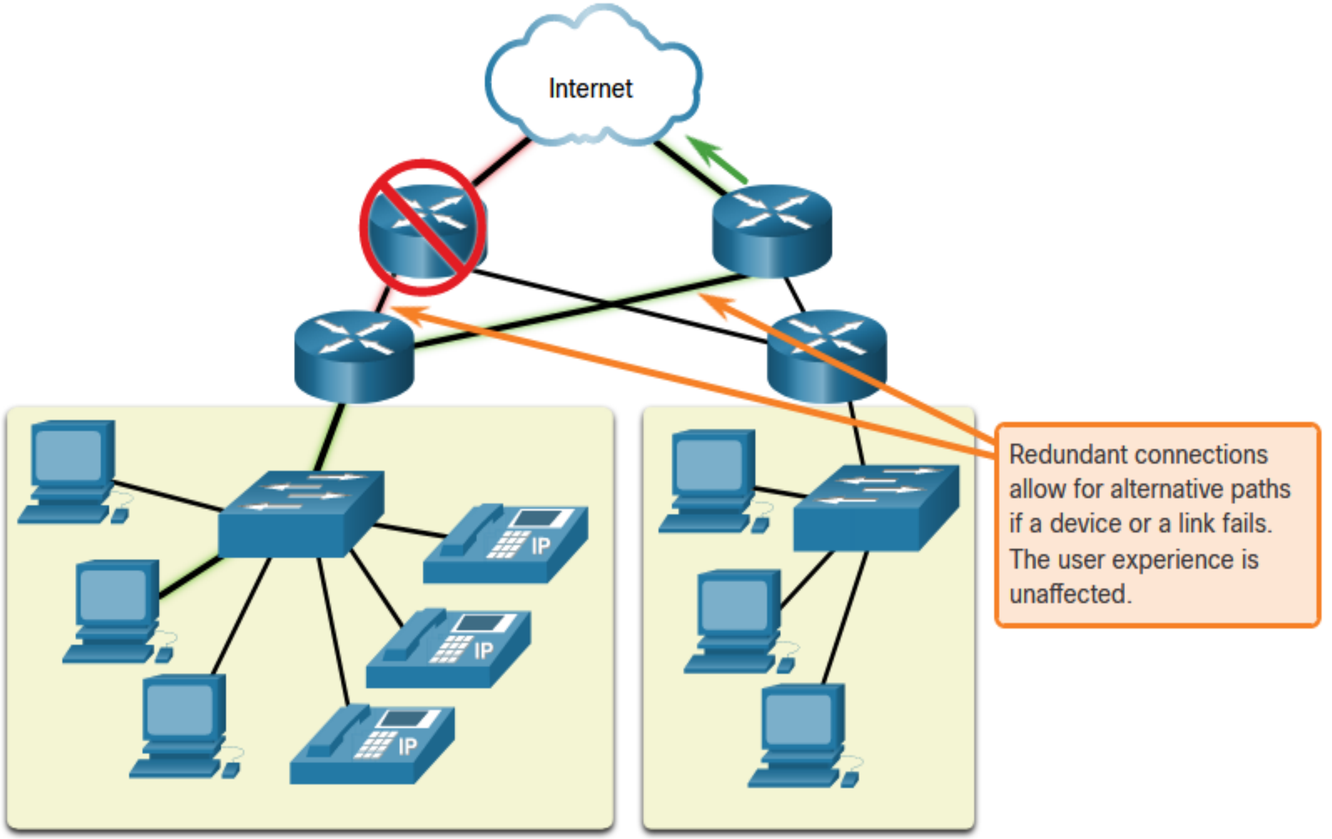
Fault Tolerance

A fault tolerant network limits the impact of a failure by limiting the number of affected devices. Multiple paths are required for fault tolerance.

Reliable networks provide redundancy by implementing a packet switched network:

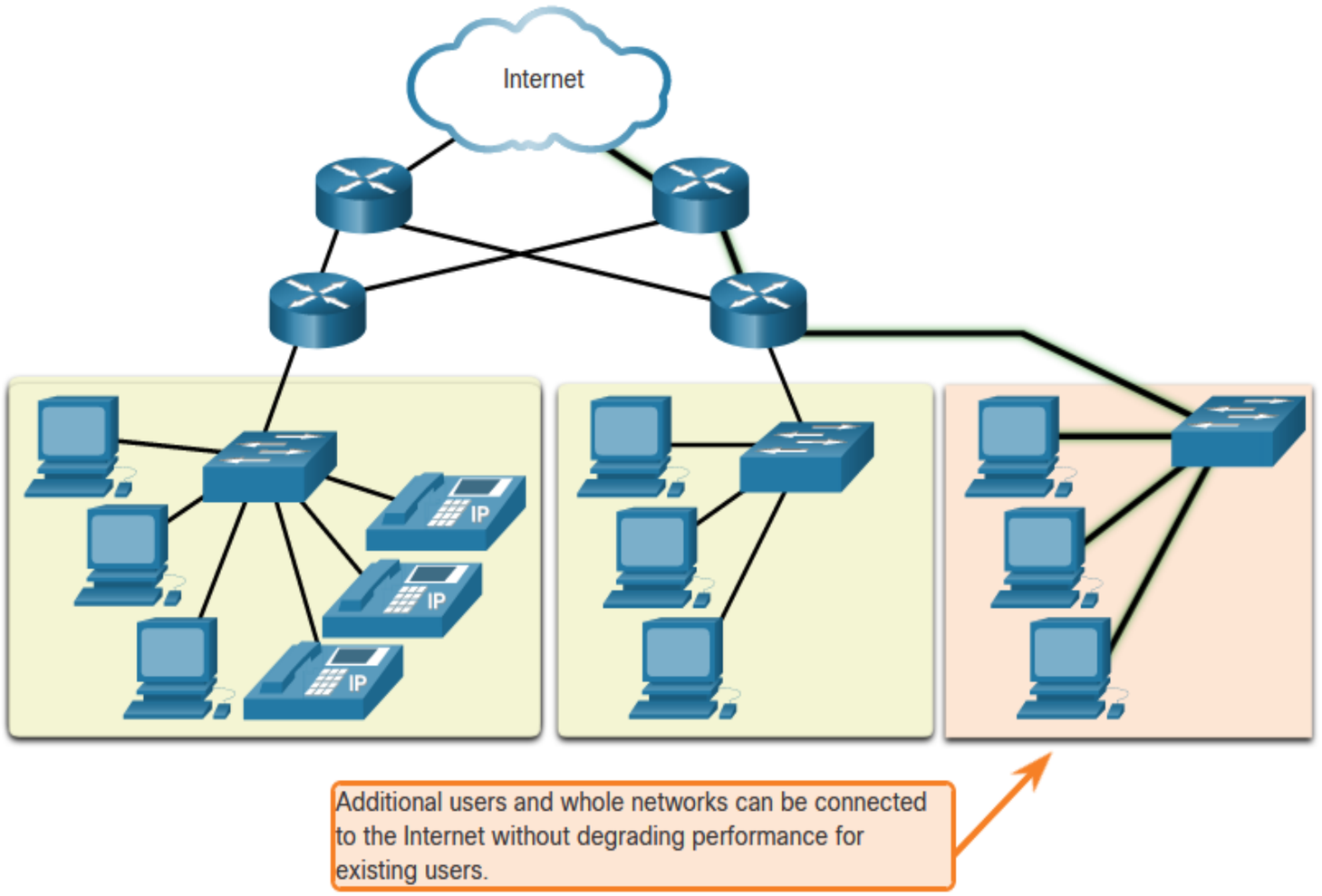
- Packet switching splits traffic into packets that are routed over a network.
- Each packet could theoretically take a different path to the destination.

This is not possible with circuit-switched networks which establish dedicated circuits.



Reliable Network

Scalability



A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.

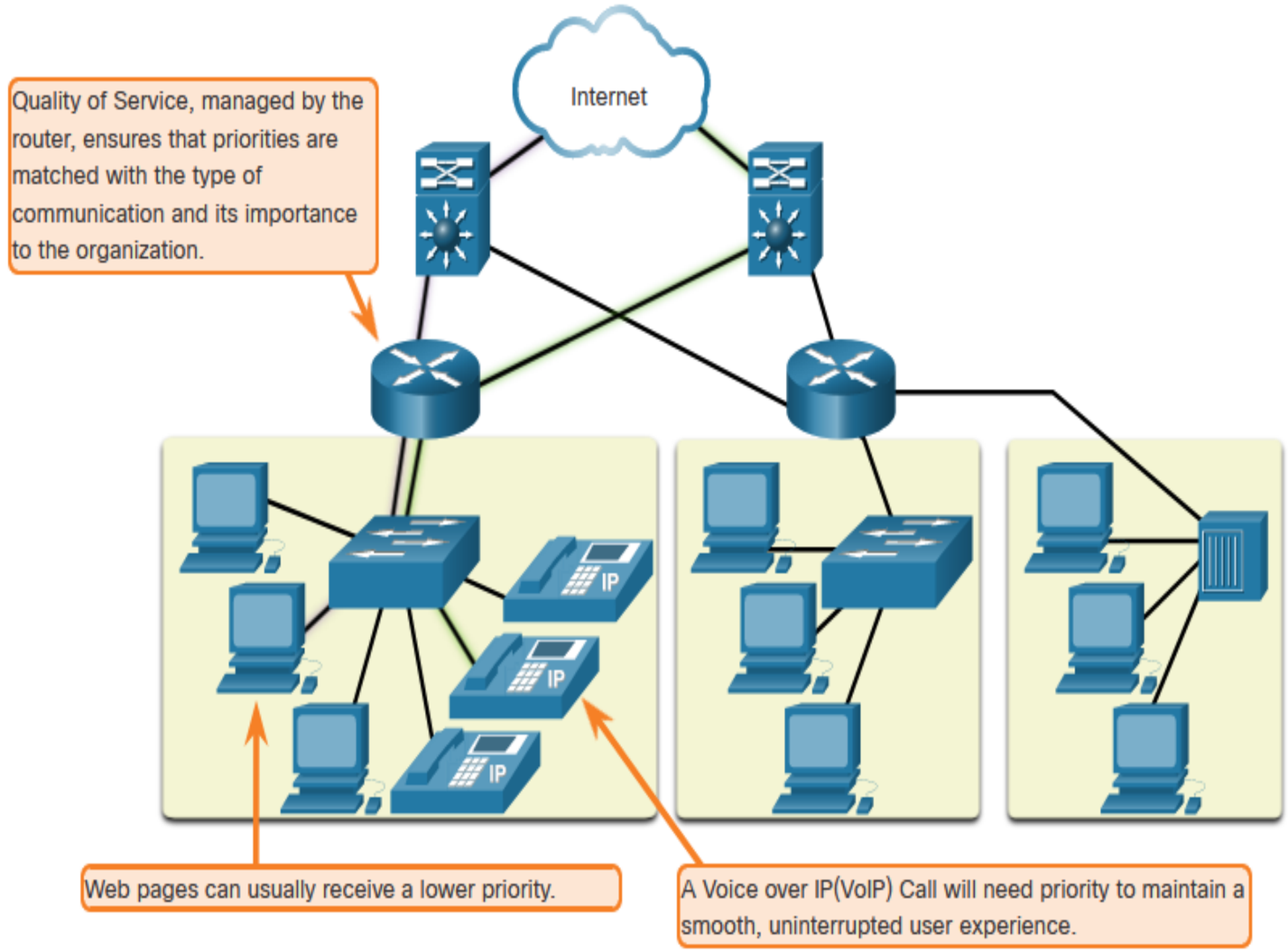
Network designers follow accepted standards and protocols in order to make the networks scalable.

Quality of Service

Voice and live video transmissions require higher expectations for those services being delivered.

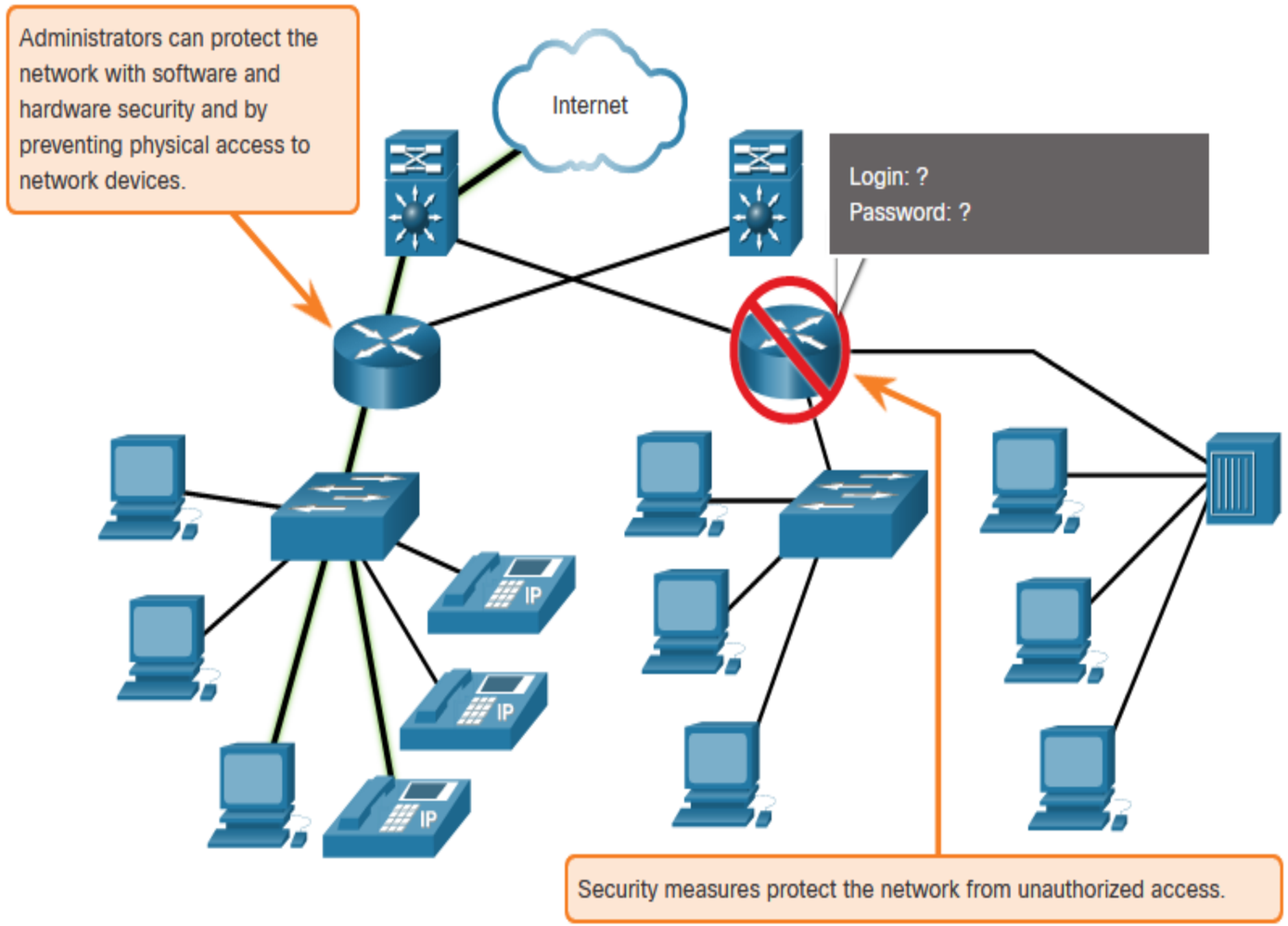
Have you ever watched a live video with constant breaks and pauses? This is caused when there is a higher demand for bandwidth than available – and QoS isn't configured.

- Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.
- With a QoS policy in place, the router can more easily manage the flow of data and voice traffic.



