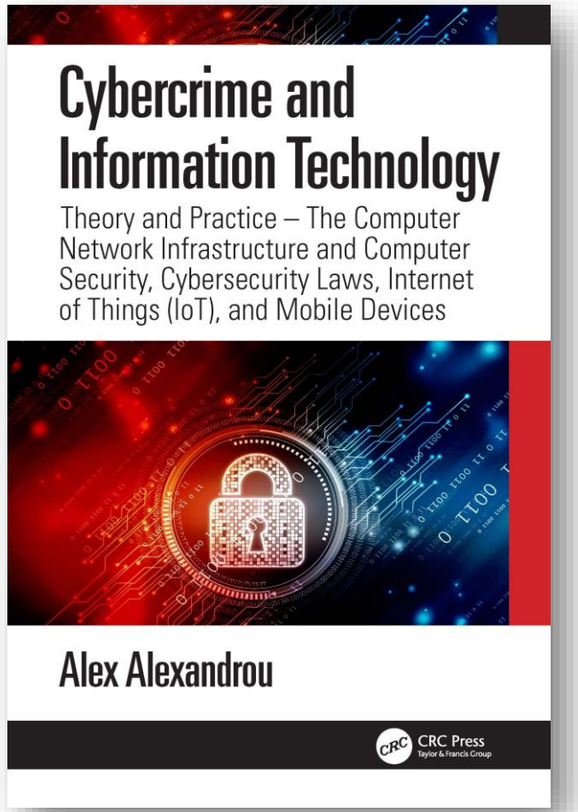


I

Cybercrime and Information Technology: Theory and Practice The Computer Network Infostructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices

The Networking Environment

Chapter 5

Objectives

- Understand computer networking, its history and evolution.
- Identify the advantages and disadvantages of computer networking.
- Understand essential computer network components and terminology.
- Understand different types of networking.
- Understand the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TPC/IP) Models.

Objectives

- Understand different types of networking.
- Network Topology
- Understand the Open Systems Interconnection (OSI)
- Transmission Control Protocol/Internet Protocol (TPC/IP) Models.
- The User Datagram Protocol (UDP)

Introduction to Computer Networking

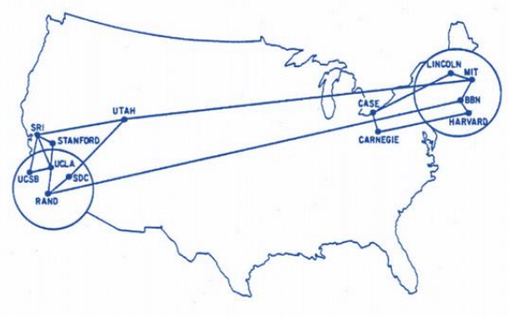
- In the **21st century the word "connected"** now describes the significant advancements in technology that have changed our world once again.

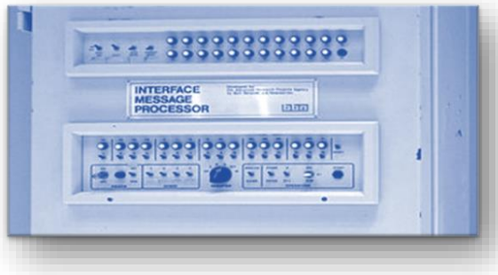
- The Internet is an enormous global network of networks that can connect every computing device to its vast resources, and to every other computer on the planet.

- In the 1960s, the **Advanced Research Projects Agency (ARPA),** part of the Department of Defense, funded a proposed network project called the **Advanced Research Projects Agency Network (ARPANET)**, through the **Association for Computing Machinery (ACM).**

Introduction to Computer Networking (cont.)

- In 1969, the experimental **ARPANET** was constructed.
  - The new network connected the Universities of California Los Angeles (UCLA) and California at Santa Barbara (UCSB), the Stanford Research Institute (SRI), and the University of Utah (UTAH) through the Internet Message Processor (IMP).
  - The four universities formed a network and communicated using software called the **Network Control Program (NCP),** which later came to be known as a protocol or a **host-to-host protocol**.





The first routers, known as Interface Message Processors or IMPs.

Introduction to Computer Networking (cont.)

- In 1981, the **National Science Foundation (NSF)** sponsored the creation of **CSNET.**
- This network was created for universities that were not qualified to use the **ARPANET** because they did not have ties to **the Defense Advanced Research Projects Agency (DARPA).**

Introduction to Computer Networking (cont.)

- In 1983, TCP/IP became the official protocol for ARPANET.
  - In 1983, the ARPANET split into two separate networks, the **MILNET** for military installations and the **ARPANET** for civilian use (mainly dedicated to research).
- In 1989, while working for the European Organization for **Nuclear Research (CERN), Tim Berners-Lee, invented the World Wide Web (WWW).**
  - The idea was the creation of a service that merged **HTML, URL and HTTP**, so that all computers could understand each other in an easy-to-use global information system.

Introduction to Computer Networking (cont.)

- In 1990, the **ARPANET** was replaced by **NSFNET.**
  - In 1995, the network became largely commercial and grew exponentially.
  - The **ARPANET,** not the **NSFNET,** that was the predecessor to our **Internet**.
- Today we take for granted this global network infrastructure called the Internet.

Protocols

- A protocol is a digital language and set of specifications and procedures followed throughout the network so that computers in different locations can share information and resources, making the network viable.
  - Networks can connect many different types of computers, and share resources that reside on widely different types of servers.
  - Without a viable protocol, no network can function.
    - During the early years of the ARPANET the Network Working Group (NWG) was formed to monitor and oversee the network's technical aspects.

Protocols (Cont.)

- The NWG was instrumental in the development of the ARPANET and set the stage for the development of the Network Control Protocol (NCP) and later the Transmission Control Protocol/Internet Protocol (TCP/IP), the most widely used communications protocol to this day.
- In 1970, the NWG, under the supervision of Steve Crocker, completed the host-to-host protocol called the NCP.
- Between 1970-1972 the NCP was implemented on the ARPANET, enabling network users to develop applications.
- Besides Crocker, Vinton G. Cerf, one of the co-founders of **TCP/IP,** had been involved in NCP design and development.

Protocols (Cont.)

- In **1974**, Vinton G. Cerf and Robert E. Kahn published a paper called ***"A Protocol for Packet Network Intercommunication Researchers"***, which recognized the significance of network intercommunication involving different types of computers, flow control, end-to-end error checking and topologies.
  - Thus, they designed the **TCP/IP protocol along with the basic architecture used to transmit data over the Internet.**
  - Their contribution is of immense significance to the digital revolution that followed. Dr. Cerf is commonly known as the **"Father of the Internet".**

Protocols (Cont.)

- Later in the **1970s**, the government decided to split **TCP** into two protocols.
- In **1981**, UC Berkeley, working under a contract with **DARPA**, expanded **TCP/IP** to include error correction, segmentation and reassembly.
- In **1981**, the government eliminated the NCP and adopted TCP/IP as the official protocol for the ARPANET.
- In **1983**, the **ARPANET** replaced **NCP** with **TCP/IP** and allowed the **ARPANET** to split into **MILNET for military and the ARPANET for research communicatio**ns.

The World Wide Web & the Internet

- The **Internet** and the **World Wide Web (WWW)** are not the same.
- The web is a way to view and share information over the internet.
  - Tim Berners-Lee, invented the World Wide Web (WWW).
  - The idea was the creation of a service that merged HTML, URL and HTTP, so that all computers could understand each other in an easy-to-use global information system.
  - The connection into a network by any device occurs either wired or wirelessly.

The World Wide Web & the Internet

- The Internet is a global network of networks that are structured to connect to each other, whereas the Web is a service that runs on the top of this infrastructure
  - In a wired connection, we physically connect a computer into a router using Ethernet cables.
  - In a wireless connection the computer is connected to the network via a radio signal.
  - The Institute of Electrical and Electronics Engineers (IEEE) has defined the standard for wireless communications with Wi-Fi-enabled devices as IEEE 802.11, and for Ethernet wired standard connections as IEEE 802.3.

Advantages and Disadvantages of Computer Networking

Advantages

- **Central data storage-**data is shared between devices/users, users can access data remotely.
- **Cost benefits of shared**
- **Centralized protection and monitoring**
- **Ability to Access information at a very fast speed**
- **Network Backup reliability-**ensures that data is backed up onto multiple servers.
- **Security-**through authentication that validates the identity of an authorized user, thereby preventing theft or unauthorized accessing of data.

Advantages and Disadvantages of Computer Networking

Disadvantages

- **Cost of network management and maintenance,** including expensive hardware and applications, Uninterruptible Power Supply (UPS), fire suppression equipment, air conditioning, stable temperature maintenance, humidity control, air filtration for dust and other airborne particles, and the training of personnel to run the data center.

- **Virus and Malware-** Infections can quickly spread on a network system and repair is time consuming and may interrupt the flow of business.

