RELEASE NOTES

Table of Contents

In House Release Notes Authors > 9.5 > Raja > TMHP

Fundamentals of Networking

This document provides a comprehensive introduction to computer networking, covering foundational concepts, components, and best practices. It begins by defining networking as the interconnection of computing devices to share data and resources and emphasizes the role of communication protocols in this process.

This guide covers the following sections:

- *Key components: IP addresses, routers, switches, gateways*

- *Network types: LAN, WAN, MAN, PAN; wired & wireless; VPNs*

- *Architectures & topologies: Peer-to-peer, client-server, bus, star, mesh, etc.*

- *Protocols: TCP/IP, HTTPS, SSH, SNMP; TCP/IP vs. OSI model*

- *Data flow example (email transmission)*

- *Best practices: Traffic monitoring, backups, security updates*

What is Networking?

A Computer Network is a collection of communicating computers and other IoT devices, such as printers, Fax Devices, and smartphones, to enable the transmission and exchange of information and resources. Networks are a fundamental part of day-to-day life and exist in homes, workplaces, and public areas. Networked devices rely on communications protocols, rules that describe how to transmit data across a network to share information over physical or wireless connections.

At their core, computer networks are built to facilitate data sharing, reduce costs by pooling resources, and increase productivity by streamlining communications across multiple devices.

Networking Components & Devices

Before we delve into more complex networking topics, it's essential to understand fundamental networking components, including:

- **IP address**: An IP address is a unique number assigned to every network device in an Internet Protocol (IP) network; each IP address identifies the device's host network and its location. When one device sends data to another, the data includes a "header" that includes the IP addresses of both the sending and receiving devices.
- **Nodes**: A node is a network connection point that can receive, send, create, or store data. It's essentially any network device, such as computers, printers, modems, bridges, or switches, that can recognize, process, and transmit information to another network node.
- **Routers**: A router is a physical or virtual device that sends data "packets" between networks. It analyzes the data within packets to determine the best transmission path and uses sophisticated routing algorithms to forward data packets until they reach their destination node.

- **Switches**: A switch connects network devices and manages node-to-node communication across a network, ensuring that data packets reach their intended destination.
- **Ports**: A port indicates a specific connection between network devices, with each port identified by a number. Computers use port numbers to determine which application, service, or process should receive which messages.
- **Gateways**: Gateways are hardware devices that facilitate communication between two different networks.
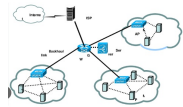

Network Devices
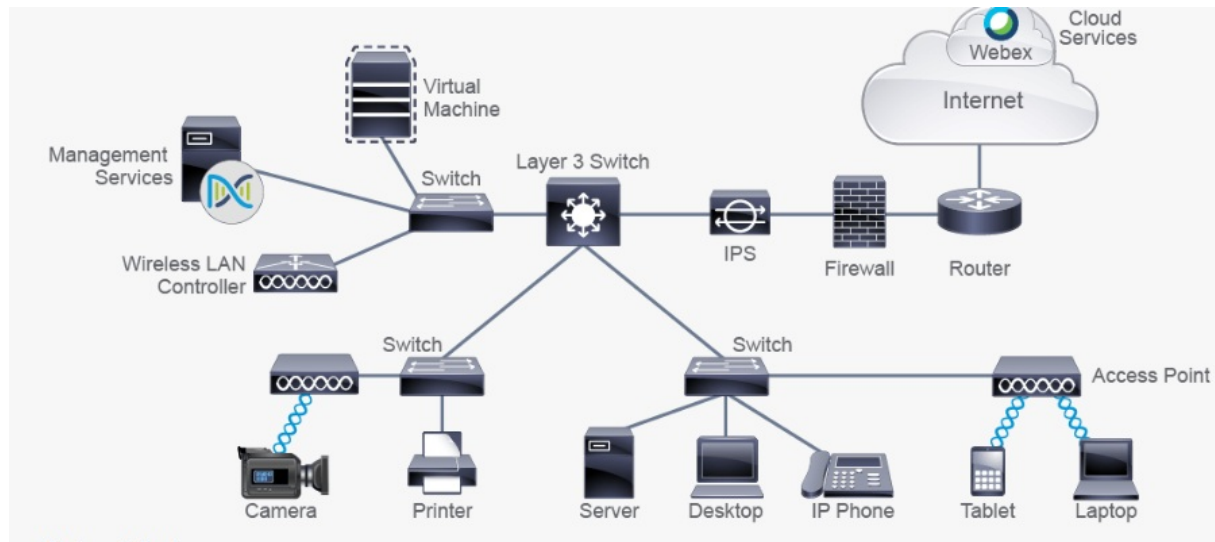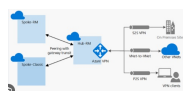
Types of Computer Networks

Typically, computer networks are defined by geographical area. A local area network (LAN) connects computers in a defined physical space, while a vast area network (WAN) can connect computers across continents. However, networks are also determined by the protocols they use to communicate, the physical arrangement of their components, how they manage network traffic, and the purpose they serve in their respective environments.