Reliable Network

Network Security



There are two main types of network security that must be addressed:

- Network infrastructure security
  - Physical security of network devices
  - Preventing unauthorized access to the devices
- Information Security
  - Protection of the information or data transmitted over the network

Three goals of network security:

- Confidentiality – only intended recipients can read the data
- Integrity – assurance that the data has not be altered with during transmission
- Availability – assurance of timely and reliable access to data for authorized users

Network Trends

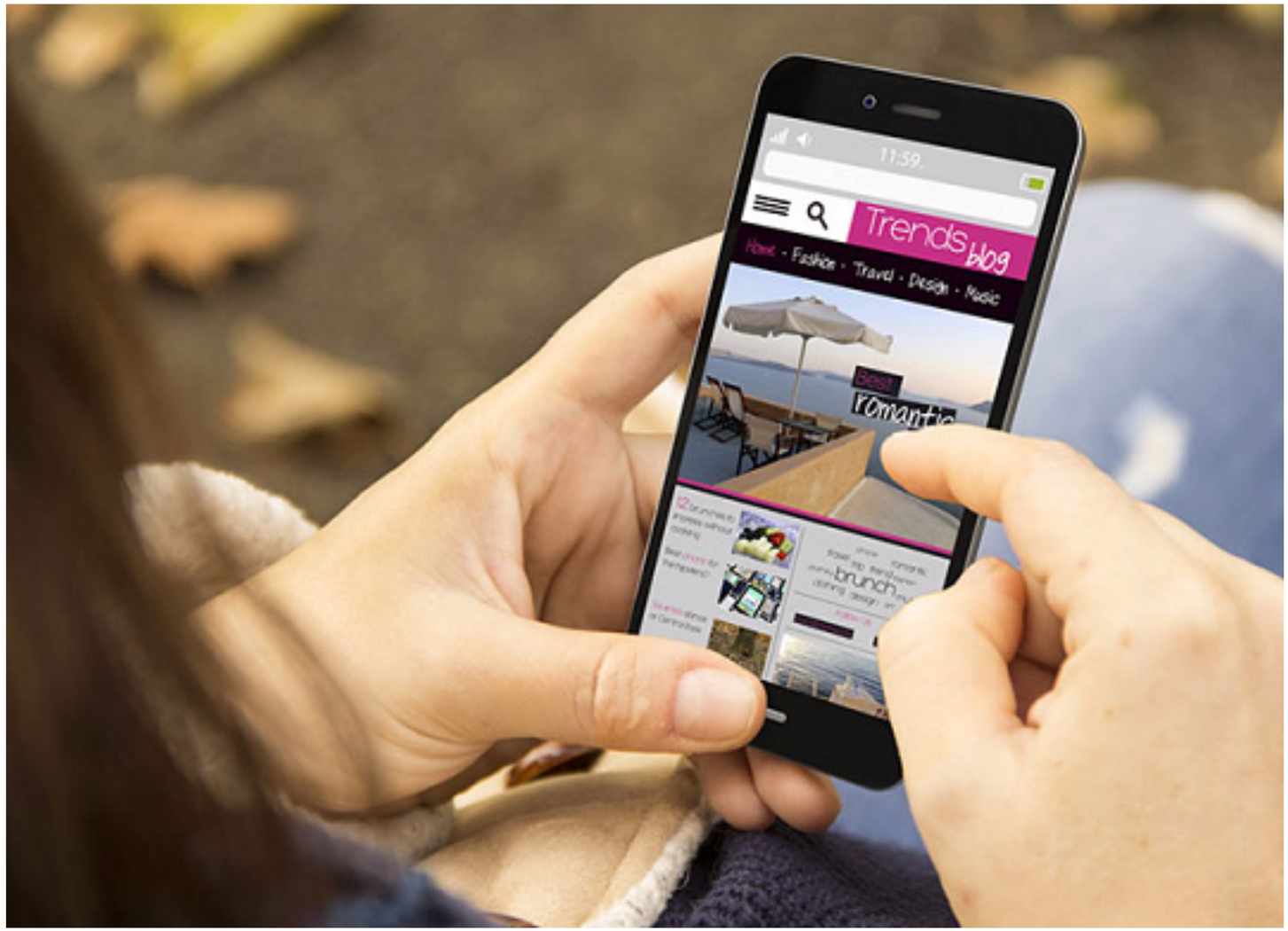
Recent Trends

The role of the network must adjust and continually transform in order to be able to keep up with new technologies and end user devices as they constantly come to the market.

Several new networking trends that effect organizations and consumers:

- Bring Your Own Device (BYOD)
- Online collaboration
- Video communications
- Cloud computing

Bring Your Own Device



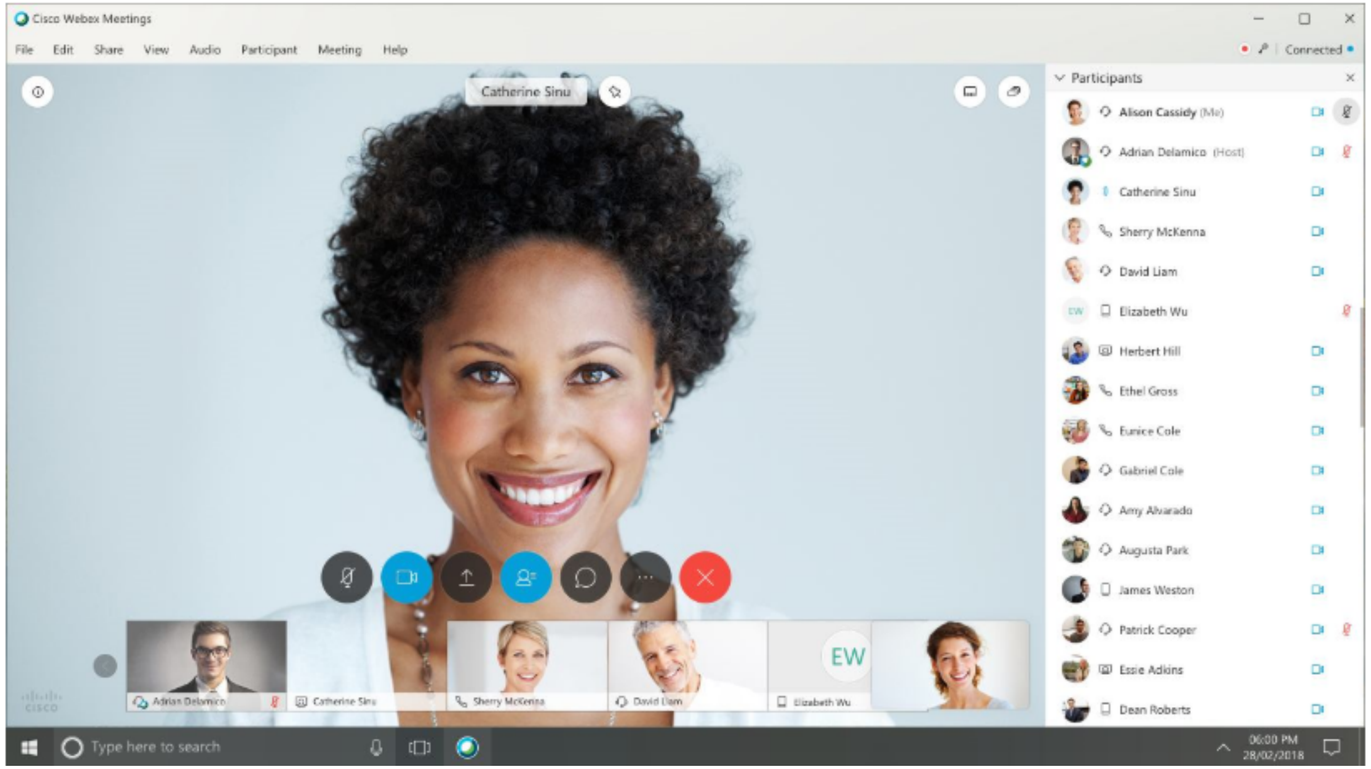
Bring Your Own Device (BYOD) allows users to use their own devices giving them more opportunities and greater flexibility.

BYOD allows end users to have the freedom to use personal tools to access information and communicate using their:

- Laptops
- Netbooks
- Tablets
- Smartphones
- E-readers

BYOD means any device, with any ownership, used anywhere.

Online Collaboration



- Collaborate and work with others over the network on joint projects.
- Collaboration tools including Cisco WebEx (shown in the figure) gives users a way to instantly connect and interact.
- Collaboration is a very high priority for businesses and in education.
- Cisco Webex Teams is a multifunctional collaboration tool.
  - send instant messages
  - post images
  - post videos and links

Cloud Computing

Cloud computing allows us to store personal files or backup our data on servers over the internet.

- Applications can also be accessed using the Cloud.
- Allows businesses to deliver to any device anywhere in the world.

Cloud computing is made possible by data centers.

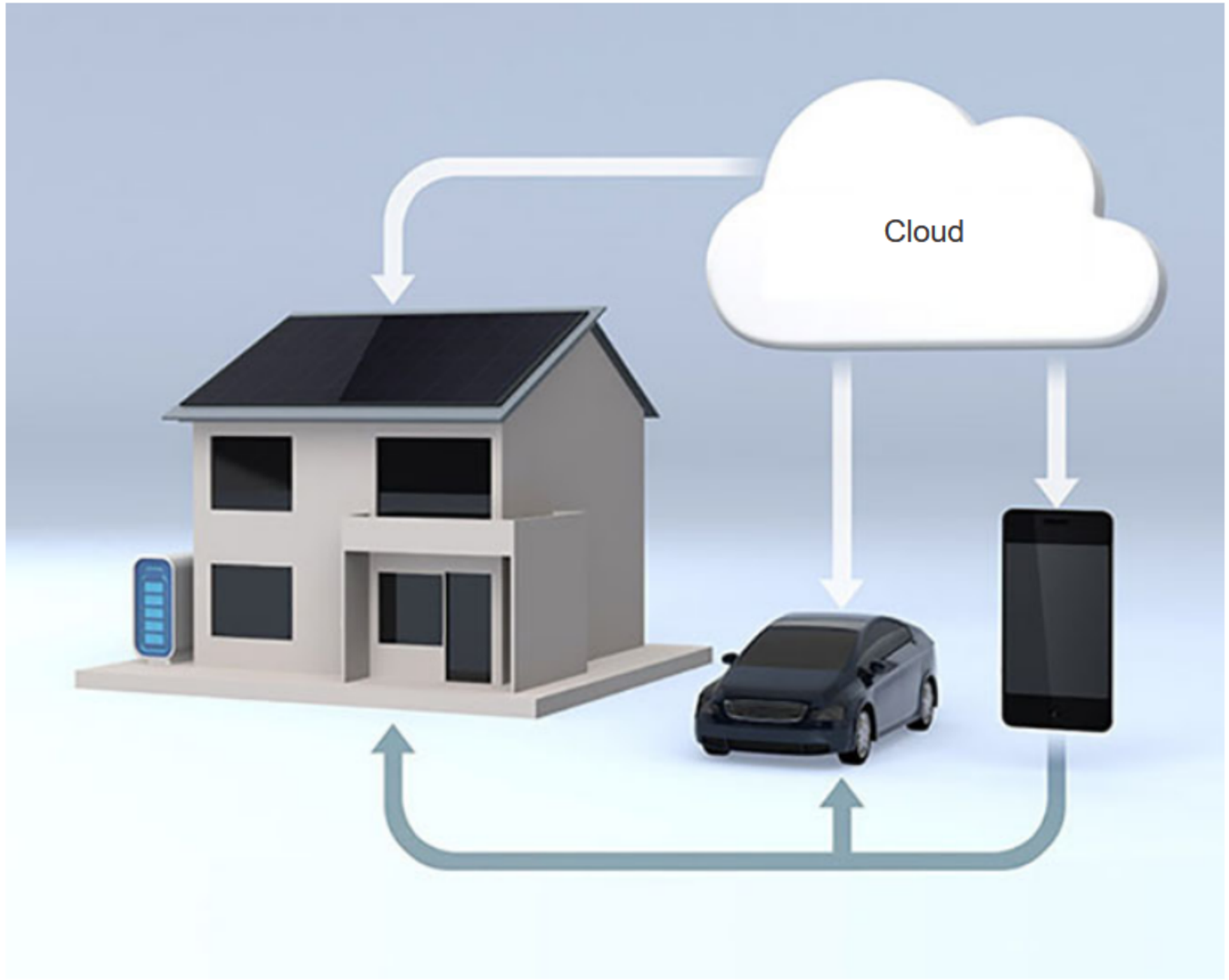
- Smaller companies that can’t afford their own data centers, lease server and storage services from larger data center organizations in the Cloud.

Cloud Computing (Cont.)

Four types of Clouds:

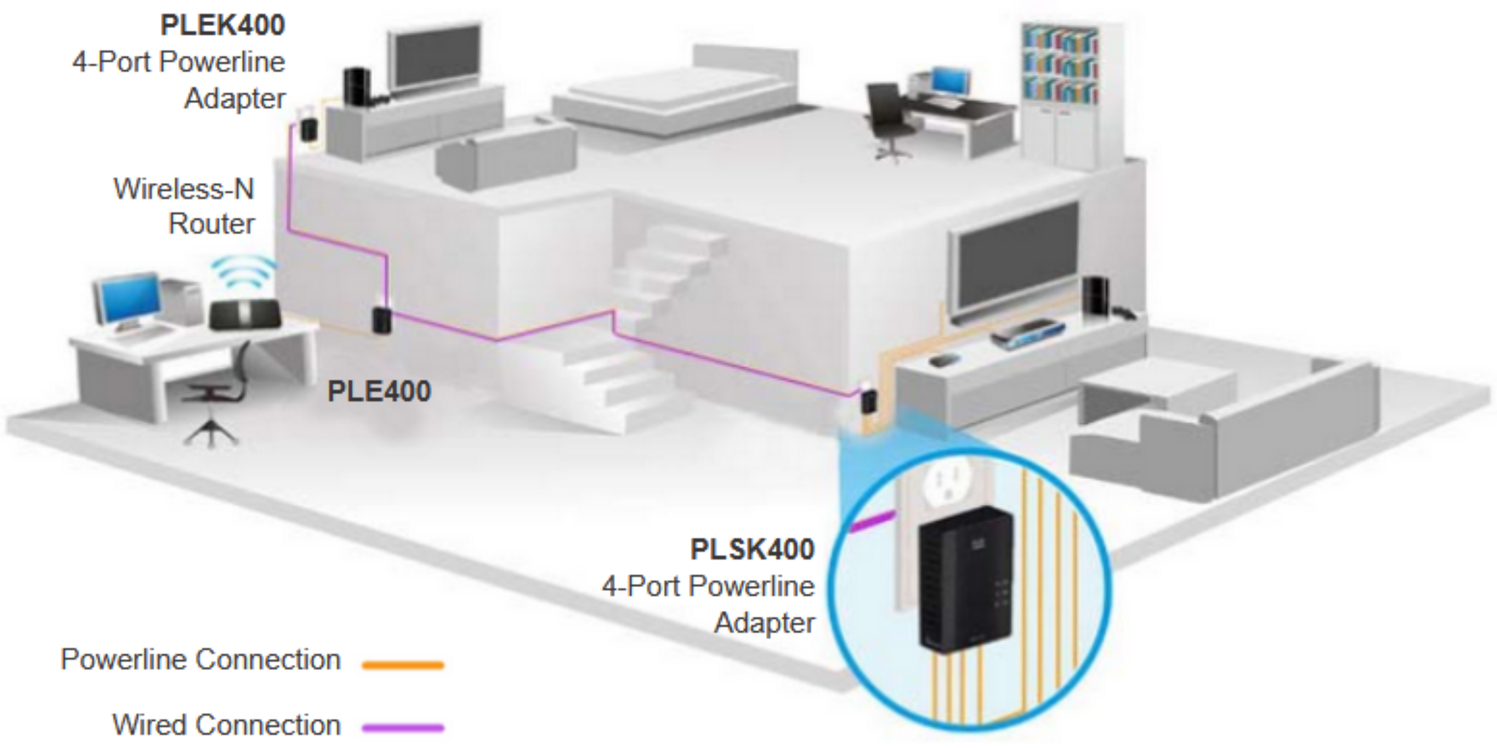
- Public Clouds
- Available to the general public through a pay-per-use model or for free.
- Private Clouds
- Intended for a specific organization or entity such as the government.
- Hybrid Clouds
- Made up of two or more Cloud types – for example, part custom and part public.
- Each part remains a distinctive object but both are connected using the same architecture.
- Custom Clouds
- Built to meet the needs of a specific industry, such as healthcare or media.
- Can be private or public.

Technology Trends in the Home



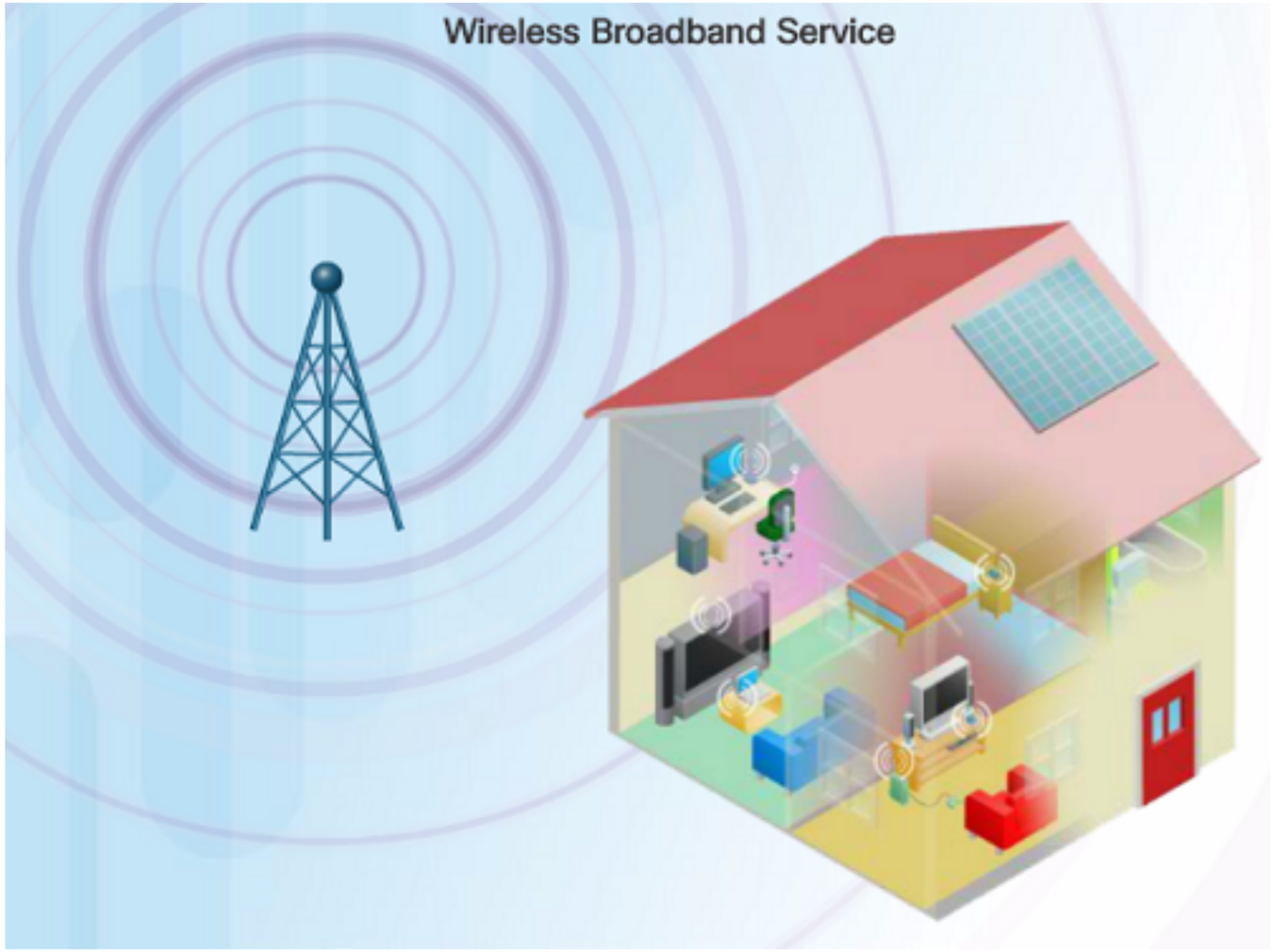
- Smart home technology is a growing trend that allows technology to be integrated into every-day appliances which allows them to interconnect with other devices.
- Ovens might know what time to cook a meal for you by communicating with your calendar on what time you are scheduled to be home.
- Smart home technology is currently being developed for all rooms within a house.

