TY B. Tech.
(Computer Engineering)
2020 Pattern

Prof Vikas K Kolekar

Unit II: Physical Layer:

- LANs, WANs, and the Internet, PAN, Ad-hoc and WLAN Network, Network Architectures: Client-Server; Peer To Peer; Network as a Platform, Network Topologies,
- OSI Model, TCP/IP protocol suite; Layer Details,
- Addressing: Physical &logical Addresses, Port Addresses, Specific Addresses.
- Connecting devices: Hubs (Passive, active, Intelligent), Switches (Layer-2, Layer-3 and Managed), Bridges, Routers, Gateway.

Globally Connected

Networks in Our Daily Lives

- Welcome to a world where we are more powerful together, than we ever could be apart.
- Welcome to the human network.

Technology Then and Now

- We live in a world we barely imagined 20 years ago.
- What wouldn't we have without the Internet?
- What will be possible in the future using the network as the platform?

No Boundaries

- Advancements in networking technologies are helping create a world without boundaries.
- The immediate nature of communications over the Internet encourages global communities.
- Cisco refers to the impact of the Internet and networks on people the “human network”.

Networks Support the Way We Work

- The globalization of the Internet has empowered individuals to create information that can be accessed globally.
- Forms of communication:
  - Texting
  - Social Media
  - Collaboration Tools
  - Blogs
  - Wikis
  - Podcasting

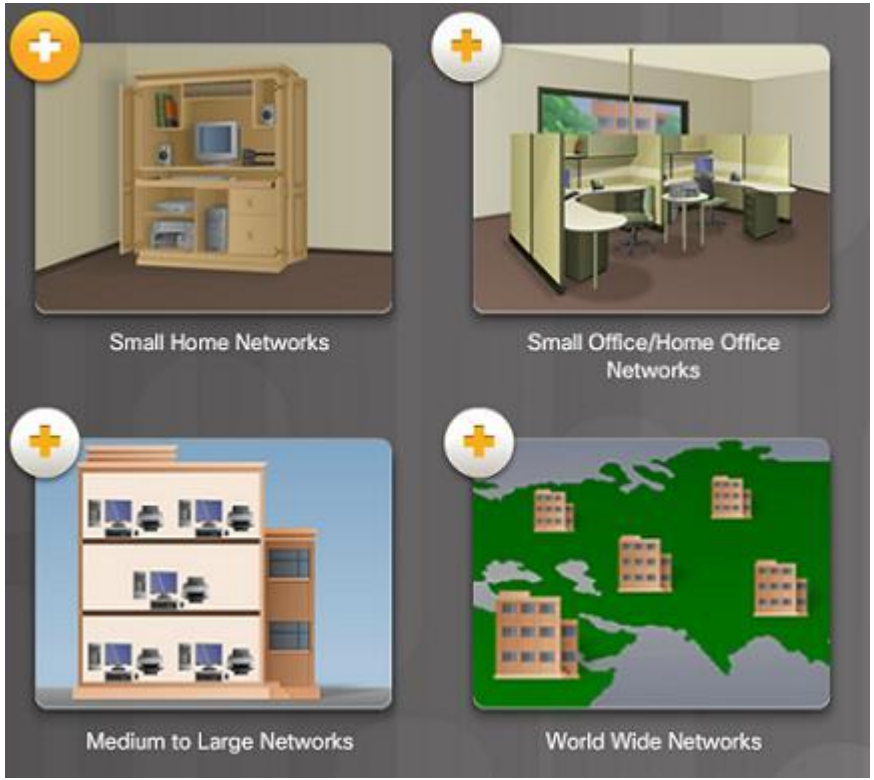
Networks Support the Way We Work

- Data networks have evolved into helping support the way we work.
- Online learning opportunities decrease costly and time consuming travel.
- Employee training is becoming more cost effective.

Networks Support the Way We Play

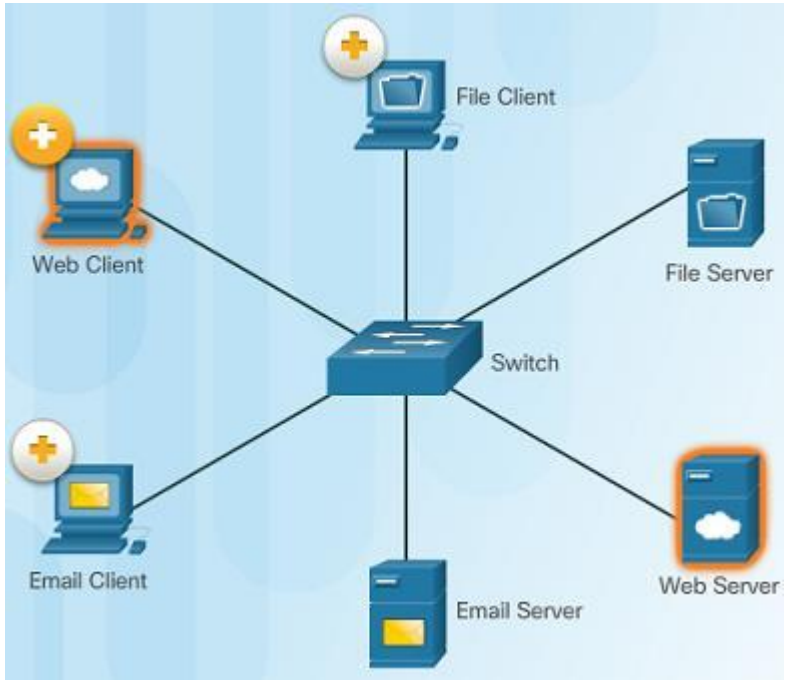
- We listen to music, watch movies, read books, and download material for future offline access.
- Networks allow online gaming in ways that were not possible 20 years ago.
- Offline activities have also been enhanced by networks including global communities for a wide range of hobbies and interests.
- How do you play on the Internet?

Networks of Many Sizes



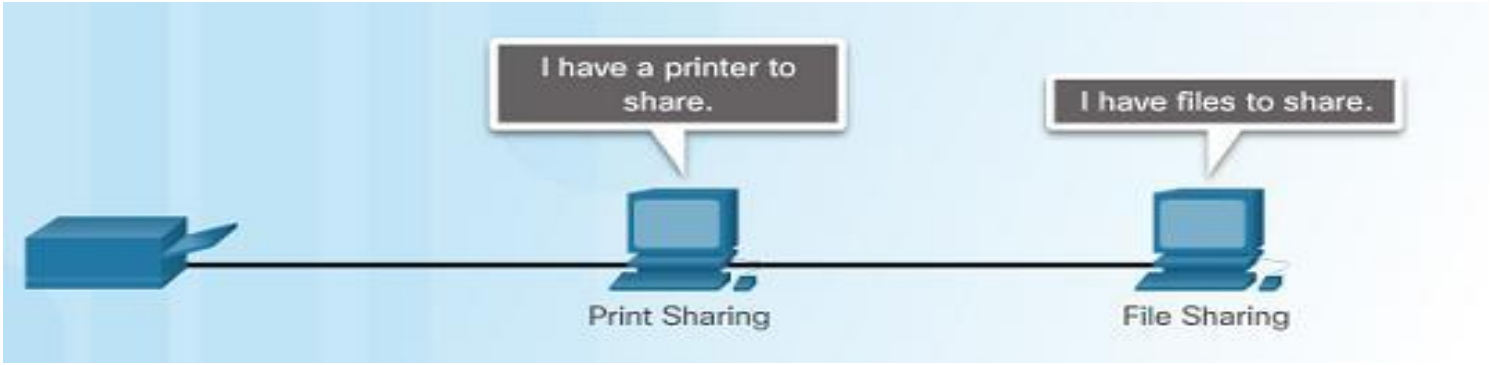
- **Small Home Networks** – connect a few computers to each other and the Internet
- **Small Office/Home Office** – enables computer within a home or remote office to connect to a corporate network
- **Medium to Large Networks** – many locations with hundreds or thousands of interconnected computers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

Clients and Servers



- Every computer connected to a network is called a host or end device.
- Servers are computers that provide information to end devices on the network. For example, email servers, web servers, or file server
- Clients are computers that send requests to the servers to retrieve information such as a web page from a web server or email from an email server.

Peer-to-Peer

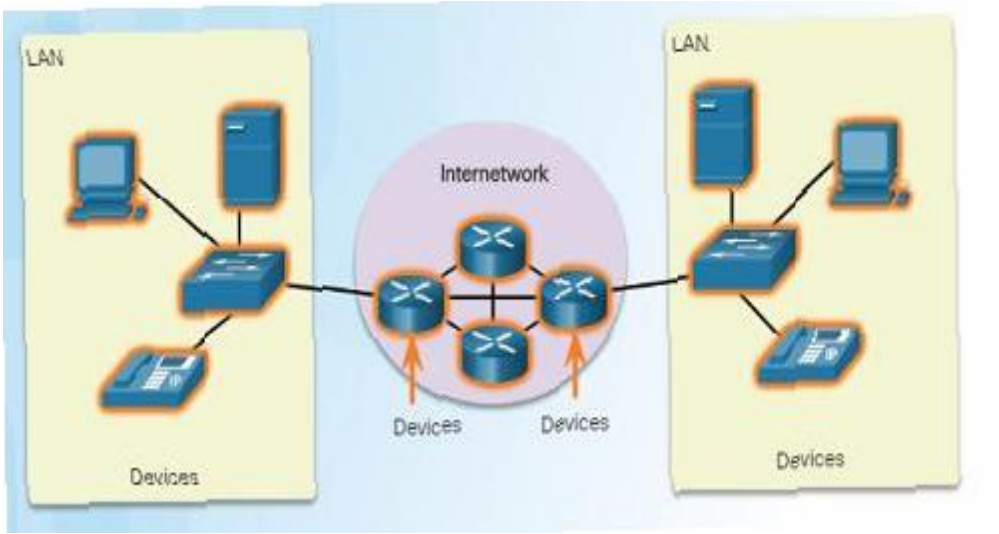


- Client and server software usually run on separate computers.
- However, in small businesses or homes, it is typical for a client to also function as the server. These networks are called peer-to-peer networks.
- Peer-to-peer networking advantages: easy to set up, less complex, and lower cost.
- Disadvantages: no centralized administration, not as secure, not scalable, and slower performance.

LANs, WANs, and the Internet

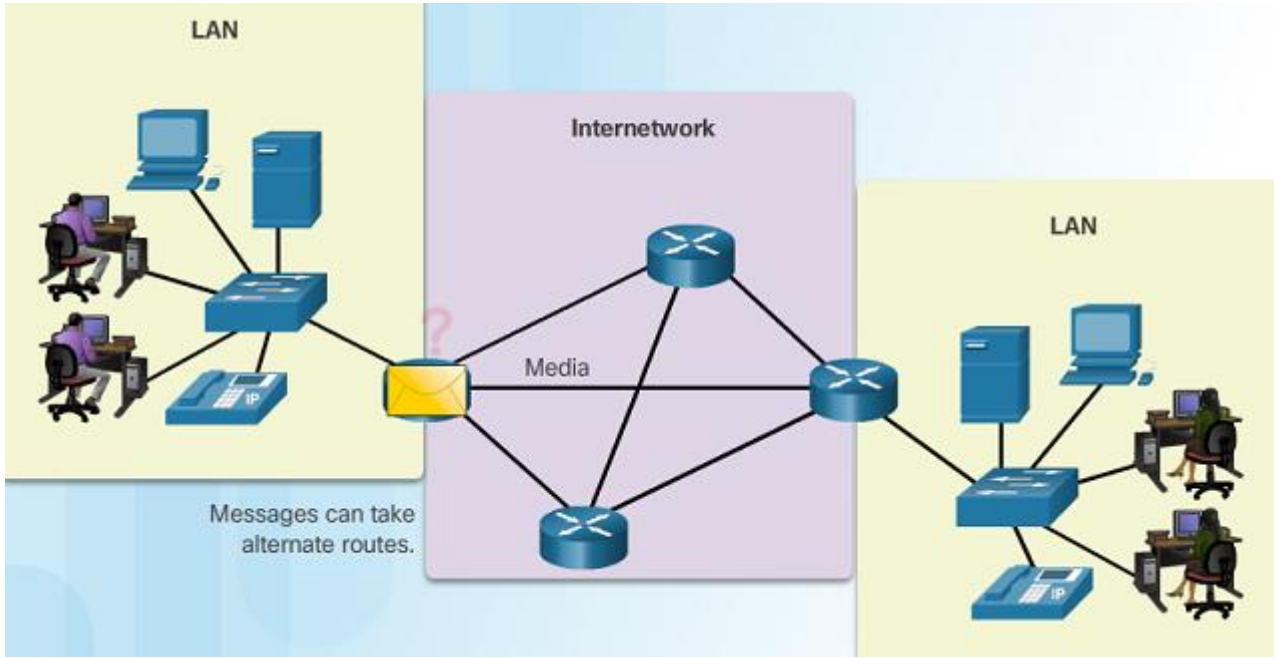
Overview of Network Components

- A network can be as simple as a single cable connecting two computers or as complex as a collection of networks that span the globe.
- Network infrastructure contains **three broad categories** of network components:
  - Devices
  - Media
  - Services



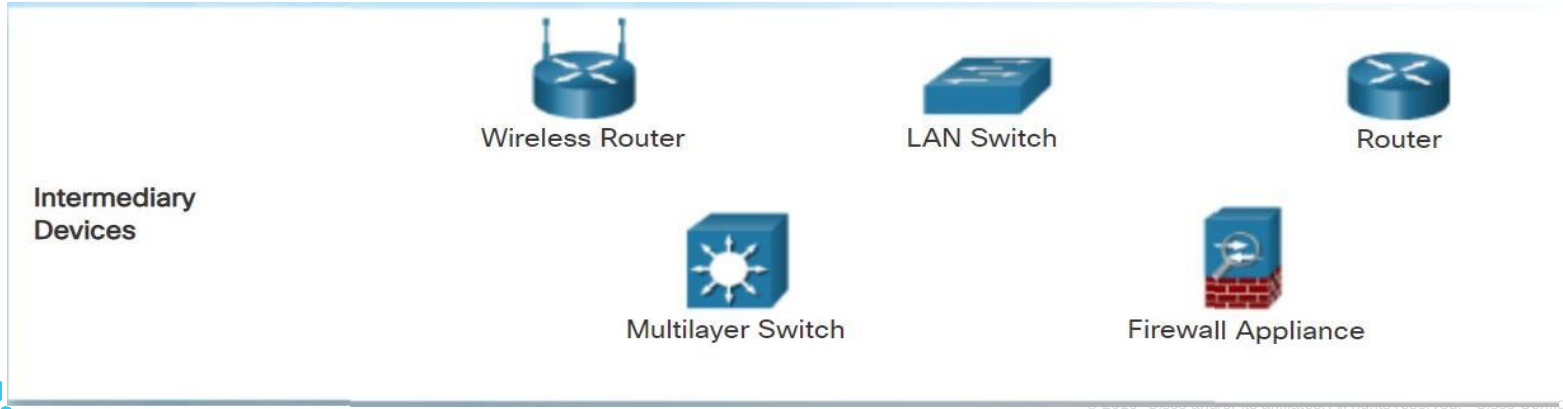
Network Components

- **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



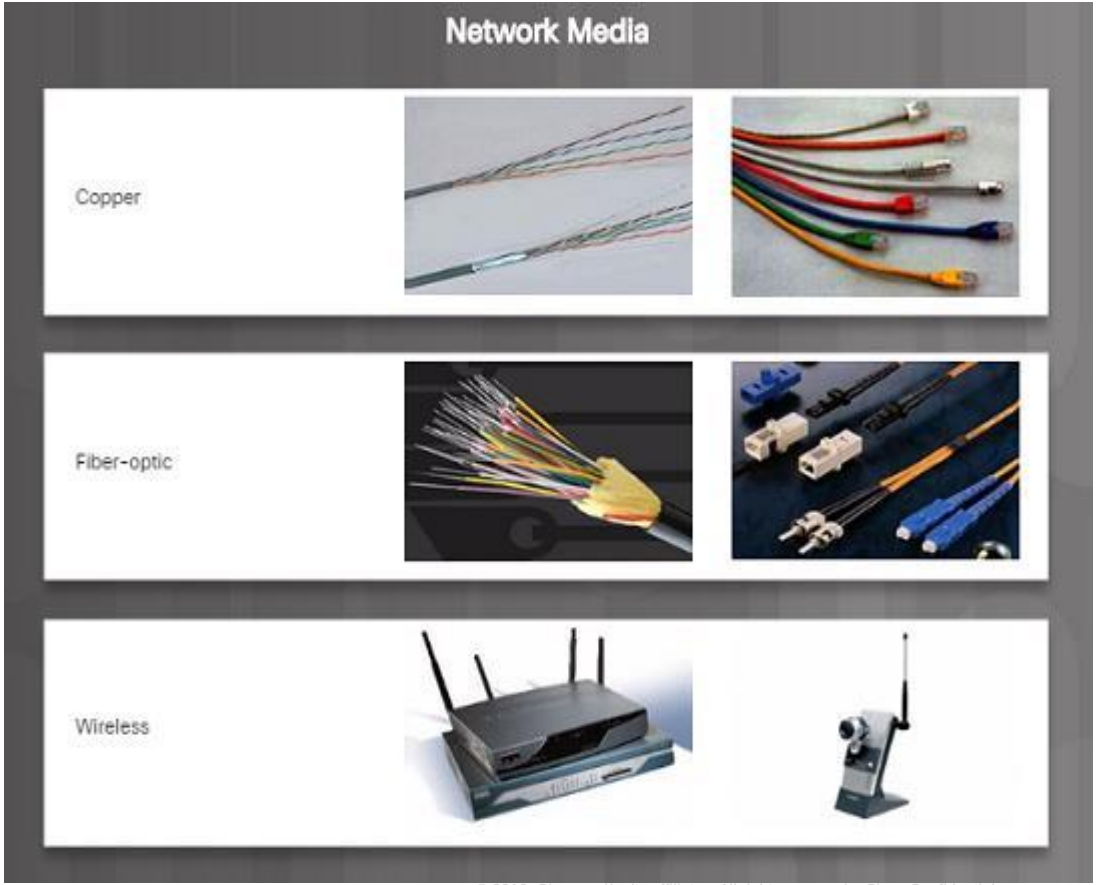
Intermediary Network Devices

- An intermediary device interconnects end devices in a network. Examples include: switches, wireless access points, routers, and firewalls.
- The 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 through the network and internetwork.
  - Notify other devices of errors and communication failures.