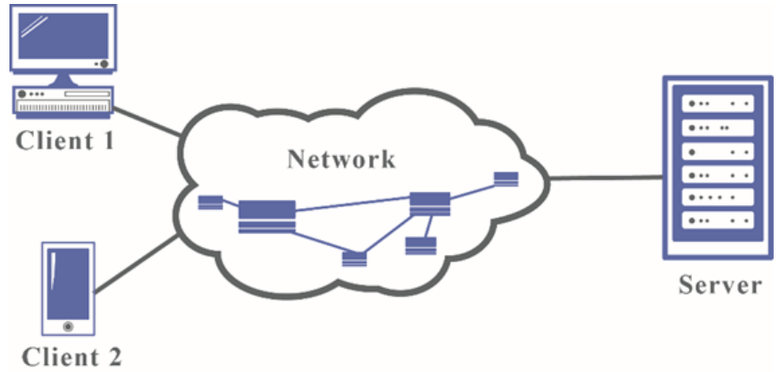
Computer Network Components and Terminology

- A computer network requires different components which must work together properly.
- The network provides methods and techniques to prevent and monitor unauthorized access, called data breaches.
- The most basic form of networking is **Peer-to-Peer (P2P).**
  - The **P2P network** is created when two or more computing devices share resources like storage devices, files, and printers without using a server.
  - All computing devices can function as both a **client and server.**

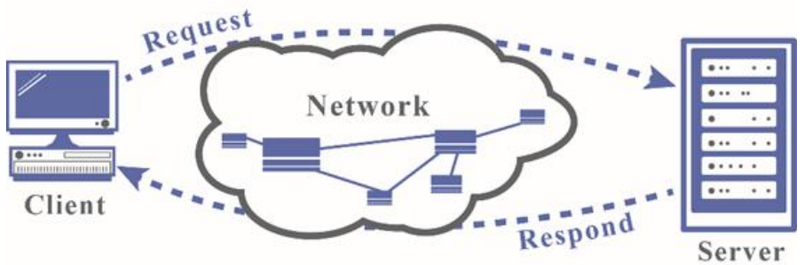
A Peer-to-Peer (P2P) network

Network Components and Terminology (cont.)

- What is a **server**? The term refers to a piece of hardware or software used to provide resources for other computers or devices, called "clients".
- In networking, a **"node"** refers to any addressable device, redistribution point, connection point, or communication endpoint that is connected to a network.
- A **"client"** is a computing device that can utilize and share network resources.
- A computing device on a TCP/IP network that handles network and node requests for applications, and offers resources and services is called a **"host".**



A network with two Clients and a Server



The client server communication

Network Components and Terminology (cont.)

- The purpose of networking is back and forth communication.
- A network allows computing devices to **exchange packets of data safely and securely**.
- **Network software refers** to the application program that runs the network, helping administrators deploy, manage and/or monitor it.
  - Network architecture signifies the way network devices and services are configured and structured.

Network Components and Terminology (cont.)

- **Access Point (AP) or Wireless Access Point (WAP)** is a networking device that contains a radio transmitter and a receiver signal, enabling other computing devices to connect to the network and communicate with each other.
  - An access point can connect routers, switches and hubs via Ethernet cables or Wi-Fi signals.
  - This small, wired connection allows the wireless network to broadcast in a designated area. Access Points operate at Layer 2-Data Link of the OSI model.
- **Address Resolution Protocol (ARP)** is a network protocol that finds the Media access control addresses (MAC) address of a device from an IP address.

Network Components and Terminology (cont.)

- **A Bridge** is a network device that connects two or more networks or segments.
  - The bridge is responsible for regulating incoming traffic by inspecting it and deciding whether to forward it or to filter it (block it), thereby reducing unnecessary traffic.
- **Data packets** are units of data sent over a TCP/IP network, with the goal of transmitting data efficiently and reliably.
  - When we send something over the Internet, the data is divided into small pieces (using specific size in bytes) to ensure each part is transmitted successfully and to accommodate various bandwidths.
  - By breaking the data into parts, the data packets can evade network congestion caused by simultaneous transfers and can be rerouted via less congested paths.

Network Components and Terminology (cont.)

- For example, in **Internet Protocol version 6 (IPv6),** the first section of each data packet is the IPv6 header. The main components of an IPv6 header are the following.
  - **Version**- indicates the version of the IP. The header size is 4 bits
  - **Traffic class**-designates the class or priority settings of IPv6 packet. Its size is 8 bits.
    - **Flow Label**-specifies that packet belong to a specific sequence. Examples include real-time data such as voice and video. The size is 20 bits.
    - **Payload length**-defines the length of the IPv6 payload in octets. An octet is a unit measuring digital information and consists of 8 bits. The size is 16 bits.

Network Components and Terminology (cont.)

- **Next header**-indicates the type of the first extension header or the Protocol Data Unit (PDU). This could be TCP, User Datagram Protocol (UDP), or others. The size is 8 bits.

- **Hop Limit**-designates the maximum number of links that the IPv6 packet can travel before the packet is released. The size is 8 bits.

- **Source Address**- the originating IPv6 host address. The size is 128 bits.

- **Destination of IPv6 address**- stores the destination host. The size is 128 bits

Network Components and Terminology (cont.)

- The **payload** delivers the actual data to its destination, and the trailer encompasses information about the destination of the packet.
- **Dynamic Host Configuration Protocol (DHCP)** is the client or server that is responsible for assigning a dynamic IP addresses to client computers and other related configuration information.
- **Domain Name System (DNS)** is a directory of the IP addresses of the entire Internet.
  - The DNS translates domain names, which people can remember, or maps host names into IP addresses.

Network Components and Terminology (cont.)

- **DNS** has anti-spam defenses, including routing security like the Resource Public Key Infrastructure (RPKI) that safeguards the Internet's routing infrastructure and firewalls.

- The **DNS** can contain an open standard called the Sender Policy Framework (SPF), an email authentication method that is used to prevent spam messages sent on behalf of the user's domain.

  - This standard helps identify the mail servers that are authorized by the domain owner to send email. SPF defines the correct IP addresses the user can send emails from.

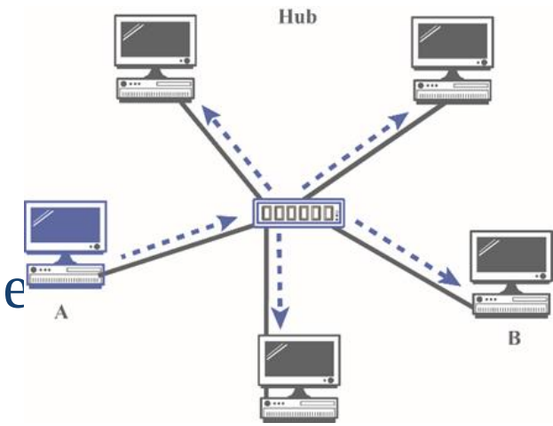
  - More specifically, SPF looks at the domain of the Return-path value (in the email's headers) for a proper SPF value.

Network Components and Terminology (cont.)

- Another standard created for the same purpose as SPF is the Domain Keys Identified Mail (DKIM).
- It also prevents cybercriminals from identifying the user as an email sender. DKIM can be added to the DNS server and provides validation for the domain name identity of the e-mail sender through cryptographic authentication. Yes, it's really me! sending this message!
- The DNS is essential because it protects users and businesses from phishing attacks.

Network Components and Terminology (cont.)

- **Gateway or Protocol Converters** are network devices (nodes) that can be employed as software, hardware, or a combination of both to connect two dissimilar networks.
  - The gateway is an entry or exit point between networks. The gateway takes data from one network, interprets it, and transfers it to another network.
  - Gateways are usually complex, and since they are found at the edges of a network, they are integrated into routers, firewalls, servers, or other devices that enable traffic to flow in and out of the network.
  - Without gateways we would not be able to communicate with devices, nodes or networks outside of our own network.
- A **Hub** connects computing devices and serves as a connection point within a private network or local area network (LAN) by broadcasting packets of data to other connected computing devices.



A hub broadcasts data to all connected hosts.

Network Components and Terminology (cont.)

- The data packets will stay within the local network, the hub does not perform filtering or routing.
- Hubs operate at Layer 1-Physical layer of the OSI model.

- A **Bandwidth** is defined as the maximum rate of data transmitted across a network path per unit of time and measured in bits per second

Network Components and Terminology (cont.)

- **Internet Protocol address (IP address)** is a unique identifier assigned to every single computing device on a TCP/IP network.
  - The IP address has two primary functions: it identifies the host's or network interface identification and location addressing.
  - When a computing device sends data to another device, the data headers contains information about the sending device's IP address along with the destination device's IP address.
  - The IP address is like a physical home address for the computer that determines where the mail should be delivered. In 1982, when TCP/IP became the official protocol for ARPANET, IP addresses first emerged.
  - The first version of modern TCP was written in 1973 by Cerf and Kahn.
  - The first and second Internet Protocols, IPv1and IPv2, were never defined; IPv3 and IPv5 were experimental. Internet Protocol 4, IPv4, was the first version that was used publicly and carried a theoretical limit of 4.3 billion (232) addresses.

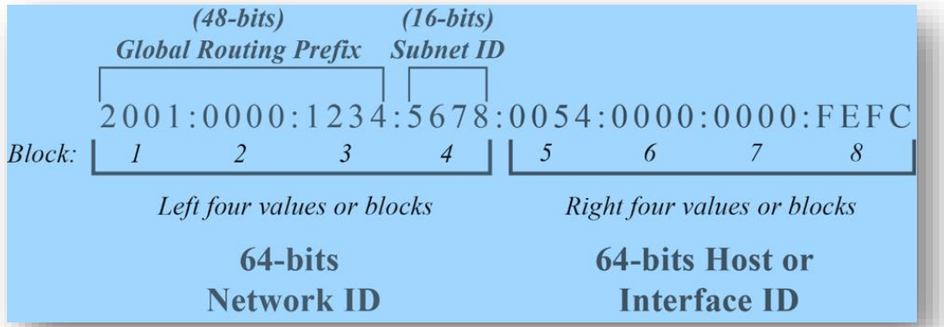
Network Components and Terminology (cont.)