Powerline Networking



- Powerline networking can allow devices to connect to a LAN where data network cables or wireless communications are not a viable option.
- Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet by sending data on certain frequencies.
- Powerline networking is especially useful when wireless access points cannot reach all the devices in the home.

Wireless Broadband

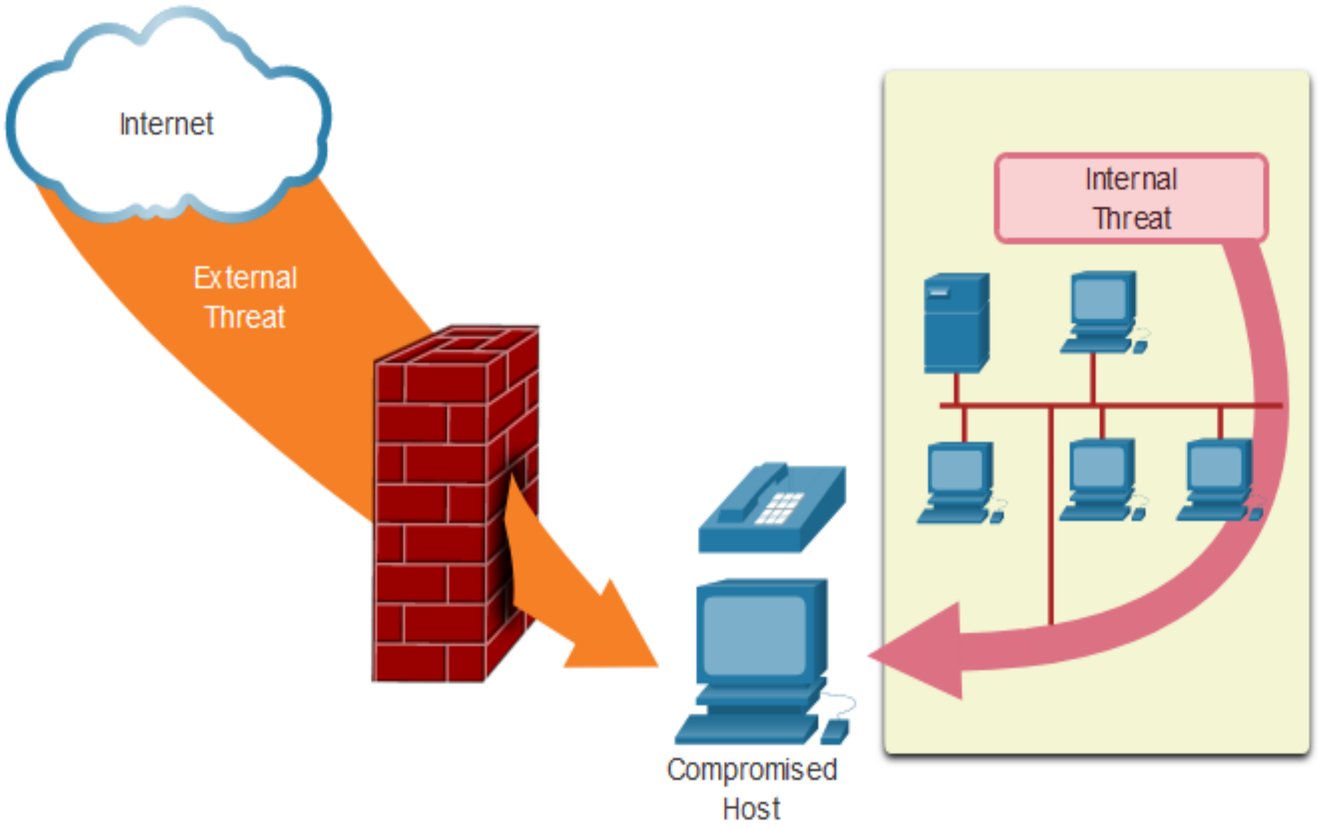


In addition to DSL and cable, wireless is another option used to connect homes and small businesses to the internet.

- More commonly found in rural environments, a Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to designated access points or hotspots.
- Wireless broadband is another solution for the home and small businesses.
  - Uses the same cellular technology used by a smart phone.
  - An antenna is installed outside the house providing wireless or wired connectivity for devices in the home.

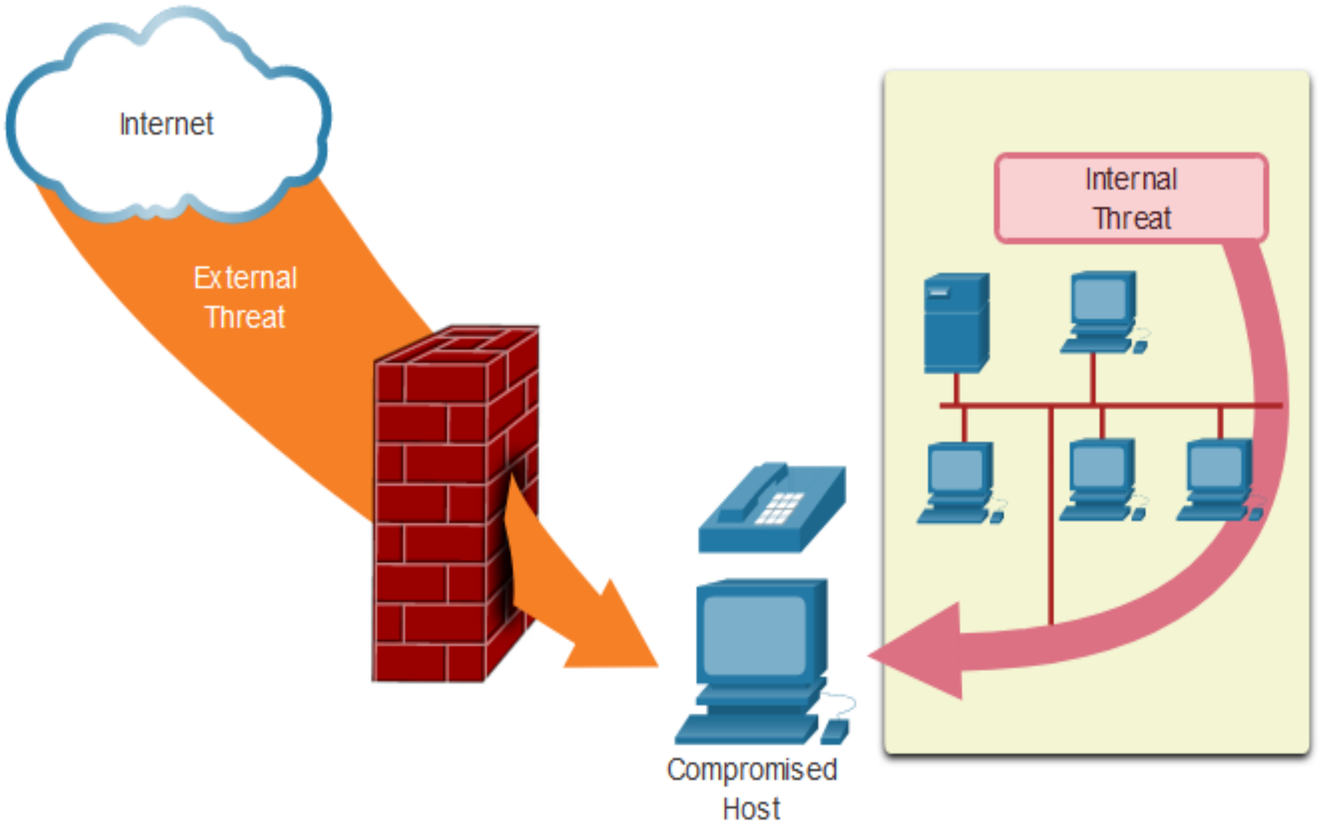
Network Security

Security Threats



- Network security is an integral part of networking regardless of the size of the network.
- The network security that is implemented must take into account the environment while securing the data, but still allowing for quality of service that is expected of the network.
- Securing a network involves many protocols, technologies, devices, tools, and techniques in order to secure data and mitigate threats.
- Threat vectors might be external or internal.

Security Threats (Cont.)



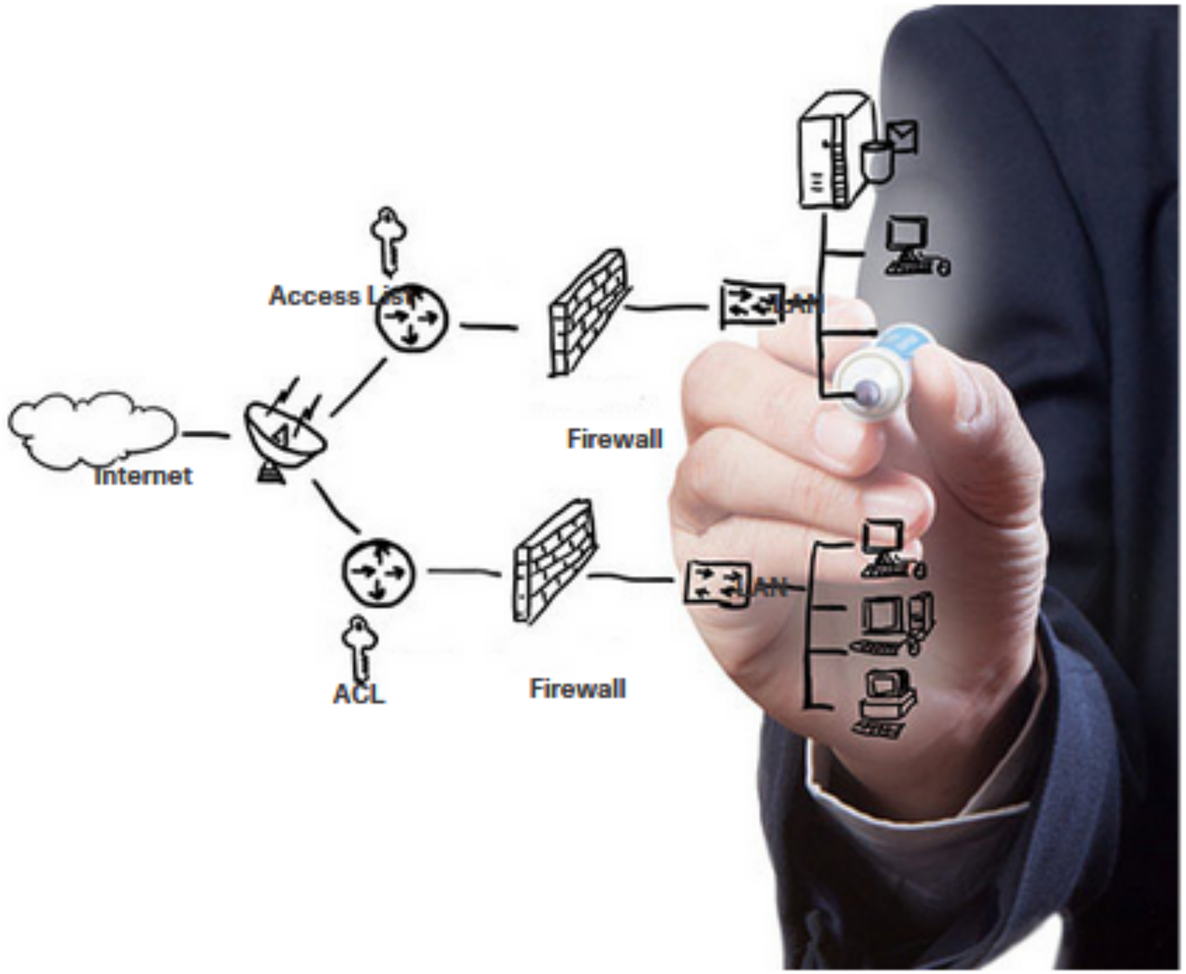
External Threats:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks
- Threat Actor attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

Internal Threats:

- lost or stolen devices
- accidental misuse by employees
- malicious employees

Security Solutions

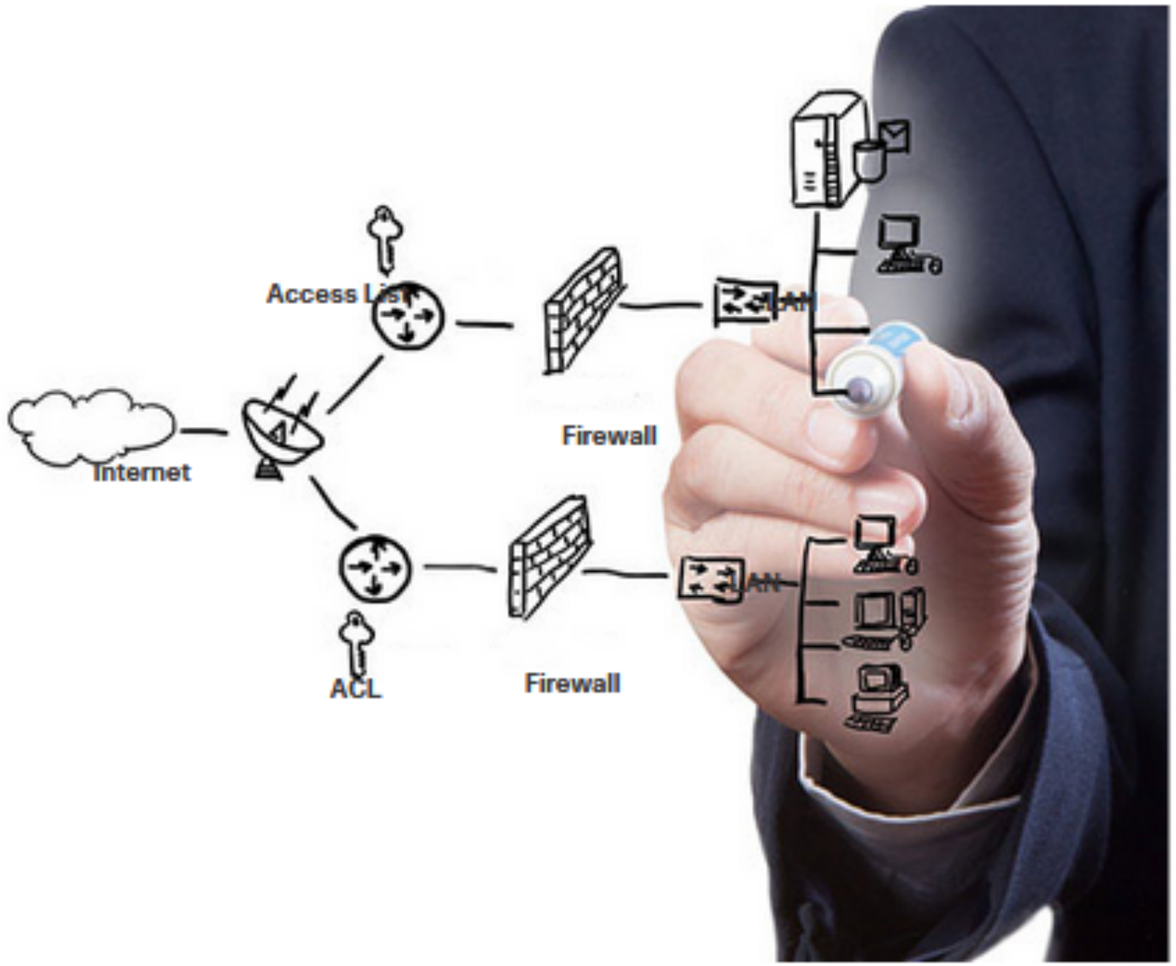


Security must be implemented in multiple layers using more than one security solution.

