Networking Basics

NETWORK DEVICES EXPLAINED

NOTE: *To better understand descriptions and product specifications for network devices please see the definitions of terms and terminology below this section.*

Router

- Description: A router is a device that directs data packets between different networks, typically between a local area network (LAN) and the internet.
- Uses:
    - Network Interconnection: Connects different networks, such as a home or office network to the internet.
    - Routing: Determines the best path for data packets to travel from source to destination.
    - Network Address Translation (NAT): Allows multiple devices on a LAN to share a single public IP address.
    - Firewall: Often includes built-in firewall features for network security.

Wireless Router

- Description: A wireless router is a device that directs data packets between different networks, such as a local area network (LAN) and the internet and provides wireless connectivity for devices within its range.
- Uses:
    - Network Interconnection: Connects a home or office network to the internet wirelessly.
    - Routing: Determines the best path for data packets between devices and networks.
    - Wireless Access: Provides Wi-Fi access for devices such as laptops, smartphones, and tablets.
    - Network Address Translation (NAT): Allows multiple devices on a LAN to share a single public IP address.
    - Firewall: Often includes built-in firewall features to enhance network security.

Managed Switch

- Description: A managed switch provides advanced features for network management and control. It allows for configuration, monitoring, and optimization of network traffic.
- Uses:

- VLAN Support: Can create and manage Virtual Local Area Networks (VLANs) to segment network traffic.
- Traffic Management: Features like Quality of Service (QoS) to prioritize certain types of traffic.
- Network Monitoring: Provides capabilities for monitoring network performance and diagnosing issues.
- Security: Offers advanced security features such as port security and access control lists (ACLs).

Unmanaged Switch

- Description: An unmanaged switch is a basic network switch that operates without the need for configuration. It works out-of-the-box with default settings.
- Uses:
  - Simple Connectivity: Provides basic network connectivity for devices in a network.
  - Plug-and-Play: Ideal for small or home networks where advanced features are not required.
  - Cost-Effective: Generally, less expensive compared to managed switches due to the lack of management features.

Layer 2 Switch

- Description: Layer 2 switch, this device operates at the Data Link layer (Layer 2) of the OSI model. It uses MAC addresses to forward data.
- Uses:
  - Frame Switching: Forwards Ethernet frames based on MAC addresses.
  - Segmentation: Divides a network into smaller collision domains to reduce network traffic.
  - VLAN Support: Can be used to implement VLANs for network segmentation.

Layer 2 Switch Managed

- Description: A Managed Layer 2 switch operates at the Data Link layer (Layer 2) of the OSI model, using MAC addresses to forward Ethernet frames with advanced management features.
- Uses:

  - Frame Switching: Forwards Ethernet frames based on MAC addresses.
  - Network Segmentation: Creates smaller collision domains to reduce traffic.
  - VLAN Support: Implements and manages VLANs for traffic segmentation.
  - Management: Offers configuration, monitoring, and security features for network control.

Layer 3 Switch

- Description: Layer 3 switch, this device operates at the Network layer (Layer 3) of the OSI model. It can perform routing functions in addition to switching.
- Uses:
    - Routing: Supports IP routing and can perform inter-VLAN routing, forwarding packets between different VLANs.
    - Layer 2 and Layer 3 Functions: Combines the features of a Layer 2 switch with the routing capabilities of a router.
    - Network Segmentation: Helps in managing and optimizing traffic between different network segments.

Layer 3 Switch Managed

- Description: Managed Layer 3 switch, this device operates at both the Data Link layer (Layer 2) and the Network layer (Layer 3) of the OSI model. It uses MAC addresses for switching and IP addresses for routing, with advanced management features.
- Uses:
    - Frame Switching: Forwards Ethernet frames based on MAC addresses.
    - Routing: Routes traffic between different VLANs or subnets using IP addresses.
    - VLAN Support: Implements and manages VLANs for network segmentation.
    - Management: Provides configuration, monitoring, and security features for enhanced network control.

