THE ACCESS LAYER

THE ACCESS LAYER

The **3-layer network design model** is a well-established framework used to design scalable and efficient network architectures. This model divides the network into three distinct layers, each serving specific roles and responsibilities. The three layers are:

1. Access Layer

2. Distribution Layer

3. Core Layer

1. ACCESS LAYER

The **Access Layer** is the bottom layer of the network design model and is responsible for **connecting end-user devices** to the network. This is where devices like computers, printers, smartphones, IP phones, and other endpoint devices access the network.

The Access Layer focuses on providing **access control**, **device connectivity**, and **basic traffic management**. Its main objective is to allow communication between end devices and the rest of the network.

KEY FUNCTIONS:

- Device Connectivity: This layer connects user devices (PCs, printers, wireless devices) to the network via switches or wireless access points (APs).
- Switching: It typically involves Layer 2 switching, where devices are connected through Ethernet switches that forward traffic based on MAC addresses.
- Access Control: Implements security measures such as port security, 802.1X authentication, and VLAN assignment to ensure that only authorized devices can connect to the network.
- Traffic Filtering and Policing: It controls traffic flow by defining policies to ensure the network performs efficiently. Features such as QoS (Quality of Service) and rate limiting might be used to prioritize certain types of traffic.
- Network Access Protocols: Handles protocols like DHCP (Dynamic Host Configuration Protocol) for IP address assignment, NAT (Network Address Translation), and DNS (Domain Name System) for device configuration.

DEVICES USED:

- Switches: Primarily Layer 2 (Ethernet) switches for local connectivity.
- Wireless Access Points (APs): If providing wireless network access.
- Firewalls/Access Control Devices: For enforcing network security and access control.

Example:

- Users' computers connecting to a Layer 2 switch via Ethernet cables or Wi-Fi.

2. **DISTRIBUTION LAYER**

The **Distribution Layer** is the middle layer and acts as the **traffic manager** of the network. It aggregates data from the access layer and then routes it appropriately to other network segments. It is the bridge between the Access and Core Layers, and its role is to **direct traffic** and **implement policies** between different network segments or VLANs.

The main purpose of the Distribution Layer is to ensure that traffic from multiple access devices is intelligently routed across the network and to make decisions on how traffic is forwarded. It also serves as the point of **policy enforcement**, where services like **quality of service (QoS)**, **security**, and **routing protocols** are applied.

KEY FUNCTIONS:

- Routing: Handles Layer 3 routing and routing between different subnets or VLANs (Virtual Local Area Networks). It connects different Access Layer switches and enables communication between them.
- Policy Enforcement: Applies network-wide policies like security filtering, firewalling, and access control lists (ACLs).
- Inter-VLAN Routing: If VLANs are used in the Access Layer, the Distribution Layer performs routing between them (also known as Layer 3 switching or Inter-VLAN routing).
- Traffic Aggregation: Aggregates traffic from multiple Access Layer switches and sends it to the Core Layer, optimizing the flow of data in the network.
- Load Balancing: If multiple paths exist between the Access Layer and the Core Layer, the Distribution Layer might perform load balancing to optimize bandwidth usage.
- Redundancy and Fault Tolerance: Ensures network resilience by providing redundant paths to the Core Layer and implementing Spanning Tree Protocol (STP) to prevent loops.

DEVICES USED:

- **Layer 3 Switches**: Handles routing and switching within the Distribution Layer.
- **Routers**: For inter-network communication and routing between different subnets/VLANs.
- **Firewalls**: May also be positioned in the Distribution Layer to enforce security policies across different network segments.

Example:

- A **Layer 3 switch** routing traffic between multiple VLANs or directing data from end devices to appropriate destinations.

3. CORE LAYER

The **Core Layer** is the topmost layer in the network design model. It provides the **high-speed backbone** that connects the Distribution Layer to other parts of the network. The Core Layer's primary role is to handle **fast data forwarding** with minimal latency and to provide **high availability** and **redundancy** for critical data paths.

In essence, the Core Layer acts as the **high-speed highway** for traffic between different parts of the network and across various geographical locations (e.g., between campuses or data centers). The focus at this layer is on **speed, reliability, and fault tolerance** rather than intelligence or functionality.

KEY FUNCTIONS:

- High-Speed Data Forwarding: The Core Layer focuses on routing traffic quickly, with low latency and minimal processing. It's optimized for high-throughput, low-latency performance.
- Redundancy and Fault Tolerance: The Core Layer should provide redundant paths to ensure network availability, with technologies like link aggregation, multiple routing protocols, and multiple ISPs (Internet Service Providers) for reliability.
- Interconnectivity: It connects different Distribution Layer devices, and provides the connection between data centers and WAN (Wide Area Network).
- Scalability: The Core Layer is designed to handle increased traffic as the network grows. It’s built to scale efficiently without major redesigns.
- Traffic Aggregation: The Core Layer aggregates traffic from the Distribution Layer and ensures that data can travel efficiently across the entire network.

DEVICES USED:

- **High-Speed Core Routers**: Often capable of handling large volumes of traffic with minimal latency.
- **Core Switches**: Can be used for high-speed Layer 3 switching.
- **Internet Gateways**: For routing traffic between the internal network and the internet or external networks.

Example:

- **Core Routers** that provide a link to an ISP or other geographical sites, ensuring communication between the company headquarters and remote branch offices.

SUMMARY OF FUNCTIONS AT EACH LAYER

Layer	Function	Key Components
Access Layer	- Connects end-user devices to the network	- Switches (Layer 2), APs, End-user devices
	- Provides network access, device connectivity, and access control	- Port Security, VLANs, Authentication (802.1X)
Distribution Layer	- Aggregates traffic from the Access Layer and forwards it to the Core Layer	- Layer 3 Switches, Routers, Firewalls
	- Implements routing, security policies, and manages inter-VLAN communication	- Inter-VLAN Routing, QoS, Policy Enforcement
Core Layer	- Provides high-speed, low-latency forwarding of traffic between different parts of the network	- Core Routers, High-speed Layer 3 Switches
	- Focuses on reliability, redundancy, and scalability for large-scale data transfer	- Redundant Paths, WAN Gateways

SUMMARY

The **3-layer network design model** is a framework that helps ensure efficient, scalable, and manageable network architectures. Each layer in the model serves a distinct role:

- The **Access Layer** connects end devices to the network and provides security and access control.
- The **Distribution Layer** acts as the traffic manager and enforces policies between network segments.
- The **Core Layer** ensures high-speed, redundant, and reliable data forwarding across the entire network.

By using this structured approach, network designers can build networks that are both **robust and flexible**, able to scale as needed while ensuring performance and security.