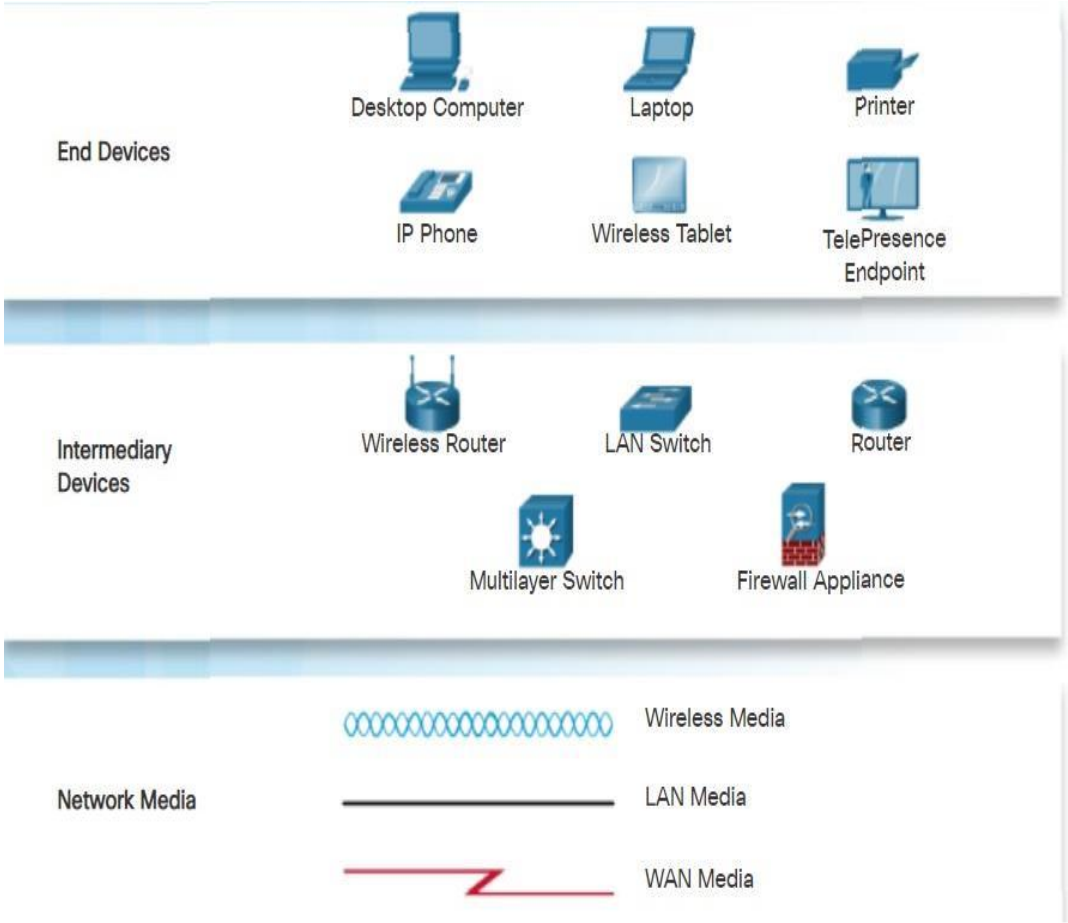
Network Media

- Communication across a network is carried through a medium which allows a message to travel from source to destination.
- Networks typically use three types of media:
  - Metallic wires within cables, such as copper
  - Glass, such as fiber optic cables
  - Wireless transmission



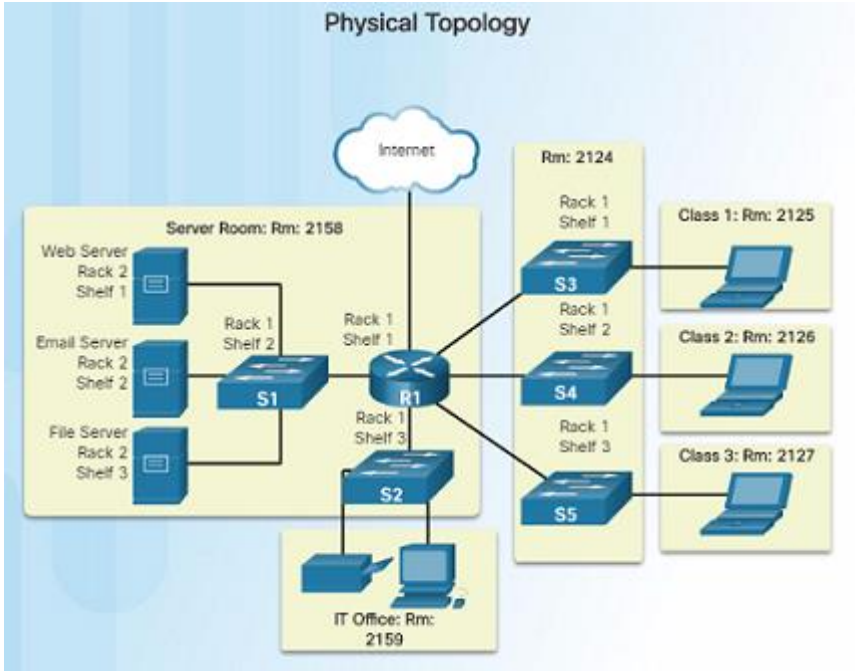
Network Representations

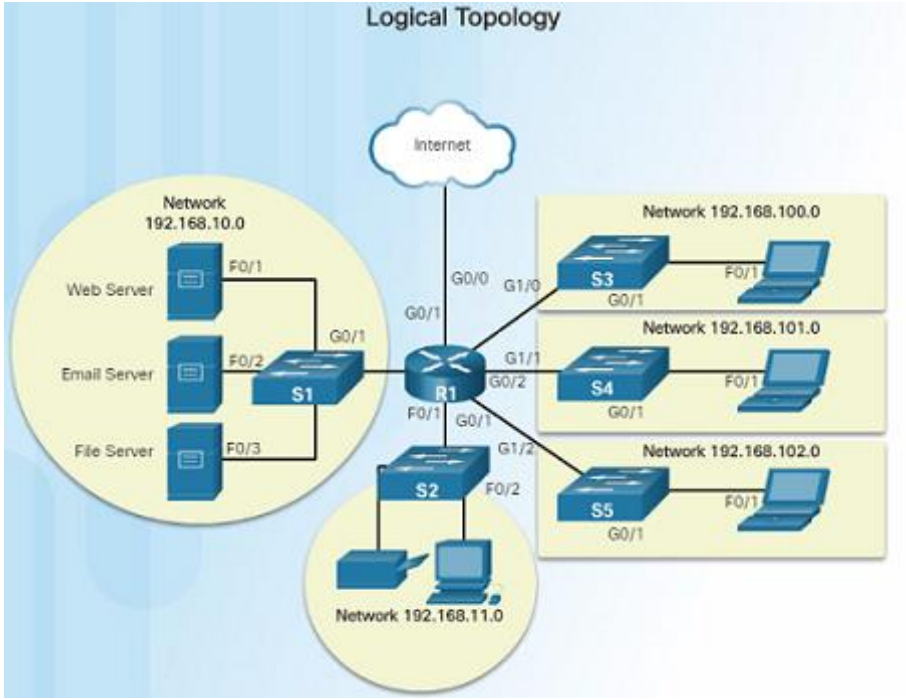
- Network diagrams, often called topology diagrams, use symbols to represent devices within the network.
- In addition to the device representations on the right, it is important to remember and understand the following terms:
  - Network Interface Card (NIC)
  - Physical Port
  - Interface



Topology Diagrams

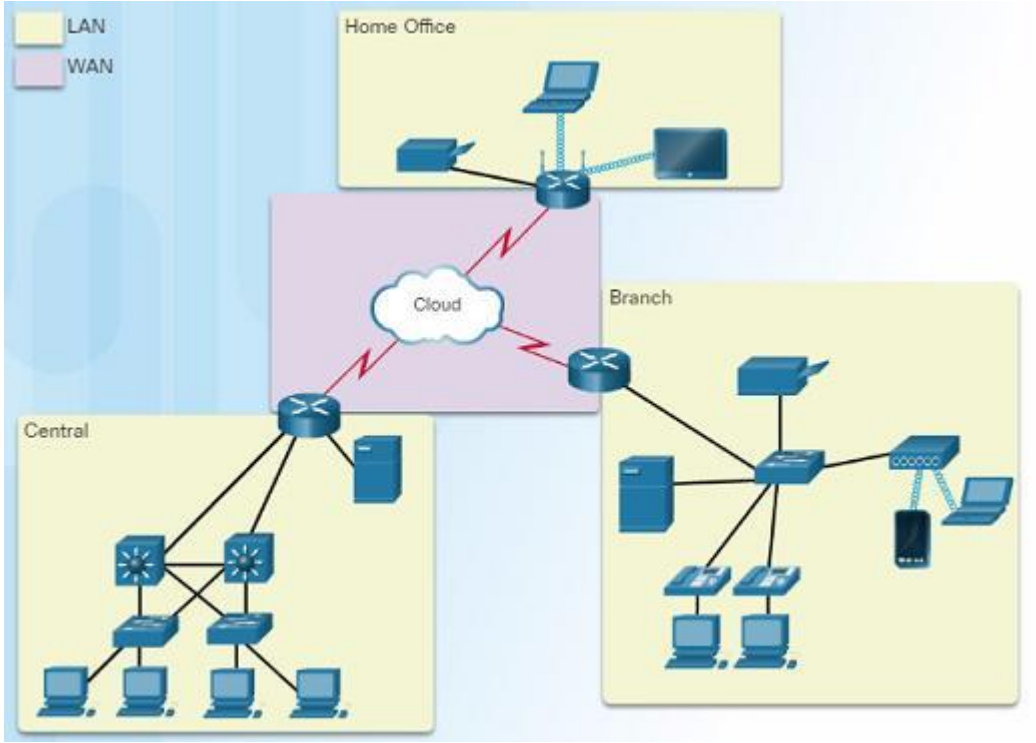
- Note the key differences between the two topology diagrams (physical location of devices vs. ports and network addressing schemes)



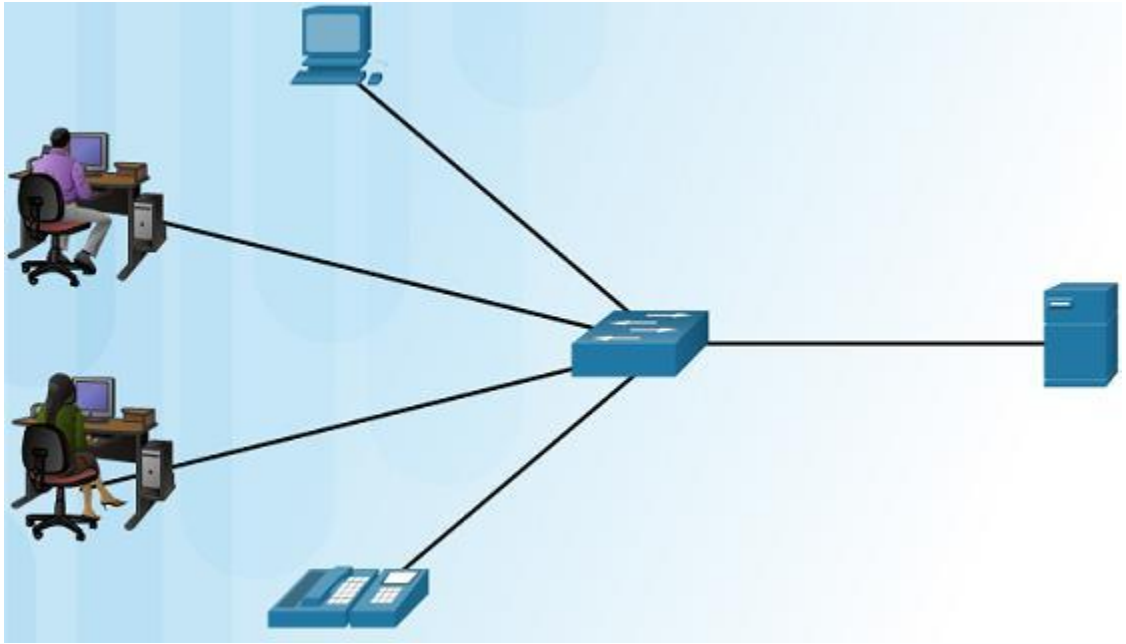


Types of Networks

- Two most common types of networks:
  - Local Area Network (**LAN**) – spans a small geographic area owned or operated by an individual or IT department.
  - Wide Area Network (**WAN**) – spans a large geographic area typically involving a telecommunications service provider.
  - Other types of networks:
    - Metropolitan Area Network (MAN)
    - Wireless LAN (WLAN)
    - Storage Area Network (SAN)

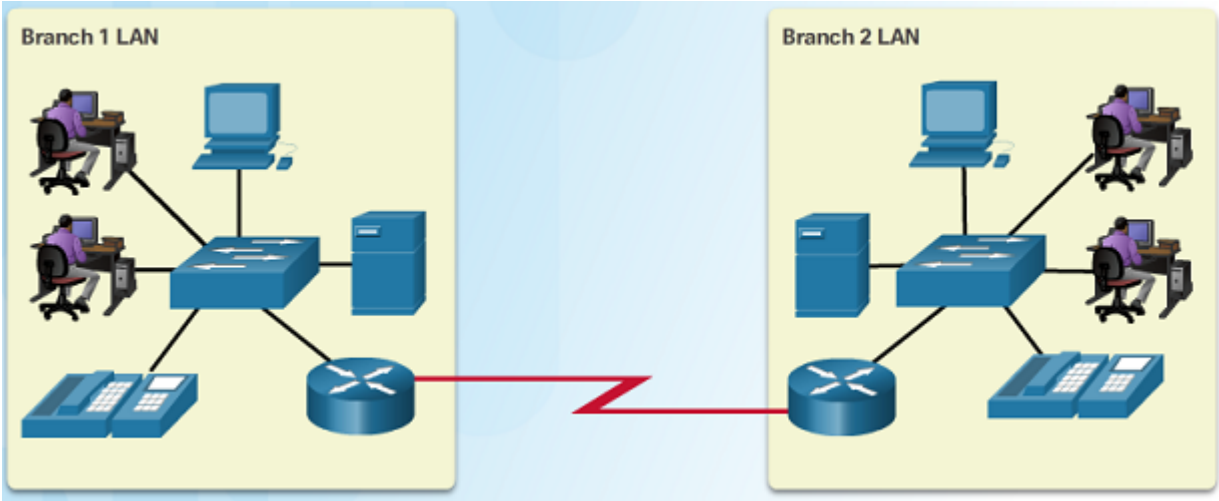


Local Area Networks



- Three characteristics of LANs:
  - Spans a small geographic area such as a home, school, office building, or campus.
  - Usually administered by a single organization or individual.
  - Provides high speed bandwidth to end and intermediary devices within the network.

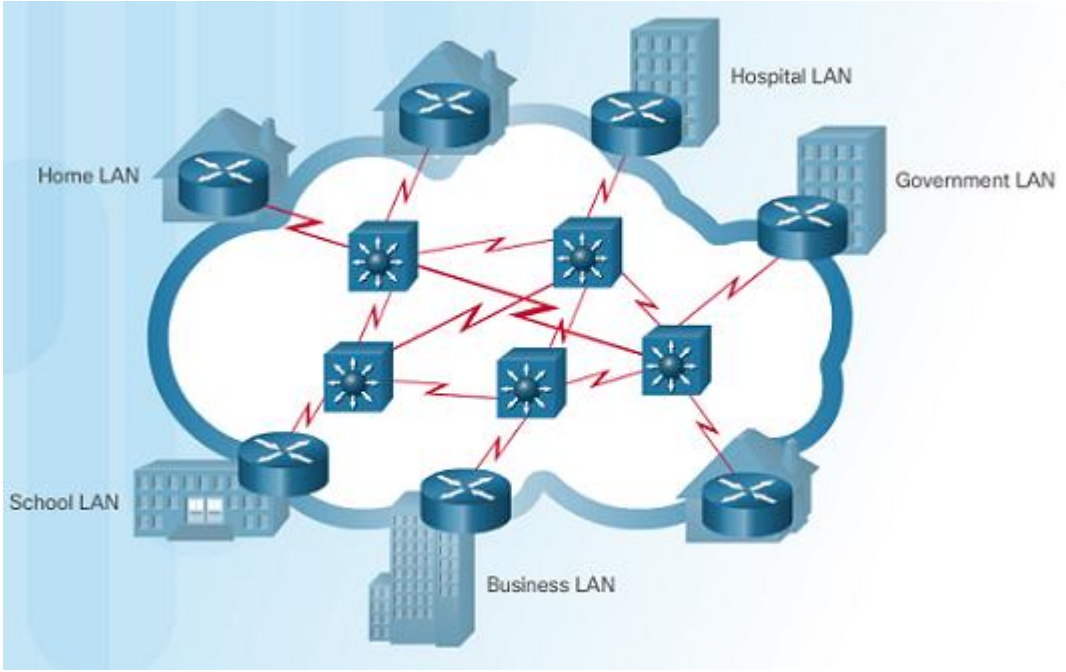
Wide Area Networks



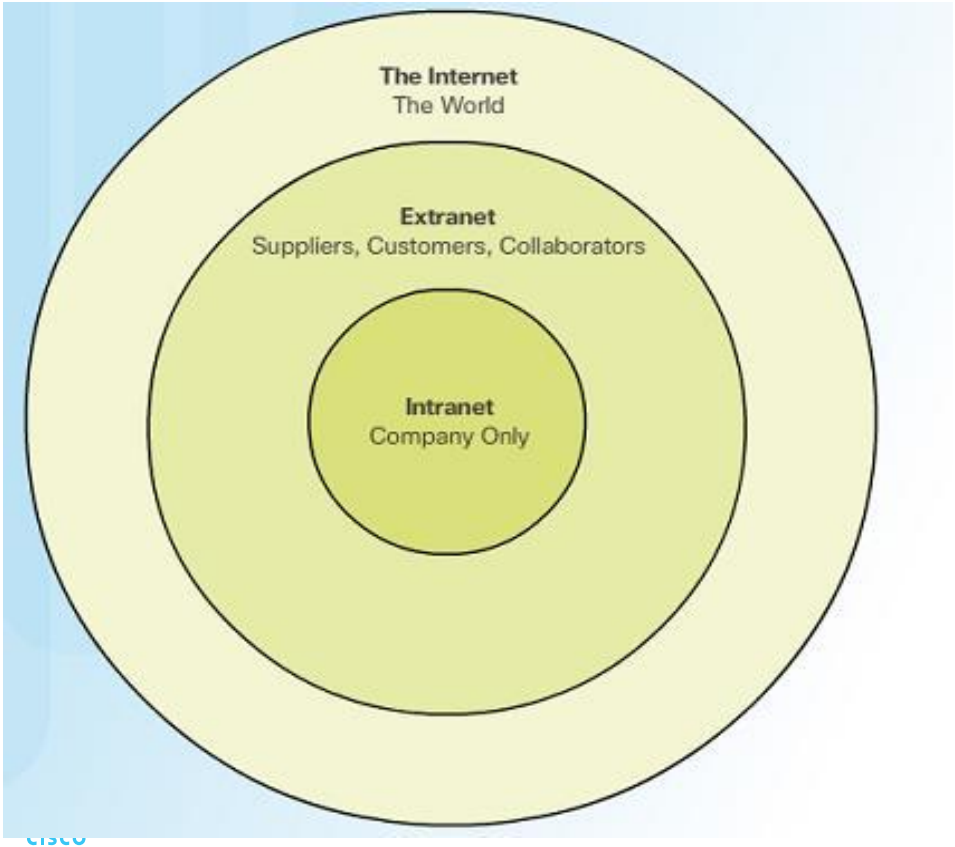
- Three characteristics of WANs:
  - WANs interconnect LANs over wide geographical areas such as between cities, states, or countries.
  - Usually administered by multiple service providers.
  - WANs typically provide slower speed links between LANs.

The Internet

- The Internet is a worldwide collection of interconnected LANs and WANs.
- LANs are connected to each other using WANs.
- WANs are then connected to each other using copper wires, fiber optic cables, and wireless transmissions.
- The Internet is not owned by any individual or group, however, the following groups were developed to help maintain structure:
  - IETF
  - ICANN
  - IAB



Intranets and Extranets

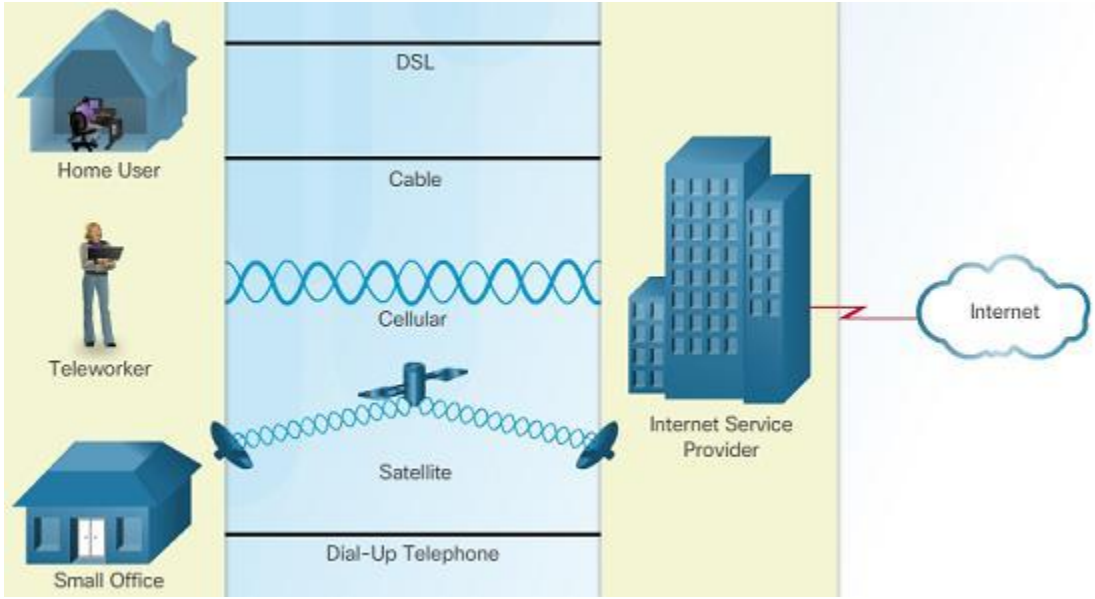


- Unlike the Internet, an intranet is a private collection of LANs and WANs internal to an organization that is meant to be accessible only to the organizations members or others with authorization.
- An organization might use an extranet to provide secure access to their network for individuals who work for a different organization that need access to their data on their network.

Internet Access Technologies

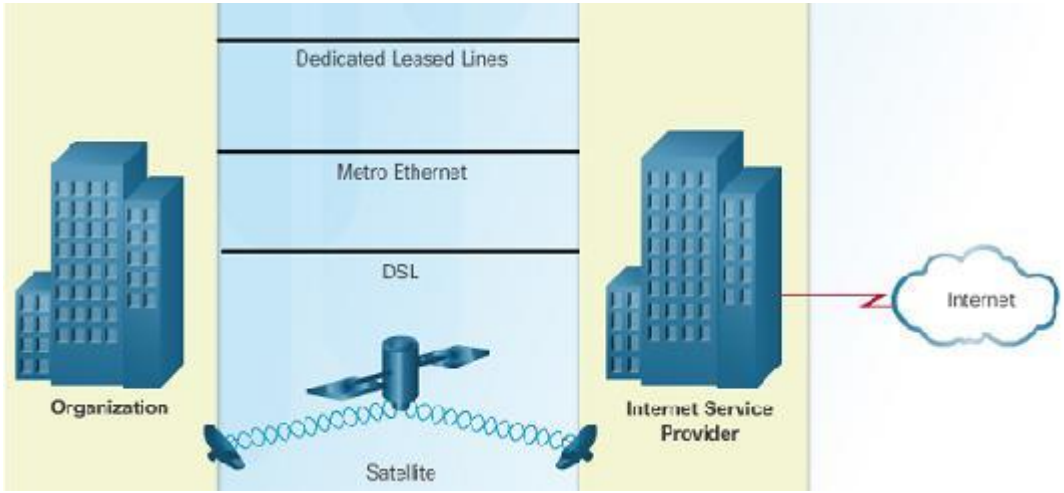
- There are many ways to connect users and organizations to the Internet:
  - Popular services for home users and small offices include broadband cable, broadband digital subscriber line (DSL), wireless WANs, and mobile services.
  - Organizations need faster connections to support IP phones, video conferencing 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



- **Cable** – high bandwidth, always on, Internet connection 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; only available where you can get a cellular signal.
- **Satellite** – major benefit to rural areas without Internet Service Providers.
- **Dial-up telephone** – an inexpensive, low bandwidth option using a modem.