- The organization that is responsible for allocating and maintaining global IP addresses is the **Internet Assigned Numbers Authority (IANA).**
  - IANA has been a division of the Internet Corporation for Assigned Names and Numbers (ICANN) since 1998 and is responsible for maintaining the Central Internet Address pools and the DNS root zone.
  - **IANA** assigns IP address blocks to five international Regional Internet Registries (RIR).
  - Globally, these five regions create smaller address blocks available to the respective Local Internet Registries (LIR) and the National Internet Registries (NIR).
  - The ISPs assign IP addresses to the users. At present, IANA is issuing two types of IP addresses, IP version 4 (IPv4) and IP version 6 (IPv6).

Registry	Area
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Network Components and Terminology (cont.)

- **IPv4,** first deployed in 1983, uses a 32-bit address and can handle 4,294,967,296 (232) unique addresses. It is still the most widely used IP version.
  - Because IPv4 is currently running out of addresses, ISPs are switching to IPv6. At the present time, IPv4 coexists harmoniously with the newer IPv6, which will eventually replace it, at which point IPv4 will become a legacy protocol.
  - IPv6 uses a 128-bit address, theoretically delivering 2128 unique addresses.
  - It offers about 340 trillion trillion trillion combinations, called undecillion, or sextillion or dodekillion and is equal to 1036.
  - As opposed to **IPv4,** which is written in dotted decimal notation, **IPv6** is written using hexadecimal notation.
  - An example of an IP address provided by IPv6 for the Microsoft Corporation in Redmond, Washington, United States is 2a01:111: f400:5254::2.



Network Components and Terminology (cont.)

In the IP world, there are two types of IP addresses: static and dynamic.

The static IP does not change until the device is retired. This type of IP is assigned by the Internet Service Provider (ISP) or by a network administrator.

- A **static IP** address is assigned to important external computing devices, a server (web server, email server, printer shared within the network) or websites that need to use the IP address so other devices can connect to it quickly.
- The **dynamic IP** is subject to change and is assigned by Dynamic Host Configuration Protocol (DHCP) servers.
  - Some of its advantages include better security.
  - It is harder for hackers to find the location and target networked equipment they are looking for, since the address may have changed.
  - Also, the dynamic IP is easier to set up with automatic configuration by the DHCP server.
  - The DHCP automatically assigns computing devices with unlimited IP addresses and is constantly reusing them.
  - The use of dynamic IP addresses is less expensive than static IPs.

Network Components and Terminology (cont.)

Typically, a network administrator or the ISP can assign a static IP. An IP can be classified as either a **public or a private IP address.**

- A **public IP address** can be either static or dynamic and is accessible to everyone on the Internet. It is unique for each device and is provided by ISPs as soon as the computing device is connected to the Internet gateway.
    - When the ISP assigns an IP address to a gateway, the gateway permits multiple devices to access the Internet through a single public IP address through a process called **Network Address Translation (NAT).**
        - The **NAT** limits the number of public IPs that an organization must use by translating a public IP to private IP for security and cost-effective purposes.
        - From a security perspective, **NAT** enhances security by hiding the internal network from the outside world.
        - **NAT** is a process in which one or multiple private IPs are translated (mapped) into one or multiple public or global IP addresses and vice versa.
- A **private IP address** is used locally only, for example in a Local Area Network (LAN) and is never routed outside of the network.

Network Components and Terminology (cont.)

- **Protocols** are a set of specifications and procedures used by systems to communicate with each another.
  - Important protocols are the Transmission Control Protocol (TCP) and Hypertext Transfer Protocol Secure (HTTPS).
- A **port** is a number used to identify a communication endpoint on a network.
  - Ports are virtual places within an OS where network connections start and end.
  - They help computing devices sort the network traffic they receive.

Port #	Protocol Name	Purpose
67 & 68	DHCP-Dynamic Host Configuration Protocol	Automatically assigns dynamic configuration of IP addresses to clients (client/server protocol).
53	DNS-Domain Name System	A standard protocol that translates host names into IP addresses. This naming scheme governs how computers exchange data on the internet.
20 & 21	FTP-File Transfer Protocol	A network protocol used for the transfer of files between a client and a server on a network.
80	HTTP-Hyper Text Transfer Protocol	An application protocol for displaying and distributing web pages. Its main goal is to send data between the web browser and a website.
443	HTTPS-Hyper Text Transfer Protocol Secure	An encrypted version of HTTP protocol with SSL/TLS used in communication. The main goal is to increase security of data transfer. This secure protocol ensures: Authenticity-being on the real website, Confidentiality- the connection is encrypted, Integrity-ensures that data has not been tampered or modified between client (visitor) and server (website).
1	ICMP-Internet Control Message Protocol	This protocol is for error testing, reporting and querying for connectivity issues.
119	NNTP-Network News Transfer Protocol	An application protocol for distributing, inquiring, retrieving, posting and transferring newsgroup articles (USENET) from both client/server and server/server.
110	POP3-Post Office Protocol version 3	Protocol for retrieving e-mail from a server.
22	SFTP-Secure File Transfer Protocol	Secure file transfer
25	SMTP-Simple Mail Transfer Protocol	E-mail is sent using this protocol.
22	SSH-Secure Shell	A protocol for secure remote access to a remote computer or a server. A secure (encrypted) method for file transferring. Is intended to execute commands like log-in remotely.
443	SSL-Secure Socket Layer	Like the TLC, creates an encrypted HTTPS connection between two computers over the Internet. Intended for data transmission.
23	Telnet	This client-server protocol for remote access or login via text-based inputs and outputs (command-line utility). This is an insecure connection.
443	TLC-Transport Layer Security protocol	An encryption protocol that provides confidentiality and integrity between two computers over the Internet.

Network Components and Terminology (cont.)

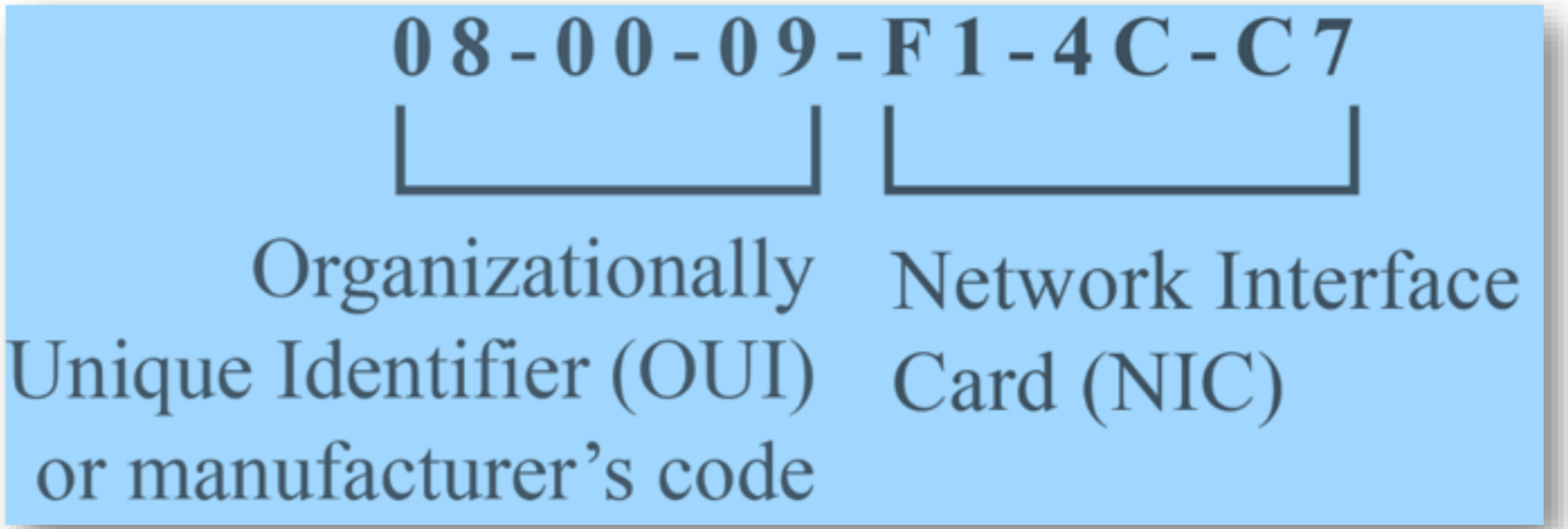
- **Media Access Control Address (MAC address)** or Physical Address is a unique, 48-bit, identification number allocated to every computing device's network interface card (NIC) by the manufacturer.
  - The MAC address does not change; it is hard coded into the NIC or stored in Read Only Memory (ROM).
  - The address can be configured using manufacturer-supplied software.
  - The MAC address is used to connect the device to the network and to filter the process on wireless networks.
    - For example, since the IP address is dynamic and changes, the MAC address can be used to identify the device.
    - From a security point of view, a weakness is that the MAC address can be used to track a computing device on a Wi-Fi network.
    - One way to do this is called MAC spoofing, a method used by hackers to manipulate and change a factory-assigned MAC address and then attempt to conceal his/her identity or to bypass the MAC address control list by pretending to be an authorized user.

Network Components and Terminology (cont.)

- The hacker can deny services on a wireless network, inject packets, send frames to all the wireless users using a broadcast address and manipulate any packet field.
- Companies like Android, Linux, iOS, and Windows have implemented MAC address randomization, which allows mobile devices to rotate across random hardware addresses.
- An interesting point is that MAC spoofing attacks happen via the Address Resolution Protocol (ARP).
- An ARP allows an IP node to verify the hardware MAC addresses. More specifically, the ARP maps a network to find out the MAC address of a device from an IP address.

Network Components and Terminology (cont.)

- MAC addresses consist of 12-digit hexadecimal numbers, 48 bits, or 6 bytes. The first 3 bytes (24 bits or 224) represent the Organizationally Unique Identifier (OUI), or manufacturer's code assigned by the Institute of Electrical and Electronics Engineers (IEEE).



