1. Explain the architecture for enterprises in detail.

A modern enterprise network typically employs a modular, scalable architecture to support diverse business needs. Cisco, in particular, promotes several key architectural frameworks. The core model is often viewed through the lens of a modular architecture with distinct areas:

Enterprise Architecture Model

This model divides the network into functional areas or modules, making design, implementation, and management more straightforward.

Module	**Description**
Enterprise Campus	The core area covering buildings, departments, and local access. It includes the backbone network, services like IP telephony, and wireless.
Enterprise Edge	The boundary between the campus and the external networks (WAN, Internet, and remote access). This area provides connectivity, security, and policy enforcement.
Service Provider Edge	Represents the external network connections provided by a service provider (e.g., MPLS, Internet access).
Remote Modules	Include connectivity for branch offices, teleworkers, and external partners.
Enterprise Data Center	The location for centralized application servers and data storage, requiring high-speed, high-availability, and specialized security.

Cisco Borderless Networks Architecture

This is a design framework focusing on connectivity, security, and sustainability across the entire organization, extending securely beyond the traditional campus boundaries. Its key services include:

- **Policy and Compliance:** Ensuring consistent security and access rules.
- **Security:** Comprehensive protection from the access layer to the edge.
- **Mobility:** Seamless access via wired and wireless connections.
- **Application Performance:** Optimizing delivery for critical business applications.

---

2. Discuss the PPDIOO phases in detail.

PPDIOO (Prepare, Plan, Design, Implement, Operate, and Optimize) is a cyclic lifecycle approach used by Cisco to design and manage enterprise networks. It ensures a systematic and well-documented process.

Phase	**Description**	**Key Deliverables**
Prepare	Establishes organizational requirements, the business case for the network, and the initial high-level architecture goals.	Business requirements document, initial architecture vision, project scope, funding.
Plan	Identifies the project's requirements, resources, and validates the technological approach. It includes a network audit to characterize the existing network.	Project plan, resource plan, updated high-level design.
Design	The core technical phase where network design requirements are translated into a detailed, robust design based on best practices (e.g., hierarchical model).	**Detailed Design Document** (topology, addressing, protocols, security plan).
Implement	The stage where the new network components are installed and configured according to the Design Document. This often involves pilot and prototype tests.	Implemented network, installation reports, migration plan.
Operate	The day-to-day management of the network. This includes monitoring, fault detection, managing performance, and maintaining security.	Trouble tickets, performance reports, change management records.
Optimize	Proactive network management to identify and fix problems before they impact the business. It involves redesigning parts of the network to improve performance, security, or capacity.	Optimization report, new or revised design documents (feeding back into the **Plan** or **Design** phase).

---

3. What are the different layers of hierarchical network design? Explain.

The **Hierarchical Network Model** is a fundamental principle in network design, organizing the network into discrete, logical layers. This approach provides simplicity, scalability, security, and ease of management.

1. Core Layer (The Backbone)

- **Function:** Provides high-speed, highly available transport between the Distribution layer devices. It's the network backbone.

- **Characteristics:** Focuses strictly on speed and reliability. No complex processing, access-lists (ACLs), or packet manipulation should occur here.
- **Devices:** High-end switches and routers optimized for throughput and minimal latency.

2. Distribution Layer (The Control)

- **Function:** Acts as the aggregation point for the Access layer and handles policy enforcement, security, and routing between different segments. It's the boundary between the Core and Access layers.
- **Characteristics:** Defines broadcast and multicast domains (via VLANs), implements policies (ACLs), routing, and quality of service (QoS).
- **Devices:** Layer 3 switches with high performance for routing and filtering.

3. Access Layer (The Edge)

- **Function:** Provides connectivity for end-user devices (PCs, printers, IP phones, servers) to the rest of the network.
- **Characteristics:** Focuses on port density, security, and Power over Ethernet (PoE). Policies such as port security are implemented here.
- **Devices:** Layer 2 switches (often with PoE capabilities).

---

4. List and explain project deliverables.

Project deliverables are the tangible outcomes or documentation produced at various stages of the network design lifecycle. Key deliverables include:

- **Business Requirements Document (BRD):** Produced in the **Prepare** phase, it details the business justification, goals, and high-level requirements for the network project.
- **Project Plan:** Produced in the **Plan** phase, outlining the scope, schedule, budget, and resources required for the project.
- **Existing Network Characterization/Audit Report:** Produced in the **Plan** phase, it details the current network's inventory, performance, utilization, and identified problems.
- **Detailed Design Document:** The most critical deliverable, produced in the **Design** phase. It includes:
    - **Topology Diagrams:** Logical and physical.
    - **IP Addressing Scheme:** Subnetting and allocation plan.
    - **Protocol Selection:** Routing (e.g., OSPF, EIGRP), switching (e.g., VTP, STP), and security.
    - **Security Plan:** ACLs, firewall placement, and VPN design.
- **Implementation and Test Plans:** Outlining the step-by-step process for deployment and the procedures for verifying functionality (e.g., pilot/prototype results).
- **Operation/Training Manuals:** Documentation for the operations team on maintaining and troubleshooting the new network.

---

5. Explain HSRP, VRRP, and GLBP.

HSRP, VRRP, and GLBP are First Hop Redundancy Protocols (FHRPs) designed to provide continuous network access for end-user devices when a router or layer 3 switch fails. They ensure that the default gateway remains available.