Bridge

- Description: A bridge is a device that connects and filters traffic between two or more network segments at the Data Link layer (Layer 2).
- Uses:
    - Network Segmentation: Connects and manages traffic between different network segments or subnets.
    - Filtering: Filters and forwards data based on MAC addresses to reduce traffic and improve network efficiency.
    - Extending Networks: Can extend the physical range of a network by connecting segments that are physically separated.

Access Point

- Description: An access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi.
- Uses:
    - Wireless Connectivity: Provides wireless access to the network for devices like laptops, smartphones, and tablets.

- Network Extension: Extends the range of a wired network by providing Wi-Fi coverage in areas where wired connections are not available.
- Network Bridge: In some cases, can also act as a bridge to connect different network segments wirelessly.

TERMS EXPLAINED

10/100/1000
Refers to Ethernet standards for network speeds. 10/100/1000 Mbps (Megabits per second) indicates support for 10 Mbps (10BASE-T), 100 Mbps (100BASE-TX), and 1000 Mbps (1000BASE-T) speeds, often referred to as Fast Ethernet and Gigabit Ethernet.

1024-QAM
1024-QAM is a modulation scheme used in communication systems to encode data into radio signals. It represents data by varying both the amplitude and phase of the carrier signal, allowing for 1024 different signal states (or symbols) to be used for data transmission.

4kV Lightening Protection
4kV lightning protection refers to a system or device designed to protect electronic equipment and electrical installations from voltage surges caused by lightning strikes. The "4kV" indicates that the protection is rated to handle **transient** voltage spikes up to 4,000 volts.

5GHz vs 2.4GHz
5 GHz: Faster speeds, less interference, more channels.
2.4 GHz: Greater range, better penetration through walls and obstacles.

802.11ax (Wi-Fi 6)
802.11ax, also known as Wi-Fi 6, is the sixth generation of Wi-Fi technology. It improves upon previous standards (like 802.11ac) by increasing speed, capacity, and efficiency in wireless networks. It is designed to perform better in high-density environments with many connected devices.

802.11ac (Wi-Fi 5)
802.11ac, also known as Wi-Fi 5, is a Wi-Fi standard that improves upon previous generations by offering faster speeds, higher capacity, and better performance in high-density environments. It operates in the 5 GHz frequency band and is designed to support high-bandwidth applications and multiple devices.

AX1800
AX1800 refers to a Wi-Fi router or access point that supports the Wi-Fi 6 (802.11ax) standard with a maximum theoretical combined wireless speed of 1800 Mbps (megabits per second). This speed is typically split between different frequency bands, such as 1201 Mbps on the 5 GHz band and 574 Mbps on the 2.4 GHz band.

AX3000
AX3000 indicates a Wi-Fi 6 router or access point with a total maximum wireless throughput of 3000 Mbps. This speed is usually divided between different frequency bands, such as 2402 Mbps on the 5 GHz band and 574 Mbps on the 2.4 GHz band.

AX6000
AX6000 refers to a Wi-Fi router or access point that supports the **Wi-Fi 6** (802.11ax) standard with a maximum theoretical combined wireless speed of 6000 Mbps (megabits per second). This speed is typically divided between the 5 GHz band and the 2.4 GHz band.

Bandwidth
The maximum rate at which data can be transferred over a network connection or interface, typically measured in bits per second (bps), megabits per second (Mbps), or gigabits per second (Gbps).

Clients
Devices or software that access services provided by a server in a network. Examples include computers, smartphones, and tablets that connect to a network.

Collision Domains
A collision domain is a network segment where data packets can "collide" with each other when two devices attempt to send data simultaneously over the same network channel. Collisions occur in networks that use shared communication mediums, leading to delays and retransmissions.

Data Link Layer
The Data Link layer (Layer 2) of the OSI model is responsible for node-to-node data transfer and error detection within a local network. It packages raw bits from the Physical layer into frames and handles MAC addressing and flow control.

DHCP
Dynamic Host Configuration Protocol is a network management protocol used to automatically assign IP addresses and other network configuration parameters to devices on a network.

DNS
Domain Name System translates domain names (like www.example.com) into IP addresses that computers use to identify each other on the network.