Network Components and Terminology (cont.)

- **Network Address Translation (NAT)** allows network devices like routers to connect private IP networks to the Internet by replacing the private IP with a public IP address.
- The NAT acts as a "receptionist or a dispatcher" between the Internet (public IPs) and local network (private IPs).
  - With this method, only a single IP address is needed to connect an entire group of local computing devices to the Internet.
- **The Network Interface Card (NIC),** also known as Network Interface Controller or Network Adapter is a piece of computer hardware that permits a computing device to connect to a network via wired or wireless connections.
  - A NIC card's address is the MAC address of the device.

Using Network Utilities

Network Utilities are software tools that analyze, diagnose, and configure many aspects of computer networking, and begin working on solutions.

Some of the most common open-source utilities include:

- Angry IP Scanner- a cross-platform network scanner.
- Cisco Packet Tracer- Network simulation, used to test network environments before implementation. It may work across different platforms
- iPerf3- network problem solving, performance measurement and tuning (Microsoft Windows, macOS, Linux).
- Netstat or Network statistics- delivers basic statistics on network activities on most operating systems.
- Nmap- network scanner and monitor for unauthorized devices and open ports (supports cross-platform).
- PuTTY- used to access and configure network devices (Microsoft Windows, macOS, Linux).
- Wireshark- collects and interprets network traffic (supported cross-platform).

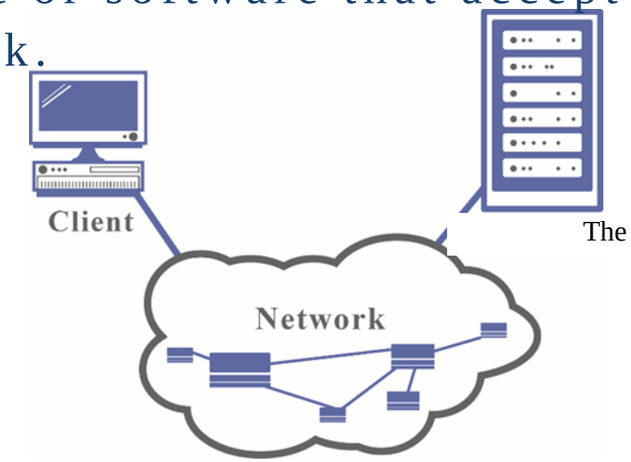
Using Network Utilities

Additionally, some of the key network utilities included with the common Operating Systems (OS) are the following:

- arp
- ipconfig
- ping
- netstat
- tracert

Network Components and Terminology (cont.)

- **Repeater** is a network device that receives and regenerates the signal over the same network.
  - A repeater does not understand frames or packets or headers and cannot perform intelligent routing but only regenerates and reproduces the signal.
  - The repeater operates at the Layer 1-Physical Layer of the OSI model.
- **Routers** are virtual or physical network devices that function as dispatchers by forwarding data packets between different IP networks.
  - A router evaluates data packets and chooses the best routes on which to send them.
- **Servers** are computer hardware or software that accept and respond to requests made by a client over a network.

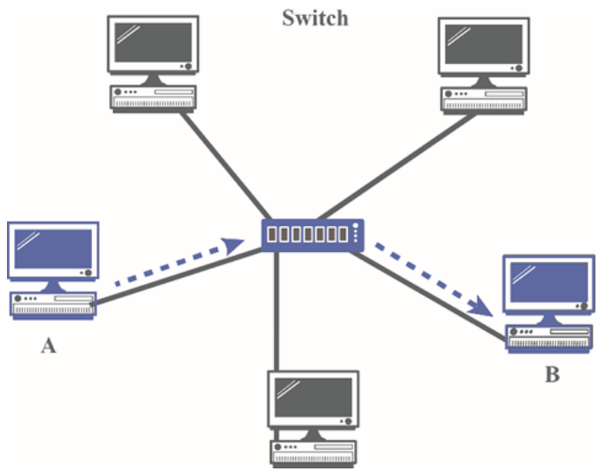


The client-server model

Network Components and Terminology (cont.)

- **Standards** are sets of rules for components and systems manufacturers that define how to communicate in different settings.
  - For example, Ethernet-based networks are defined by IEEE 802.3 standards, issued by the Institute of Electrical and Electronics Engineers (IEEE), and Bluetooth devices are defined by Bluetooth Low Energy 5.1, which is a wireless technology standard for exchanging data over short distances.

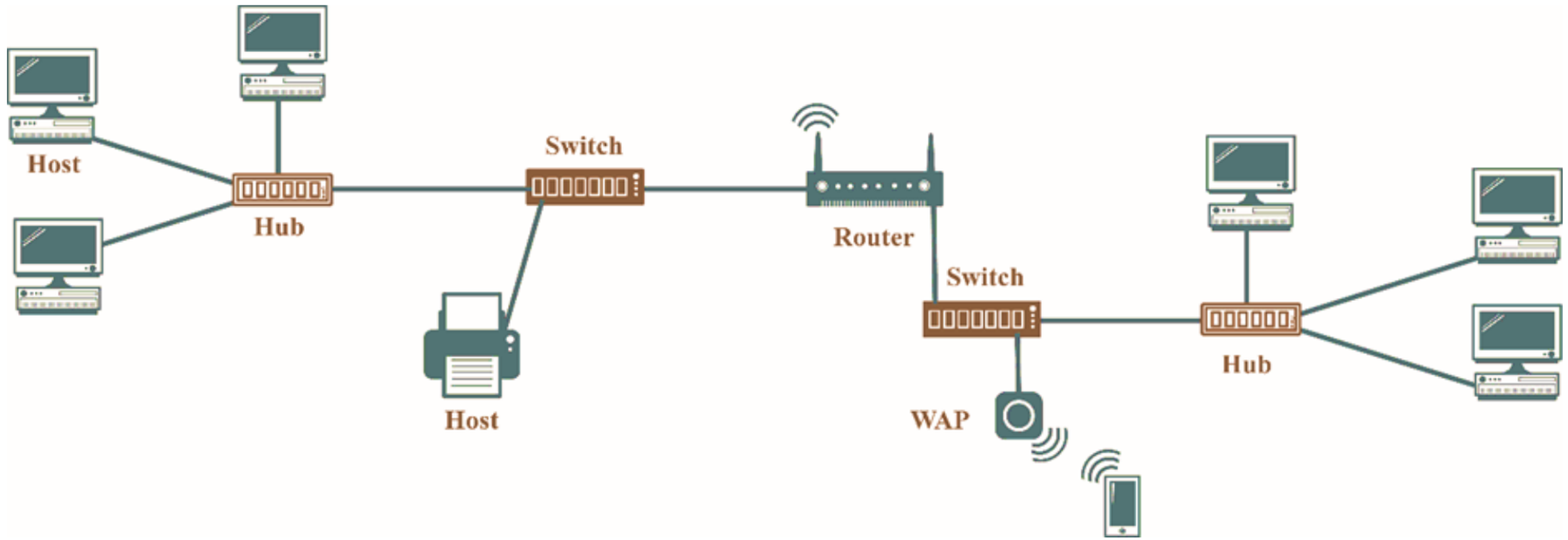
- **Switches** are multiport devices that connect computing devices in a network and act like controllers. Switches vary from hubs because they handle data packets differently, by performing error checking and by not forwarding data packets that have errors.
  - Switches improve efficiency and performance. A switch is a device in the data link layer, or layer two of the seven-layer OSI model (see OSI model) that allows devices on a network to communicate with each other as well as with other networks.



The Network Switch

Network Components and Terminology (cont.)

- **Virtualization** in computing or VM, is the technology of creating software-based or virtual services like operating systems, servers etc., by distributing capabilities and enabling a single machine to act like multiple simulated devices.
  - Virtualization is a cost-saving method. A hypervisor is the software that creates and manages virtual machines.



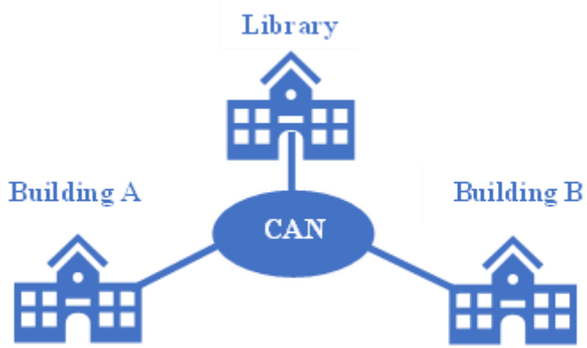
A Typical Network

Types of Networks

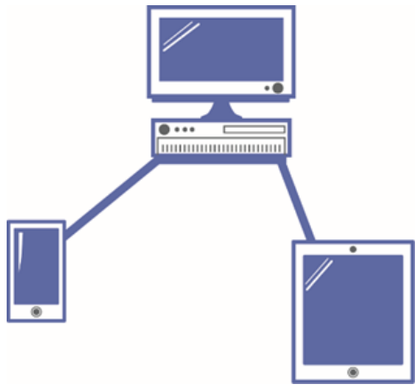
To be able to meet evolving demands and needs, different types of networks have been designed.

- **CAN (Campus Area Network)** As the name indicates, this type of network is designed for educational institutions like campuses, colleges, schools and universities.
  - A CAN network is larger than a Local Area Network (LAN) and smaller than a Wide Area Network (WAN).

- **PAN (Personal Area Network)** is a short-range network, that serves one person as the name indicates.
  - For example, using an app on a mobile device like a wrist fitness tracker, heart rate monitor or pedometer with a Bluetooth device is a PAN.
  - When a person connects any two devices such as a mobile phone and a computing device, or shares e-mails, photos, text messages and more, this also is done within a Personal Area Network.