Network security components for home or small office network:

- Antivirus and antispyware software should be installed on end devices.
- Firewall filtering used to block unauthorized access to the network.

Security Solutions (Cont.)



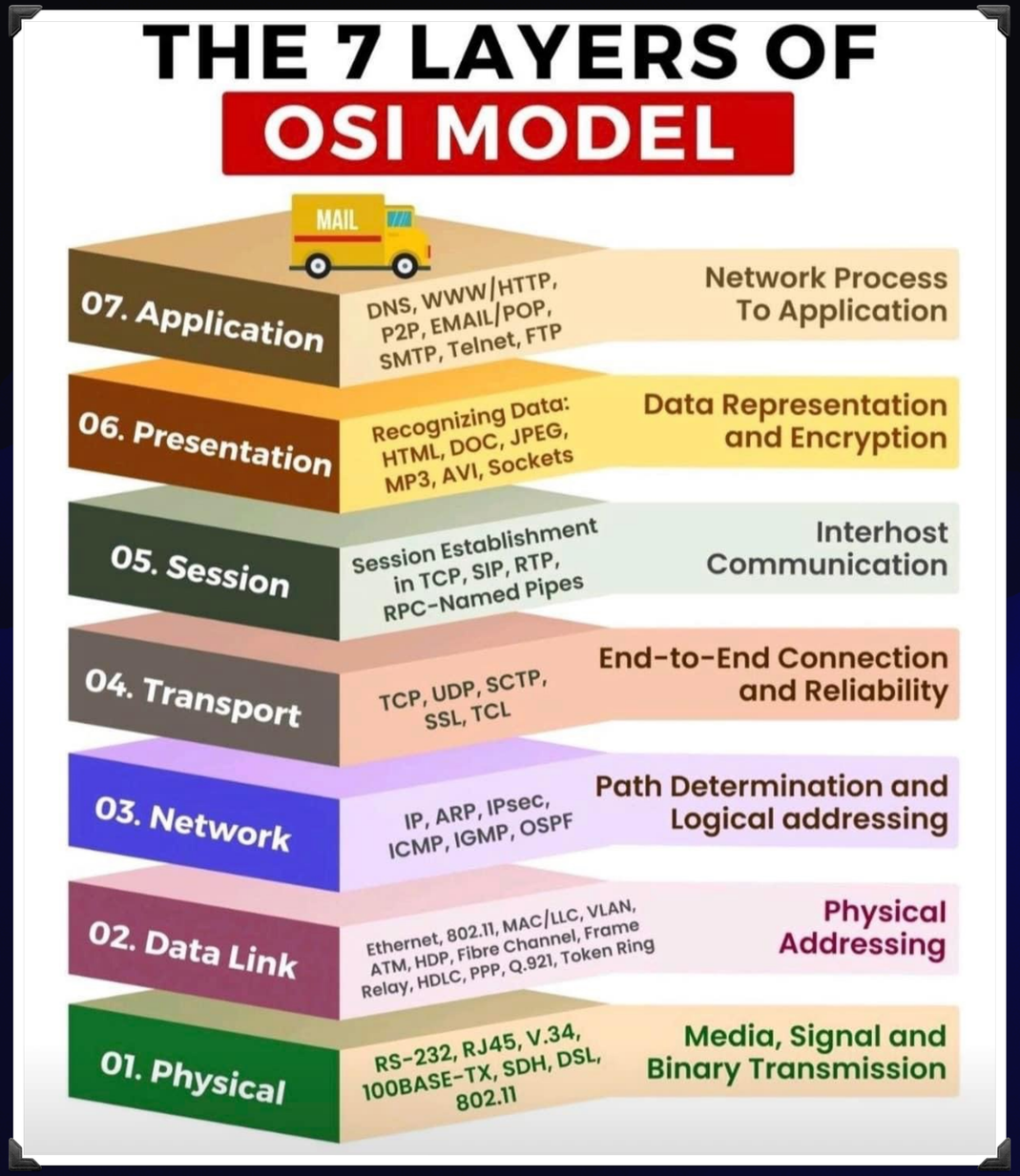
Larger networks have additional security requirements:

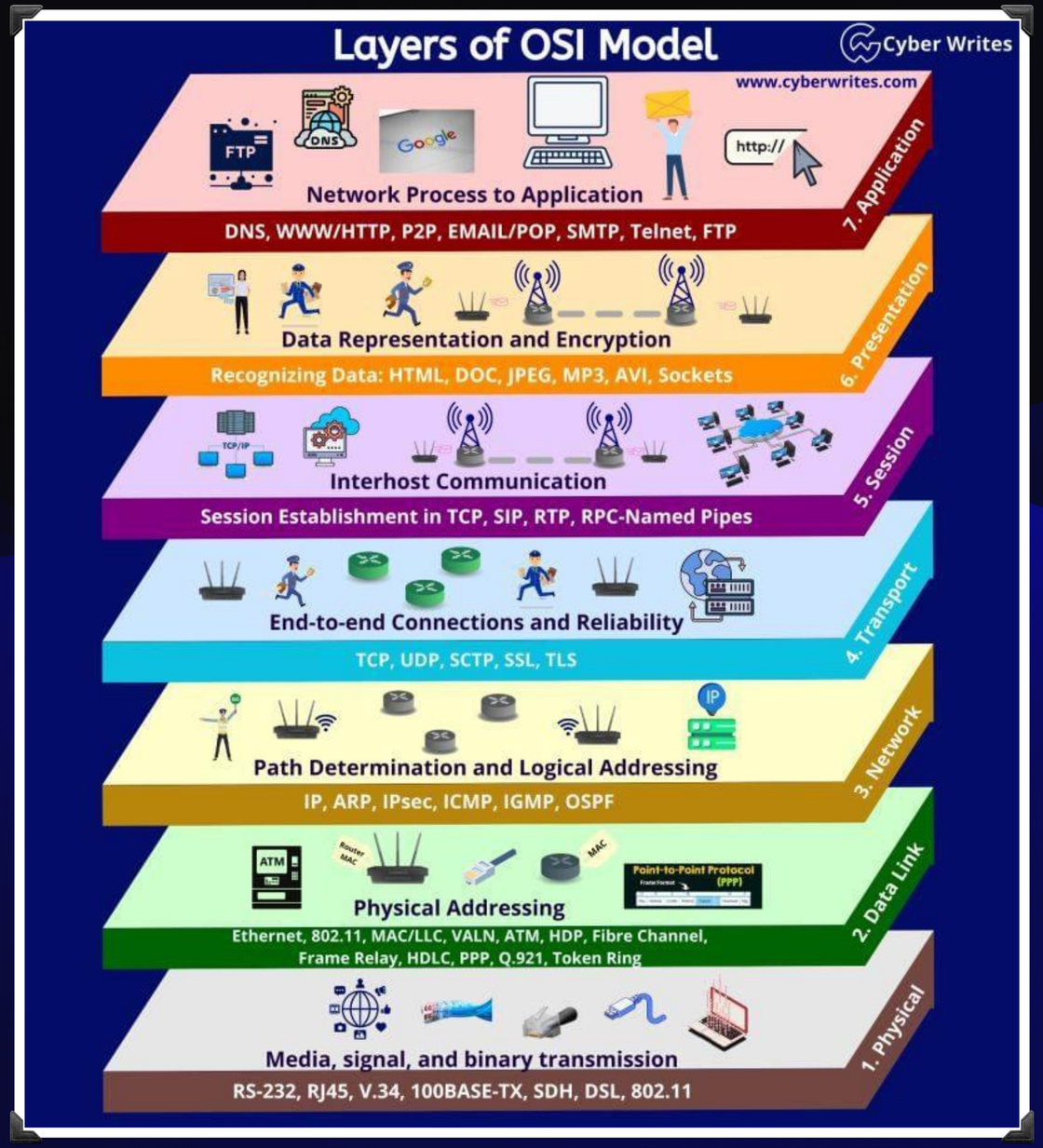
- Dedicated firewall system
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

The study of network security starts with a clear understanding of the underlying switching and routing infrastructure.

OSI and TCP/IP Protocol Fundamental

Session II


THE 7 LAYERS OF
OSI MODEL
MAIL
07. Application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
Network Process To Application
06. Presentation
Recognizing Data: HTML, DOC, JPEG, MP3, AVI, Sockets
Data Representation and Encryption
05. Session
Session Establishment in TCP, SIP, RTP, RPC-Named Pipes
Interhost Communication
04. Transport
TCP, UDP, SCTP, SSL, TCL
End-to-End Connection and Reliability
03. Network
IP, ARP, IPsec, ICMP, IGMP, OSPF
Path Determination and Logical addressing
02. Data Link
Ethernet, 802.11, MAC/LLC, VLAN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring
Physical Addressing
01. Physical
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
Media, Signal and Binary Transmission


Layers of OSI Model
Cyber Writes
www.cyberwrites.com
FTP
DNS
Google
http://
Network Process to Application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
7. Application
Data Representation and Encryption
Recognizing Data: HTML, DOC, JPEG, MP3, AVI, Sockets
6. Presentation
TCP/IP
Interhost Communication
Session Establishment in TCP, SIP, RTP, RPC-Named Pipes
5. Session
End-to-end Connections and Reliability
TCP, UDP, SCTP, SSL, TLS
4. Transport
IP
Path Determination and Logical Addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
3. Network
ATM
Router MAC
MAC
Point-to-Point Protocol (PPP)
Physical Addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel, Frame Relay, HDLC, PPP, Q.921, Token Ring
2. Data Link
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
1. Physical

Networking Essentials

Cyber Writes

Network Topologies

The physical topology of a network refers to the physical configuration of cables, computers, and network devices. Logical topology is the method used to pass information between network devices.


BUS Topology


MESH Topology


STAR Topology


RING Topology


TREE Topology


HYBRID Topology

Coaxial Cable

The 5-4-3 Rule states that a 10Base2 network can have 5 cable segments connected with 4 repeaters but only 3 of the segments can be occupied by computers with a maximum of 30 computers per segment.

- *Thicknet cables are 0.5 inches thick and have a 50 ohm impedance.*
- *Thinnet cables are 0.25 inches thick and have a 50 ohm impedance.*

Thicknet is often used as a backbone. A transceiver with a vampire tap penetrates the core of the cable. From the transceiver a DB-15 connector plugs into the AUI port on a given device.

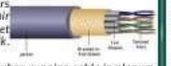
Type: 10Base5 (Coaxial)

Name(s) : RG-8, RG-11 Thicknet Coax
Speed : 10 Mbps
Connector : AUI / DIX
Max.Length : 500 meters (1,640 ft)

Type: 10Base2 (Coaxial)

Name(s) : RG-58 Thicknet Coax
Speed : 10 Mbps
Connector : BNC
Max.Length : 185 meters (670 ft)

Twisted-Pair Cabling (10 Base-T)



Shielded Twisted Pair (STP) differs from UnShielded Twisted Pair (UTP) in that it has a foil jacket that helps prevent crosstalk. Crosstalk is interference from an

Plenum grade cabling is required when running cable in plenum spaces. The plenum is the space between building floors that is used for air circulation in heating and air conditioning systems, typically between the structural ceiling and the suspended ceiling or under a raised Fa floor. Plenum grade cable is resistant to fire and does not emit poisonous gasses when burned.

Type: 10BaseT (Twisted Pair)

Name(s) : Cat 3, 4, 5 Twisted Pair
Speed : 10 -100 Mbps
Connector : RJ - 45
Max.Length : 100 meters (328 ft.)

Type: 100BaseT (Twisted Pair)

Name(s) : Cat 5 Twisted Pair
Speed : 100 Mbps
Connector : RJ - 45
Max.Length : 100 meters (328 ft.)

Fiber-Optic Cable

Fiber Optic cabling has built in security. Unlike other cable mediums, the dielectric nature of optical fiber makes it impossible to remotely detect the signal being transmitted within the cable.

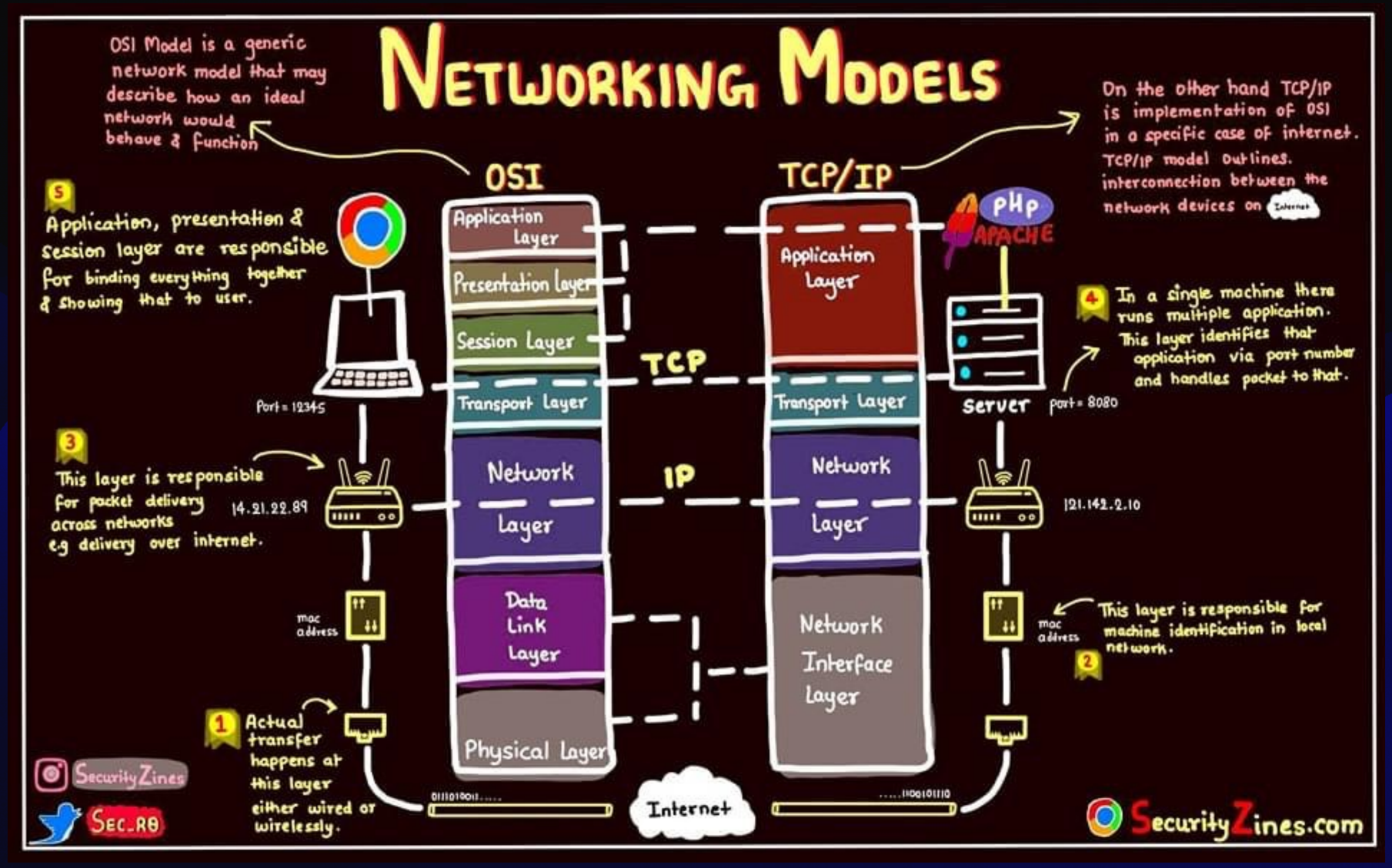
The only way to detect fiber signal is by accessing the optical fiber itself which is easily detectable by security surveillance.

Type: 10BaseFL (Fiber Optic)

Name(s) : Cat. 5 Twisted Pair
Speed : 100 Mbps
Connector : RJ - 45
Max.Length : 100 meters (328 ft.)