EIGRP
Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol that combines the benefits of distance-vector and link-state protocols. It efficiently manages and routes data within an autonomous system using metrics such as bandwidth, delay, and reliability.

Ethernet Frames
Ethernet frames are the data packets used in Ethernet networks to encapsulate and transmit data over the network. They follow a specific structure defined by the Ethernet protocol, which is part of the Data Link layer (Layer 2) of the OSI model

Firewall
A security device or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules to protect networks from unauthorized access and threats.

Forwarding rate
Forwarding rate refers to the speed at which a network device, such as a switch or router, can process and forward data packets from one port to another. It is typically measured in packets per second (pps) and indicates the device's capacity to handle network traffic.

Frame Switching
Frame switching is a process used in network switches to forward data frames from one port to another based on MAC addresses. It operates at Layer 2 (Data Link Layer) of the OSI model, handling Ethernet frames.

IGMP Snooping
A network switch feature that listens to Internet Group Management Protocol (IGMP) messages to manage multicast traffic efficiently. It helps prevent unnecessary multicast traffic from flooding across all switch ports.

ISP Router Bridge Mode
Converting an ISP router to bridge mode involves configuring the router so that it acts purely as a modem, passing the internet connection through to another router without performing any routing functions. This setup is often used to allow a more advanced router to handle network management and routing duties.

LAN
Local Area Network is a network that connects devices within a limited area, such as a home, office, or campus, allowing them to share resources and communicate with each other.

Latency
The time delay between sending a request and receiving a response, usually measured in milliseconds (ms). Lower latency indicates faster communication.

Link Aggregation
The practice of combining multiple network connections in parallel to increase bandwidth and provide redundancy. Commonly implemented using IEEE 802.3ad (LACP - Link Aggregation Control Protocol).

Layer 2
Layer 2 of the OSI model, known as the Data Link Layer, is responsible for node-to-node data transfer and error detection within a local network. It provides reliable communication between devices on the same network segment by using MAC addresses.

Layer 3
Layer 3 of the OSI model, known as the Network Layer, is responsible for routing packets of data between devices across different networks. It handles logical addressing, packet forwarding, and routing decisions to ensure data reaches its intended destination.

MAC Address
Media Access Control address is a unique identifier assigned to network interfaces for communications at the data link layer. It is used to identify devices on a network.

MIMO
Multiple Input Multiple Output is a technology used in wireless communication to improve performance and data rates by using multiple antennas for both transmitting and receiving data.

Mesh Network
A network topology where each node connects to multiple other nodes, creating a web-like structure. It enhances reliability and coverage by allowing multiple paths for data to travel.

MTBF
Mean Time Between Failures, a measure of reliability for hardware. It indicates the average time between failures of a component or system.

MU-MIMO
Multi User Multiple Input Multiple Output is a technology used in Wi-Fi networks that allows a router to communicate with multiple devices simultaneously, rather than sequentially. This improves network efficiency and performance by enabling the simultaneous transmission of data streams to multiple devices.

Network Segments
A network segment is a distinct part of a network separated by devices such as routers or switches, designed to manage and isolate network traffic. Each segment can operate independently to reduce congestion and improve network performance.

OFDMA
OFDMA is a multi-user version of Orthogonal Frequency Division Multiplexing (OFDM) used in Wi-Fi 6 (802.11ax) and other communication technologies. It allows multiple devices to share the same frequency band by dividing it into smaller sub-channels, or "subcarriers."

OSI Model
The OSI Model is a conceptual framework used to understand and standardize the functions of a network or communication system. It divides network communication into seven distinct layers, each responsible for specific aspects of data transmission.

OSPF
Open Shortest Path First (OSPF) is a link-state routing protocol used for distributing IP routing information within a single autonomous system. It uses a link-state database and the Dijkstra algorithm to compute the shortest path for routing packets. OSPF is widely used due to its scalability and efficiency in large networks

POE
Power over Ethernet allows network cables to carry electrical power to devices such as IP cameras, phones, and wireless access points, eliminating the need for separate power supplies.