Here, we'll discuss the most common and widely used computer network types in three broad categories.

Category	Network Types	Description	Illustration
Based on Geographical Area	Local Area Network (LAN)	A LAN connects computers over a relatively short distance, such as in an office building, school or hospital. LANs are typically privately owned and managed.	
	Wide Area Network (WAN)	A WAN connects computers across large geographical areas, such as regions and continents. For network management purposes, WANs often have collective or distributed ownership models. Cloud networks are one example since they're hosted and delivered by public and private cloud infrastructures worldwide.	
	Metropolitan Area Network (MAN)	MANs are larger than LANs but smaller than WANs. Cities and government entities typically own and manage MANs.	
	Personal Area Network (PAN)	A PAN serves one person. If a user has multiple devices from the same manufacturer (an iPhone and a MacBook, for instance), they've likely set up a PAN that shares and syncs content, text messages, emails, photos, and more across devices.	
Based On Transmission Medium	Wired Networks	Wired network devices are connected by physical wires and cables, including copper wires and Ethernet, twisted pair, coaxial or fiber optic cables. Network size and speed requirements typically dictate the choice of cable, the arrangement of network elements, and the physical distance between devices.	

|			
	Wireless Networks	Wireless networks forgo cables for infrared, radio, or electromagnetic wave transmission across wireless devices with built-in antennae and sensors.	
Based on the Communication Type	**Multipoint networks**	In a multipoint network, multiple devices share channel capacity and network links.	
	Point-to-point networks	Network devices establish a direct node-to-node link to transmit data.	
	Broadcast networks	On broadcast networks, several interested "parties" (devices) can receive one-way transmissions from a single sending device. Television stations are a great example of broadcast networks.	
	Virtual private networks (VPNs)	A VPN is a secure, point-to-point connection between two network endpoints. It establishes an encrypted channel that keeps a user's identity and access credentials and any data transferred inaccessible to hackers.	

Network Architectures

Computer network architecture establishes the theoretical framework of a computer network, including design principles and communications protocols.

Primary types of network architectures include,

Peer-to-peer (P2P) architectures: In a P2P architecture, two or more computers are connected as "peers," meaning they have equal power and privileges on the network. A P2P network doesn't require a central server for coordination. Instead, each computer on the network acts as a client (a computer that needs to access a service) and a server (a computer that provides services to clients). Every peer on the network makes some of its resources available to other network devices, sharing storage, memory, bandwidth, and processing power across the network.

Client-server architectures: In a client-server network, a central server (or group of servers) manages resources and delivers services to client devices on the network; clients in this architecture don't share their resources and only interact through the server. Client-server architectures are often called tiered architectures because of their multiple layers.
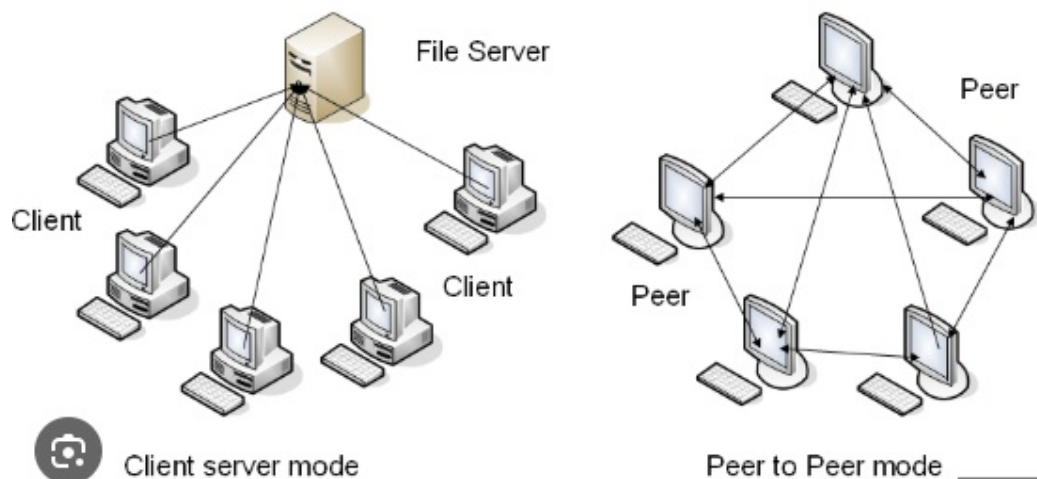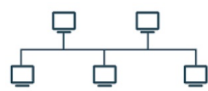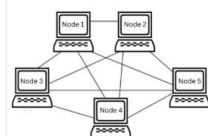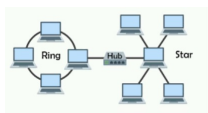
Hybrid architectures: Hybrid architectures incorporate elements of both the P2P and client-server models.