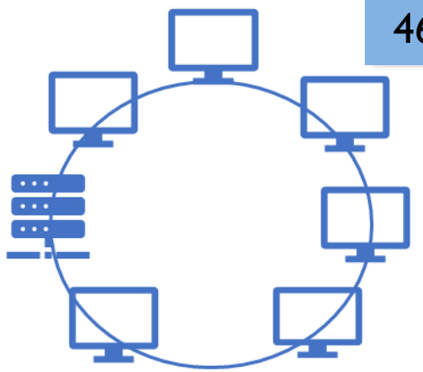
A CAN Network



A PAN Network

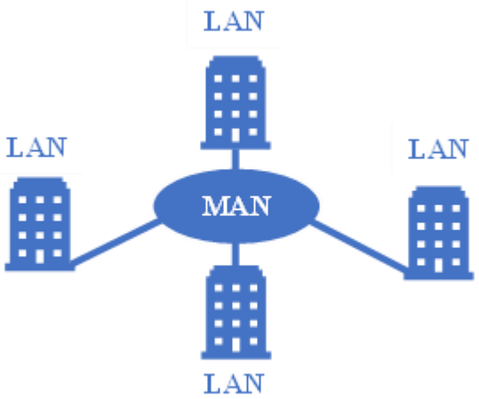
Types of Networks (cont.)

- **LAN (Local Area Network)** is a medium range network that spans an area inside a single room, building or group of buildings, office, factory or school, allowing the sharing of data, files, and resources.
  - A LAN might connect all the computers in a school or a building and could contain both wired and wireless devices.



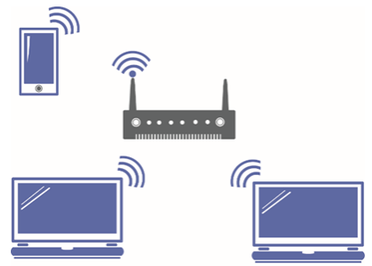
A LAN Network

- **MAN (Metropolitan Area Network)** is a long-range network that provides communications over a larger area than a LAN and a smaller area than a WAN.
  - Examples include citywide networks; governmental bodies typically own and administer MANs.



A MAN Network

- **WAN (Wide Area Network)** is the largest area communications network. It can span a large geographic area and can connect multiple networks in a country, from region to region or throughout the world.
  - The largest WAN is the Internet, connecting millions of networks around the globe. WAN connectivity can be accomplished by leased fiber lines and satellite links.



A WLAN Network

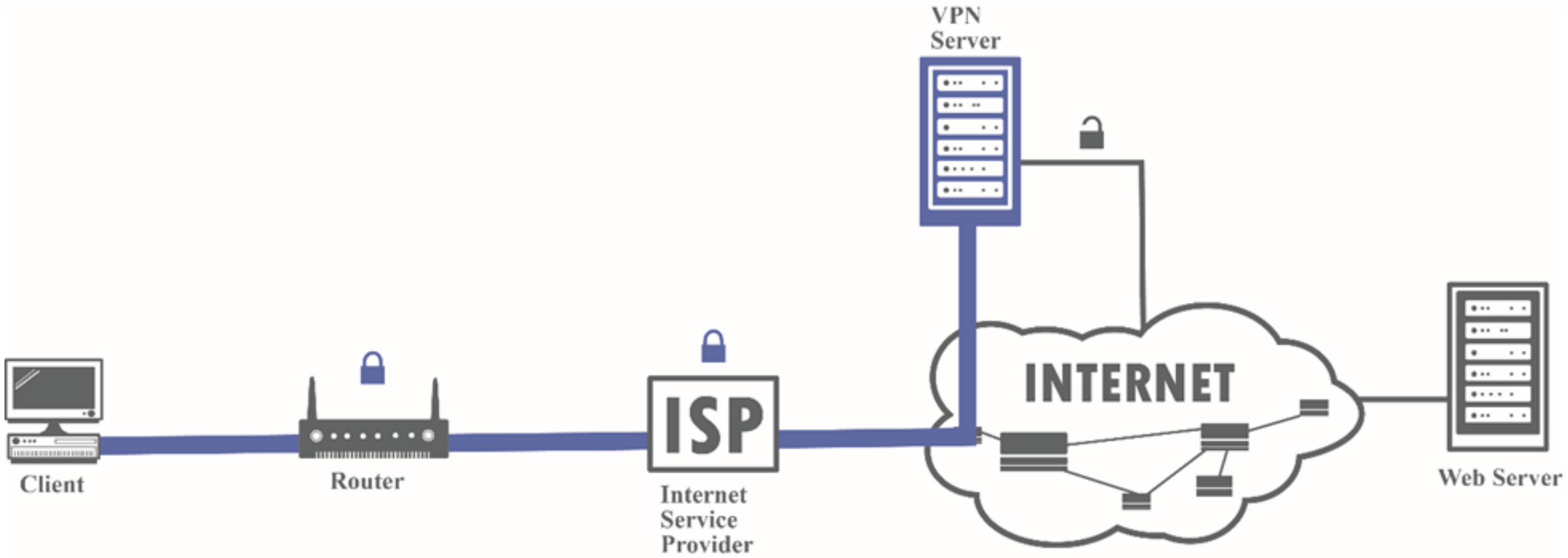
Types of Networks (cont.)

- **Virtual Local Area Network (VLAN)** is a logical instead of physical connection of different nodes in one or more LANs. Additionally, the LANS are configured to communicate as if they are physically connected.
  - For example, LAN nodes can be connected to each other with switches or repeaters and can propagate or broadcast data throughout the network.
  - Usually, when two people try to send data at the same time, a data collision may occur, and the switches or repeaters will continue to propagate on the network. After a collision, the original data must be resent once the collision is repaired.
  - VLANs help to reduce traffic passing through routers by dividing and creating segments without having to disconnect physical nodes or modify existing LANs.

Types of Networks (cont.)

- **VPN (Virtual Private Network)** is a point-to-point secure network connection for traffic in transit across the Internet.
  - A VPN establishes some privacy by encrypting a personal tunnel and encircling the user's identity.
  - It directs the user's traffic through a VPN server and masks the user's IP original address, acting as a middleman.
  - The mixture of routing to a VPN server, masking of IP address and the private tunnel encryption makes snooping more difficult for cybercriminals, the government, and ISPs.

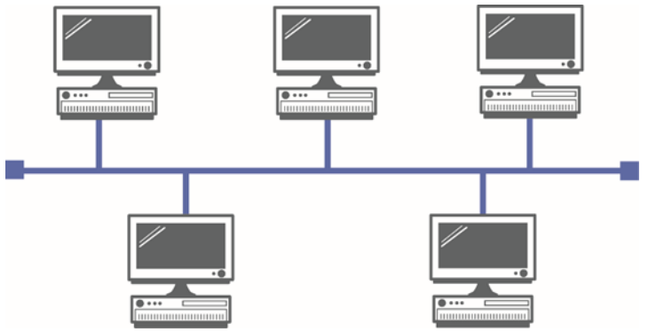
Types of Networks (cont.)



A Virtual Private Network

Network Topology

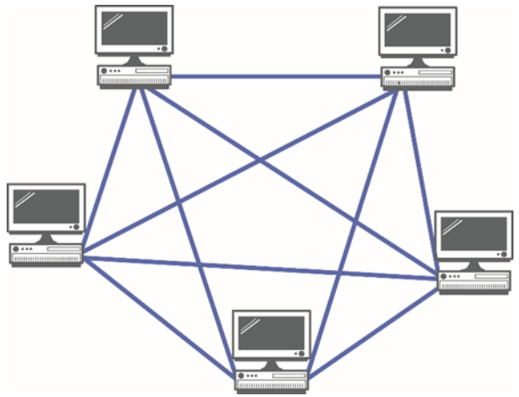
- **Network topology** shows the layout of the network and how its nodes and links are structured to forward, receive, send, and store data.
  - Network topology consists of two categories; **physical**, which contains the devices, maintenance, and wires) and **logical** which describes the way the network transmits and how data flows.
  - The correct topology improves performance by assigning resources efficiently across the network and helps in finding errors.
  - **A bus network topology** or line topology is when all network nodes and computing devices are connected to a central continuous cable in a single direction.
    - Bus network topology features a simple layout and is a cost-effective method for smaller networks.
    - This topology may be vulnerable, since the network is based on one central cable, and if the cable fails the entire network will go down.



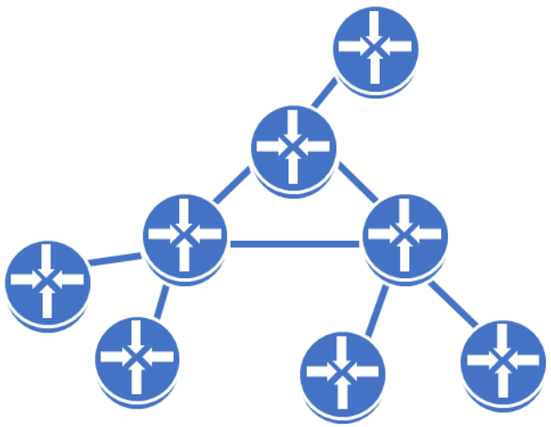
A bus network topology connects all network nodes and computing devices to a central continuous cable in a single direction

Network Topology (cont.)