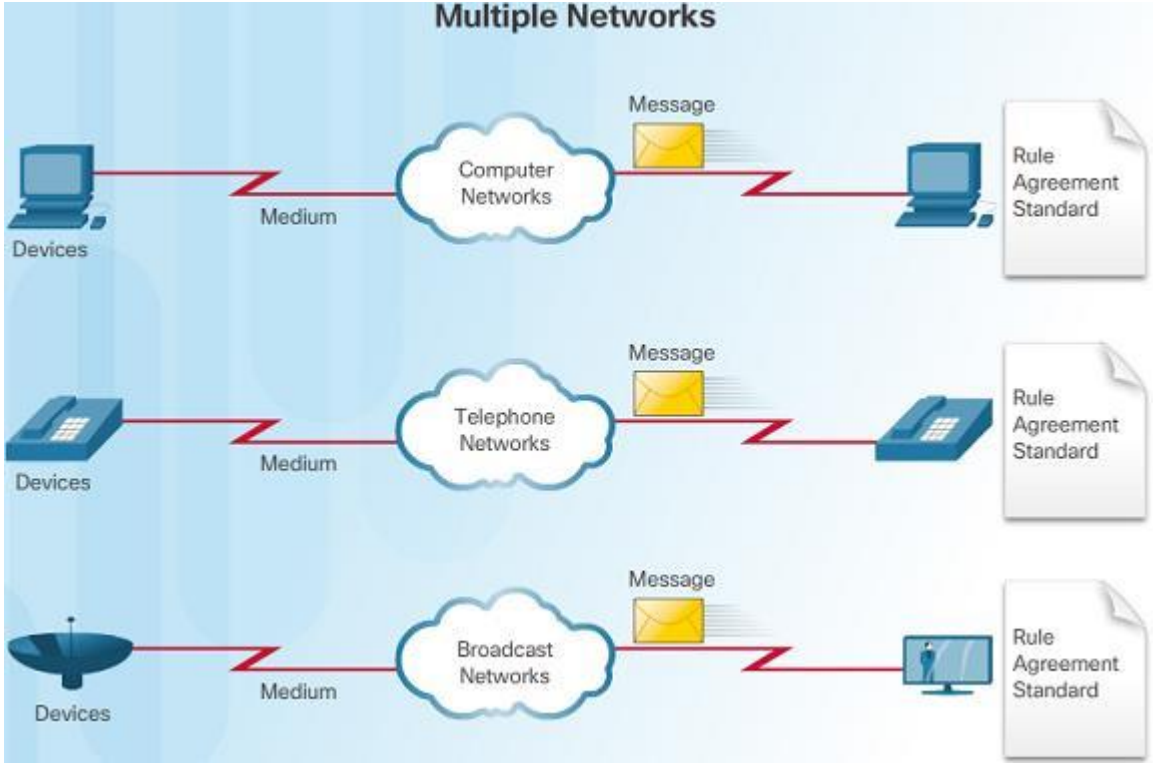
Businesses Internet Connections



- Corporate business connections may require higher bandwidth, dedicated connections, or managed services. Typical connection options for businesses:
  - Dedicated Leased Line – reserved circuits within the service provider's network that connect distant offices with private voice and/or data networking.
  - Ethernet WAN – extends LAN access technology into the WAN.
  - DSL – Business DSL is available in various formats including Symmetric Digital Subscriber Lines (SDSL).
  - Satellite – can provide a connection when a wired solution is not available.

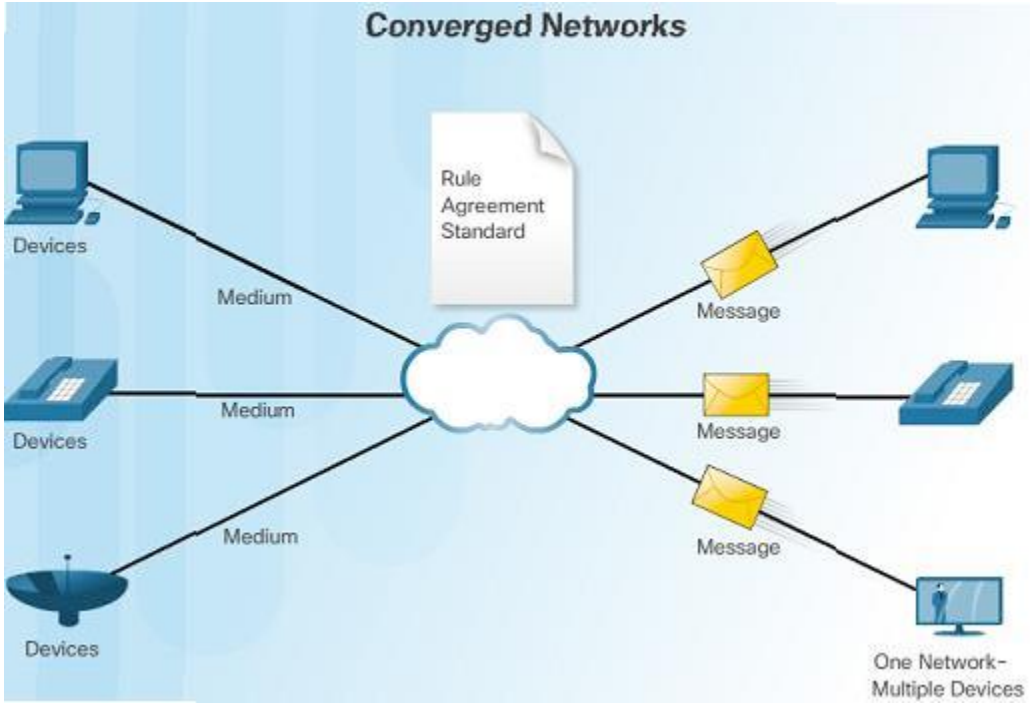
The Network as a Platform

Traditional Separate Networks



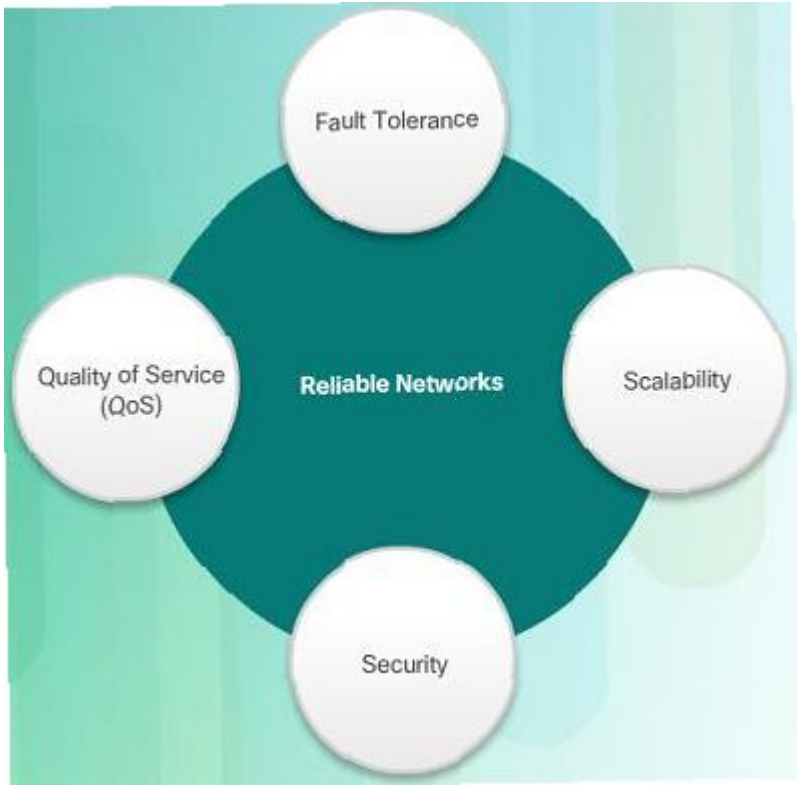
- An example of multiple networks might be a school 30 years ago. Some classrooms were cabled for data networks. Those same classrooms were cabled for telephone networks, and also cabled separately for video.
- Each of these networks used different technologies to carry the communication signals using a different set of rules and standards.

The Converging Network



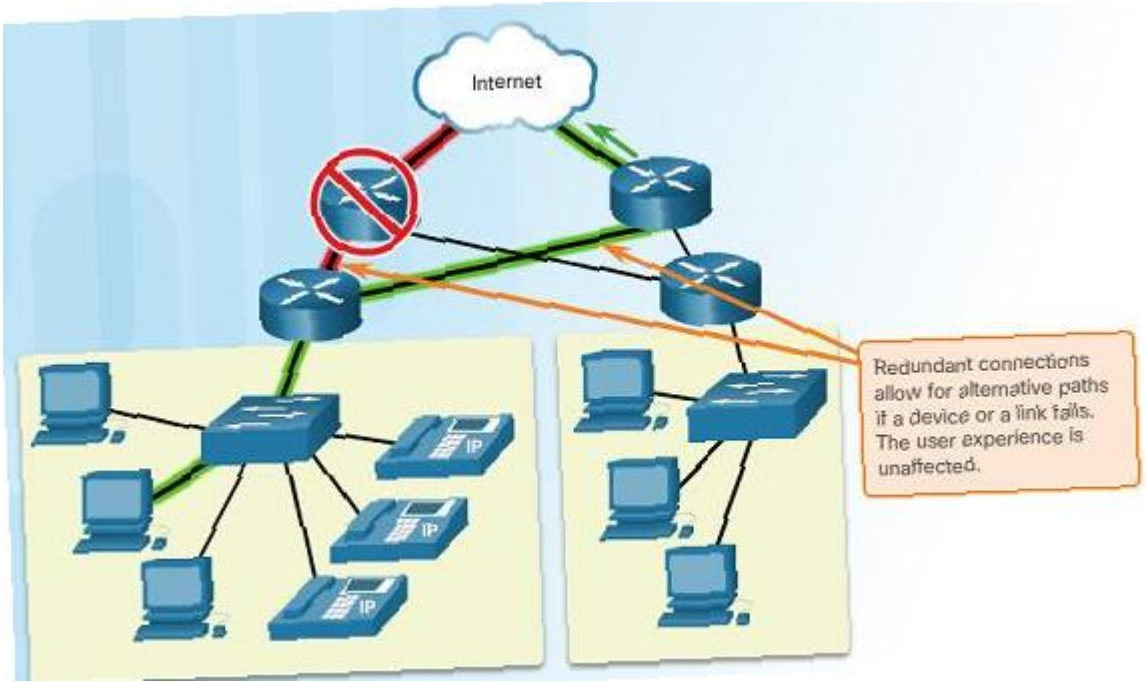
- Converged data networks carry multiple services on one link including data, voice, and video.
- Unlike dedicated networks, converged networks can deliver data, voice, and video between different types of devices over the same network infrastructure.
- The network infrastructure uses the same set of rules and standards.

Network Architecture



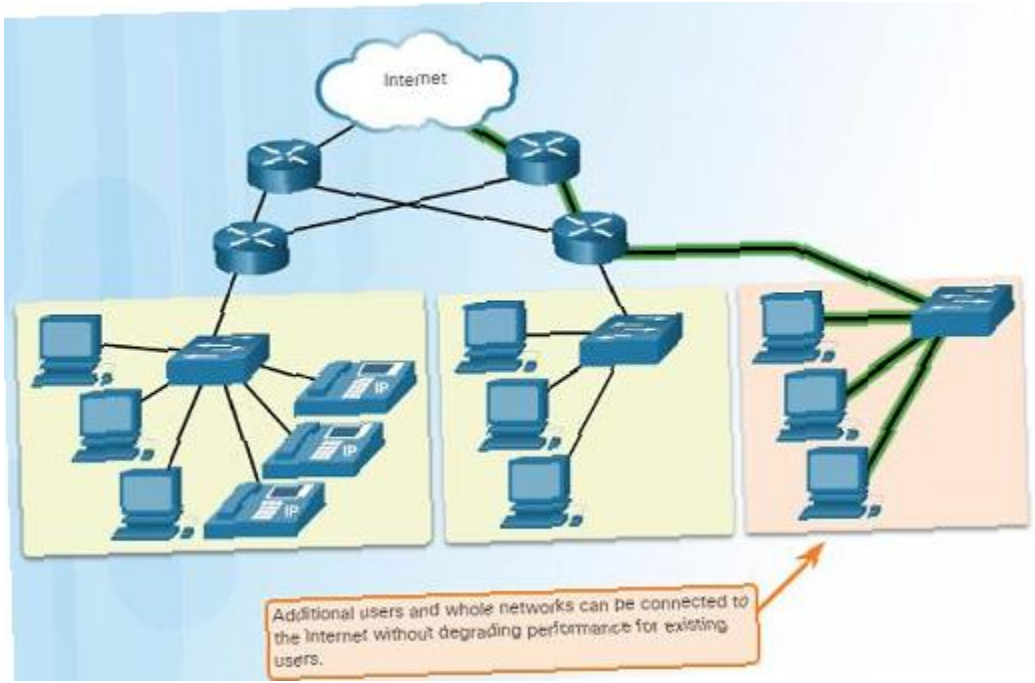
- Network Architecture refers to the technologies that support the infrastructure that moves data across the network.
- There are four basic characteristics that the underlying architectures need to address to meet user expectations:
  - Fault Tolerance
  - Scalability
  - Quality of Service (QoS)
  - Security

Fault Tolerance



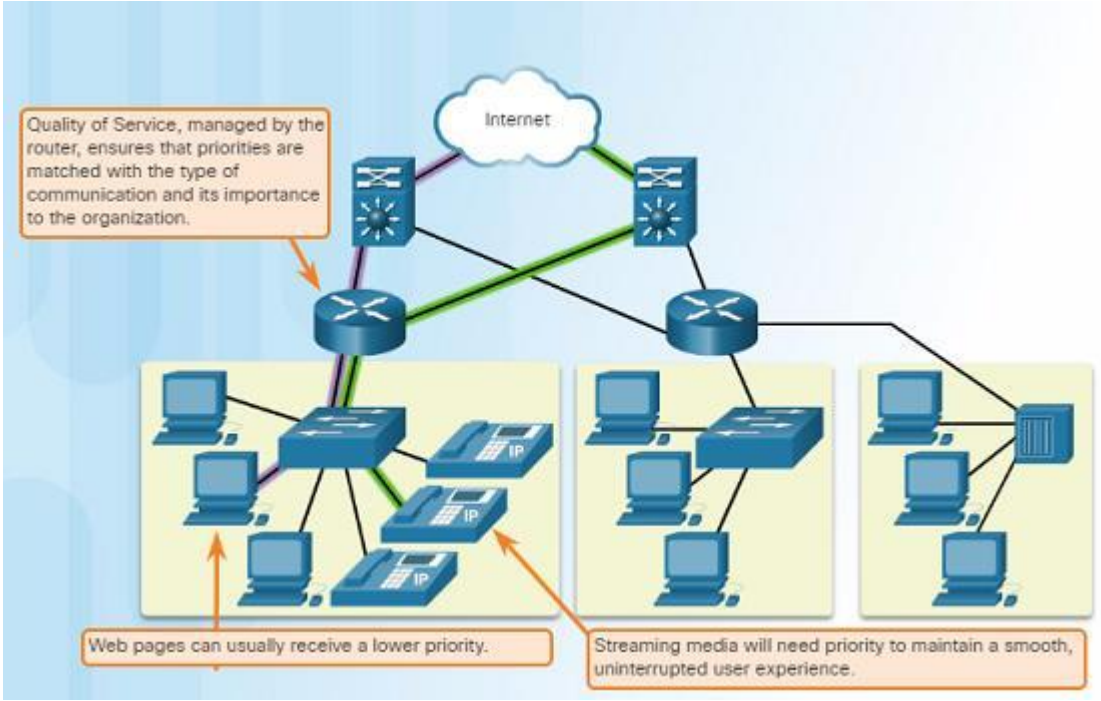
- A fault tolerant network limits the impact of a failure by limiting the number of affected devices.
- Multiple paths are required for fault tolerance.
- Reliable networks provide redundancy by implementing a packet switched network. Packet switching splits traffic into packets that are routed over 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.

Scalability



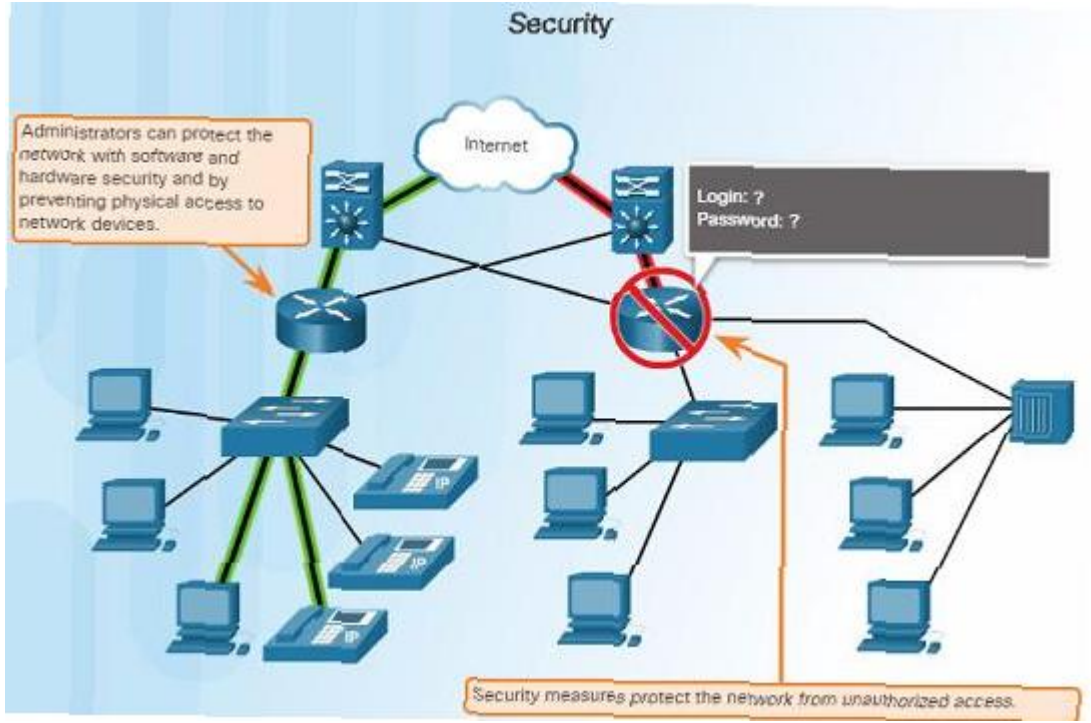
- A scalable network can expand quickly and easily to support new users and applications without impacting the performance of services to existing users.
- Network designers follow accepted standards and protocols in order to make the networks scalable.

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.

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 management software on those 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

The Changing Network Environment

New 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) is a major global trend that 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

Online Collaboration

- Individuals want to 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, interact and achieve their objectives.
- Collaboration is a very high priority for businesses and in education.

Video Communication

- Cisco TelePresence powers the new way of working where everyone, everywhere, can be more productive through face to face collaboration.
- Around the world each day, we transform organizations by transforming our customer experiences.

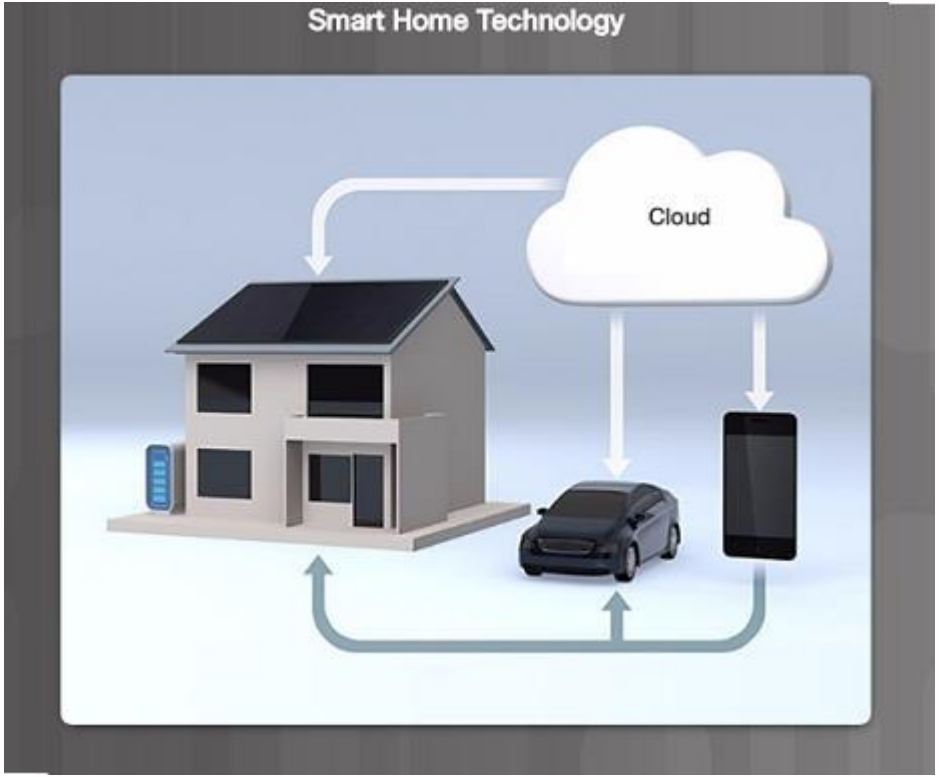
Cloud Computing

- Cloud computing is a global trend that allows us to store personal files or backup our data on servers over the Internet.
- Applications such as word processing and photo editing can also be accessed using the Cloud.
- Cloud computing also allows businesses to extend their capabilities on demand and delivered automatically 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.)