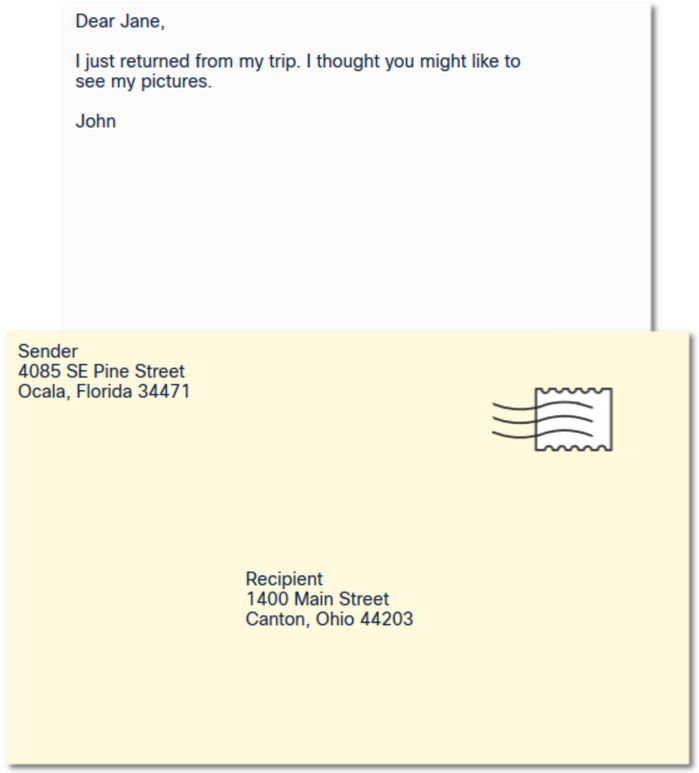
THE OSI MODEL

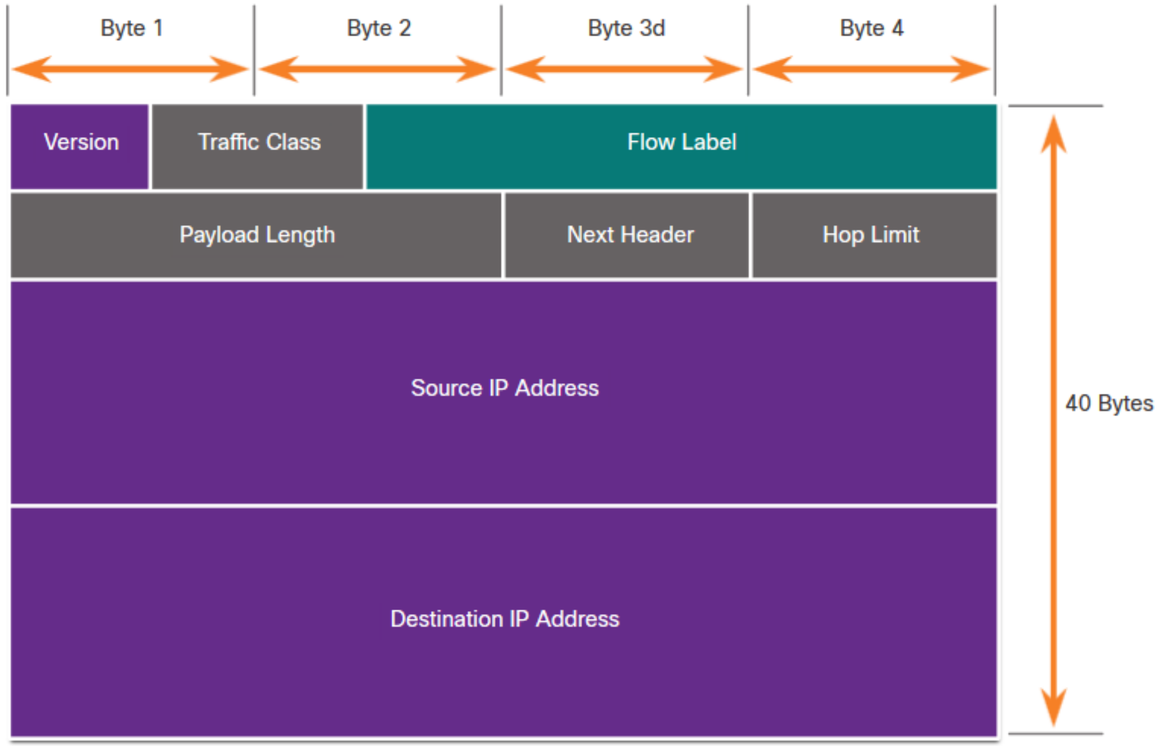
Layer	Description	Device	Implementations & Protocols
Application (7)	Provides services directly to user applications. Identifies communication partners, identifies quality of service, considers user authentication and privacy, and determines if adequate resources are present.	Gateway	SMB, HTTP, SMTP, FTP, SNMP, Telnet, AppleTalk
Presentation (6)	Performs data transformations and services including formatting, compression, and encryption services to provide a common interface for user applications.	Gateway & Redirectors	HTTP, FTP, Telnet, SMTP, AFP, TDI
Session (5)	Establishes, manages and terminates connections between applications at each end. Allows 2 applications to communicate over a network by opening a session and synchronizing the involved computers.	Gateway	NetBEUI, TCP, UDP, SPX
Transport (4)	Provides transparent transfer of data between end systems by insulating layers 5-7 from complexities of layers 1-3. Responsible for end-to-end error recovery and flow control and ensures complete data transfer.	Gateway	IP, IPX, NWLink NetBEUI
Network (3)	Establishes, maintains, and terminates network connections. Handles traffic management including addressing, routing, switching, forwarding, logical paths and virtual circuits, error handling, congestion control and packet sequencing.	Router & Brouter	IP, IPX, NWLink NetBEUI
Data Link (2)	Divided into two sub-layers: The Media Access Control (MAC) sub-layer controls how a networked computer gains access to the data and permission to transmit it. The Logical Link Control (LLC) sub-layer controls frame synchronization, flow control and error checking.	Switch, Bridge & Router	Ethernet, PPP HDLC
Physical (1)	Controls transmission of the bit stream data over the physical medium. Standards for this layer address transmission at the electrical and mechanical level including signal voltage swing, voltage duration, etc..	Multiplexer & Repeater	Ethernet, Token Ring, FDDI


NETWORKING MODELS
OSI Model is a generic network model that may describe how an ideal network would behave & function
On the other hand TCP/IP is implementation of OSI in a specific case of internet. TCP/IP model outlines. interconnection between the network devices on Internet
OSI
TCP/IP
5 Application, presentation & session layer are responsible for binding everything together & showing that to user.
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Transport Layer
Network Layer
Network Interface Layer
TCP
IP
PHP
APACHE
4 In a single machine there runs multiple application. This layer identifies that application via port number and handles packet to that.
Port = 12345
Server
port = 8080
3 This layer is responsible for packet delivery across networks e.g delivery over internet.
14.21.22.89
121.142.2.10
mac address
mac address
This layer is responsible for machine identification in local network.
2
1 Actual transfer happens at this layer either wired or wirelessly.
Internet
SecurityZines
SEC_R0
SecurityZines.com

Message Formatting and Encapsulation

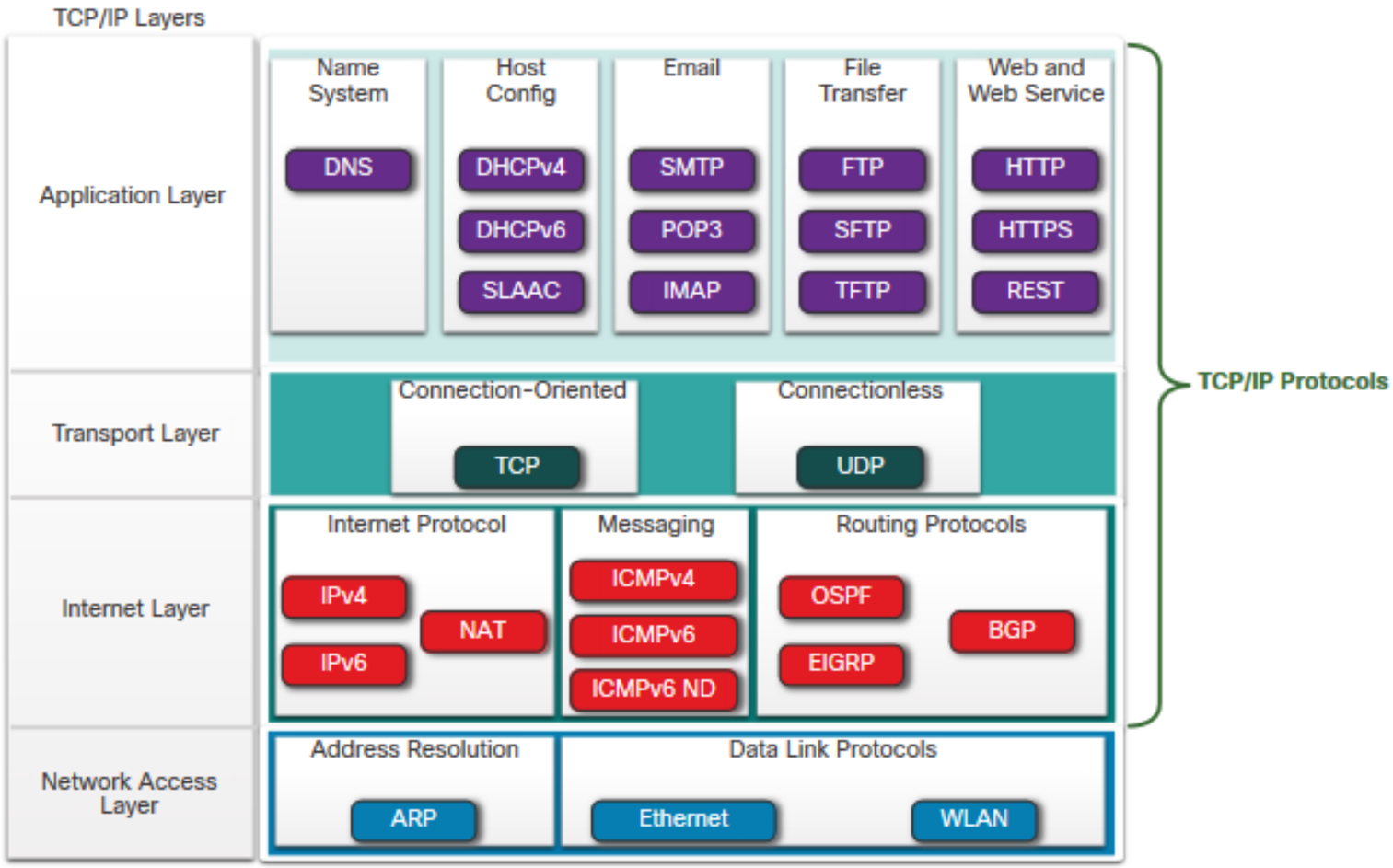
- When a message is sent, it must use a specific format or structure.
- Message formats depend on the type of message and the channel that is used to deliver the message.





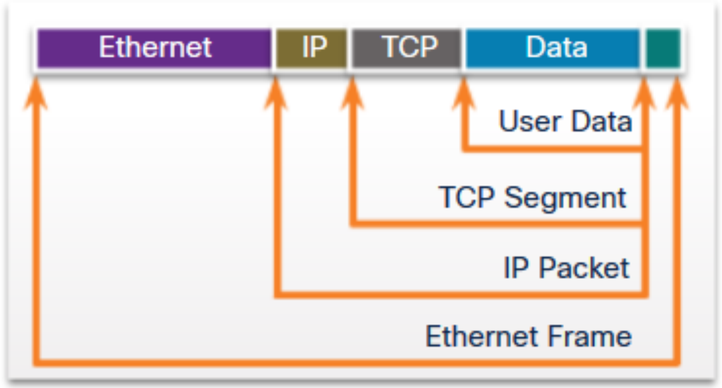
TCP/IP Protocol Suite

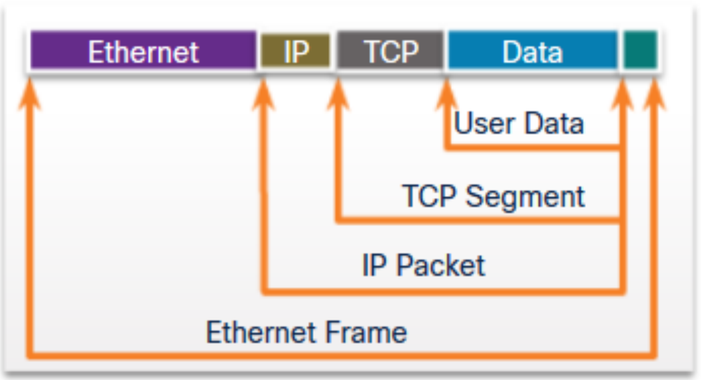
- TCP/IP is the protocol suite used by the internet and includes many protocols.
- TCP/IP is:
  - An open standard protocol suite that is freely available to the public and can be used by any vendor
  - A standards-based protocol suite that is endorsed by the networking industry and approved by a standards organization to ensure interoperability

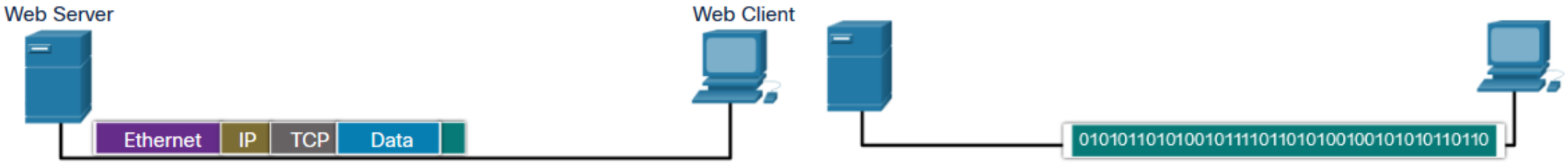


TCP/IP Communication Process

- A web server encapsulating and sending a web page to a client.
- A client de-encapsulating the web page for the web browser







IP Command Cheat Sheet

Syntax

$ ip [options] OBJECT COMMAND

Display the command syntax and lists all available options

$ ip help

IP Objects

OBJECTS	DESCRIPTION
address	IPv4 or IPv6 addresses on a device
link	Network interfaces for example Wi-Fi adaptors and wired connections
route	Routing table entry
maddress	Multicast address
neighbour	Neighbor entry, which contains information about a neighboring device on the network.
mroute	Multicast routing cache entry
rule	Rule in routing policy database

Quick Tip

When working with the IP command, you can save time by using shortened or abbreviated object names. For instance, instead of typing "address," you can simply use "addr" or even just "a." Give it a shot!

IP Options

OPTION	DESCRIPTION
-a	Executes specified command over all objects
-d	Output more detailed information
-j	Displays the output in JSON format
-p	Adds indentation to the JSON output for readability
-s	Display extra statistics
-6	Instructs IP to display only IPv6 Addresses
-h	Output statistics with human readable values
-c	Enable colored output
-t	Display timestamps in the output
-br	Print only basic information in a tabular format

IP Command vs Net-Tools

NET-TOOLS	IPROUTE COMMANDS (IP)
$ arp -a	**$ ip neigh**
$ ifconfig -a	**$ ip addr**
$ netstat -g	**$ ip maddress**
$ route	**$ ip route**

Manage IP Addresses

COMMAND	DESCRIPTION
$ ip addr help	Display a list of commands and arguments for the address object.
$ ip addr show	Display information about all ip addresses.
$ ip addr show dev wlan0	Display IP addresses on the specified network interface
$ sudo ip addr add 192.168.1.21/24 dev wlan0	Add IP Address to the specified interface. Note you can add multiple addresses on the same by repeating the command with a different IP Address.
sudo ip addr del 192.168.1.22/24 dev wlan0	Delete IP Address on the specified interface.

Manage Network Interfaces

COMMAND	DESCRIPTION
$ ip link help	Display a list of commands and arguments for the link object.
$ ip link show	Display information about all available network interfaces
$ ip link show dev wlan0	Display information about a specific network interface
$ ip link set dev wlan0 down	Bring the specified interface down.
$ ip link set dev wlan0 up	Bring the specified interface up.

Manage Routing Table

COMMAND	DESCRIPTION
$ ip route help	Display a list of commands and arguments for the route object.
$ ip route list	List all of the route entries in the kernel
$ ip route list 10.18.0.0/17	Display routing information for a specific network
$ ip route add 10.18.0.0/17 via 192.168.1.1	Add a new entry to the routing table
$ ip route add 10.18.0.0/17 dev wlan0	Add a new entry to the routing table via the interface wlan0
$ ip route add default via 192.168.1.1 dev wlan0	Add the default route
$ ip route del default	Delete the default route
$ ip route del 192.168.92.0/24 via 192.168.92.1	Delete the specified route

Manage Neighbour Entries

COMMAND	DESCRIPTION
$ ip neigh help	Display a list of commands and arguments for the neighbour object.
$ ip neigh show	Display neighbour table entries
$ ip neigh add 192.168.0.2 lladdr A4:C3:F0:9F:56:B9 dev wlan0	Add entry to the ARP table
$ ip neigh del 192.168.0.2 dev wlan0	Remove the ARP entry

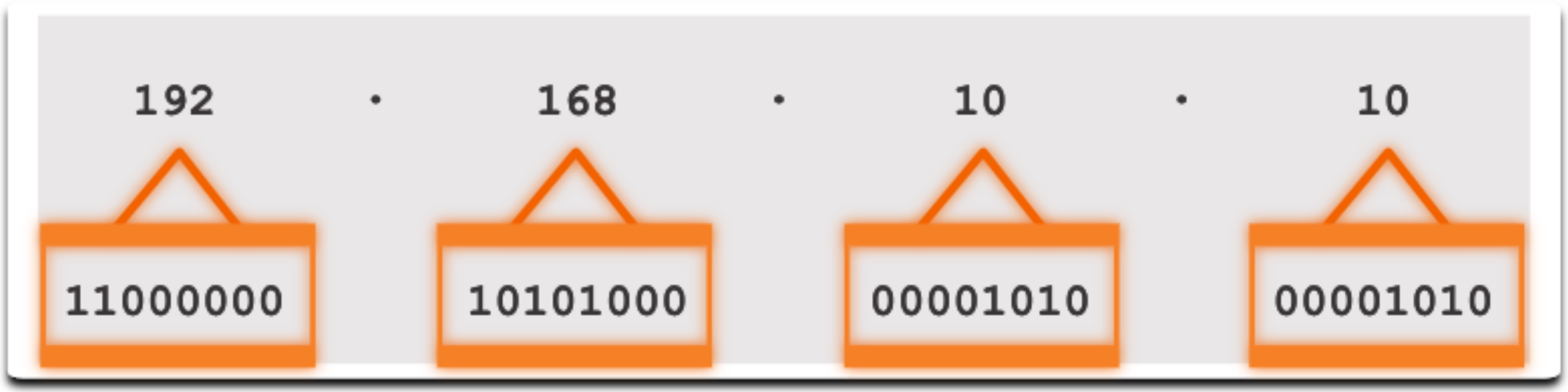
Important

When making changes to network interfaces, addresses, or routes, exercise extreme caution. It is simple to disconnect the server from the main network, which may require a system reboot to fix. When experimenting with new commands in a test environment or non-critical systems.