- A **mesh topology** is used when network nodes and computing devices have multiple paths or have overlapped connections.
  - There are two types of mesh topology, full mesh topology, in which every node is connected to every other node in a network and partial mesh topology, where only selected nodes are connected to each other, and others are connected to only one or two devices in the network.
  - Mesh topology provides reliability and robustness, because it offers redundancy to avoid failure; one link cannot cause a break in the network or in transmission of data or affect other links.
  - Full mesh topology can be expensive, time-consuming and labor-intensive to implement.
  - Partial mesh on the other hand, offers fewer redundancies and is less expensive to implement



A full mesh topology



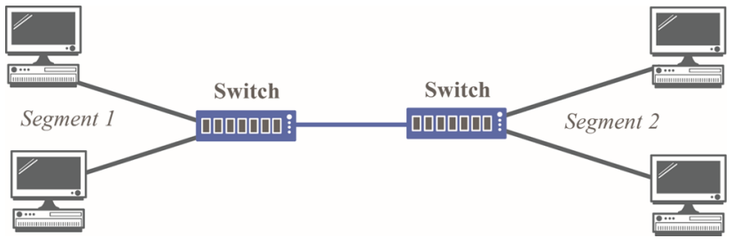
In partial mesh topology, only selected nodes are connected to each other

Network Topology (cont.)

- A **point-to-point topology** is the simplest communication connection between two nodes directly connected to each other.

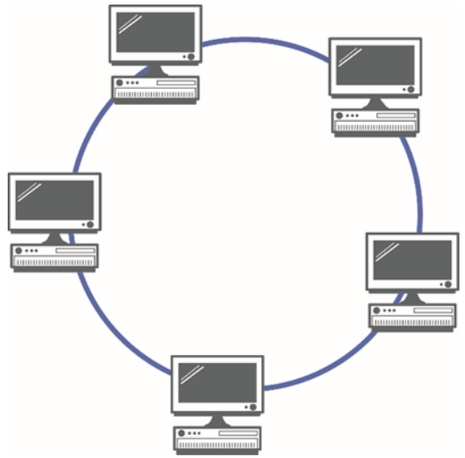
A point-to-point connection between two computers

A point-to-point connection between two routers



A point-to-point connection between two networks

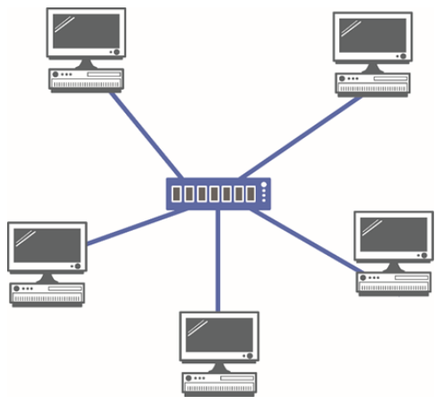
- A **ring topology** is a configuration where all network nodes and computing devices are connected in a ring or circle.
  - Data can travel either direction, and each node has only two neighbors.
  - This topology is characterized by efficiency in transmitting data without errors and without collision in the network and is easy to troubleshoot.
  - A possible disadvantage is that when we take the ring network down to reconfigure devices or troubleshoot, the entire network is offline.
  - Another disadvantage in this topology is that computer devices share bandwidth, which means there is more traffic on the network, and more delays.



A ring topology connects computing devices in a ring or a circle configuration

Network Topology (cont.)

- A **star network topology** is configured when all network nodes and computing devices are connected into a central switch that manages data transmission.
  - Data flows from any node through a central hub, which works as a repeater, preventing data loss.
  - The star is the most popular topology, providing higher data transfer speed, easy installation and management from a single location.
  - A major disadvantage is that when the central switch fails, the entire network cannot function.
  - Additional network topologies include the Hybrid and Tree topologies.



A star network topology connecting all network nodes and computing devices with a central switch

The Open Systems Interconnection (OSI) model

The Open Systems Interconnection (OSI) is a reference or conceptual model that describes the functions and specified protocols and standards of each conceptual layer, tier, or stratum, of a network communication.

- It was created in 1984, when the International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee, known in France as the Comité Consultatif International Téléphonique et Télégraphique (CCITT), merged their ideas and procedures to shape the OSI Reference Model.
- The OSI model divides the Internet into seven theoretical layers and provides a visual narrative to a particular network system.
- These 'layers' make it easier to understand the tasks of network communication, and the order in which they occur.
- The ITU Telecommunication Standardization Sector (ITU-T) provides the OSI standards as recommendations X.200 standards.

The Open Systems Interconnection (OSI) model (cont.)

The OSI model is not meant to be an exact science, but it does define the network framework and should be viewed as a guideline; often it does not match the real world exactly.

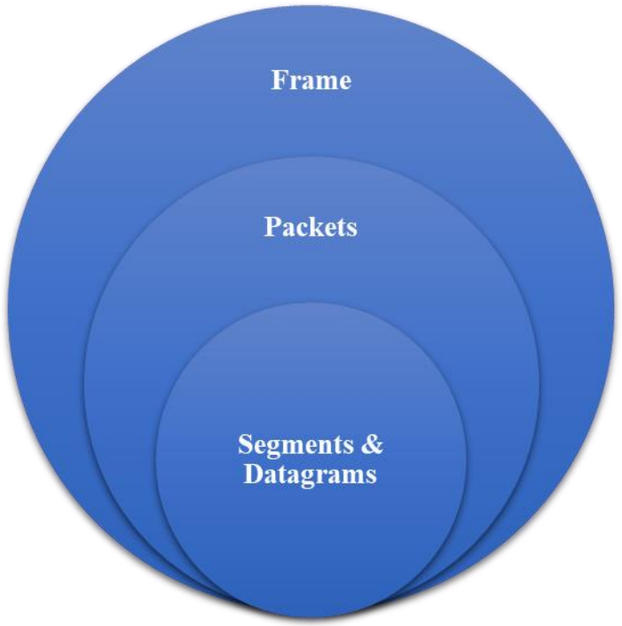
- **Layer 7 – Application** is the interface between the user and the network.
  - This layer is closest to the end user, allowing access to network services like e-mail, Directory Services, Web browsers, video conferencing applications like Zoom and Skype, file transfer and more.
  - The hands-on work of the user is done in Layer 7.
- **Layer 6 – Presentation** handles the syntax, which is the structure, format or organization of data, and semantics, the "meaning" of the data, of the information being transmitted by the network.
  - This layer specifies and handles presentation of data by translating and changing the native data representations to the transfer syntax.
  - Examples include encryption by transforming the original information to another form or ciphertext, and decryption by transforming the message to its original form or to plain text.
  - This layer also provides data compression to reduce the size of the data, and code conversion, including ASCII, Unicode, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI, DOCX, HTML, MP3, AVI and others.
  - The protocols used in this layer are Network Data Representation (NDR) and Lightweight Presentation Protocol (LPP).

The Open Systems Interconnection (OSI) model (cont.)

- **Layer 5 – Session** coordinates the mechanisms that organize and structure communication between application processes.
  - Simply put, when two machines need to talk to each other, a session is established to synchronize which machine has the right to transmit or to re-synchronize in case of an error.
  - The Session layer is involved in coordinating, setting up, managing and ending sessions between applications.
- **Layer 4 – Transport** delivers end-to-end reliable communication over the network.
  - More specifically, this layer receives data from the upper layers (5-7), at which point the data is broken into smaller pieces called segments and is passed to the Network layer.
  - The Transport layer also ensures that the segments correctly reach their destination. Examples of protocols used in Layer 4 are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

The Open Systems Interconnection (OSI) model (cont.)

- **Layer 3 – Network** is responsible for transferring and routing packets through different routers between sub-networks.
  - In this layer, the segments are further processed and form packets.
  - A segment is inside a packet and consists of control information such as the source and destination of an IP address, version of IP used, headers, trailer and data payload (size of the data, defined in octets) and more.
  - This layer is responsible for packet forwarding, including routing/switching the packets through different routers, and through error and congestion control.
  - For example, if we would like to connect to a server in Germany, the router at this layer will find the most efficient way to reach the server.
  - Examples of protocols used are IP, NAT and ICMP. Next, the packets are forward to the Data Link layer.



Segment, Packet and a Frame.

The Open Systems Interconnection (OSI) model (cont.)

- **Layer 2 – Data Link** coordinates node-to-node data transfers, detects and corrects transmitting errors, forms packets into frames, and synchronizes the frames.
  - A frame is a collection of bits. MAC addresses are part of the frames because frames use MAC addresses, rather than IP addresses.
  - The Data Link layer accepts packets from the Network layer and adds headers and trailers, making them into frames.
    - This layer sends them to the Physical layer.
    - In order to fulfil these tasks, the Physical layer is split into two sublayers.
  - The first is the upper sublayer known as the Logical Link Control (LLC) sublayer, which provides data transfer by communicating with the Network layer and is responsible for frame synchronization, flow and error control and multiplexing (transmission of multiple data simultaneously over a shared link).
  - The lower sublayer, known as the Media Access Control (MAC) sublayer, is responsible for communicating with the Physical layer.
  - The protocols used in this layer are the Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP), Address Resolution Protocol (ARP) Automatic Repeat ReQuest (ARQ), Asynchronous Transfer Mode (ATM), Integrated Services Digital Network (ISDN) and IEEE 802.3.

The Open Systems Interconnection (OSI) model (cont.)

- **Layer 1 – Physical** represents the mechanical and electrical interfaces, a setup of physical connections between devices such as ethernet cables, optical fiber or radio signals, NIC cards, procedures and functions of the network.
  - The Physical layer receives frames from the Data Link layer, converts them into a signal, and transmits them over local media.
  - The protocols used in this layer are Bluetooth, IEEE 802.3, Digital Subscriber Line (DSL), synchronous digital hierarchy (SDH), Request for Comments (RFCs), and varieties of 802.11.