Protocol	Full Name	Description	Active/Standby Role
HSRP	**Hot Standby Router Protocol** (Cisco Proprietary)	Allows a group of routers to share a single virtual MAC address and IP address. Only one router is **Active** at a time, handling all traffic. The **Standby** router monitors the Active one and takes over if it fails.	One Active, one or more Standby
VRRP	**Virtual Router Redundancy Protocol** (Industry Standard/IETF)	Functionally similar to HSRP but is an open standard. It uses a **Master** router (equivalent to Active) and one or more **Backup** routers (equivalent to Standby).	One Master, one or more Backup
GLBP	**Gateway Load Balancing Protocol** (Cisco Proprietary)	Provides both redundancy and load balancing. It allows multiple routers to participate in a virtual router group and forward traffic. It uses one **Active Virtual Gateway (AVG)** to assign different **Active Virtual Forwarders (AVFs)** (the actual routers) to different hosts using distinct virtual MAC addresses.	Up to four Active Virtual Forwarders (AVFs)

---

6. Define enterprise campus modules.

The **Enterprise Campus Module** is the core functional area of the enterprise network where the end-users and resources are physically located. It provides the network infrastructure for local area networking (LAN).

Key Components:

- **Campus Core:** The high-speed backbone connecting all other layers.
- **Building Distribution:** Aggregation point for building access switches, handling routing, security, and policy for the building.
- **Building Access:** Provides port density for connecting end devices (workstations, IP phones, access points) using Layer 2/3 switching.
- **Server Farm/Data Center Connection:** The link to the centralized server infrastructure.

The goal of the Campus Module is to deliver **high availability, high-speed access, and uniform security/QoS policies** to all users within the main corporate location(s).

---

7. Explain in detail different network audit tools.

Network audit tools are used during the **Plan** phase of PPDIOO to characterize the existing network by gathering data on its inventory, configuration, health, and performance.

Tool Category	Example Tools	Purpose/Explanation
Network Discovery & Inventory	Cisco Prime Infrastructure, NMAP	Automatically discover all devices (routers, switches, servers, endpoints) on the network, collect their configuration files, hardware/software versions, and map the physical and logical topology.
Performance Monitoring/Management (NMS)	SolarWinds, PRTG, Nagios	Monitor key performance indicators (KPIs) like link utilization, CPU/memory usage on devices, latency, and packet loss. They provide real-time and historical trend data.
Protocol Analyzers/Sniffers	Wireshark, tcpdump	Capture and analyze network traffic at the packet level. Used to troubleshoot application issues, identify unusual traffic patterns, and verify protocol behavior.
Baseline & Utilization Tools	iPerf, Path-Trace utilities	Tools used to establish a baseline of normal network performance and measure throughput between two points, helping to identify bottlenecks.
Configuration Management Tools	RANCID, oxidized	Track and manage changes to device configurations, ensuring consistency and providing a rollback mechanism. Used to compare current configurations against a best-practice standard.

---

8. Explain E-commerce and Internet connectivity module.

These two are typically part of the **Enterprise Edge Area**, which connects the internal campus network to external services and the public Internet.

E-commerce Module

- **Function:** Provides highly secure, specialized connectivity for application servers that interact directly with customers or partners over the public Internet (e.g., web servers, application servers, databases for online transactions).
- **Security:** This module is heavily secured, typically residing in a **Demilitarized Zone (DMZ)**, isolated from both the internal campus network and the external Internet by firewalls.
- **Characteristics:** Requires high availability and load balancing for public-facing services.

Internet Connectivity Module

- **Function:** Provides the main, shared ingress/egress point for all internal users to access the public Internet.
- **Security:** Implements core security policies (firewalls, intrusion prevention/detection systems, URL filtering) to protect the internal network from Internet-based threats.
- **Characteristics:** Often employs redundant connections to one or more Internet Service Providers (ISPs) and Network Address Translation (NAT/PAT) to translate private internal addresses to public external ones.

---

9. Write a short note on network checklist.

A **network checklist** is a crucial, structured document used primarily during the **Plan** and **Design** phases of the PPDIOO lifecycle.

- **Purpose:** It ensures that all necessary data is collected during the planning phase and that all required design elements are addressed before implementation. It acts as a guide to prevent critical omissions.

- **Content (Planning Phase):** Questions covering current network inventory, device configurations, physical topology, security policies, existing applications, user counts, and current performance metrics.
- **Content (Design Phase):** Verification items to ensure the detailed design is complete, such as: "Is the IP addressing scheme fully documented?", "Has the routing protocol been verified for scalability?", "Are all high-availability protocols configured correctly?", and "Is the security policy applied consistently?"

---

10. Explain hierarchical network model and state advantages of it.

Hierarchical Network Model Explanation

As discussed in Q3, the hierarchical network model organizes a complex network into three distinct layers: **Core, Distribution, and Access**. This structure is foundational to modern scalable network design. The layers allow designers to select the right equipment and apply the correct features (speed, policy, density) where they are most needed.

Advantages of the Hierarchical Model

1. **Scalability:** You can add new access switches and users without impacting the Core layer, making the network easy to grow.
2. **Increased Performance:** By collapsing the network's complex functions into the Distribution layer, the Core layer is free to perform high-speed packet switching, improving overall throughput.
3. **Simplified Management and Troubleshooting:** The distinct boundaries between layers simplify fault isolation. If a problem is in the Access layer, it's unlikely to be in the Core.
4. **Improved Security:** Policies (ACLs, filtering) can be enforced consistently at the Distribution layer, providing a logical separation and control point for traffic flow.
5. **Cost Savings:** Lower-cost, feature-light devices can be used at the Access layer, reserving expensive, high-speed devices for the Core and Distribution layers where they are truly needed.