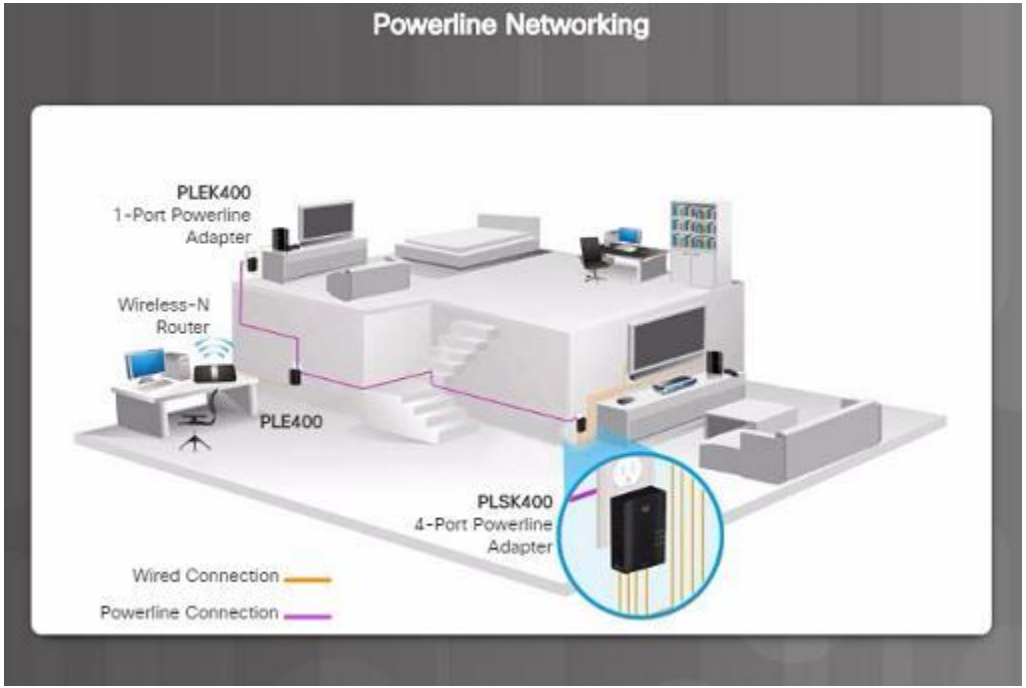
- Four types of Clouds:
  - Public Clouds
    - Services and applications are made available to the general public through a pay-per-use model or for free.
  - Private Clouds
    - Applications and services are intended for a specific organization or entity such as the government.
  - Hybrid Clouds
    - 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

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.

Powerline Networking

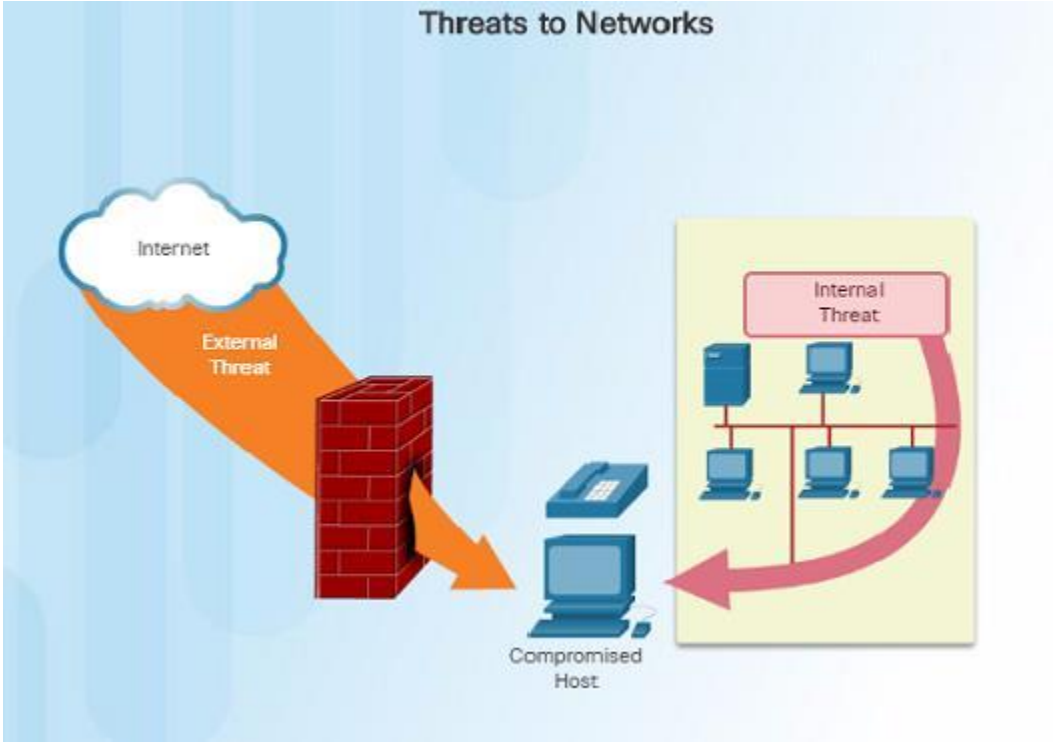


- Powerline networking can allow devices to connect to a LAN where data network cables or wireless communications are not a viable option.
- Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet by sending data on certain frequencies.

Wireless Broadband

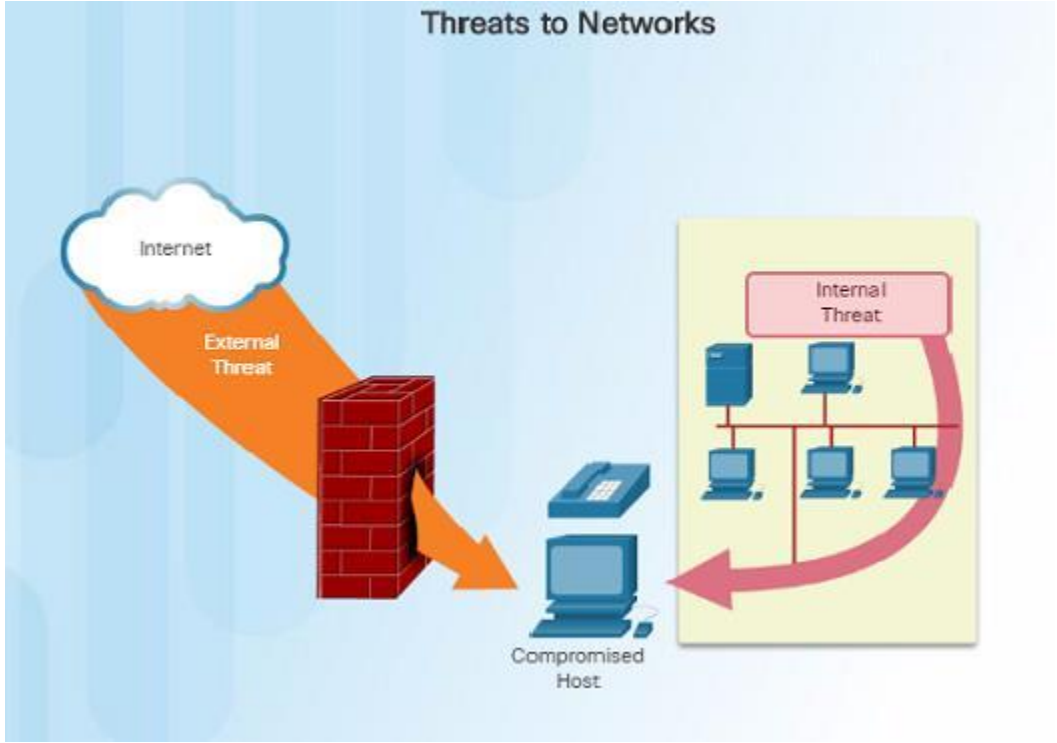
- In addition to DSL and cable, wireless is another option used to connect homes and small businesses to the Internet.
- More commonly found in rural environments, a Wireless Internet Service Provider (WISP) is an ISP that connects subscribers to designated access points or hotspots.
- Wireless broadband 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.

Security Threats



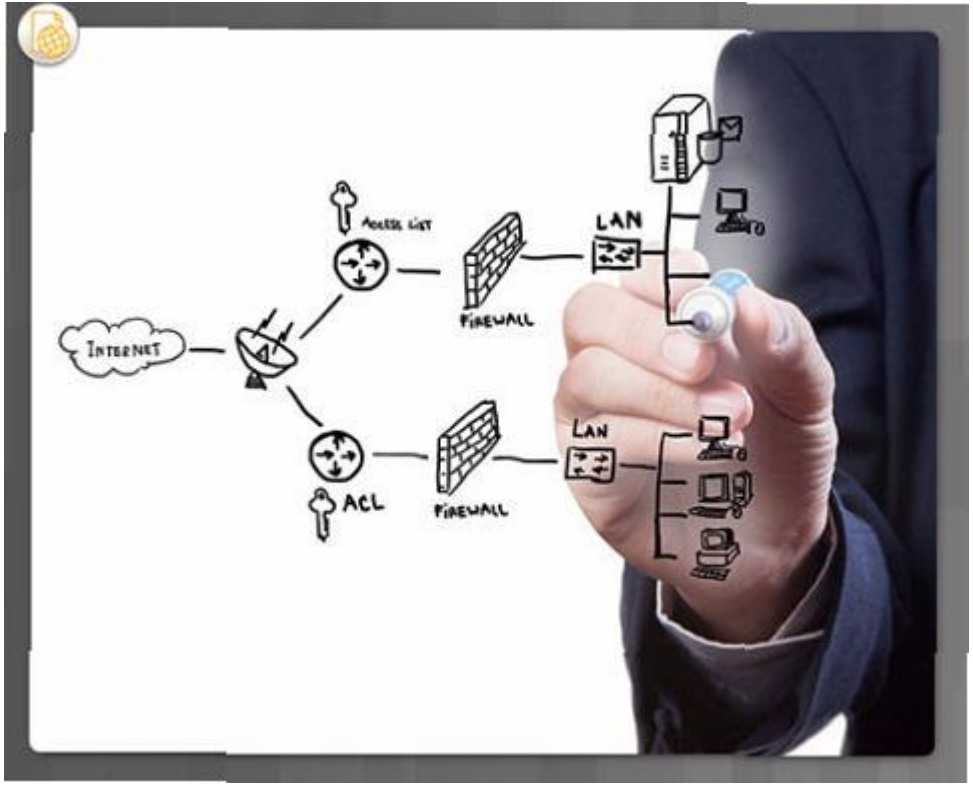
- Network security is an integral part of networking regardless of the size of the network.
- The network security that is implemented must take into account the environment while securing the data, but still allowing for quality of service that is expected of the network.
- Securing a network involves 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.)



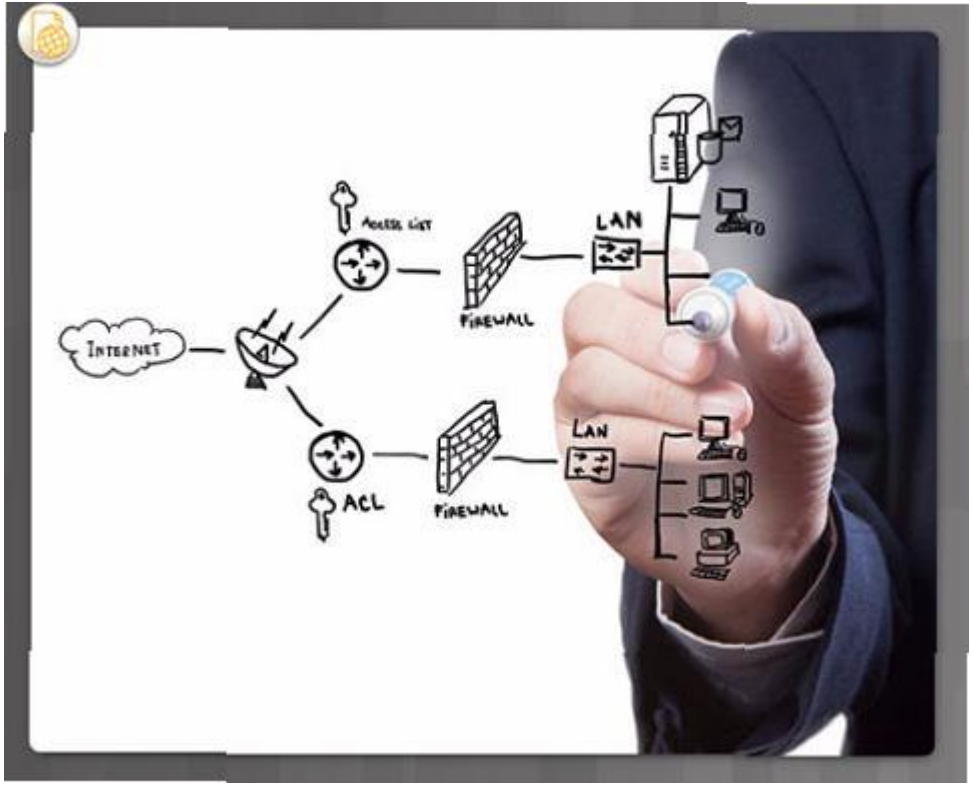
- External threats:
  - Viruses, worms, and Trojan horses
  - Spyware and adware
  - Zero-day attacks, also called zero-hour attacks
  - Hacker attacks
  - Denial of Service attacks
  - Data interception and theft
  - Identify Theft
- Internal threats:
  - Whether intentional or not, many studies show that the internal users of the network cause the most security breaches.
  - With BYOD strategies, corporate data is more vulnerable.

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 to provide more advanced firewall capabilities.
  - Access control lists (ACL) – used to further filter access and traffic forwarding.
  - Intrusion prevention systems (IPS) – used to identify fast-spreading threats such as zero-day attacks.
  - Virtual private networks (VPN) – used to provide secure access for remote workers.

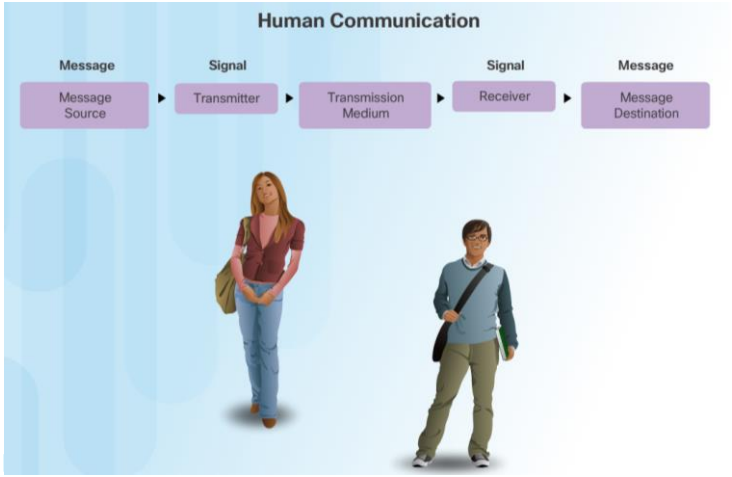
Network Architecture

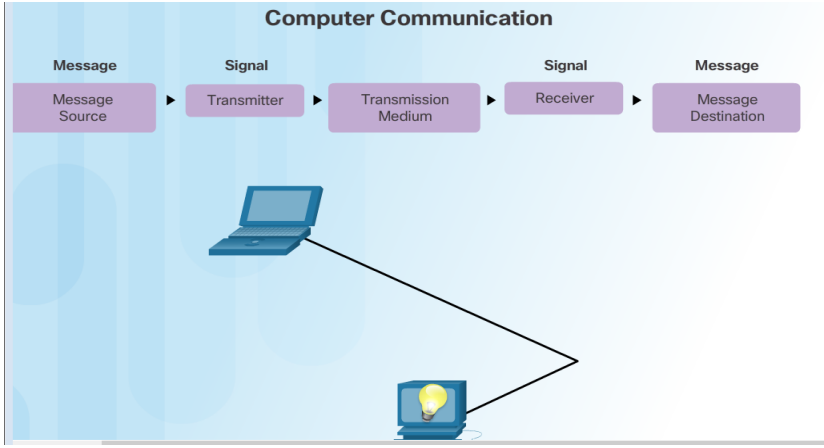
- In order for networks to function while efficiently supporting connections of people, devices, and information in a media rich converged environment, the network must be built upon a standard network architecture.
- Network architecture refers to the devices, connections, and products that are integrated to support the necessary technologies and applications.
- The foundation of all network architectures including the Internet are routers and switches.

Rules of Communication

Communication Fundamentals

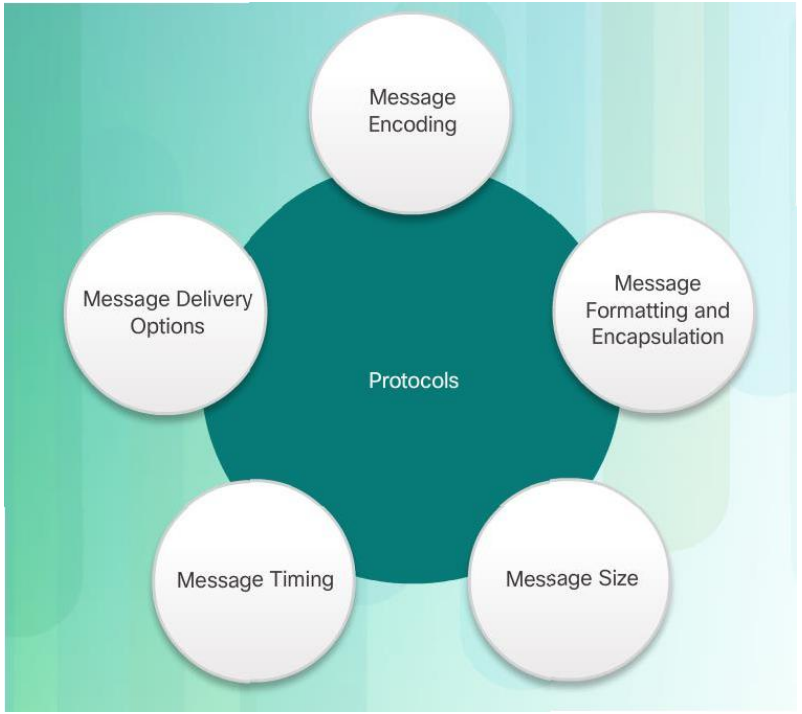
- All communication methods have three elements in common:
  - Source or sender
  - Destination or receiver
  - Channel or media
- Rules or protocols govern all methods of communication.





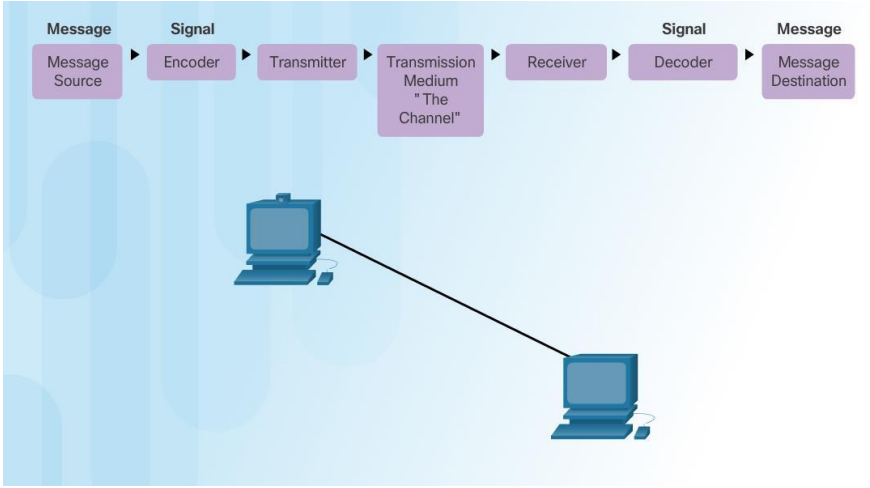
Rule Establishment

- Protocols are necessary for effective communication and include:
  - An identified sender and receiver
  - Common language and grammar
  - Speed and timing of delivery
  - Confirmation or acknowledgment requirements
- Protocols used in network communications also define:
  - Message encoding
  - Message delivery options
  - Message Formatting and Encapsulation
  - Message Timing
  - Message Size



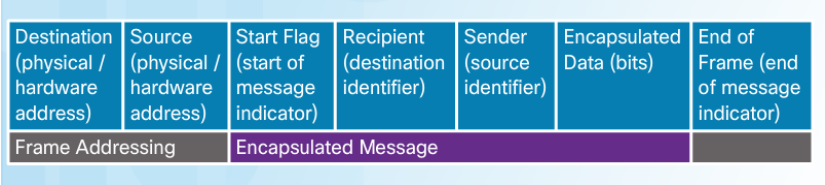
Message Encoding

- Encoding between hosts must be in appropriate format for the medium.
- Messages are first converted into bits by the sending host.
- Each bit is encoded into a pattern of sounds, light waves, or electrical impulses depending on the network media
- The destination host receives and decodes the signals in order to interpret the message.