Network Topology

Whereas architecture represents the theoretical framework of a network, topology is the practical implementation of the architectural framework. Network topology describes the physical and logical arrangement of nodes and links on a network, including all hardware (routers, switches, cables), software (apps and operating systems), and transmission media (wired or wireless connections).

Some common Network Topologies are tabulated below,

Topology Type	Description	Illustration
Bus	In bus topology, all devices are connected to a single central cable called a bus. Data is sent along this cable, and all devices share the same connection.	
Star	In star topology all devices are connected to a central node called hub or switch. The hub controls the flow of data between devices. If one device fails the rest of the network is unaffected. But, if the central hub fails the whole network stops working.	
Ring	In ring topology, devices are connected in a circular loop, each connected to two others. Data travels in one direction (or sometimes both), passing through each device until it reaches its destination. A failure in one device can affect the whole network.	
Mesh	In mesh topology every device is connected to every other device in the network. It provides multiple paths for data so if one path fails another can take over.	
Hybrid	A hybrid topology combines two or more different topologies (like star and mesh). It is flexible and can be customized based on the network's specific needs.	

Networking Protocols

Whether it's the Internet protocol (IP) suite, Ethernet, wireless LAN (WLAN), or cellular communication standards, all computer networks follow communication protocols and sets of rules that every node on the network must follow to share and receive data. The network protocol is an essential building block in the design of an organization's network architecture. There are several network protocols available, each with many properties that govern its use and implementation.

Protocol Categories

Several types of applications and hardware devices depend on specific network protocols on a typical network. For example, browsing the internet by using a web browser relies on a different protocol than sending or receiving an email. Converting the data that you see in the browser and sending this information over the network requires another protocol.

Protocols fall into three categories:

- Network communication protocols
- Network security protocols
- Network management protocols

Let's look at some of the protocols in these categories below.

Category	Protocol	Description
Network Communication Protocols	Transmission Control Protocol (TCP)	TCP divides data into data packets that can be sent securely and quickly while minimizing the chance of data loss. It provides a stable and reliable mechanism for delivering data packets across an IP-based network.
	Internet Protocol (IP)	IP is responsible for addressing a data packet. It encapsulates the data packet to be delivered and adds an address header.
	User Datagram Protocol (UDP)	UDP is a connectionless protocol that offers a low-latency and loss-tolerant implementation. UDP is used with processes that don't need to verify that the recipient device received a datagram.
	Simple Mail Transfer Protocol (SMTP)	SMTP is another of the three email protocols. It is most commonly used to send emails from an email client to an email server.
	Secure Socket Layer (SSL)	SSL is a standard encryption and security protocol. It provides a secure and encrypted connection between your computer and the target server or device that you accessed over the internet.
	Transport Layer Security (TLS)	TLS is the successor to SSL and provides a more robust security encryption protocol. Based on the Internet Engineering Task Force (IETF) standard, it helps stop message forgery, tampering, and eavesdropping and is typically used to protect web browser communications, email, VoIP, and instant messaging.

Network Security Protocol	**Hypertext Transfer Protocol Secure (HTTPS)**	HTTPS provides a more secure version of the standard HTTP protocol by using the TLS or SSL encryption standard. This combination of protocols ensures that all data transmitted between the server and the web browser is encrypted and secure from eavesdropping or data packet sniffing.
	Secure Shell (SSH)	SSH is a cryptographic network security protocol that provides a secure data connection across a network. SSH is designed to support command-line execution of instructions, which includes remote authentication to servers
	Kerberos	This validation protocol provides a robust authentication for client-server-based applications through secret-key cryptography. It constantly enforces strong encryption for all communications and data.
Network Management Protocols	**Simple Network Management Protocol (SNMP)**	SNMP is an internet protocol that allows for the collection of data from devices on your network and the management of those devices. The device has to support SNMP to gather information. Devices that support SNMP typically include switches, routers, servers, laptops, desktops, and printers.
	Internet Control Message Protocol (ICMP)	ICMP is a protocol included within the Internet Protocol suite (IPS). It allows network-connected devices to send warning and error messages, along with operation information about the success or failure of a connection request or if a service is unavailable.

Many modern networks run on TCP/IP models, which include four network layers.

- **Network access layer:** Also called the data link layer or the physical layer, the network access layer of a TCP/IP network includes the network infrastructure (hardware and software components) necessary for interfacing with the network medium. It handles physical data transmission using Ethernet and protocols such as the address resolution protocol (ARP) between devices on the same network.