OSI Layers
Cyber Attacks
Possible Cyber Attacks
OSI Layers
Attack Controls
SQL injection, Cross-Site Scripting (XSS)
Remote Code Execution (RCE).
Application
Regular Patching, remediate known vulnerabilities, Input validation, WAF
Data format manipulation, code injection,
and serialization attacks.
Presentation
Validate / sanitize user inputs to prevent
code injection, use secure data serialisation
libraries
Session hijacking, token-based attacks, and
session sidejacking.
Session
randomize session IDs, enforce secure logout
mechanisms, and use secure tokens for user
authentication.
SYN flood attacks, TCP session hijacking, and UDP flooding
Transport
monitor/ control FW traffic at the transport layer, mitigate SYN flood attacks,
implement secure data exchange
IP spoofing, ICMP attacks (e.g., ping flood, ping of death), and denial-of-service (DoS) attacks.
Network
Firewall filtering, use IDS and IPS and configure routers to prevent IP address
spoofing.
MAC address spoofing, ARP spoofing, VLAN
hopping, and Ethernet frame manipulation.
Data Link
Port security to limit the number of MAC IDs
per port, utilize ARP spoofing, enable VLAN
trunking protocols
Physical tampering, eavesdropping, and MITM at the physical level, such as
tapping into network cables or disrupting power supply
Physical
Access controls, CCTV surveillance, and secured cabling to prevent unauthorized access to networking infrastructure. Regularly inspection and monitoring

IPv4 Addresses

- Routers and computers only understand binary, while humans work in decimal. It is important for you to gain a thorough understanding of these two numbering systems and how they are used in networking.



Hexadecimal and IPv6 Addresses

- To understand IPv6 addresses, you must be able to convert hexadecimal to decimal and vice versa.
- Hexadecimal is a base sixteen numbering system, using the digits 0 through 9 and letters A to F.
- It is easier to express a value as a single hexadecimal digit than as four binary bit.
- Hexadecimal is used to represent IPv6 addresses and MAC addresses.

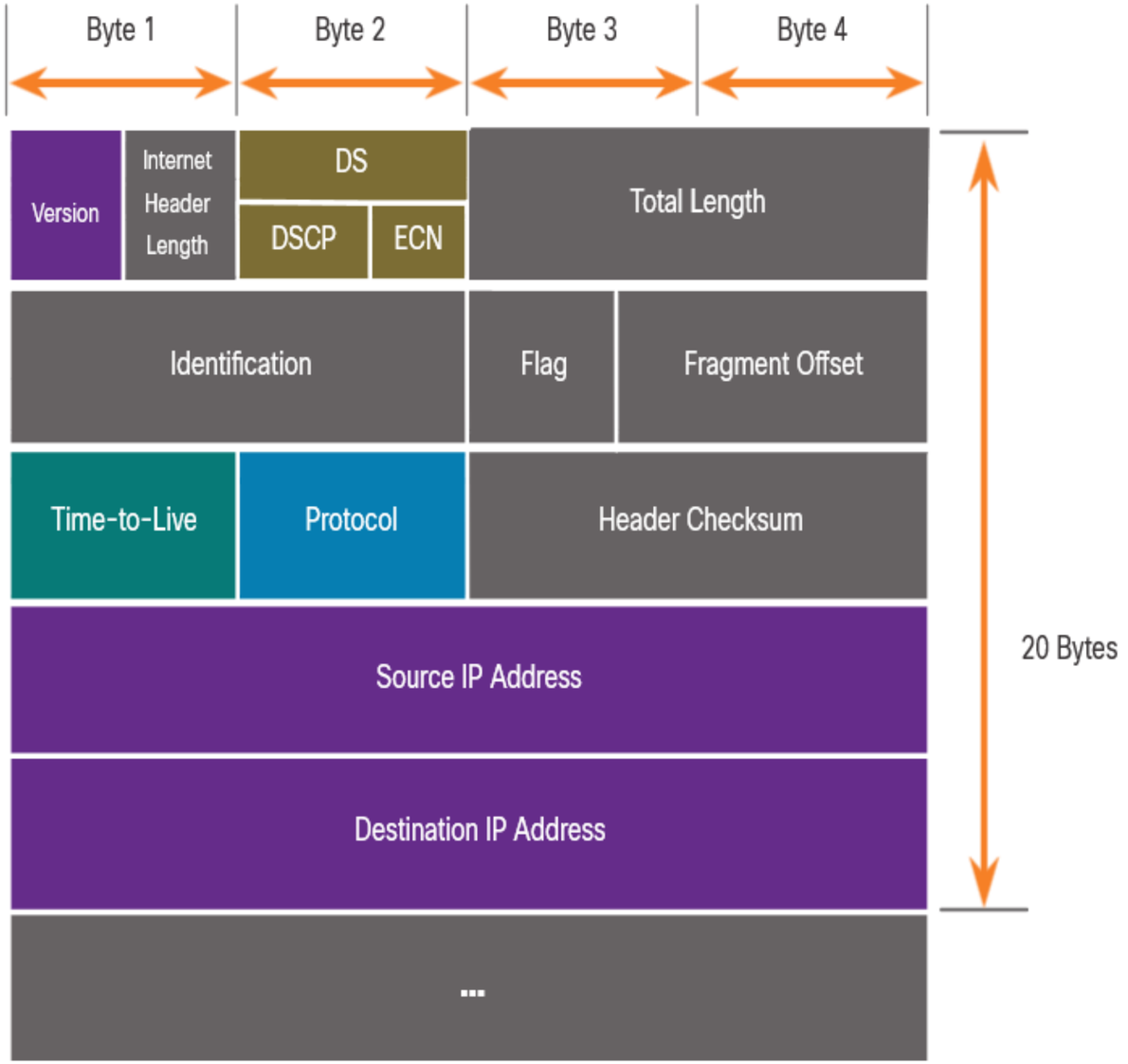
Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

IPv4 Packet Header Fields

The IPv4 network header characteristics:

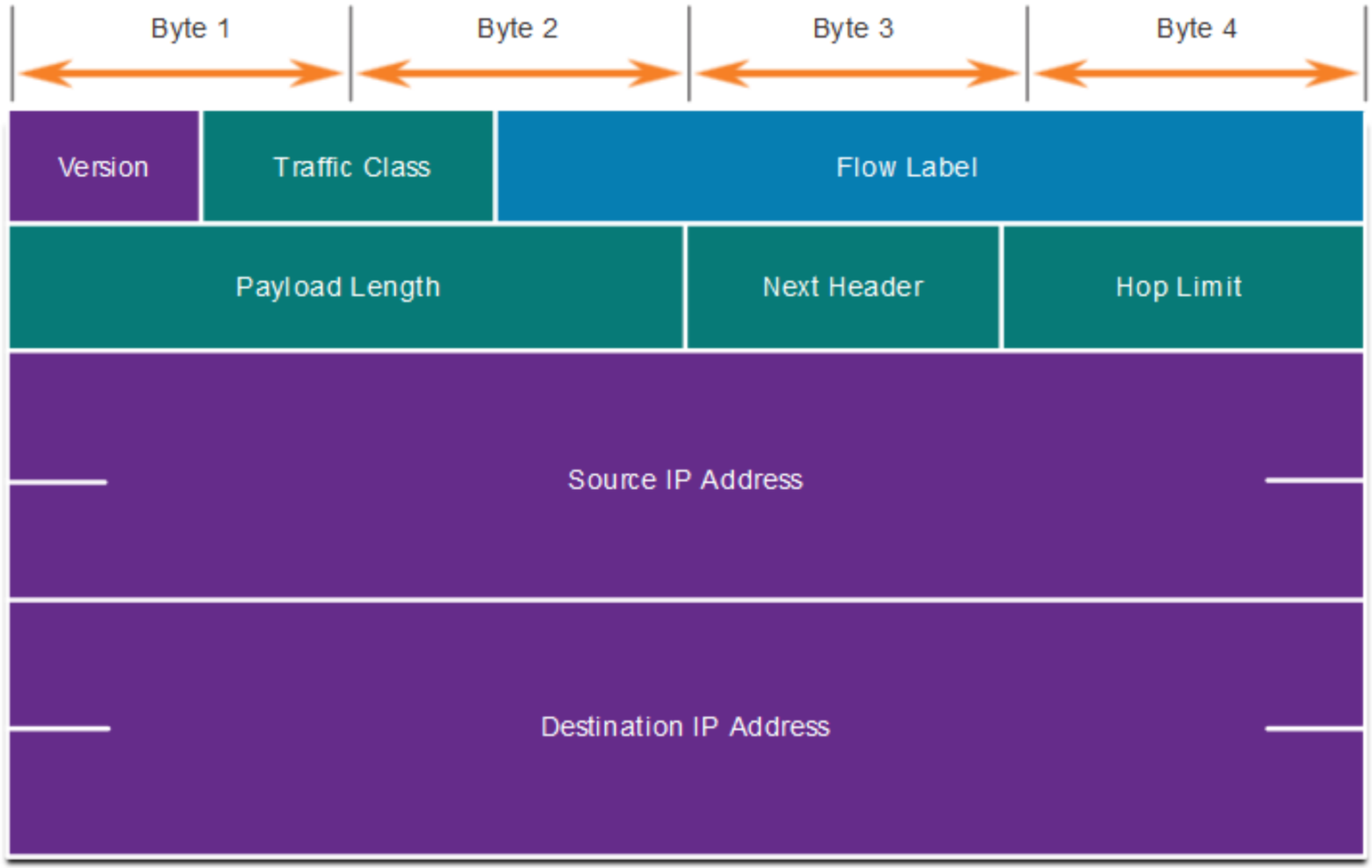
- It is in binary.
- Contains several fields of information
- Diagram is read from left to right, 4 bytes per line
- The two most important fields are the source and destination.

Protocols may have may have one or more functions.



IPv4 Packet Header Fields in the IPv6 Packet Header

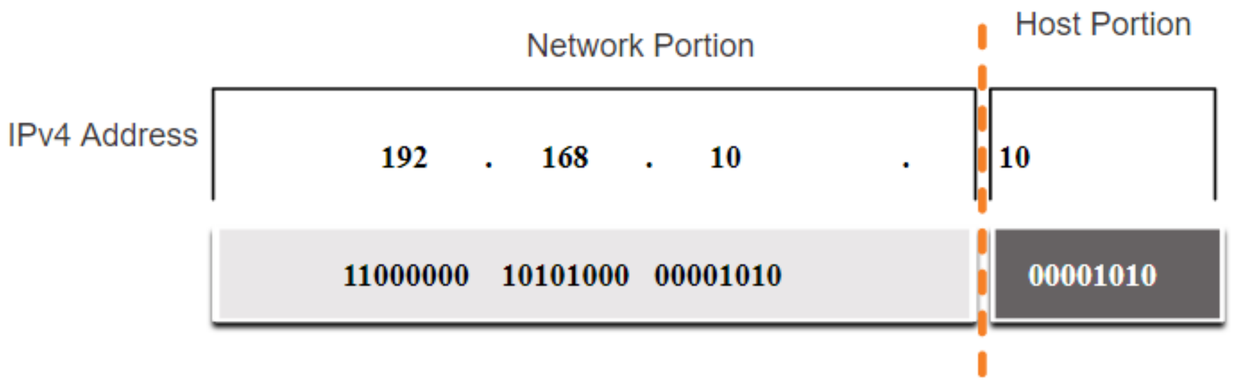
- The IPv6 header is simplified, but not smaller.
- The header is fixed at 40 Bytes or octets long.
- Several IPv4 fields were removed to improve performance.
- Some IPv4 fields were removed to improve performance:
  - Flag
  - Fragment Offset
  - Header Checksum



Network and Host Portions

- An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.

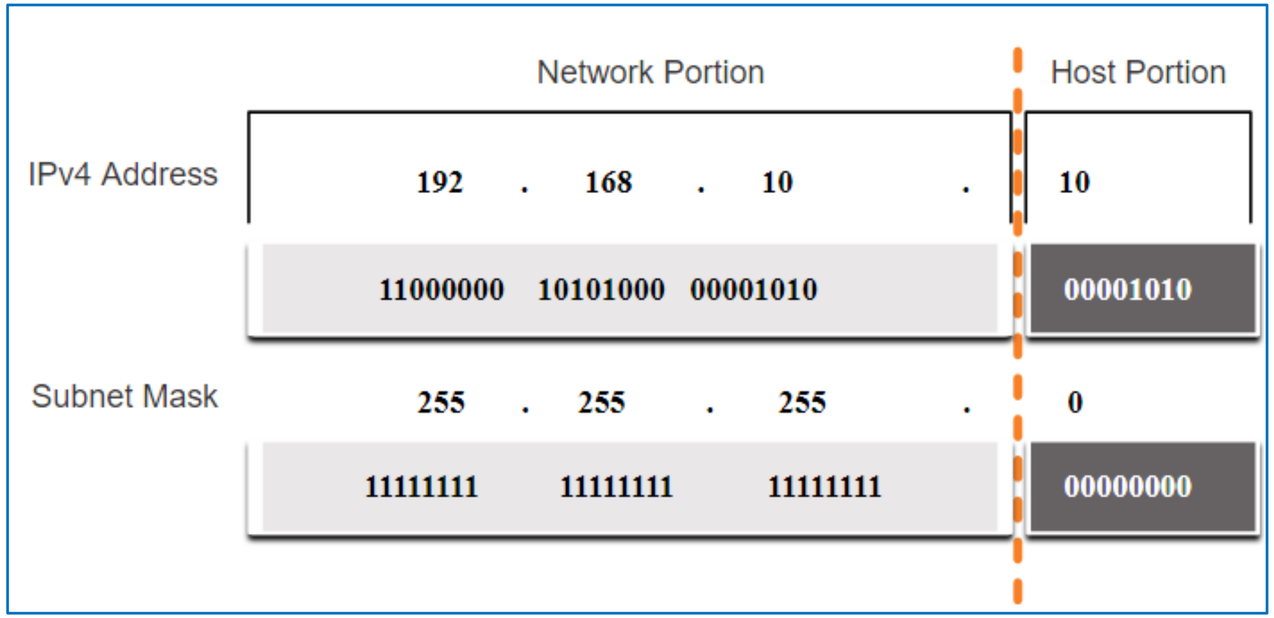
- When determining the network portion versus the host portion, you must look at the 32-bit stream.
- A subnet mask is used to determine the network and host portions.



The Subnet Mask

- To identify the network and host portions of an IPv4 address, the subnet mask is compared to the IPv4 address bit for bit, from left to right.

- The actual process used to identify the network and host portions is called ANDing.



The Prefix Length

- A prefix length is a less cumbersome method used to identify a subnet mask address.

- The prefix length is the number of bits set to 1 in the subnet mask.

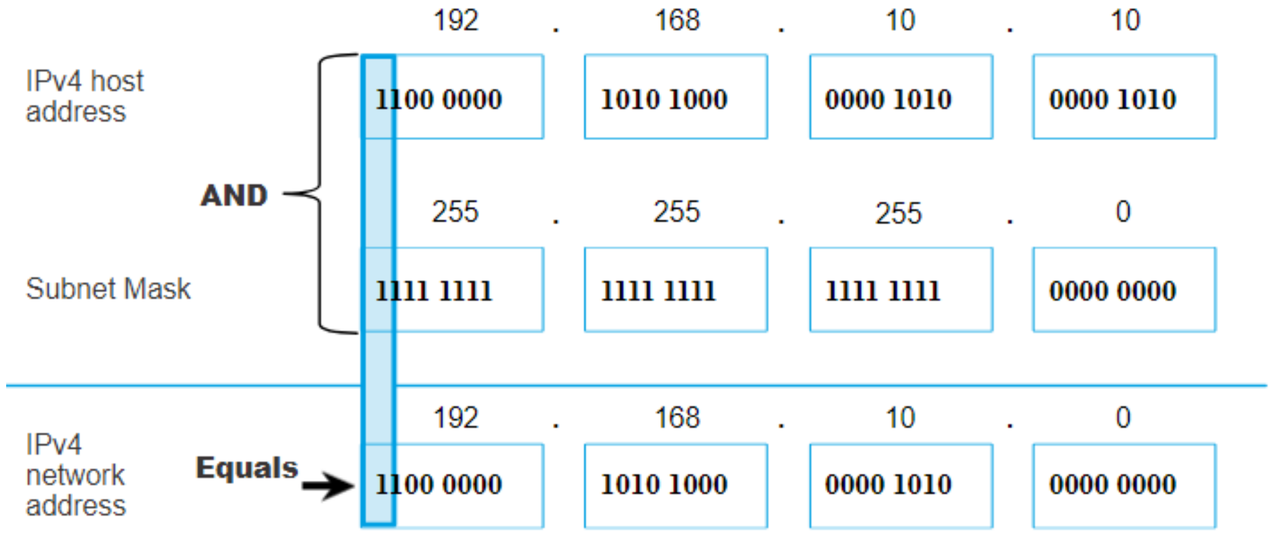
- It is written in “slash notation” therefore, count the number of bits in the subnet mask and prepend it with a slash.