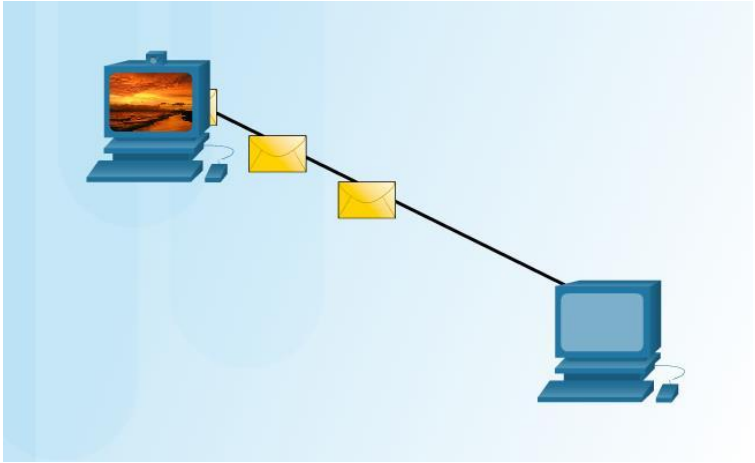
Message Formatting and Encapsulation

- There is an agreed format for letters and addressing letters which is required for proper delivery.
- Putting the letter into the addressed envelope is called encapsulation.
- Each computer message is encapsulated in a specific format, called a frame, before it is sent over the network.
- A frame acts like an envelope providing destination address and source address.



Message Size

- Humans break long messages into smaller parts or sentences.
- Long messages must also be broken into smaller pieces to travel across a network.
  - Each piece is sent in a separate frame.
  - Each frame has its own addressing information.
  - A receiving host will reconstruct multiple frames into the original message.

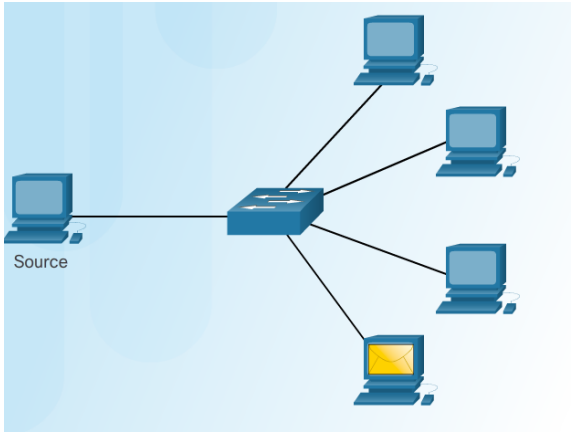


Message Timing

- Access Method
  - Hosts on a network need to know when to begin sending messages and how to respond when collisions occur.
- Flow Control
  - Source and destination hosts use flow control to negotiate correct timing to avoid overwhelming the destination and ensure information is received.
- Response Timeout
  - Hosts on the network have rules that specify how long to wait for responses and what action to take if a response timeout occurs.

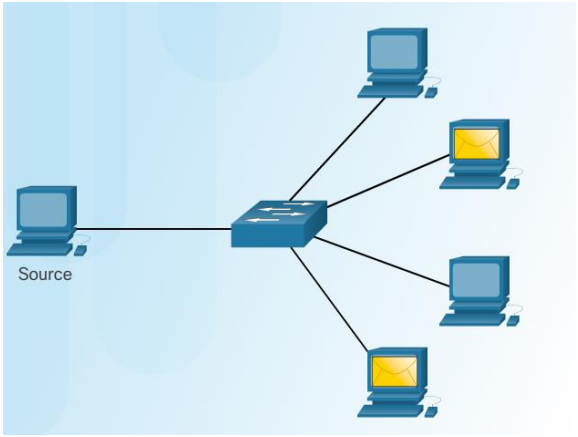
Message Delivery Options

Unicast Message



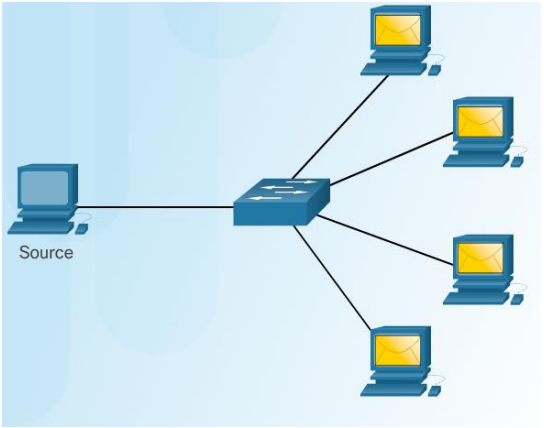
One-to-one delivery

Multicast Message



One-to-many delivery

Broadcast Message

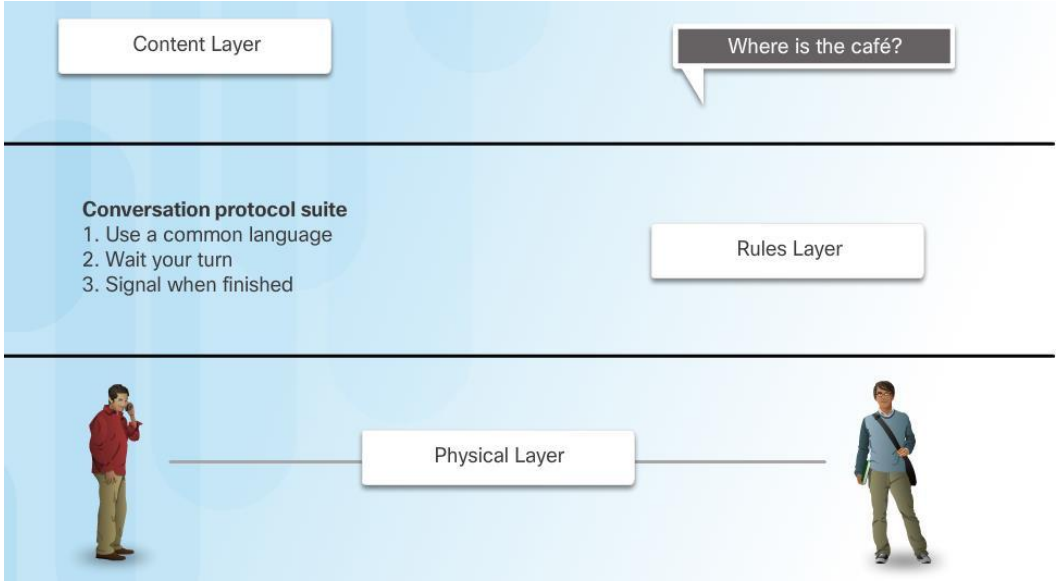


One-to-all delivery

Network Protocols and Standards

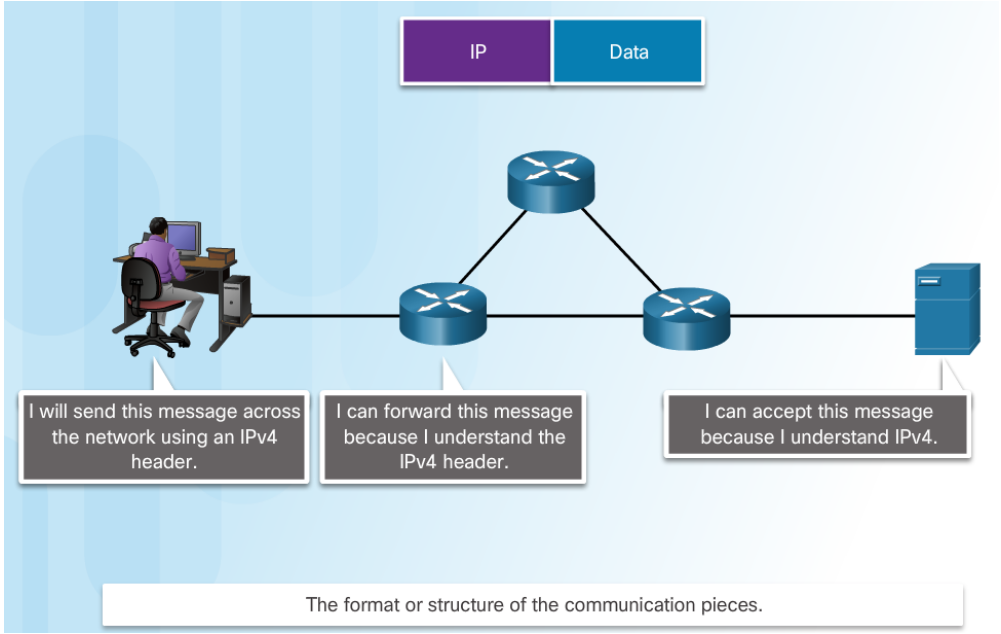
Rules that Govern Communications

- Protocol suites are implemented by hosts and networking devices in software, hardware or both.
- The protocols are viewed in terms of layers, with each higher level service depending on the functionality defined by the protocols shown in the lower levels.



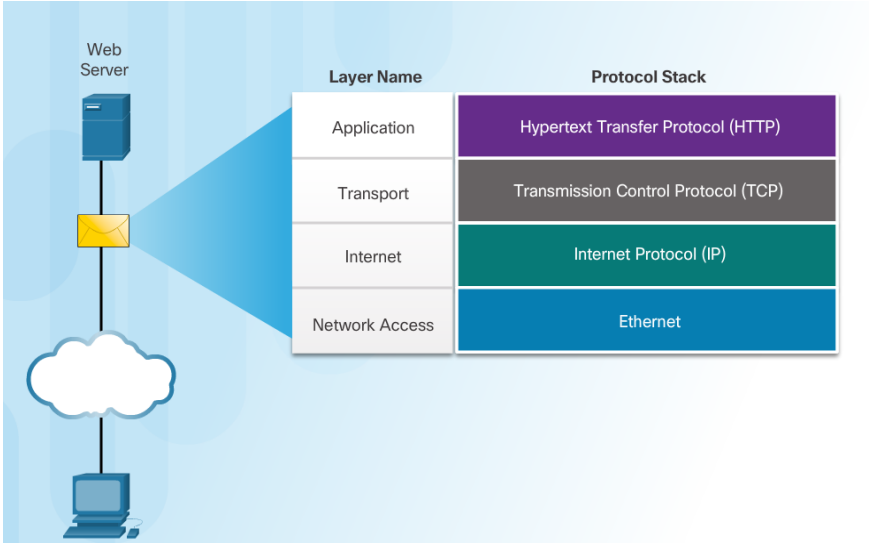
Network Protocols

- Networking protocols define a common format and set of rules for exchanging messages between devices.
- Some common networking protocols are Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP), and Internet Protocol (IP).



Protocol Interaction

- Communication between a web server and web client is an example of an interaction between several protocols:
  - **HTTP -** an application protocol that governs the way a web server and a web client interact.
  - **TCP** - transport protocol that manages the individual conversations.
  - **IP –** encapsulates the TCP segments into packets, assigns addresses, and delivers to the destination host.
  - **Ethernet** - allows communication over a data link and the physical transmission of data on the network media.



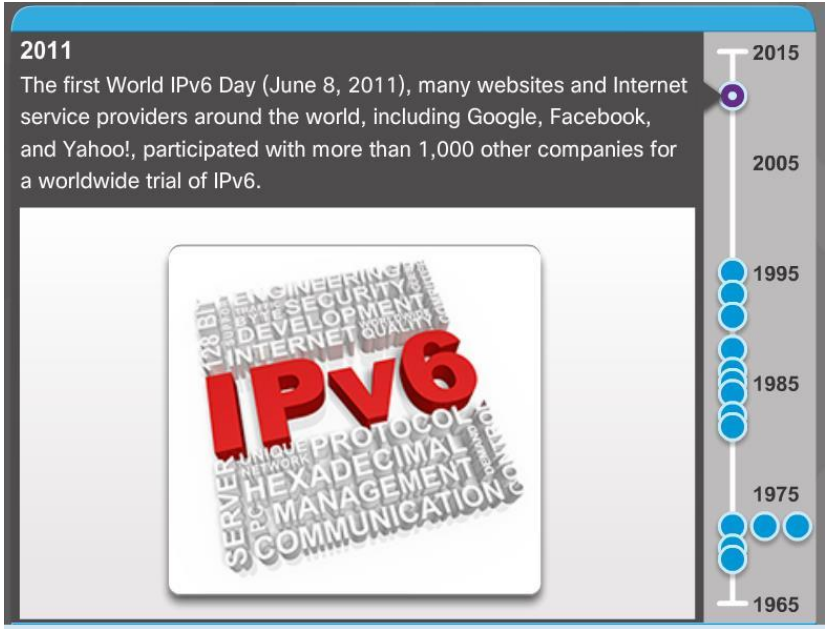
Protocol Suites and Industry Standards

- A protocc
  protocols
  together t
  comprehe
  communi
  - May be
    standar
    develop
- The TCP/
  is an ope
  protocols
  available,
  is able to
  protocols
  hardware
  software.

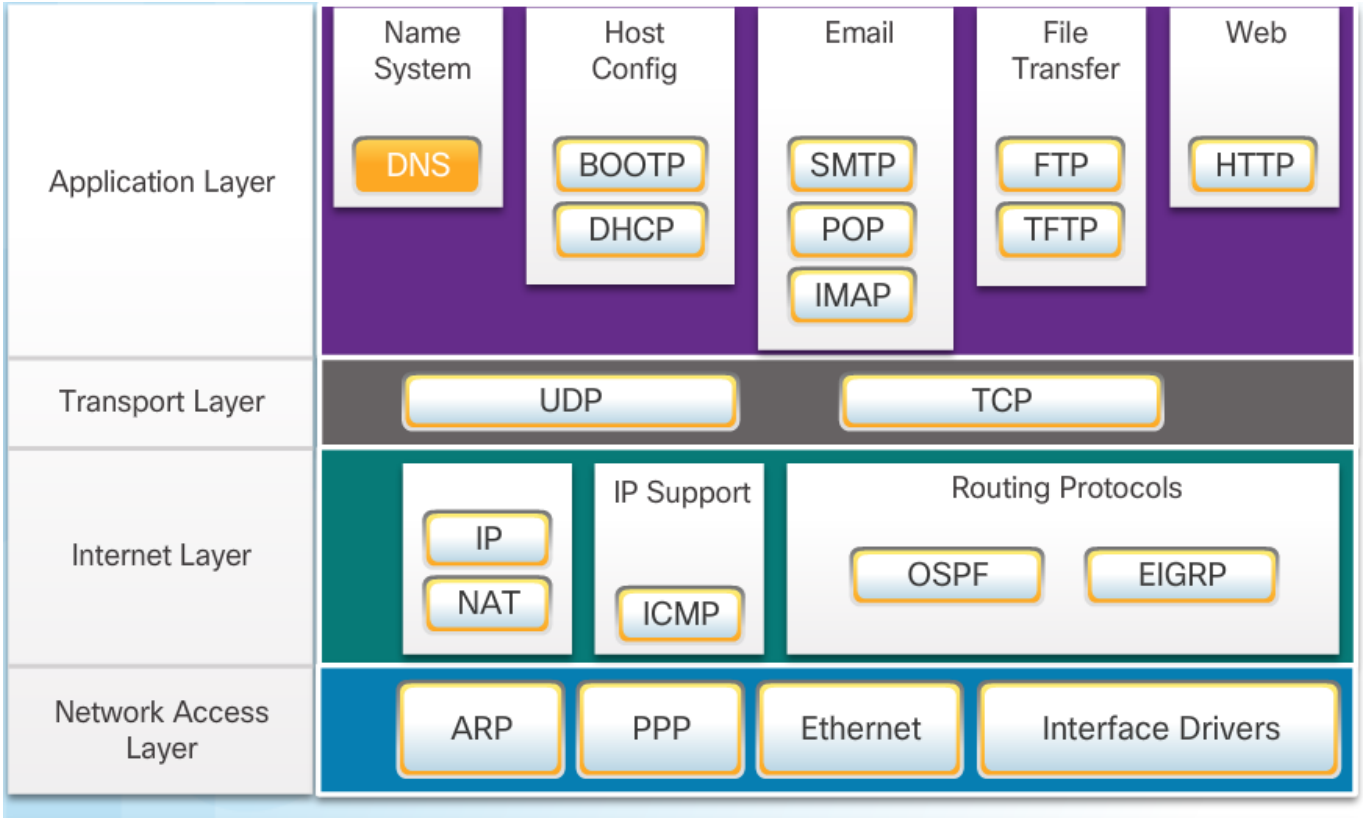
Layer Name	TCP/IP	ISO	AppleTalk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Network Access	Ethernet PPP Frame Relay ATM WLAN			

Development of TCP/IP

- Advanced Research Projects Agency Network (ARPANET) was the predecessor to today's Internet.
  - ARPANET was funded by the U.S. Department of Defense for use by universities and research laboratories.

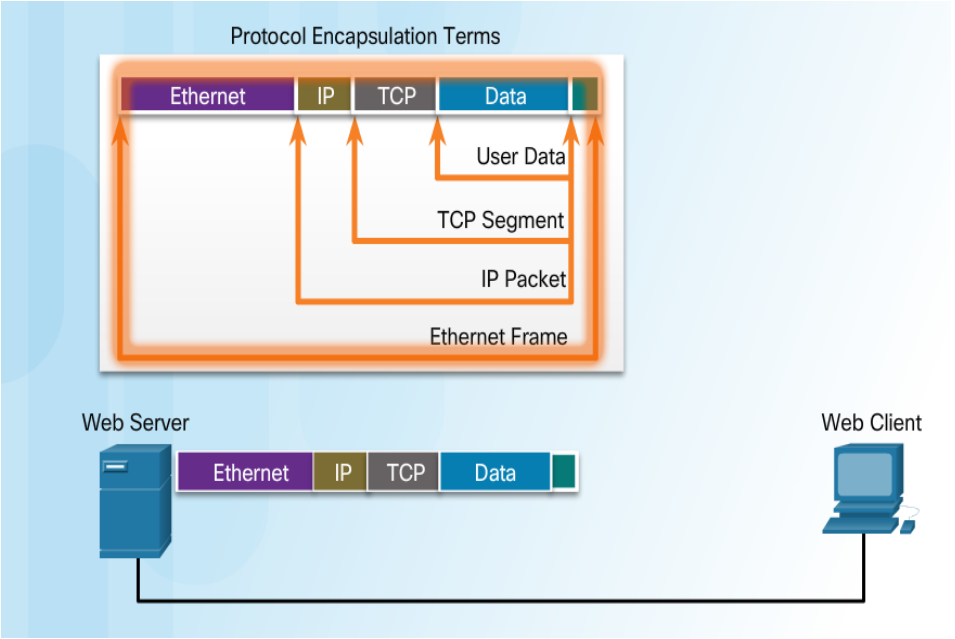


TCP/IP Protocol Suite



TCP/IP Communication Process

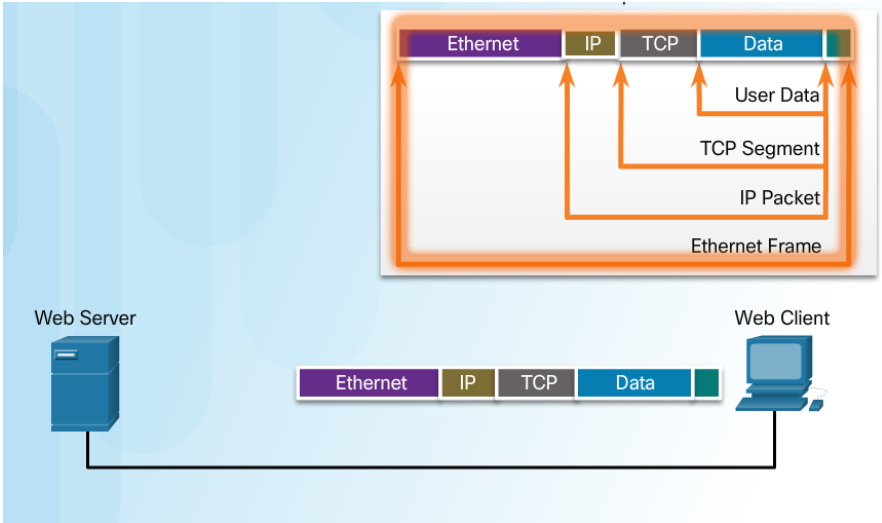
- When sending data from a web server to a client the encapsulation procedure would be as follows:
  - The webserver prepares the Hypertext Markup Language (HTML) page. The HTTP application layer protocol sends the data to the transport layer.
  - The transport layer breaks the data into segments and identifies each.
  - Next the IP source and destination addresses are added, creating an IP Packet.
  - The Ethernet information is then added creating the Ethernet Frame, or data link frame.



- This frame is delivered to the nearest router along the path towards the web client. Each router adds new data link information before forwarding the packet.

TCP/IP Communication Process (Cont.)

- When receiving the data link frames from the web server, the client processes and removes each protocol header in the opposite order it was added:
  - First the Ethernet header is removed
  - Then the IP header
  - Then the Transport layer header
  - Finally the HTTP information is processed and sent to the client's web browser

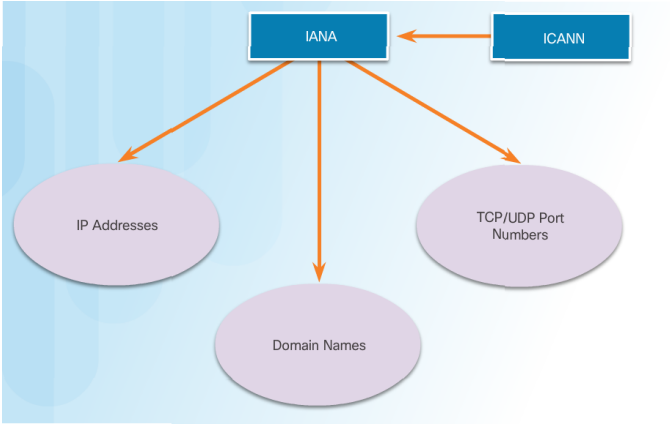


Open Standards

- Open standards encourage interoperability, competition, and innovation.
- Standards organizations are usually vendor-neutral, non-profit organizations established to develop and promote the concept of open standards.