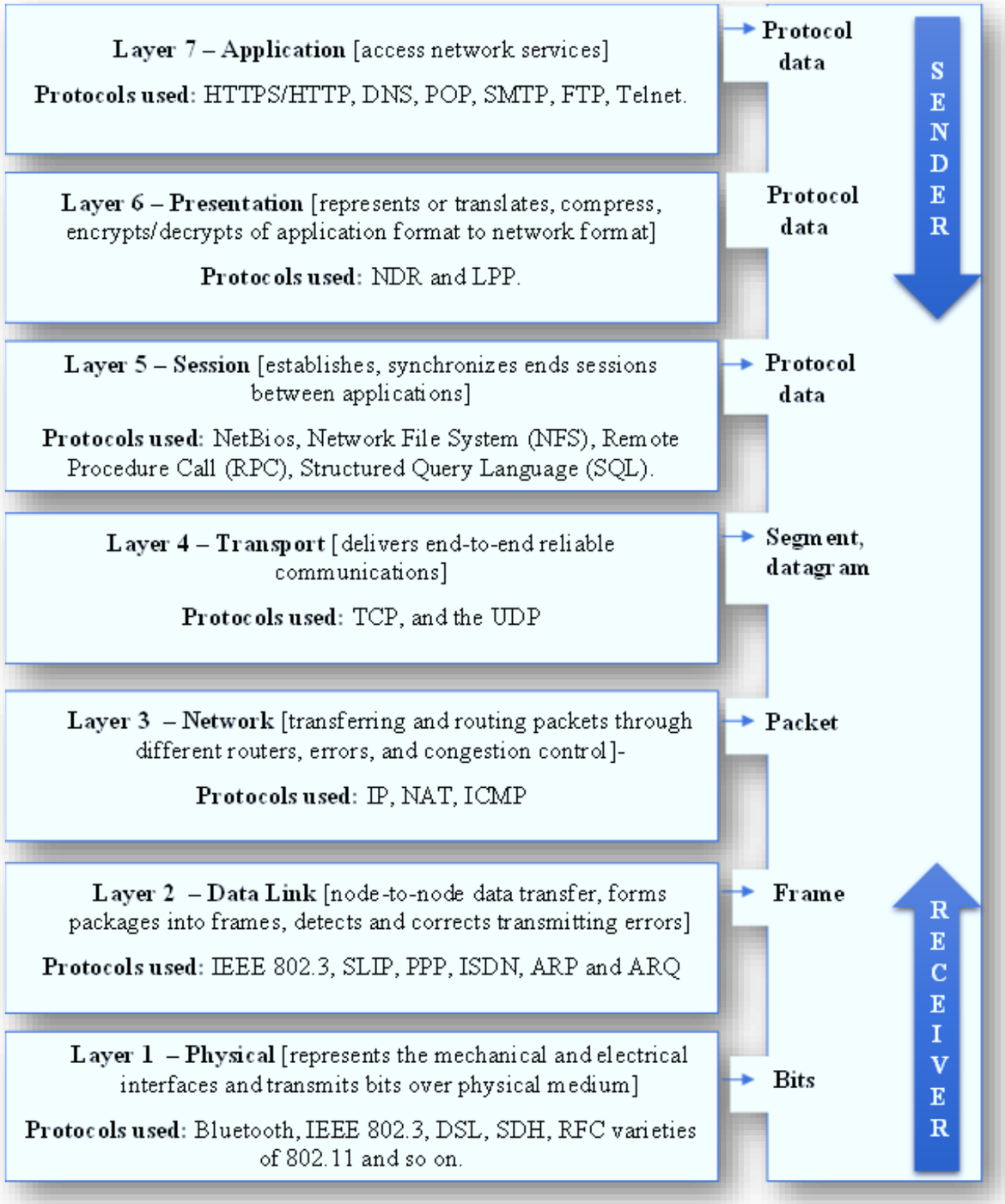
These seven layers consist of two major groups and have different level of significance.

Layers 1-4 (Physical, Data Link, Network and Transport) are the lower layers and perform the processes for data transfer around the network.

- The primary goal of the lower layers is formatting, encoding and transmission of data, using both hardware and software.

Layers 5-7 (Session, Presentation, and Application) comprise the upper layers, and signify the application component or application-level data. Their primary goal is to interact with the user interface and run applications to fulfill the user's requests.

The Open Systems Interconnection (OSI) model (cont.)



The Internet Protocol Suite (TPC/IP)

The **TCP/IP protocol suite** is a large family of protocols that is named after TCP and IP.

- TCP/IP enables the Internet to work by helping computers talk to each other from anywhere on the Internet.
- The TPC/IP model emerged from the ARPANET and was invented in 1974 by Drs. Vinton G. Cerf and Robert E. Kahn.
- In 1982, the government adopted TCP/IP as the official protocol for the ARPANET.
- The TCP/IP model contains four layers and constitutes a simplified version of the OSI model.
- The OSI and TCP/IP models are the two most widely used networking models for Internet communications.
  - TCP/IP encompasses multiple processes that are required in sending and receiving data; these processes must be sent using the same interface, the IP layer.
  - The data is then directed to the transport layer and is managed there by either TCP or UDP.

The Internet Protocol Suite (TPC/IP)

The TCP/IP is essentially a shorter version of the OSI model, consisting of four instead of seven layers. The four layers are:

I. **Application Layer** (corresponding to layers 5-7 in OSI): This layer is responsible for the user interface, allowing users to access its services.

- Examples of these services include the web browser, e-mail client and file transfer clients. Like the Application layer of the OSI model, the following are protocols are used by this layer:

  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name System (DNS)
  - File Transfer Protocol (FTP)
  - Hypertext Transfer Protocol (HTTP)
  - Multipurpose Internet Mail Extensions (MIME)
  - Post Office Protocol (POP)
  - Real Time Streaming Protocol (RTSP)
  - Secure Hypertext Transfer Protocol (SHTTP)
  - Simple Mail Transfer Protocol (SMTP)
  - Secure Shell Protocol (SSH)
  - Telnet Remote Protocol (Telnet)
  - Trivial File transfer Protocol (TFTP)
  - Transport Layer Security Protocol (TLS)
  - Universe Resource Locator (URL)

The Internet Protocol Suite (TPC/IP)

II. **Host-to-Host Layer** (layer 4 in OSI): This layer corresponds to the Transport layer of the OSI model, providing flow control, segmentation, data transmission, reliability, error control, and end-to-end data integrity. This layer uses the following protocols:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Datagram Congestion Control Protocol (DCCP)
- Stream Control Transmission Protocol (SCTP)

- The standard protocols used by the Host-to-Host layer to provide transfer data and ensure functionality between end systems are the User Datagram Protocol (UDP) and TCP.
- Both protocols move data between the Application layer and the Internet layer.
- The TCP protocol provides a reliable service and connection by ensuring that data packets are resubmitted in case of error.
- Unlike TCP, which is a connection-oriented protocol, UDP provides unreliable connectionless services.
- UDP provides fast transmission, and leaves reliability to be controlled by the Application layer.
- Both TCP and UDP divide data into packets, including IP addresses of the sender and receiver, along with several configurations, the trailer that indicates the end of the packet, and the actual application data.
- **The main difference between the two protocols is how the data packets are transported.**

The Internet Protocol Suite (TPC/IP)

TCP	UDP
Reliable protocol	Unreliable datagram protocol
Lower speed	Higher speed
Connection-oriented protocol	Connectionless
Error detection & correction	No error detection & correction
Congestion control	No congestion control
Acknowledge segments	Only via checksum
Segment retransition and flow control	No retransition and flow control

A brief summary of key-characteristics of TCP and UDP protocols

The Internet Protocol Suite (TPC/IP)

TCP

- The Transmission Control Protocol (TCP) is a reliable host-to-host, connection-based protocol.

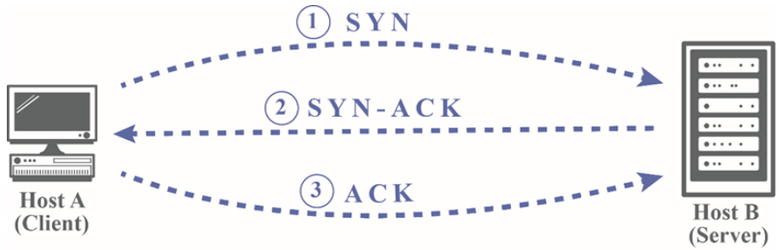
- Connection-based protocol means that before any data can be transmitted, a reliable connection between hosts must be achieved and acknowledged.

  - Its speed is slower than UDP, but it is more reliable, with fewer errors occurring.

  - TCP, unlike UDP, requires the recipient and the sender to communicate and establish a connection acknowledging that packets have been received. If packets are not acknowledged by the recipient, they are sent again.

  - If the message has not been received the TCP sends it again. Only when the connection is established can the user's data be sent from either direction. This connection is called a 'handshake'.

  - TCP uses a **three-way handshake**. **SYN for Synchronize**, **SYN-ACK**, for Synchronize Acknowledgement and ACL for **Acknowledgement**, respectively.



TCP uses a three-way handshake.