Subnet Mask	32-bit Address	Prefix Length
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Determining the Network: Logical AND

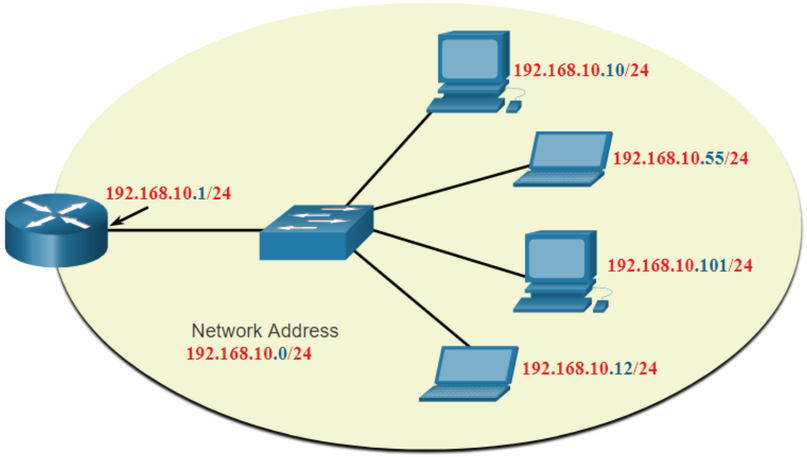
- A logical AND Boolean operation is used in determining the network address.
- Logical AND is the comparison of two bits where only a 1 AND 1 produces a 1 and any other combination results in a 0.
- 1 AND 1 = 1, 0 AND 1 = 0, 1 AND 0 = 0, 0 AND 0 = 0
- 1 = True and 0 = False

- To identify the network address, the host IPv4 address is logically ANDed, bit by bit, with the subnet mask to identify the network address.



Network, Host, and Broadcast Addresses

- Within each network are three types of IP addresses:
  - Network address
  - Host addresses
  - Broadcast address



	Network Portion			Host Portion	Host Bits
Subnet mask **255.255.255.**0 or **/24**	255 11111111	255 11111111	255 11111111	0 00000000	
Network address **192.168.10.**0 or **/24**	192 11000000	168 10100000	10 00001010	0 00000000	All 0s
First address **192.168.10.**1 or **/24**	192 11000000	168 10100000	10 00001010	1 00000001	All 0s and a 1
Last address **192.168.10.**254 or **/24**	192 11000000	168 10100000	10 00001010	254 11111110	All 1s and a 0
Broadcast address **192.168.10.**255 or **/24**	192 11000000	168 10100000	10 00001010	255 11111111	All 1s

Subnet on an Octet Boundary

- Networks are most easily subnetted at the octet boundary of /8, /16, and /24.
- Notice that using longer prefix lengths decreases the number of hosts per subnet.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	**255**.0.0.0	**nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh **11111111**.00000000.00000000.00000000	16,777,214
/16	**255.255**.0.0	**nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh **11111111.11111111**.00000000.00000000	65,534
/24	**255.255.255**.0	**nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh **11111111.11111111.11111111**.00000000	254

Subnet on an Octet Boundary (Cont.)

- In the first table 10.0.0.0/8 is subnetted using /16 and in the second table, a /24 mask.

Subnet Address (256 Possible Subnets)	**Host Range** (65,534 possible hosts per subnet)	**Broadcast**
10.0.0.0/**16**	**10.0**.0.1 - **10.0**.255.254	**10.0**.255.255
10.1.0.0/**16**	**10.1**.0.1 - **10.1**.255.254	**10.1**.255.255
10.2.0.0/**16**	**10.2**.0.1 - **10.2**.255.254	**10.2**.255.255
10.3.0.0/**16**	**10.3**.0.1 - **10.3**.255.254	**10.3**.255.255
10.4.0.0/**16**	**10.4**.0.1 - **10.4**.255.254	**10.4**.255.255
10.5.0.0/**16**	**10.5**.0.1 - **10.5**.255.254	**10.5**.255.255
10.6.0.0/**16**	**10.6**.0.1 - **10.6**.255.254	**10.6**.255.255
10.7.0.0/**16**	**10.7**.0.1 - **10.7**.255.254	**10.7**.255.255
…	…	…
10.255.0.0/**16**	**10.255**.0.1 - **10.255**.255.254	**10.255**.255.255

Subnet Address (65,536 Possible Subnets)	**Host Range** (254 possible hosts per subnet)	**Broadcast**
10.0.0.0/**24**	**10.0.0**.1 - **10.0.0**.254	**10.0.0**.255
10.0.1.0/**24**	**10.0.1**.1 - **10.0.1**.254	**10.0.1**.255
10.0.2.0/**24**	**10.0.2**.1 - **10.0.2**.254	**10.0.2**.255
…	…	…
10.0.255.0/**24**	**10.0.255**.1 - **10.0.255**.254	**10.0.255**.255
10.1.0.0/**24**	**10.1.0**.1 - **10.1.0**.254	**10.1.0**.255
10.1.1.0/**24**	**10.1.1**.1 - **10.1.1**.254	**10.1.1**.255
10.1.2.0/**24**	**10.1.2**.1 - **10.1.2**.254	**10.1.2**.255
…	…	…
10.100.0.0/**24**	**10.100.0**.1 - **10.100.0**.254	**10.100.0**.255
…	…	…
10.255.255.0/**24**	**10.255.255**.1 - **10.2255.255**.254	**10.255.255**.255

Subnet within an Octet Boundary

- Refer to the table to see six ways to subnet a /24 network.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of subnets	# of hosts
/25	255.255.255.128	nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh 11111111.11111111.11111111.**1**0000000	**2**	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh 11111111.11111111.11111111.**11**000000	**4**	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh 11111111.11111111.11111111.**111**00000	**8**	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh 11111111.11111111.11111111.**1111**0000	**16**	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh 11111111.11111111.11111111.**11111**000	**32**	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh 11111111.11111111.11111111.**111111**00	**64**	2

IPv6 Addressing Formats

- IPv6 addresses are 128 bits in length and written in hexadecimal.
- IPv6 addresses are not case-sensitive and can be written in either lowercase or uppercase.
- The preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values.
- In IPv6, a hextet is the unofficial term used to refer to a segment of 16 bits, or four hexadecimal values.
- Examples of IPv6 addresses in the preferred format:

```
2001:0db8:0000:1111:0000:0000:0000:0200
2001:0db8:0000:00a3:abcd:0000:0000:1234
```

Rule 1 – Omit Leading Zero

The first rule to help reduce the notation of IPv6 addresses is to omit any leading 0s (zeros).

Examples:

- 01ab can be represented as 1ab
- 09f0 can be represented as 9f0
- 0a00 can be represented as a00
- 00ab can be represented as ab

Note: This rule only applies to leading 0s, NOT to trailing 0s, otherwise the address would be ambiguous.

Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200
No leading zeros	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

Rule 2 – Double Colon

A double colon (::) can replace any single, contiguous string of one or more 16-bit hextets consisting of all zeros.

Example:

- 2001:db8:cafe:1:0:0:0:1 (leading 0s omitted) could be represented as 2001:db8:cafe:1::1

Note: The double colon (::) can only be used once within an address, otherwise there would be more than one possible resulting address.

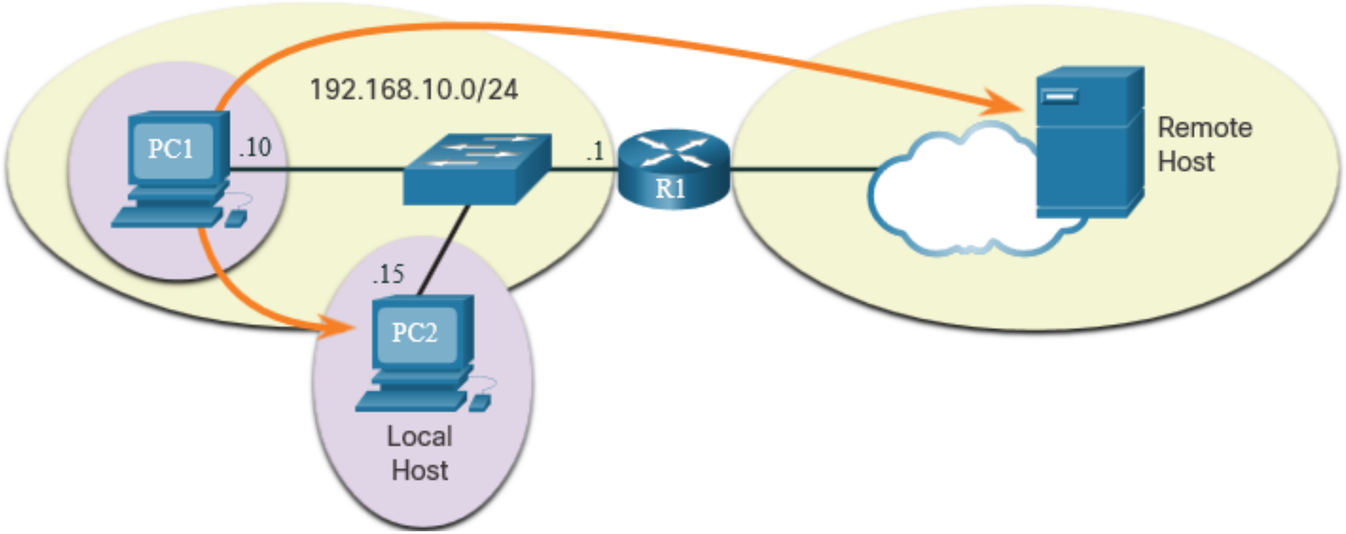
Type	Format
Preferred	2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200
Compressed	2001:db8:0:1111::200

- Internet Protocol Version 6 Address Space

How a Host Routes

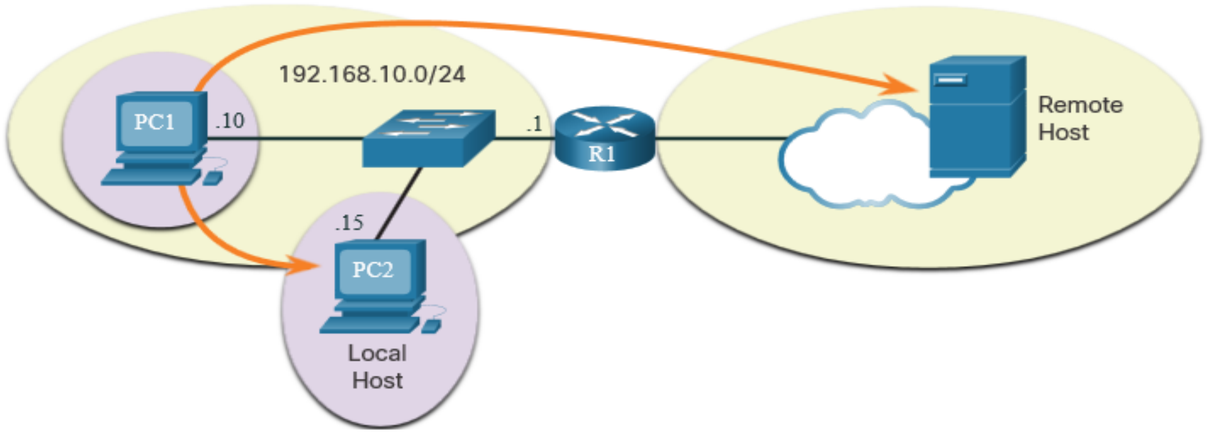
Host Forwarding Decision

- Packets are always created at the source.
- Each host devices creates their own routing table.
- A host can send packets to the following:
  - Itself – 127.0.0.1 (IPv4), ::1 (IPv6)
  - Local Hosts – destination is on the same LAN
  - Remote Hosts – devices are not on the same LAN



Host Forwarding Decision (Cont.)

- The Source device determines whether the destination is local or remote
- Method of determination:
  - IPv4 – Source uses its own IP address and Subnet mask, along with the destination IP address
  - IPv6 – Source uses the network address and prefix advertised by the local router
- Local traffic is dumped out the host interface to be handled by an intermediary device.
- Remote traffic is forwarded directly to the default gateway on the LAN.



Default Gateway

A router or layer 3 switch can be a default-gateway.

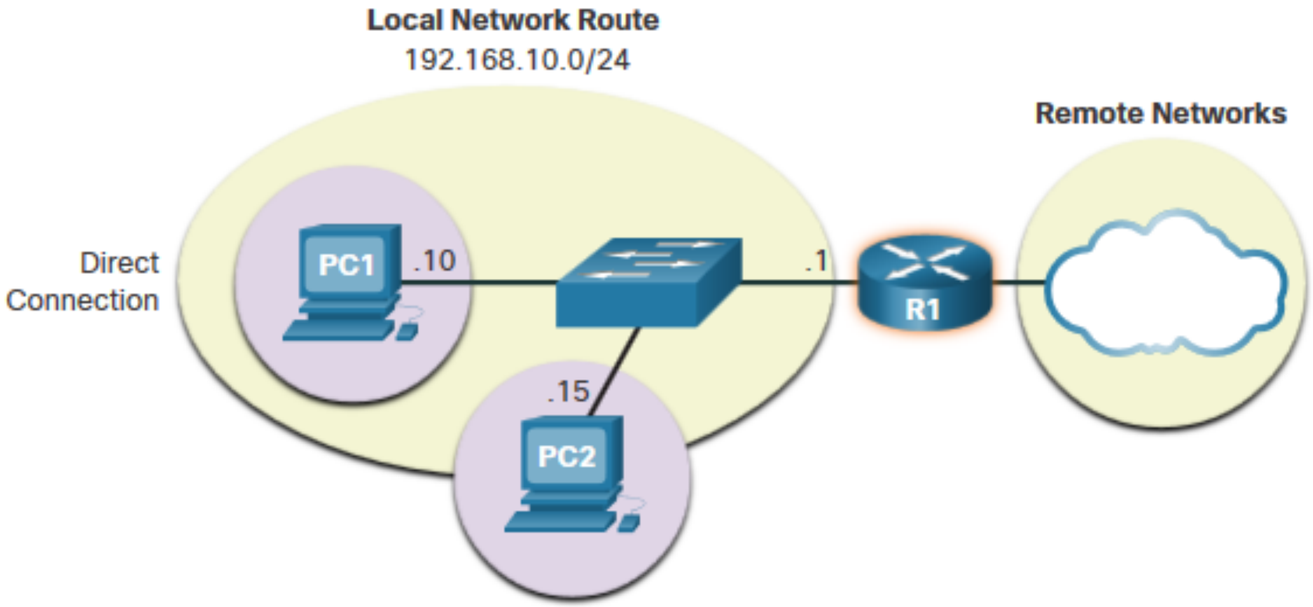
Features of a default gateway (DGW):

- It must have an IP address in the same range as the rest of the LAN.
- It can accept data from the LAN and is capable of forwarding traffic off of the LAN.
- It can route to other networks.

If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

A Host Routes to the Default Gateway

- The host will know the default gateway (DGW) either statically or through DHCP in IPv4.
- IPv6 sends the DGW through a router solicitation (RS) or can be configured manually.
- A DGW is static route which will be a last resort route in the routing table.
- All device on the LAN will need the DGW of the router if they intend to send traffic remotely.