Internet Standards

- **Internet Society (ISOC)** –promotes open development and evolution of Internet use globally.
- **Internet Architecture Board (IAB)** - management and development of Internet standards.
- **Internet Engineering Task Force (IETF)** - develops, updates, and maintains Internet and TCP/IP technologies.
- **Internet Research Task Force (IRTF)** - focused on long-term research related to Internet and TCP/IP protocols.
- **Internet Corporation for Assigned Names and Numbers (ICANN)** - coordinates IP address allocation and management of domain names.
- **Internet Assigned Numbers Authority (IANA)** - manages IP address allocation, domain name management, and protocol identifiers for ICANN.



Electronics and Communications Standard Organizations

- **Institute of Electrical and Electronics Engineers** (**IEEE**) - dedicated to advancing technological innovation and creating standards in a wide area of industries including networking.
- **Electronic Industries Alliance (EIA)** - standards related to electrical wiring, connectors, and network racks.
- **Telecommunications Industry Association (TIA)** standards for radio equipment, cellular towers, Voice over IP (VoIP) devices, and satellite communications.
- **International Telecommunications Union-Telecommunication Standardization Sector (ITU-T**) standards for video compression, Internet Protocol Television (IPTV), and broadband communications.

The Postal Analogy

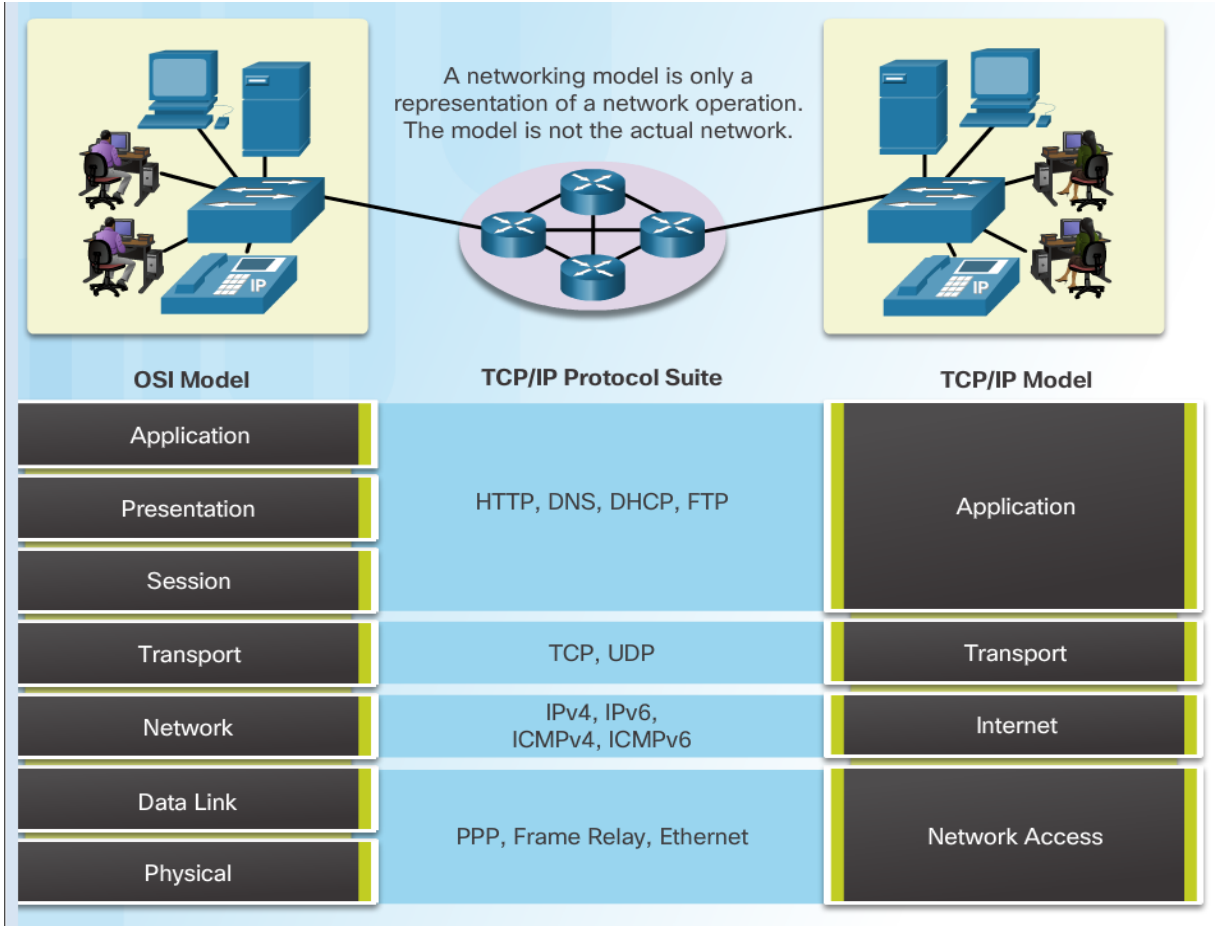
How would the OSI compare to the regular Post Office

- Application
- Presentation
- Session
- Transport
- Network
- Data-Link
- Physical

- **A-** Write a 20 page letter to a foreign country.
- **P-** Translate the letter so the receiver can read it.
- **S-** Insure the intended recipient can receive letter.
- **T-** Separate and number pages. Like registered mail, tracks delivery and requests another package if one is “lost” or “damaged” in the mail.
- **N-** Postal Center sorting letters by zip code to route them closer to destination.
- **D-** Local Post Office determining which vehicles to deliver letters.
- **P-** Physical Trucks, Planes, Rail, autos, etc which carry letter between stations.

The Benefits of Using a Layered Model

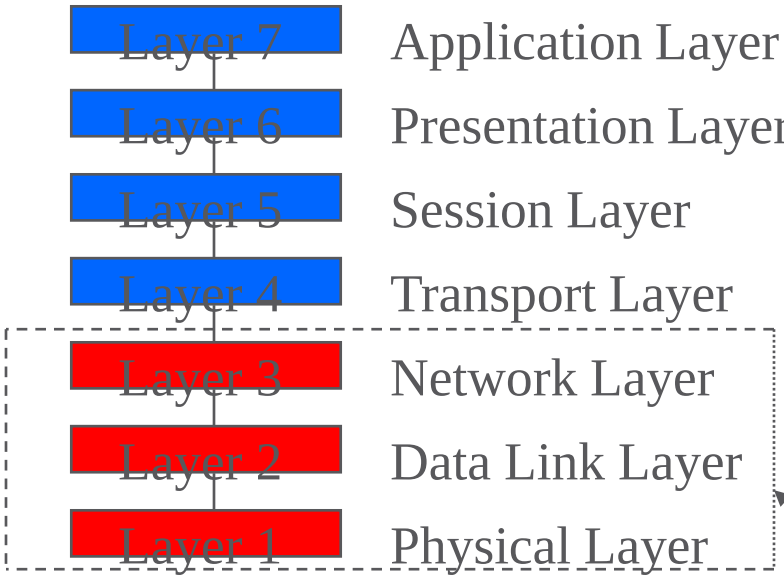
- The benefits of using a layered model include:
  - Assisting in protocol design since protocols at each layer have defined functions.
  - Fostering competition because products from different vendors can work together.
  - Preventing technology changes in one layer from affecting other layers.
  - Providing a common language to describe networking functions and capabilities.



OSI Reference Model

- OSI Reference Model - internationally standardised network architecture.
- OSI = *Open Systems Interconnection*: deals with *open systems*, i.e. systems open for communications with other systems.
- Specified in ISO 7498.
- Model has 7 layers.

7-Layer OSI Model



- Layers 1-4 relate to communications technology.
- Layers 5-7 relate to user applications.

Layer 7: Application Layer

- Level at which applications access network services.
  - Represents services that directly support software applications for file transfers, database access, and electronic mail etc.

Layer 6: Presentation Layer

- Related to representation of transmitted data
  - Translates different data representations from the Application layer into uniform standard format
- Providing services for secure efficient data transmission
  - e.g. data encryption, and data compression.

Layer 5: Session Layer

- Allows two applications on different computers to establish, use, and end a session.
  - e.g. file transfer, remote login
- Establishes dialog control
  - Regulates which side transmits, plus when and how long it transmits.
- Performs *token management* and *synchronization*.

Layer 4: Transport Layer

- Manages transmission packets
  - Repackages long messages when necessary into small packets for transmission
  - Reassembles packets in correct order to get the original message.
- Handles error recognition and recovery.
  - Transport layer at receiving acknowledges packet delivery.
  - Resends missing packets

Layer 3: Network Layer

- Manages addressing/routing of data within the subnet
  - Addresses messages and translates logical addresses and names into physical addresses.
  - Determines the route from the source to the destination computer
  - Manages traffic problems, such as switching, routing, and controlling the congestion of data packets.
- Routing can be:
  - Based on static tables
  - determined at start of each session
  - Individually determined for each packet, reflecting the current network load.

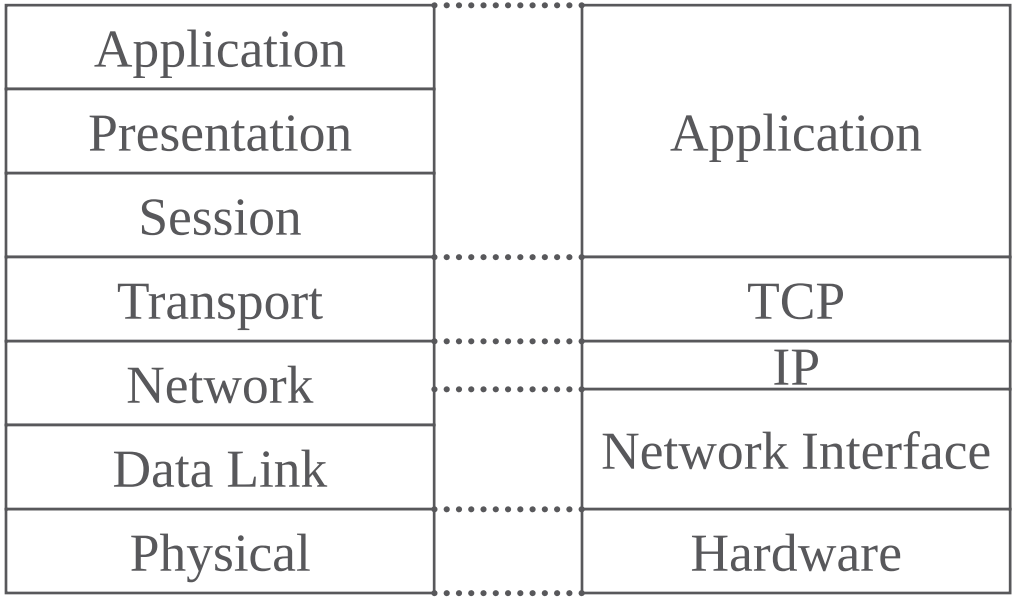
Layer 2: Data Link Layer

- Packages raw bits from the Physical layer into frames (logical, structured packets for data).
- Provides reliable transmission of frames
  - It waits for an acknowledgment from the receiving computer.
  - Retransmits frames for which acknowledgement not received

Layer 1: Physical Layer

- Transmits bits from one computer to another
- Regulates the transmission of a stream of bits over a physical medium.
- Defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable. Deals with issues like
  - The definition of 0 and 1, e.g. how many volts represents a 1, and how long a bit lasts?
  - Whether the channel is simplex or duplex?
  - How many pins a connector has, and what the function of each pin is?

Internet Protocols vs OSI

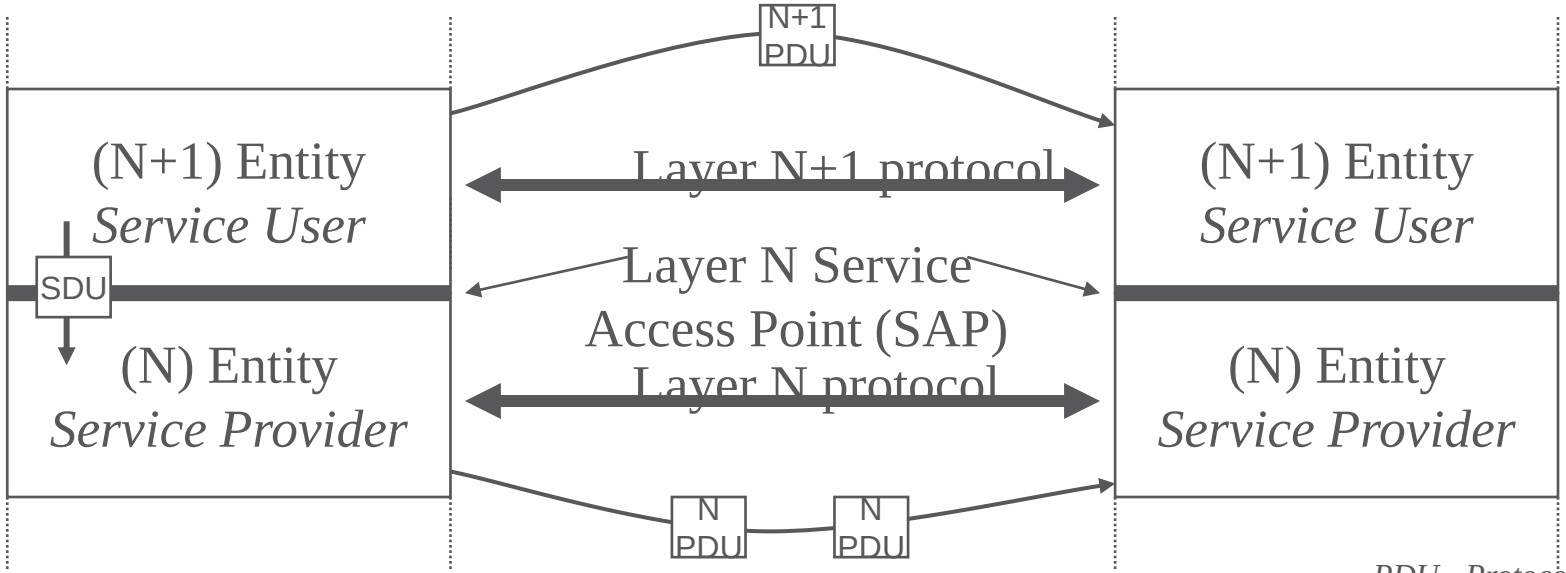


- Explicit Presentation and session layers missing in Internet Protocols
- Data Link and Network Layers redesigned

Services in the OSI Model

- In OSI model, each layer provide services to layer above, and ‘consumes’ services provided by layer below.
- Active elements in a layer called *entities*.
- Entities in same layer in different machines called *peer entities*.

Layering Principles



PDU - Protocol Data Unit
SDU - Service Data Unit

- Layer N provides service to layer N+1

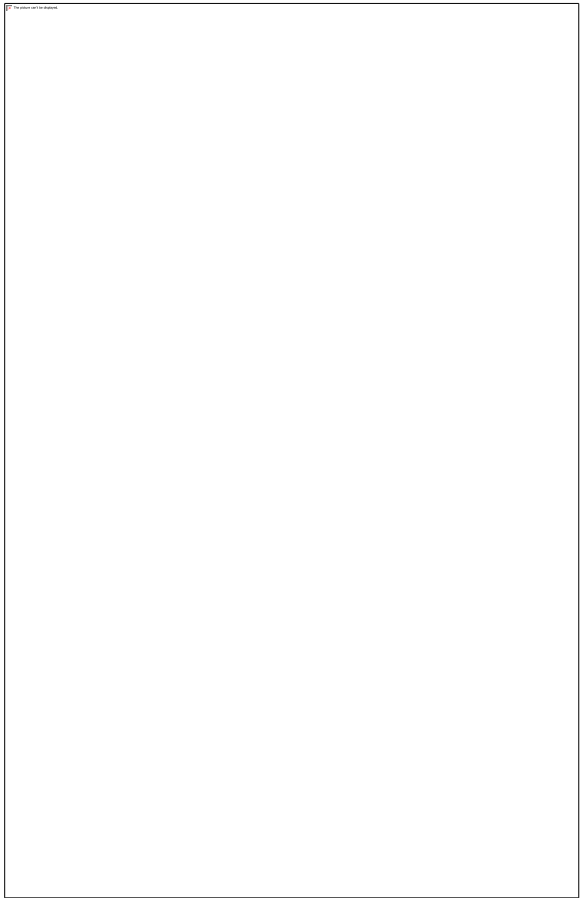
Connections

- Layers can offer *connection-oriented* or *connectionless* services.
- Connection-oriented like telephone system.
- Connectionless like postal system.
- Each service has an associated *Quality-of-service* (e.g. reliable or unreliable).

Reliability

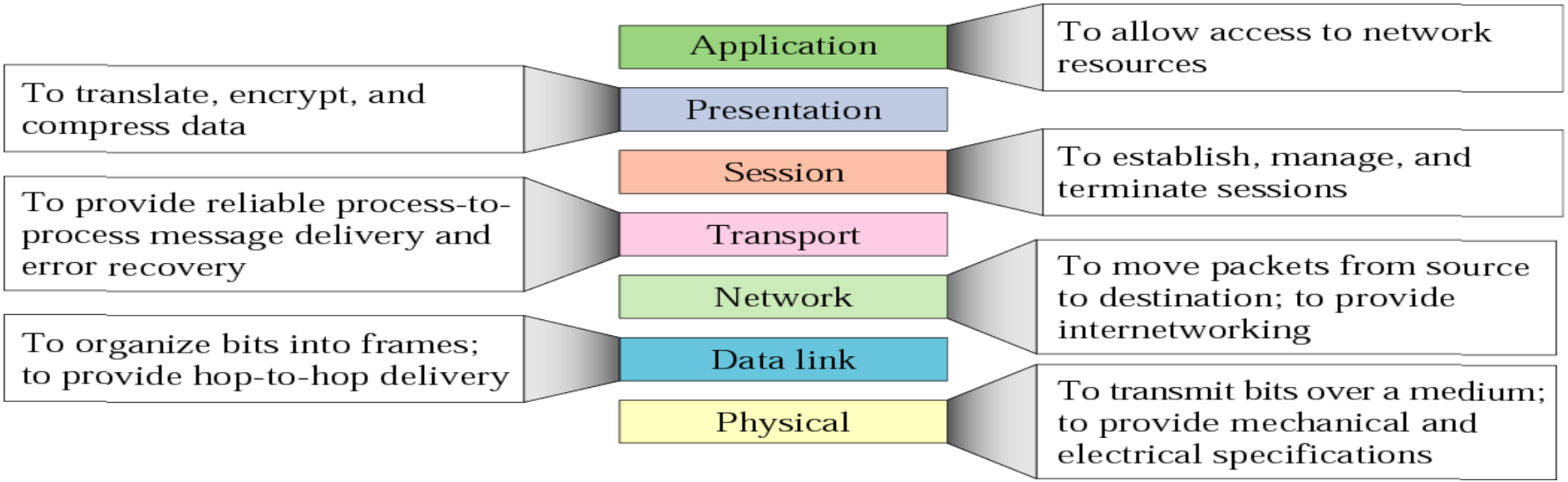
- Reliable services never lose/corrupt data.
- Reliable service costs more.
- Typical application for reliable service is file transfer.
- Typical application not needing reliable service is voice traffic.
- Not all applications need connections.