- **The Internet layer** is responsible for logical addressing, routing, and packet forwarding. It primarily relies on the IP protocol and the Internet Control Message Protocol (ICMP), which manage packet addressing and routing across different networks.
- **Transport layer:** The TCP/IP transport layer enables data transfer between the upper and lower layers of the network. Using TCP and UDP protocols, it also provides mechanisms for error checking and flow control.
- **Application layer:** TCP/IP's application layer uses HTTP, FTP, Post Office Protocol 3 (POP3), SMTP, domain name system (DNS), and SSH protocols to provide network services directly to applications. It also manages all the protocols that support user applications.

Though TCP/IP is more directly applicable to networking, the Open Systems Interconnection (OSI) model, sometimes called the OSI reference model, has also had a substantial impact on computer networking and computer science, writ broadly.

OSI is a conceptual model that divides network communication into seven abstract layers (instead of four), providing a theoretical underpinning that helps engineers and developers understand its intricacies. The OSI model's primary value lies in its educational utility and its role as a conceptual framework for designing new protocols that can interoperate with existing systems and technologies.

| Layer		Description
APPLICATION LAYER	7	Human-computer interaction layer, where applications can access the network services
PRESENTATION LAYER	6	Ensures that data is in a usable format and is where data encryption occurs
SESSION LAYER	5	Maintains connections and is responsible for controlling ports and sessions
TRANSPORT LAYER	4	Transmits data using transmission protocols including TCP and UDP
NETWORK LAYER	3	Decides which physical path the data will take
DATA LINK LAYER	2	Defines the format of data on the network
PHYSICAL LAYER	1	Transmits raw bit stream over the physical medium

However, the TCP/IP model's practical focus and real-world applicability have made it the backbone of modern networking. Its robust, scalable design and horizontal layering approach have driven the explosive growth of the internet, accommodating billions of devices and massive amounts of data traffic.

How Does a Computer Network Work?

Using email as an example, let's walk through an example of how data moves through a network.

If a user wants to send an email, they write it and press the "send" button. When the user presses "send," an SMTP or POP3 protocol uses the sender's wifi to direct the message from the sender node and through the network switches, where it's compressed and broken down into smaller and smaller segments (and ultimately into bits, or strings of 1s and 0s).
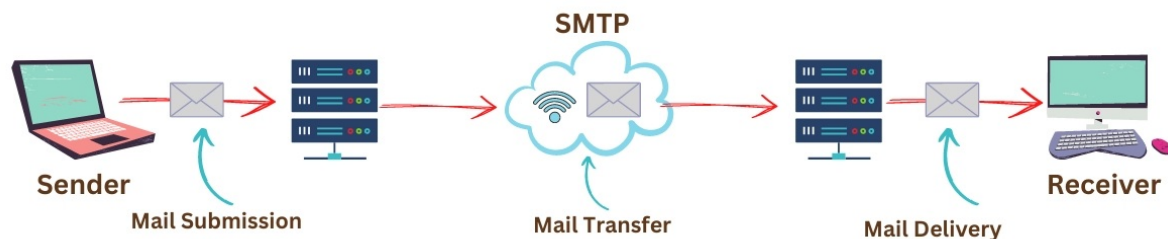
Network gateways direct the bit stream to the recipient's network, converting data and communication protocols as needed. When the bit stream reaches the recipient's computer, the same protocols direct the email data through the network switches on the receiver's network. In the process, the network reconstructs the original message until the email arrives in human-readable form in the recipient's inbox (the receiver node).

Best Practices for Network Management

Effective network management is essential for maintaining a stable, high-performing, secure network environment. It involves various strategies to optimize network health, prevent disruptions, and safeguard data. Here are some core practices:

Monitoring Network Traffic

Continuous monitoring of network traffic allows administrators to identify unusual patterns or potential bottlenecks that could indicate security threats or network inefficiencies. Advanced monitoring tools can alert administrators in real time to any spikes in traffic or irregularities, enabling quick, proactive troubleshooting before minor issues escalate into major disruptions. This monitoring is essential for ensuring smooth network performance and preventing downtime.

Regular Backups

Scheduling regular backups of network configurations and critical data is crucial for disaster recovery. In the event of a failure, cyber-attack, or data loss, these backups enable swift restoration of network settings and data, minimizing operational interruptions. Automated backup solutions ensure data and configurations are consistently saved, reducing the risk of human error and allowing for faster recovery times.

Implementing & Updating Security Protocols

Security protocols such as firewalls, encryption, and access controls must be regularly updated to counter emerging threats. By keeping these protocols current and periodically reviewing security settings, organizations can significantly reduce vulnerabilities and better protect against cyber threats. This includes using multifactor authentication (MFA) and regularly updating antivirus software to strengthen network defenses.

References

- *Basic of Computer Networking*
- *Networking Fundamentals*
- *Network Components*
- *Wireless Networking*
- *Fundamentals of Computer Networking by Microsoft*
- *OSI Network Model*