Host Routing Tables

- On Windows, route print or netstat -r to display the PC routing table
- Three sections displayed by these two commands:
  - Interface List – all potential interfaces and MAC addressing
  - IPv4 Routing Table
  - IPv6 Routing Table

IPv4 Routing Table for PC1

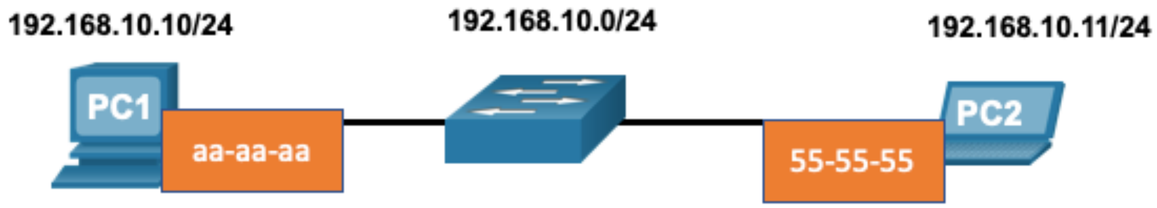
```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```

Destination on Same Network

There are two primary addresses assigned to a device on an Ethernet LAN:

- **Layer 2 physical address (the MAC address)** – Used for NIC to NIC communications on the same Ethernet network.
- **Layer 3 logical address (the IP address)** – Used to send the packet from the source device to the destination device.

Layer 2 addresses are used to deliver frames from one NIC to another NIC on the same network. If a destination IP address is on the same network, the destination MAC address will be that of the destination device.

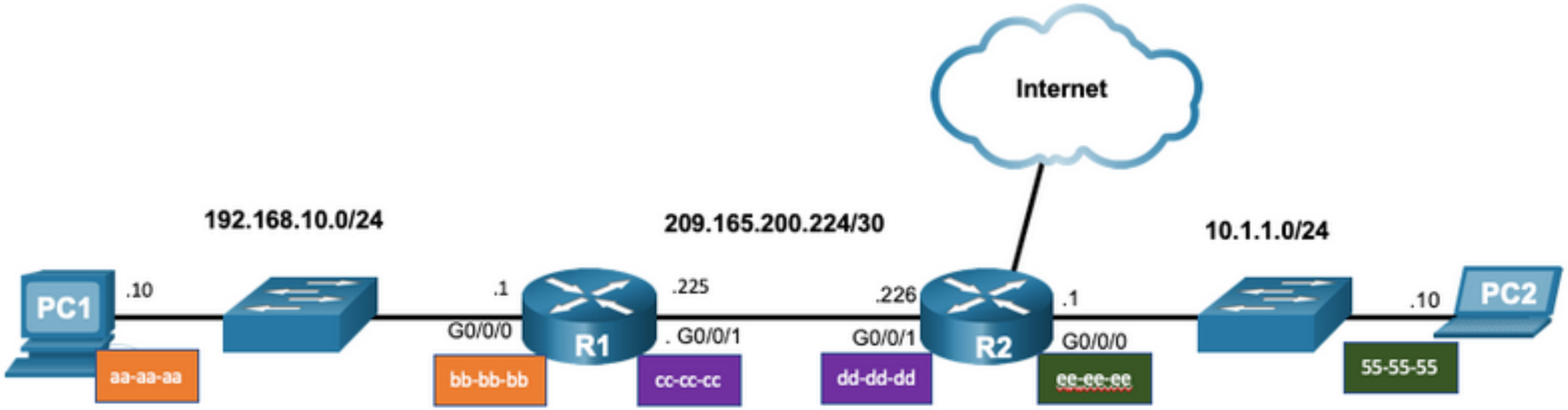


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

Destination on Remote Network

When the destination IP address is on a remote network, the destination MAC address is that of the default gateway.

- ARP is used by IPv4 to associate the IPv4 address of a device with the MAC address of the device NIC.
- ICMPv6 is used by IPv6 to associate the IPv6 address of a device with the MAC address of the device NIC.



Destination MAC	Source MAC	Source IPv4	Destination IPv4
bb-bb-bb	aa-aa-aa	192.168.10.10	10.1.1.10

Switch Architecture, Operation, Configure and Management
Session III

Packet Tracer Program

https://skillsforall.com/course/getting-started-cisco-packet-tracer?courseLang=en-US

IOS Navigation

Primary Command Modes

User EXEC Mode:

- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

```
Router>

Switch>
```

Privileged EXEC Mode:

- Allows access to all commands and features
- Identified by the CLI prompt that ends with the # symbol

```
Router#

Switch#
```

Configuration Mode and Subconfiguration Modes

Global Configuration Mode:

- Used to access configuration options on the device

```
Switch(config)#
```

Line Configuration Mode:

- Used to configure console, SSH, Telnet or AUX access

```
Switch(config-line)#
```

Interface Configuration Mode:

- Used to configure a switch port or router interface

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

Video – IOS CLI Primary Command Modes

This video will cover the following:

- User EXEC mode
- Privilege EXEC mode
- Global Config mode

Navigation Between IOS Modes

- **Privileged EXEC Mode:**
  - To move from user EXEC mode to privilege EXEC mode, use the **enabled** command.

```
Switch> enable
Switch#
```

- **Global Configuration Mode:**
  - To move in and out of global configuration mode, use the **configure terminal** command. To return to privilege EXEC mode, use the **exit** command.

```
Switch(config)#
Switch(config)#exit
Switch#
```

- **Line Configuration Mode:**
  - To move in and out of line configuration mode, use the **line** command followed by the management line type. To return to global configuration mode, use the **exit** command.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

Navigation Between IOS Modes (Cont.)

Subconfiguration Modes:

- To move out of any subconfiguration mode to get back to global configuration mode, use the **exit** command. To return to privilege EXEC mode, use the **end** command or key combination **Ctrl +Z**.

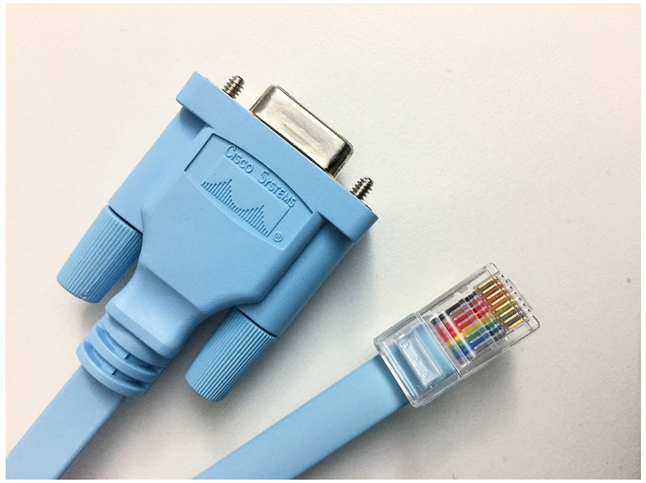
```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

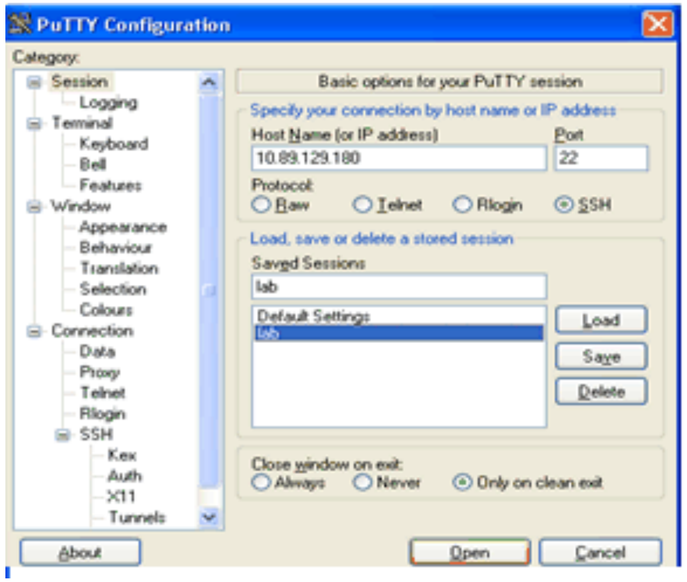
- To move directly from one subconfiguration mode to another, type in the desired subconfiguration mode command. In the example, the command prompt changes from **(config-line)#** to **(config-if)#**.

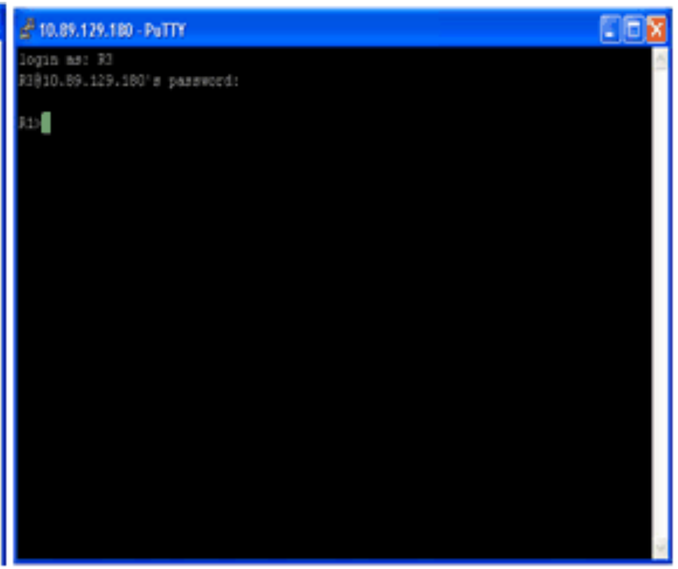
```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```

Access Methods

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.
- **Secure Shell (SSH)** – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network. (Note: This is the recommended method for remotely connecting to a device.)
- **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)

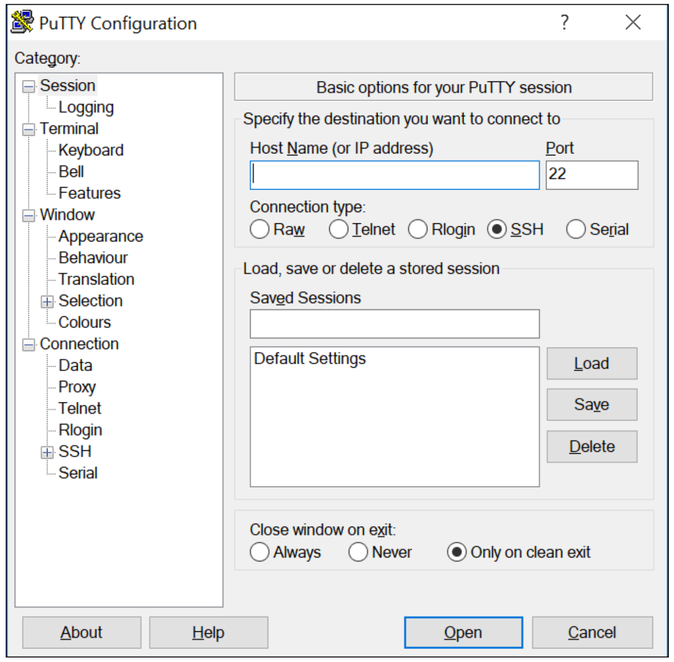


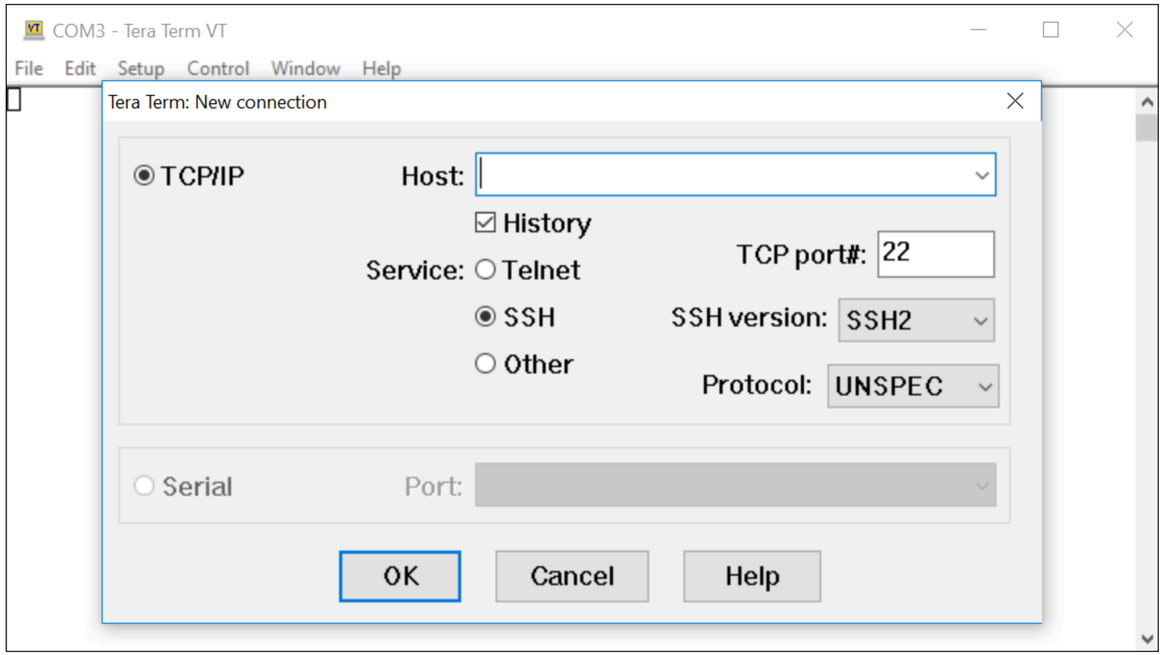




Terminal Emulation Programs

- Terminal emulation programs are used to connect to a network device by either a console port or by an SSH/Telnet connection.
- There are several terminal emulation programs to chose from such as PuTTY, Tera Term and SecureCRT.





Basic Device Configuration

Device Names

- The first configuration command on any device should be to give it a unique hostname.
- By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

- Guideline for naming devices:
  - Start with a letter
  - Contain no spaces
  - End with a letter or digit
  - Use only letters, digits, and dashes
  - Be less than 64 characters in length

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Note: To return the switch to the default prompt, use the **no hostname** global config command.

Password Guidelines

- The use of weak or easily guessed passwords are a security concern.
- All networking devices should limit administrative access by securing privileged EXEC, user EXEC, and remote Telnet access with passwords. In addition, all passwords should be encrypted and legal notifications provided.

- Password Guidelines:
  - Use passwords that are more than eight characters in length.
  - Use a combination of upper and lowercase letters, numbers, special characters, and/or numeric sequences.
  - Avoid using the same password for all devices.
  - Do not use common words because they are easily guessed.

Note: Most of the labs in this course use simple passwords such as **cisco** or **class**. These passwords are considered weak and easily guessable and should be avoided in production environments.

Configure Passwords

Securing user EXEC mode access:

- First enter line console configuration mode using the **line console 0** command in global configuration mode.
- Next, specify the user EXEC mode password using the **password** *password* command.
- Finally, enable user EXEC access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Securing privileged EXEC mode access:

- First enter global configuration mode.
- Next, use the **enable secret** *password* command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Configure Passwords (Cont.)

Securing VTY line access:

- First enter line VTY configuration mode using the **line vty 0 15** command in global configuration mode.
- Next, specify the VTY password using the **password** *password* command.
- Finally, enable VTY access using the **login** command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

- Note: VTY lines enable remote access using Telnet or SSH to the device. Many Cisco switches support up to 16 VTY lines that are numbered 0 to 15.

Encrypt Passwords

- The startup-config and running-config files display most passwords in plaintext.
- To encrypt all plaintext passwords, use the **service password-encryption** global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

- Use the **show running-config** command to verify that the passwords on the device are now encrypted.

```
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

Banner Messages

- A banner message is important to warn unauthorized personnel from attempting to access the device.
- To create a banner message of the day on a network device, use the **banner motd # *the message of the day*** **#** global config command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

The banner will be displayed on attempts to access the device.

```
Press RETURN to get started.



Authorized Access Only!

User Access Verification

Password:
```

Note: The “#” in the command syntax is called the delimiting character. It is entered before and after the message.

Save Configurations

Configuration Files

- There are two system files that store the device configuration:
  - **startup-config** - This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.
  - **running-config** - This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.
  - To save changes made to the running configuration to the startup configuration file, use the **copy running-config startup-config** privileged EXEC mode command.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

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

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

Alter the Running Configurations

If changes made to the running config do not have the desired effect and the running-config has not yet been saved, you can restore the device to its previous configuration. To do this you can:

- Remove the changed commands individually.
- Reload the device using the **reload** command in privilege EXEC mode. *Note: This will cause the device to briefly go offline, leading to network downtime.*

If the undesired changes were saved to the startup-config, it may be necessary to clear all the configurations using the **erase startup-config** command in privilege EXEC mode.

- After erasing the startup-config, reload the device to clear the running-config file from RAM.

```
Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

Lab: Basic Configure

Objectives

- Configure hostnames and IP addresses on two Cisco Internetwork Operating System (IOS) switches using the command-line interface (CLI).
- Use Cisco IOS commands to specify or limit access to the device configurations.
- Use IOS commands to save the running configuration.
- Configure two host devices with IP addresses.
- Verify connectivity between the two PC end devices.

Logical | Physical x:, y:

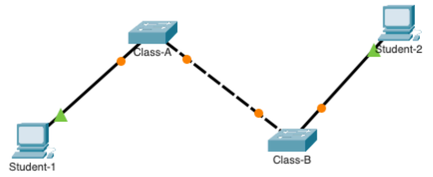
Packet Tracer - Basic Switch and End Device Configuration

Addressing Table

Device	Interface	IP Address
Class-A	VLAN 1	10.10.10.100
Class-B	VLAN 1	10.10.10.150
Student-1	NIC	10.10.10.4
Student-2	NIC	10.10.10.5

Objectives

- Configure hostnames and IP addresses on two Cisco Internetwork Operating System (IOS) switches using the command-line interface (CLI).
- Use Cisco IOS commands to specify or limit access to the device configurations.
- Use IOS commands to save the running configuration.
- Configure two host devices with IP addresses.
- Verify connectivity between the two PC end devices.



https://ipv9.me/rmutp_lab1

Q&A

See you tomorrow.