The OSI Reference Model



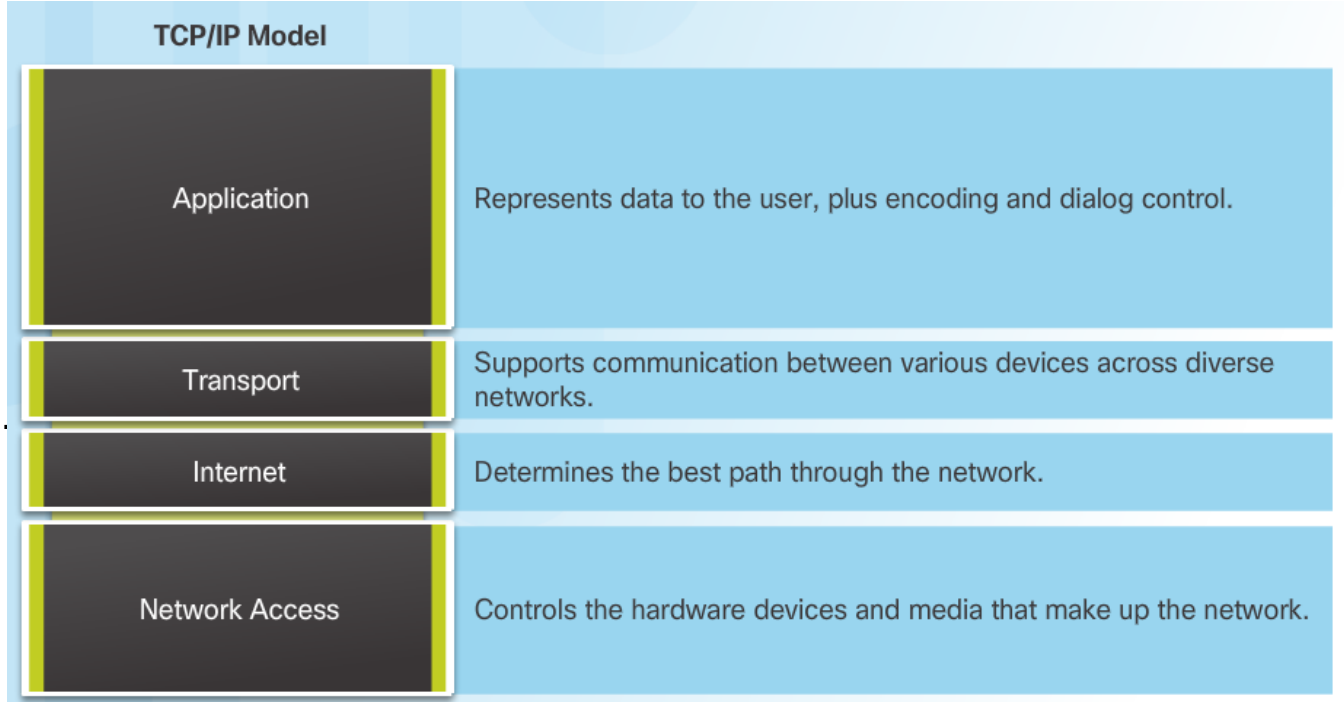
- Application - contains protocols used for process-to-process communications.
- Presentation - provides for common representation of the data.
- Session - provides services to the presentation layer to organize its dialogue and to manage data exchange.
- Transport - defines services to segment, transfer, and reassemble the data.
- Network - provides services to exchange the individual pieces of data over the network between identified end devices.
- Data Link - provides methods for exchanging data frames between devices over a common media.
- Physical - describes the mechanical, electrical, functional, and procedural means to transmit bits across physical connections.

Figure 2.14 *Summary of OSI layers*



The TCP/IP Protocol Model

- The TCP/IP Protocol Model
  - Created in the early 1970s for internetwork communications.
  - Open Standard.
  - Also called The TCP/IP Model or the Internet Model.



OSI Model and TCP/IP Model Comparison

- In the OSI model, the network access layer and the application layer of the TCP/IP model are further divided to describe discrete functions that must occur at these layers.

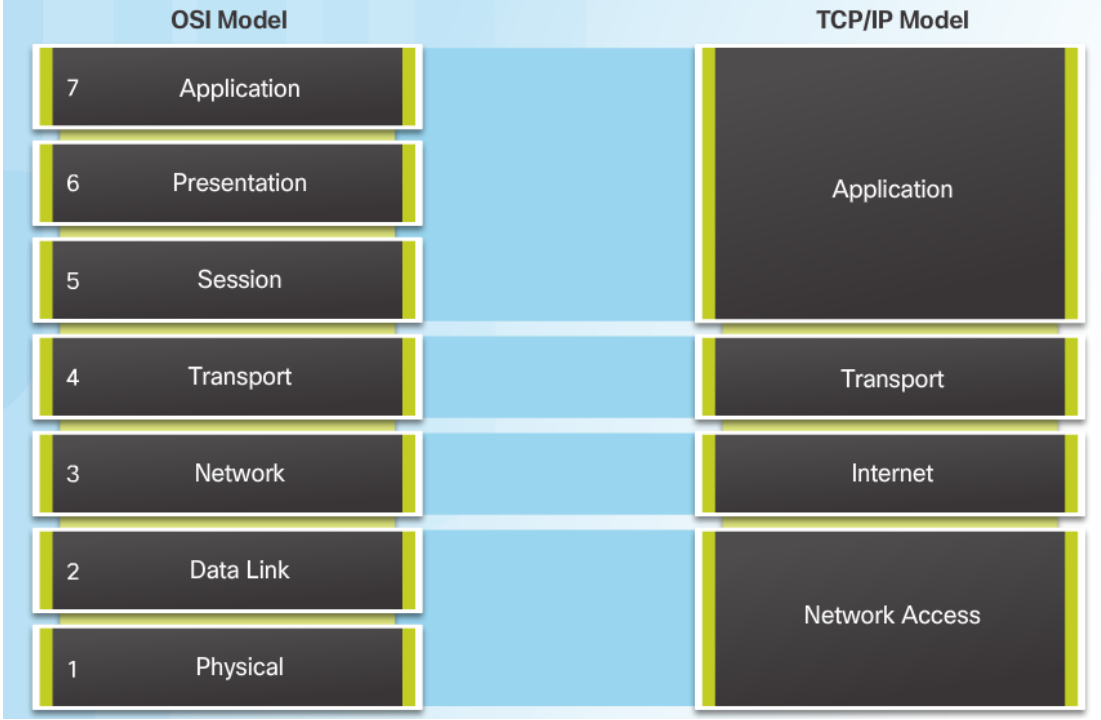
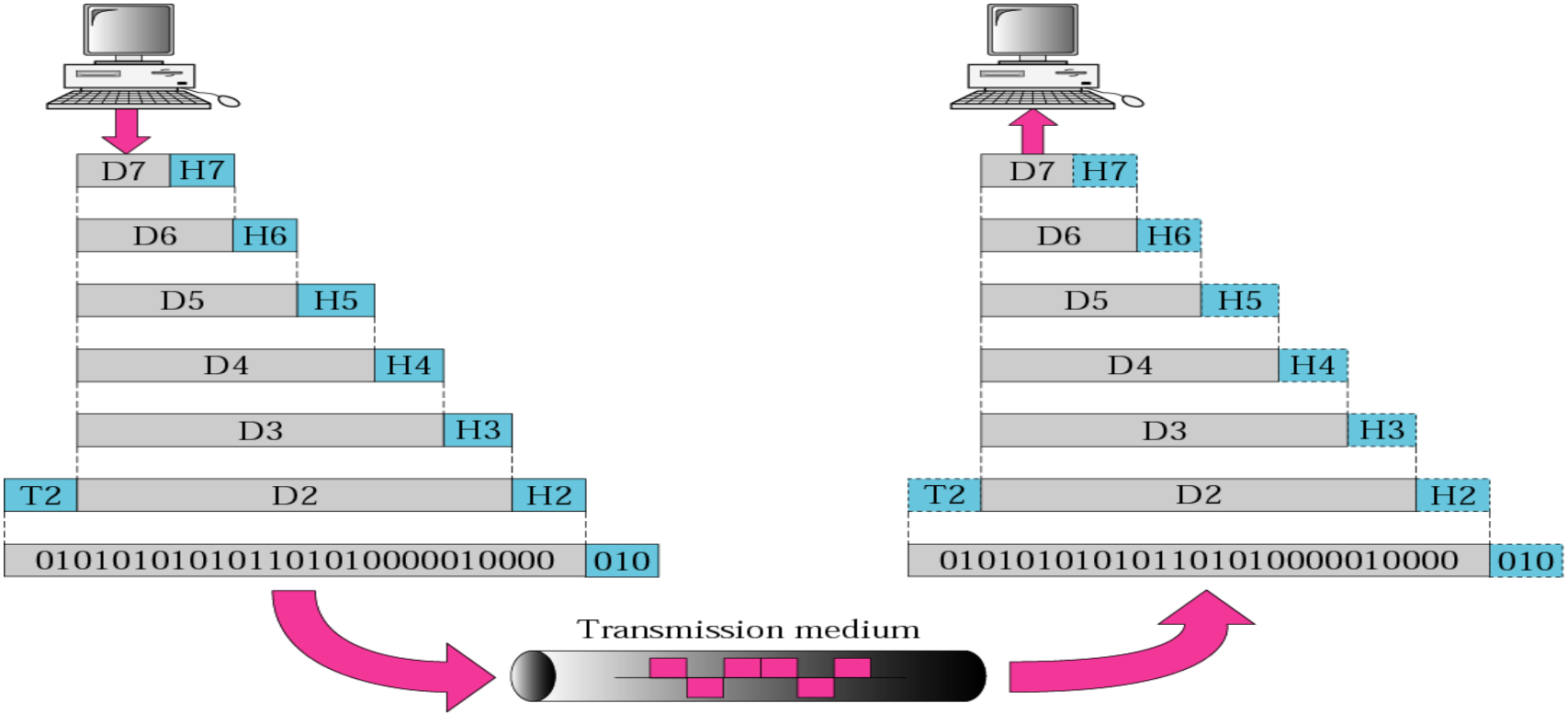


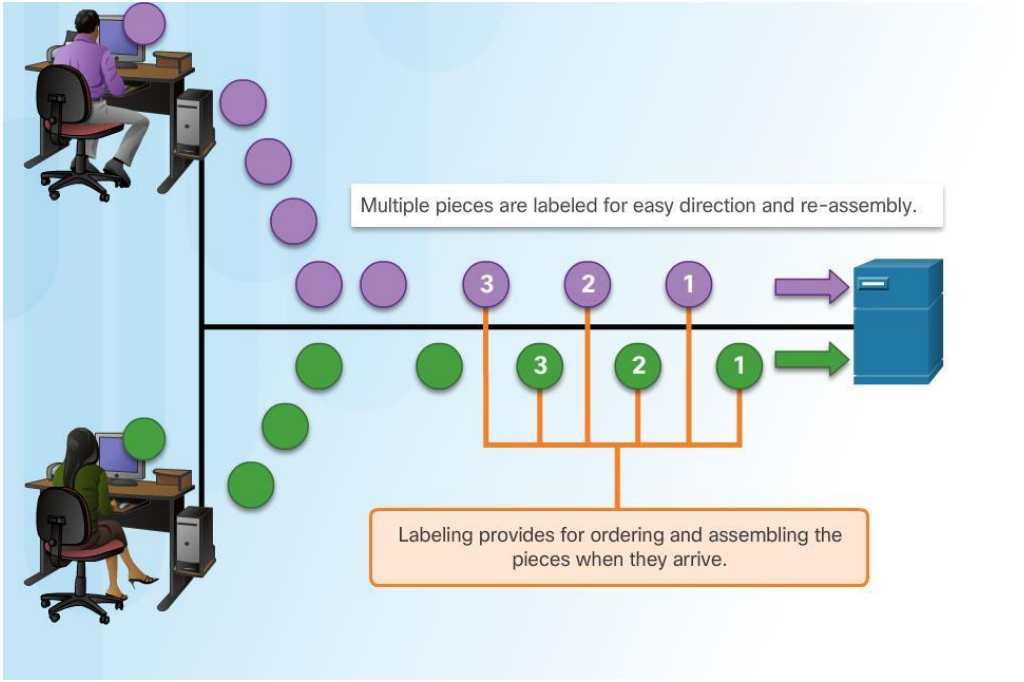
Figure 2.3 *An exchange using the OSI model*



Data Transfer in the Network

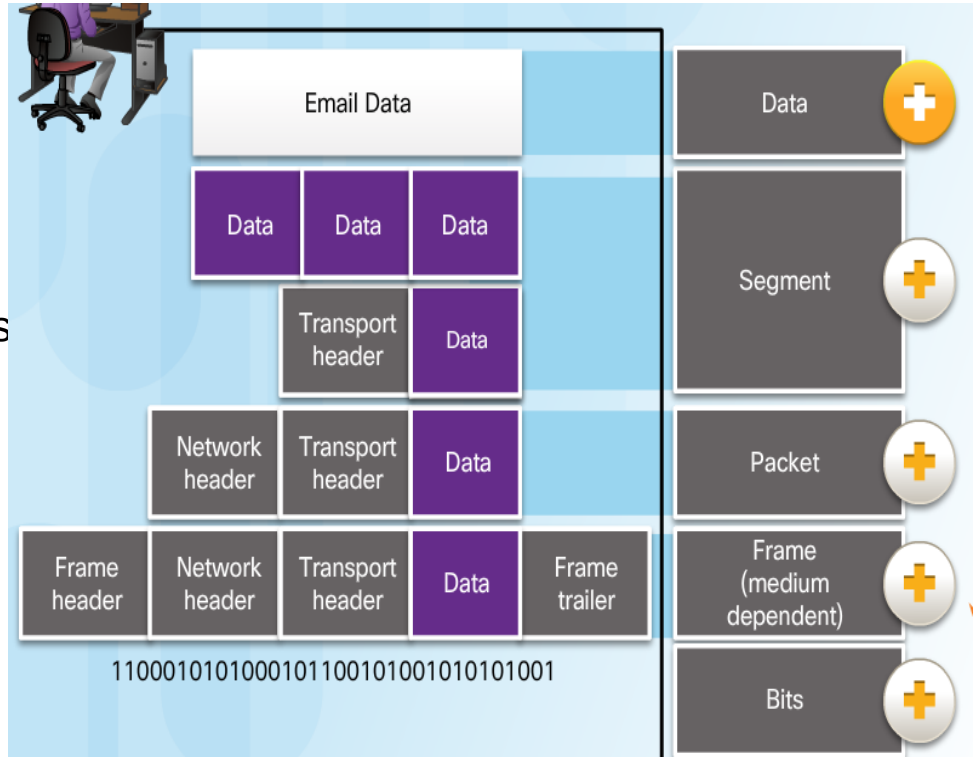
Message Segmentation

- Large streams of data are divided into smaller, more manageable pieces to send over the network.
  - By sending smaller pieces, many different conversations can be interleaved on the network, called **multiplexing.**
  - Each piece must be labeled.
  - If part of the message fails to make it to the destination, only the missing pieces need to be retransmitted.



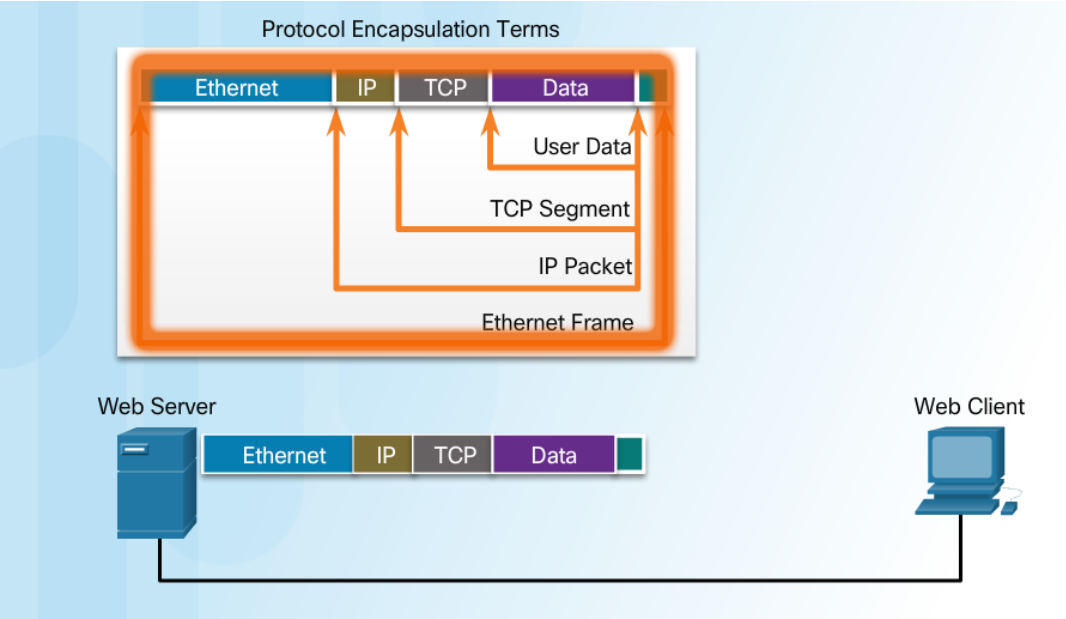
Protocol Data Units

- As application data is passed down the protocol stack, information is added at each level. This is known as the **encapsulation** process.
- The form that the data takes at each layer is known as a Protocol Data Unit (PDU).
  - Data - application layer PDU
  - Segment – Transport layer PDU
  - Packet – Network layer PDU
  - Frame – Data Link Layer PDU
  - Bits – Physical Layer PDU



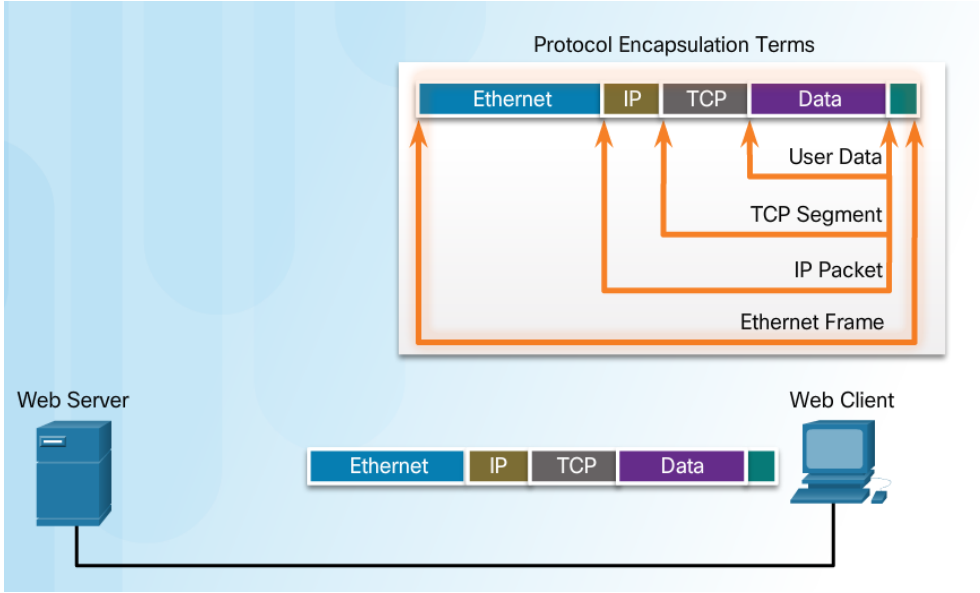
Encapsulation Example

- The encapsulation process works from top to bottom:
  - Data is divided into segments.
  - The TCP segment is encapsulated in the IP Packet.
  - The IP packet is encapsulated in the Ethernet Frame.



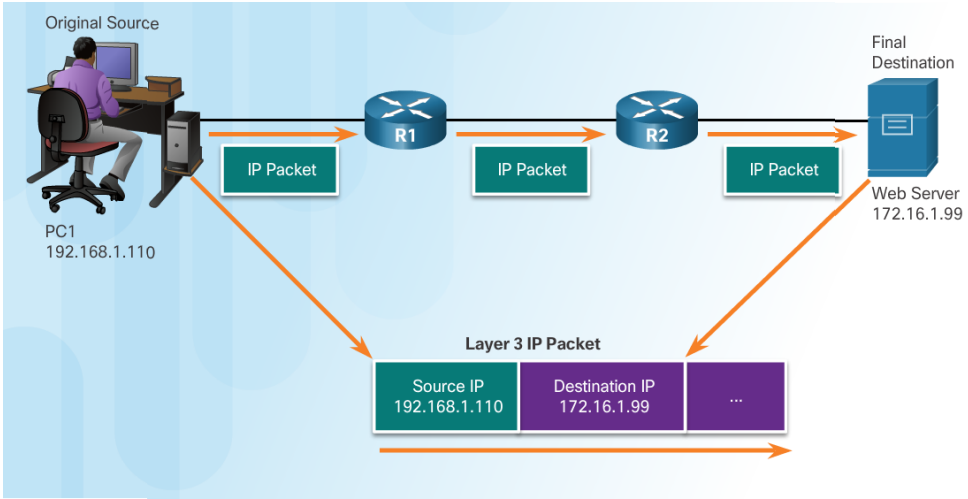
De-encapsulation

- The de-encapsulation process works from bottom to top.
- De-encapsulation is the process used by a receiving device to remove one or more of the protocol headers.
  - The data is de-encapsulated as it moves up the stack toward the end-user application.



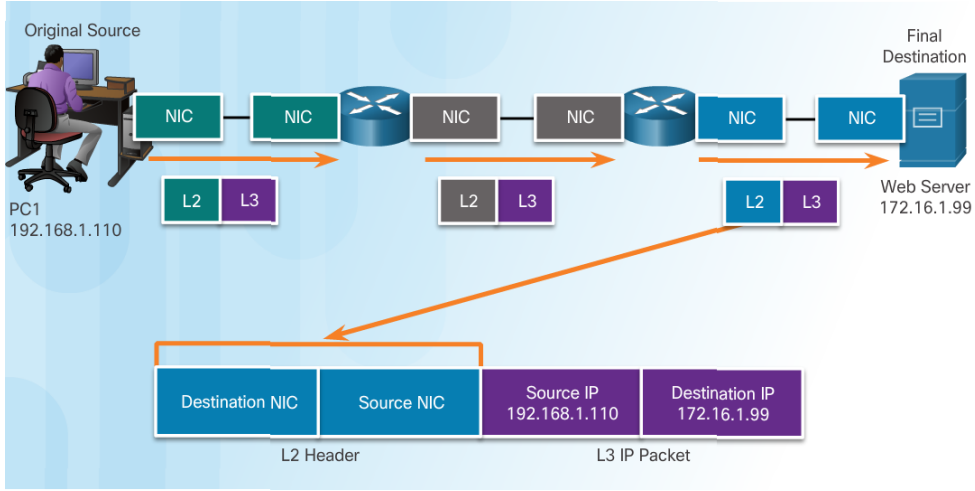
Network Addresses

- Network layer source and destination addresses - Responsible for delivering the IP packet from the original source to the final destination.
  - **Source IP address** - The IP address of the sending device, the original source of the packet.
  - **Destination IP address** - The IP address of the receiving device, the final destination of the packet.