POE+
PoE+ is an enhancement of the original Power over Ethernet (PoE) standard that provides higher power levels over Ethernet cables. It is defined by the IEEE 802.3at standard and delivers up to 25.5 watts of power per port, compared to the 15.4 watts provided by standard PoE.

PTP
Precision Time Protocol (PTP) is a protocol used to synchronize clocks across a network with high precision. Defined by IEEE 1588, PTP provides greater accuracy compared to

other time synchronization methods like Network Time Protocol (NTP), with precision often in the sub-microsecond range.

PTMP
Point-to-Multipoint (PTMP) is a network topology where a single central point (or base station) communicates with multiple endpoints or client devices. This configuration is often used in wireless and cellular networks to efficiently distribute services to multiple users from a single access point.

NAT
Network Address Translation (NAT) is a process used in networking to modify the source or destination IP address of packets as they pass through a router or firewall. NAT is commonly used to manage and conserve IP addresses and to enhance security by masking internal IP addresses.

Network Segment
A network segment is a portion of a network that is separated by a switch, router, or other network devices. It typically contains a group of devices that can communicate directly with each other without requiring routing, often used to manage and reduce network traffic and improve performance.

Network Monitoring
Network monitoring involves the continuous observation of a network's performance, availability, and health. It tracks data traffic, device status, and network activity to identify and resolve issues, optimize performance, and ensure network reliability and security.

Node to Node
Node-to-Node refers to the direct communication or data exchange between two network devices (nodes) on the same network segment. This term is commonly used to describe interactions within a network where two devices send and receive data directly between each other.

QoS
Quality of Service is a set of technologies that manage network resources to ensure the performance of critical applications by prioritizing certain types of traffic over others.

PBR
Policy-Based Routing (PBR) is a technique used in networking to make routing decisions based on policies set by the network administrator rather than relying solely on the destination IP address. It allows for customized routing based on various criteria like source IP address, application type, or traffic type.

Physical Layer
The Physical Layer is the first layer of the OSI model responsible for the actual transmission and reception of raw binary data (bits) over a physical medium. It deals with the hardware elements of networking, such as cables, switches, and network interface cards.

SFP
Small Form-Factor Pluggable is a compact, hot-swappable transceiver used in network equipment to connect to various types of media (e.g., fiber optic, copper). Modules come in various data rates (SFP, SFP+ as example), typically measured in gigabits per second (Gbps)

Security Policy
A set of rules and guidelines to protect network resources and data from unauthorized access, misuse, or attacks. It defines acceptable use, access controls, and incident response procedures.

SON
Self-Organizing Network refers to network systems that automatically configure, optimize, and manage themselves. It is commonly used in mobile networks to improve efficiency and performance.

Smart AI Roaming
Smart AI Roaming is a feature in wireless networking that uses artificial intelligence (AI) to optimize the connectivity and roaming experience of devices within a wireless network. It intelligently manages and improves how devices connect to different access points or routers as they move around.

Subnets
Subnets are divisions of a larger IP network into smaller, more manageable segments. They help in organizing and isolating network traffic, improving security, and optimizing performance by reducing broadcast domains within the network.

Switching Capability
The ability of a network switch to handle and forward traffic efficiently based on MAC addresses and other criteria. It is an indicator of the switch's performance and capacity.

Throughput
The actual amount of data transmitted successfully over a network in a given time period, often measured in bits per second (bps). It reflects the network's effective performance.

Uplink
A connection that links a network device (e.g., switch, router) to a higher-level network or upstream network, such as connecting a switch to a router or another switch.

VLAN
Virtual Local Area Network is a logical partition of a physical network that groups devices into separate segments to improve performance, security, and management. Example separate your camera system onto its own VLAN.

VPN
Virtual Private Network is a technology that creates a secure and encrypted connection over a less secure network, such as the internet, to protect data and maintain privacy.

WAN
Wide Area Network is a telecommunications network that extends over a large geographical area, connecting multiple LANs (Local Area Networks) and providing communication between distant locations.