The Internet Protocol Suite (TPC/IP)

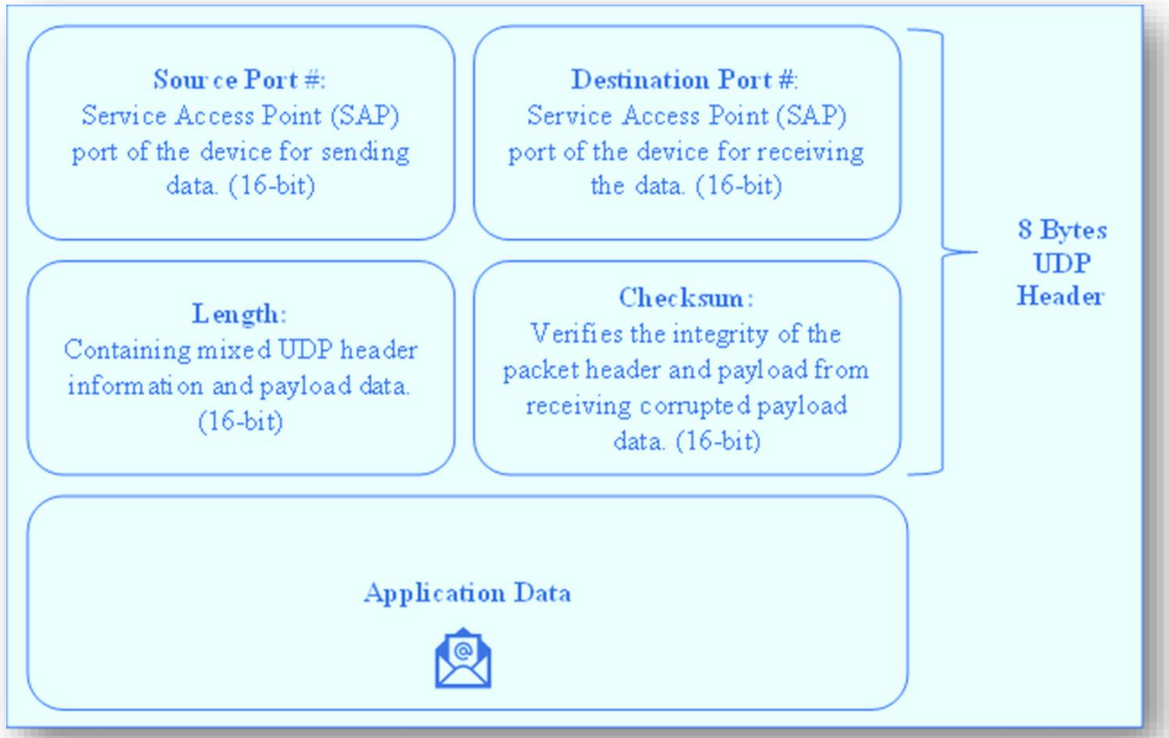
UDP

- The **User Datagram Protocol (UDP)** is a faster communication protocol than TCP but it is unreliable. UDP is a transport layer protocol defined by RFC 768.
  - Like TCP, this protocol divides data into datagrams or packets.
  - The term datagram is a basic transfer unit associated with a packet-switched network and provides a connectionless communication.
  - Datagrams are synonymous with the packets used by UDP. However, a datagram's arrival and its content are not guaranteed by UDP.
  - Both protocols are built on top of the Internet Protocol (IP), and both send data across the internet from one IP address to another.

The Internet Protocol Suite (TPC/IP)

UDP

- In summary, UDP does not offer reliable delivery and extra security overhead, offering no acknowledgement that packets have been received.
- With UDP, when one computing device sends packets of data to another, delivery cannot be guaranteed, a kind of 'send it and forget it' technique.
- UDP is faster than TCP because it eliminates functions like error checking and recovery services.
- UDP chooses speed over integrity, and data received may not exactly match data sent.
- UDP is faster and TCP is more reliable. UDP is used for streaming games, live broadcasts, and video.



The User Datagram Protocol (RFC 768)

The Internet Protocol Suite (TPC/IP)

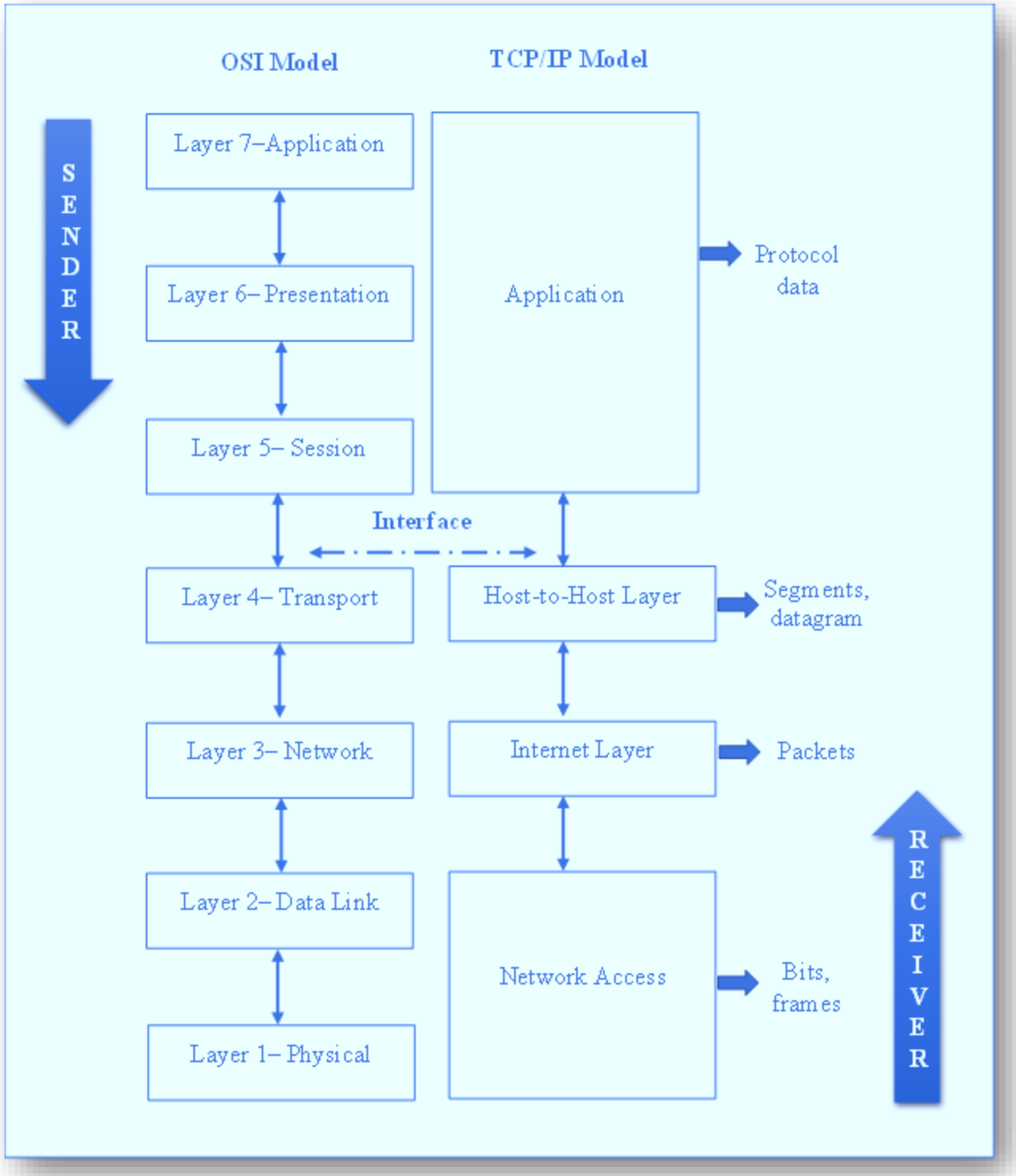
III. Internet Layer: This layer provides the same services as OSIs Network layer.

- The layer routes packets, or datagrams, from a source to a destination host and defines addressing of the host by identifying on which network the device resides.
- The IP uses the TCP/IP transmission method.
- The main task of this layer is to send packets, regardless of the route they use to arrive at the destination.

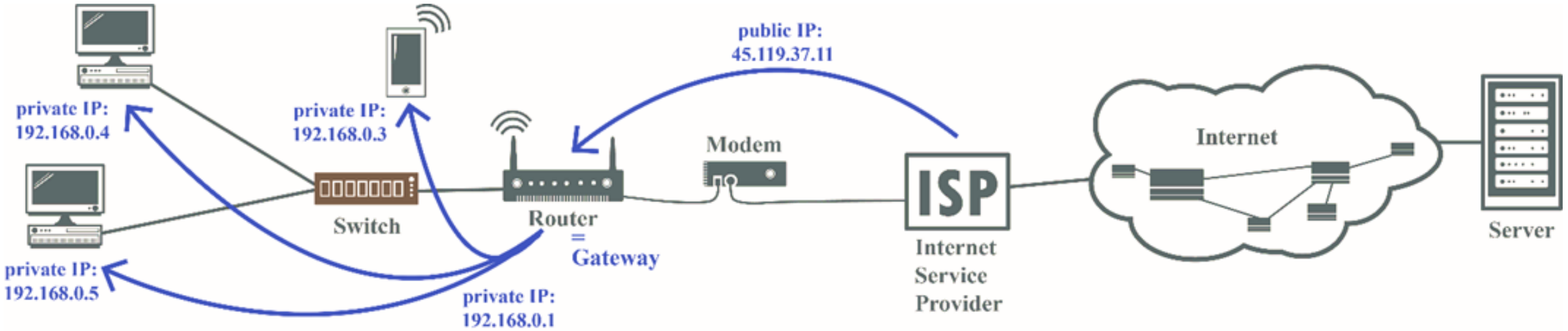
IV. Network Access or Network Interface (Layers 1-2): This layer is responsible for physical connections to the network, providing a blend of the OSI model's Data link and Physical layers.

- The Network layer includes Ethernet and optical, or wireless, radio wave technology, such as cellular and Wi-Fi standards that work along with the NIC card on a computer device.
- This allows the computer to access the network infrastructure and send data to other devices.
- The main responsibility for this layer is to transmit information over the same network between devices. The following protocols are used in this layer.

The Internet Protocol Suite (TPC/IP)



How everything works together on the Internet: a Review



A typical LAN Network connected to the Internet

Any Questions?