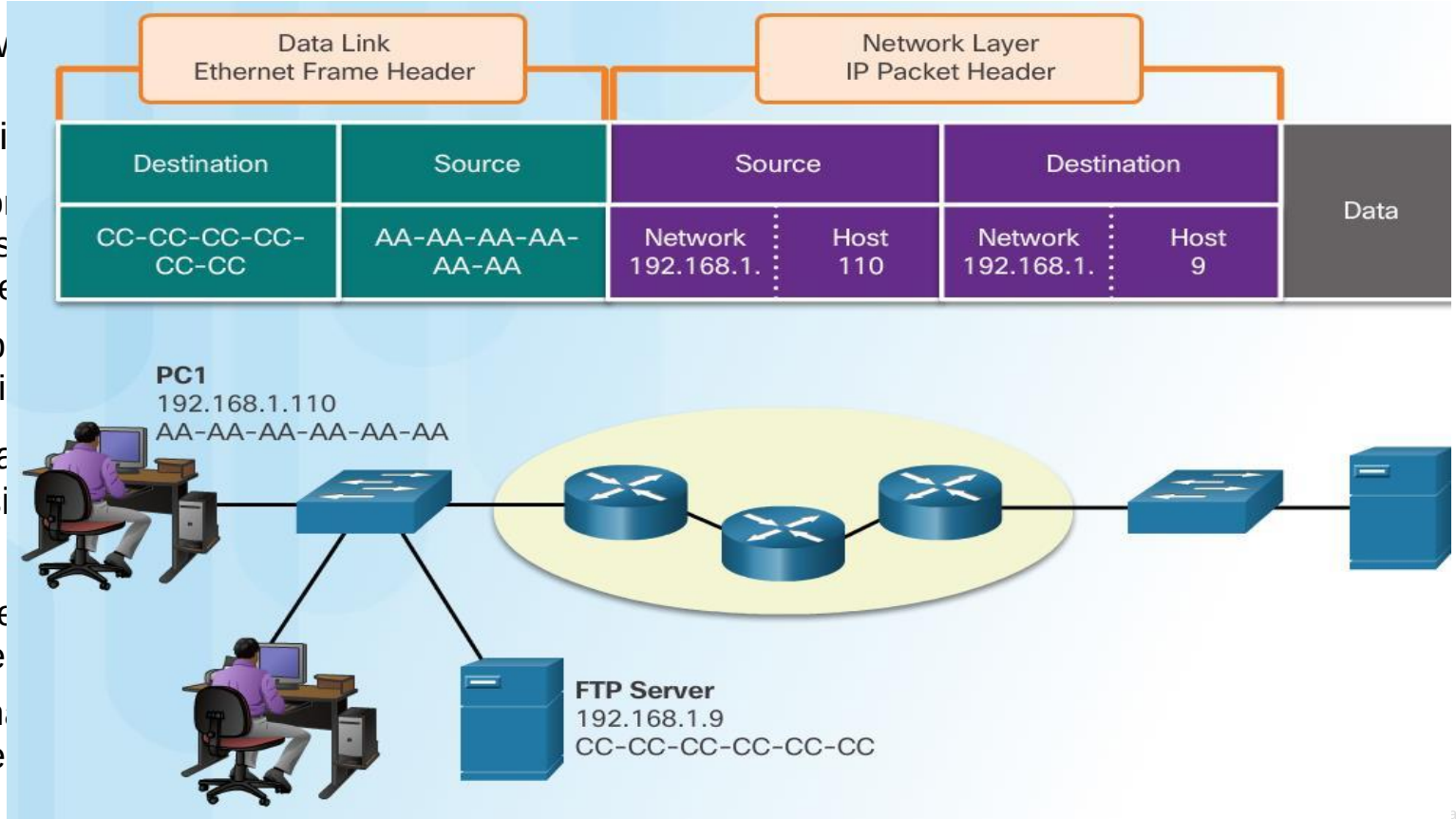
Data Link Addresses

- The purpose of the data link address is to deliver the data link frame from one network interface to another network interface on the same network.
  - As the IP packet travels from source to destination it is encapsulated in a new data link frame when it is forwarded by each router.



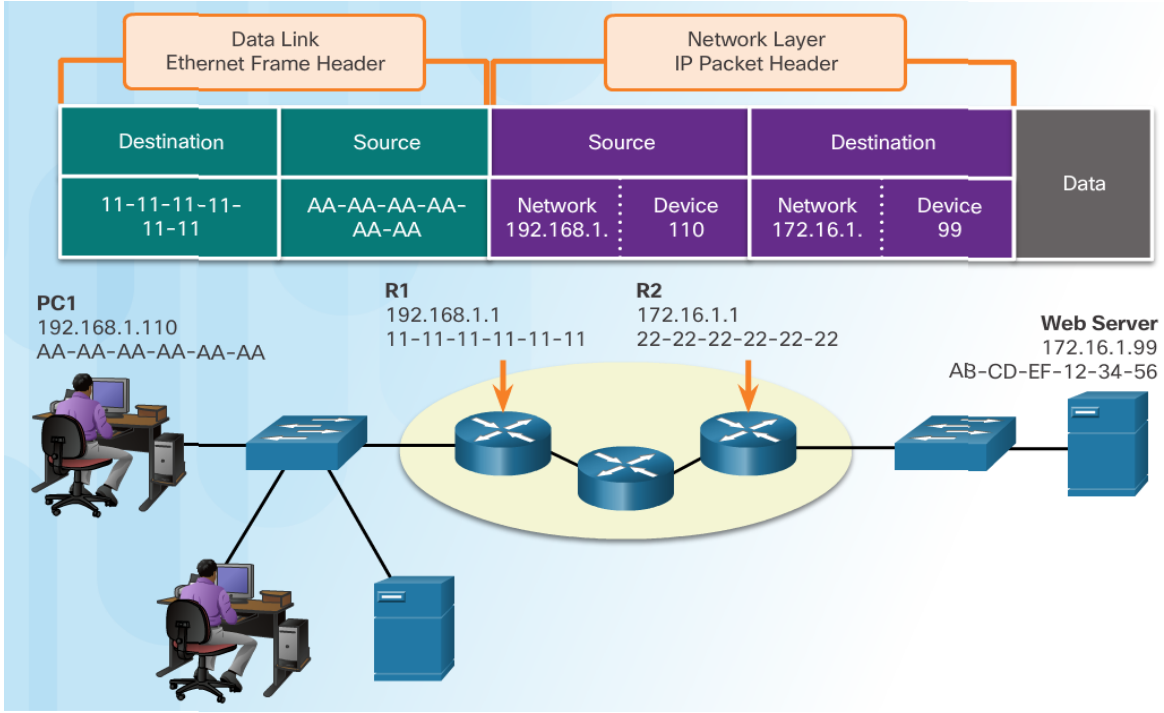
Devices on the Same Network

- The netw
  indicate
  destinati
  - Networ
    addres
    is a me
  - Host p
    identifi
- The data
  addressi
  device.
  - Source
    device
  - Destin
    device



Devices on a Remote Network

- Sending to a remote network - the source and destination IP addresses represent hosts on different networks.
- The data link frame cannot be sent directly to the remote destination host. Therefore the frame is sent to the default gateway (nearest router interface).
- The router removes the received Layer 2 information and adds new data link information before forwarding out the exit interface.



2-5 ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

Topics discussed in this section:

Physical Addresses
Logical Addresses
Port Addresses
Specific Addresses

Figure 2.17 *Addresses in TCP/IP*

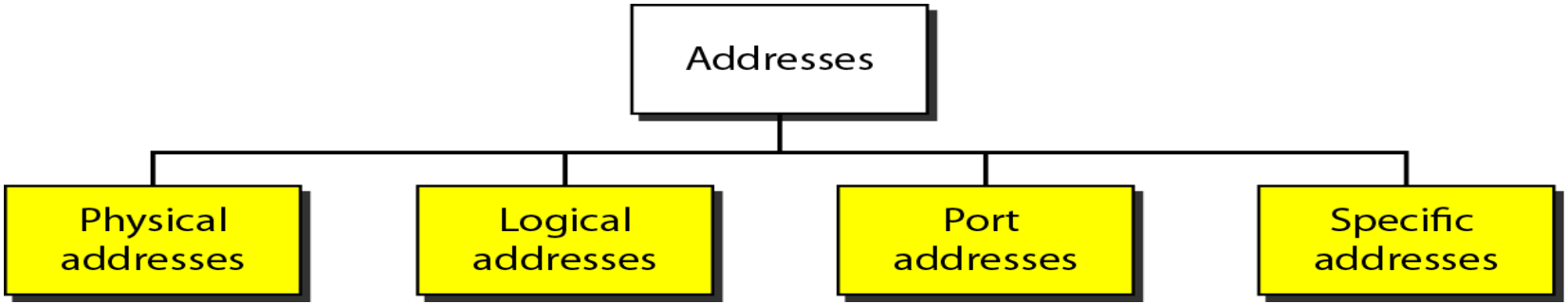
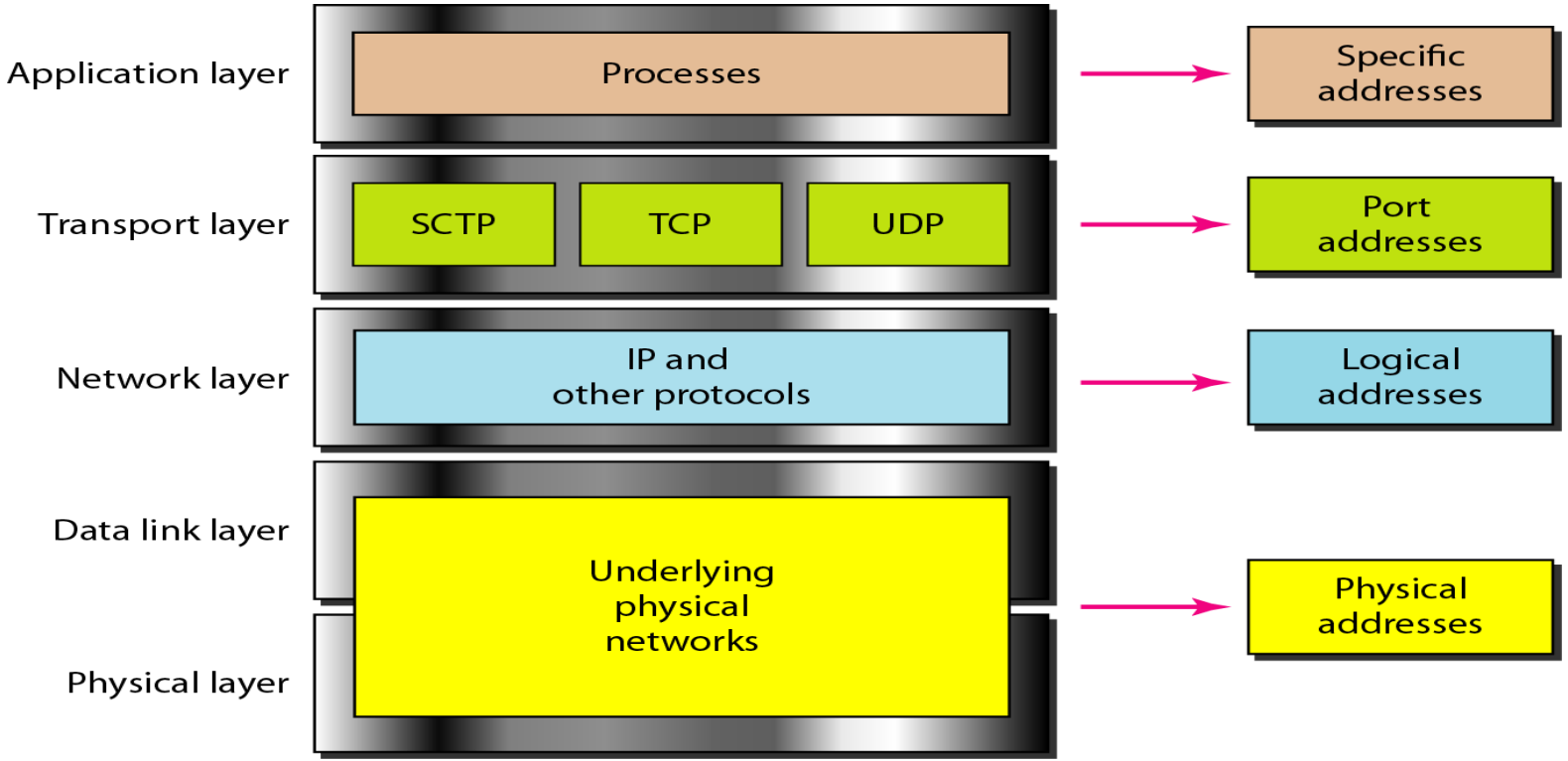


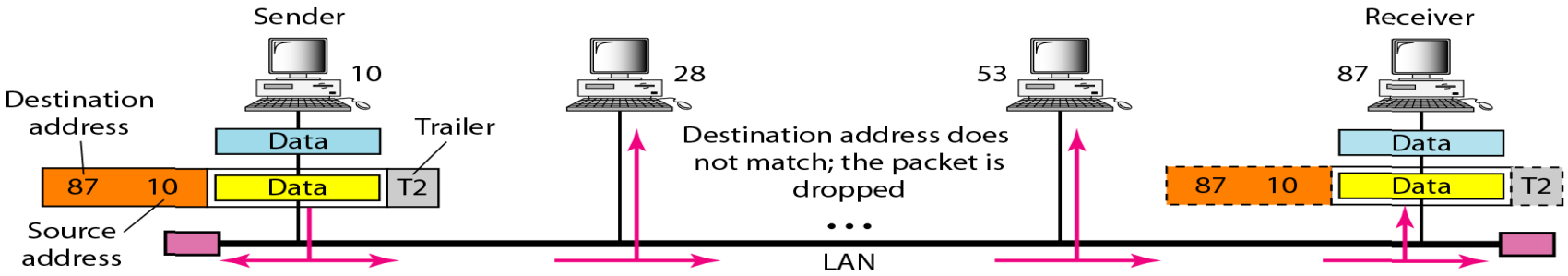
Figure 2.18 *Relationship of layers and addresses in TCP/IP*



Example 2.1

In Figure 2.19 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

Figure 2.19 *Physical addresses*



Example 2.2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

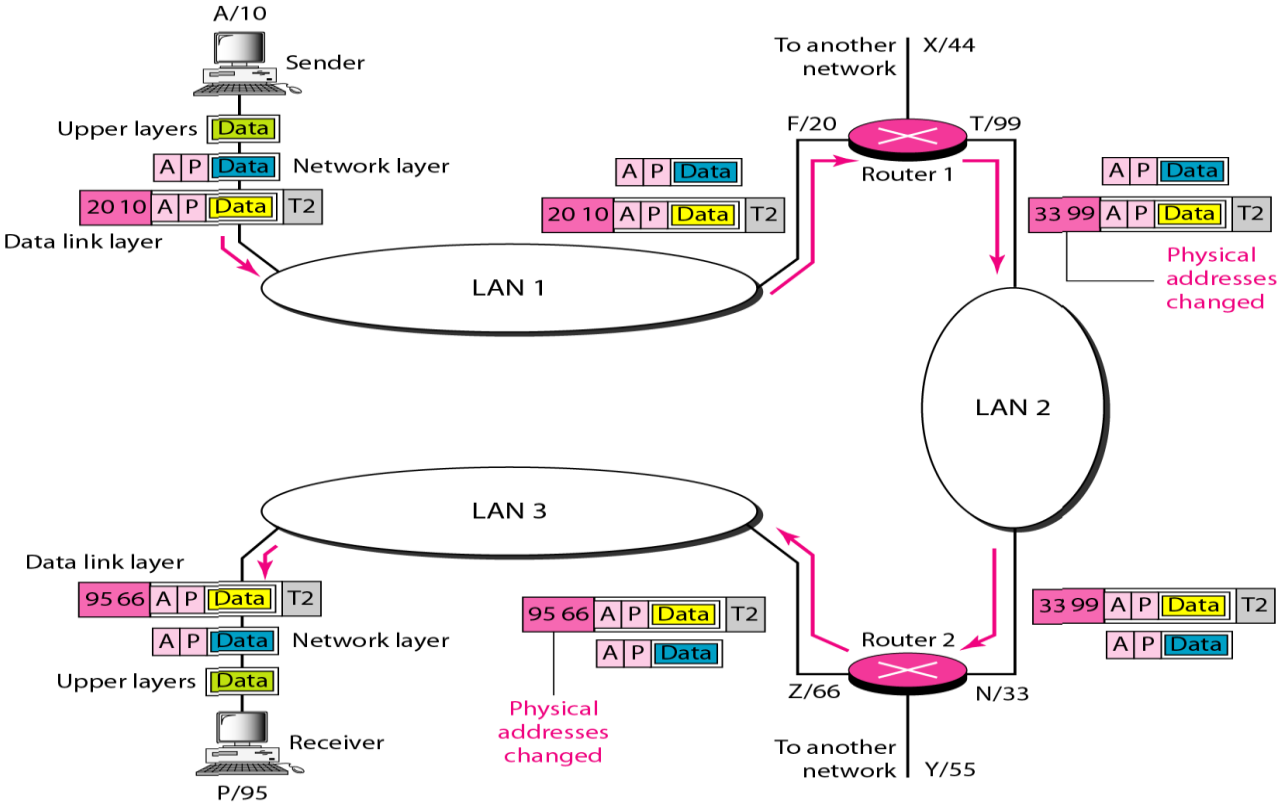
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

Example 2.3

Figure 2.20 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

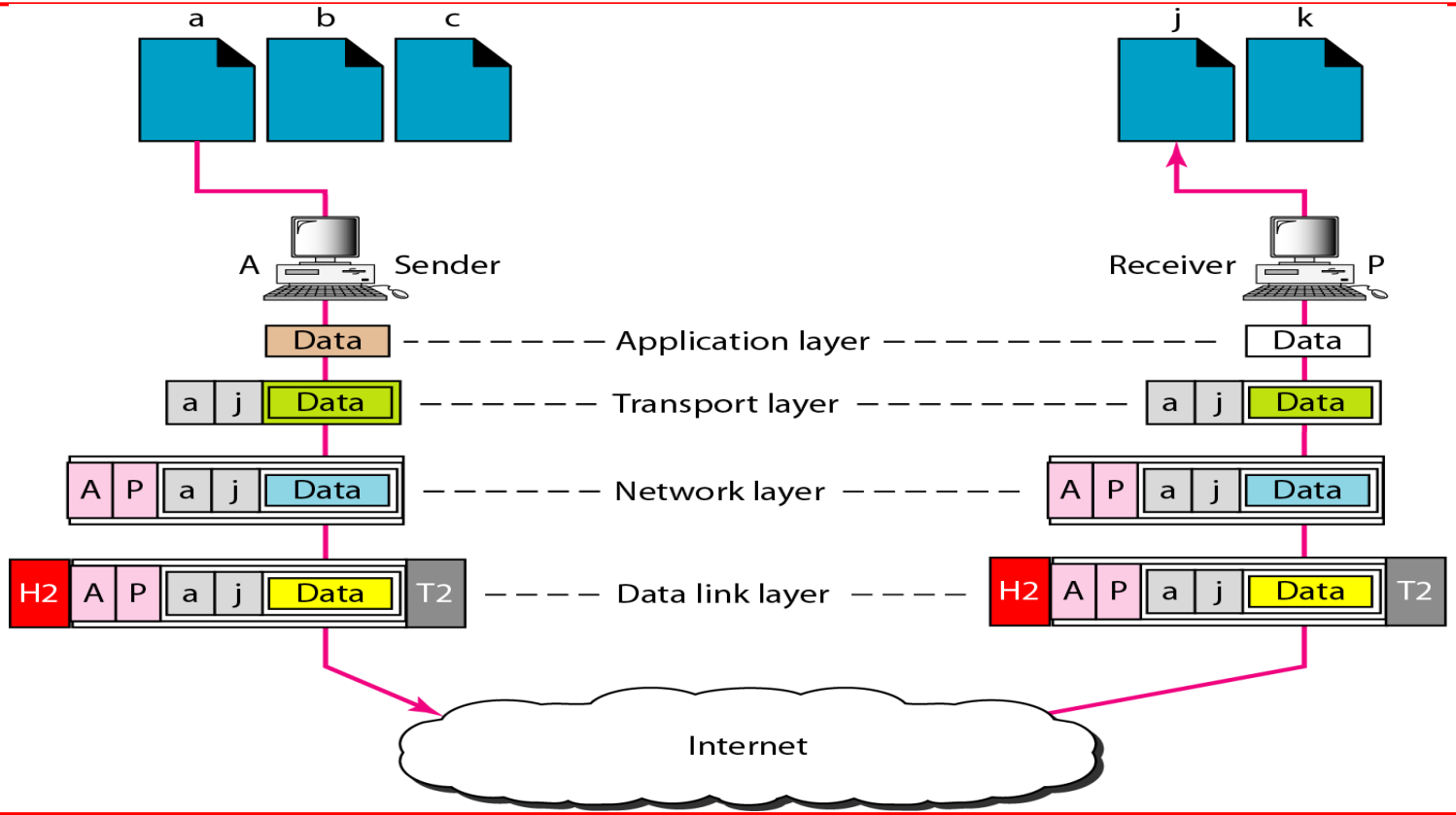
Figure 2.20 *IP addresses*



Example 2.4

Figure 2.21 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Figure 2.21 *Port addresses*



Note

The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

Example 2.5

A port address is a 16-bit address represented by one decimal number as shown.

753

A 16-bit port address represented as one single number.

2.114