(3 Hours) **[Total Marks: 80]**

N.B.: (1) Question No.1 is compulsory.

(2) Attempt any three questions from the remaining five questions.

(3) Make suitable assumptions wherever necessary but justify your assumptions

1. a) Explain SONA framework for flexible network design. **10**

   b) Compare the Top-Down vs Bottom-Up Network Design Approach **10**

2. a) State and Explain in brief different external threats hampering the integrity of the enterprise network. **10**

   b) Explain different phases in PPDIOO Network Lifecycle. **10**

3. a) Explain the role SNMP in network management. **10**

   b) Explain the hierarchical network model of network design. **10**

4. a) Explain VPN and its implementation techniques. **10**

   b) Explain EIGRP in detail and highlight its characteristics which make it suitable for Enterprise Networks. **10**

5. a) State and Explain IPv4 to IPv6 Transition strategies. **10**

   b) State and explain suitable routing protocols for Enterprise architecture. **10**

6. Write a note on **(any two)** **20**
   a. SDN Architecture
   b. MPLS
   c. Enterprise WAN architecture technologies

****

Cisco SONA Framework

SONA stands for Service-Oriented Network Architecture. It is an architectural framework by Cisco providing guidelines to build an integrated system. It helps enhancing business performance by the standardisation of business processes and applications, and virtualisation of resources. This results in a dynamic yet flexible network architecture. It is depicted in Figure 33:

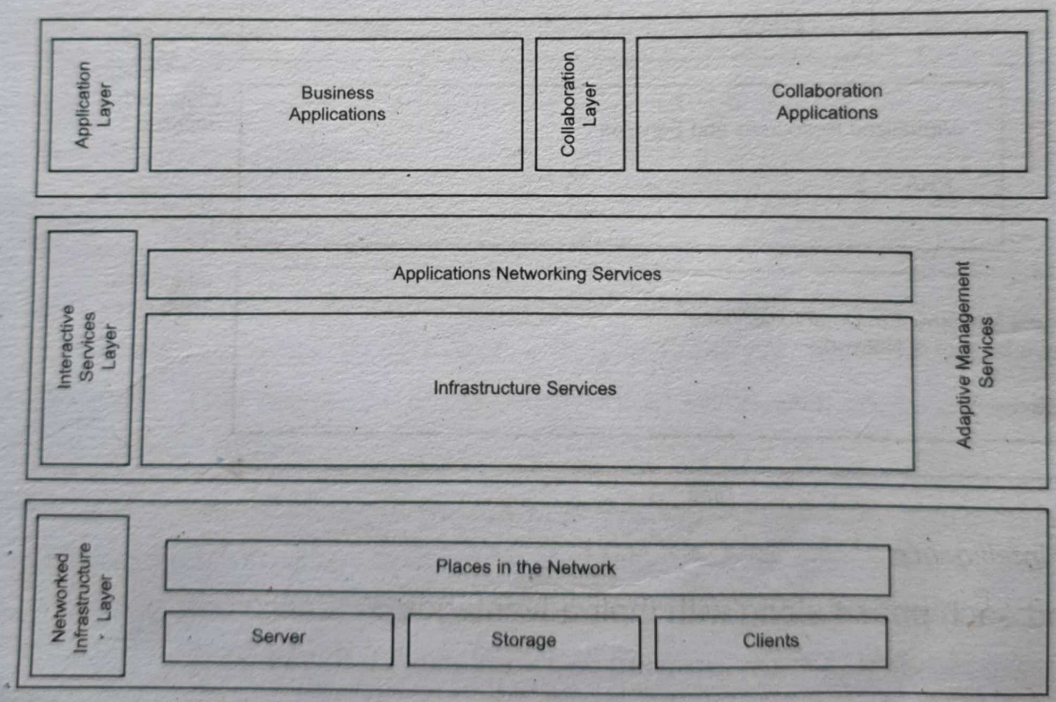


Figure 33: Cisco SONA Framework

Analogous to the three phases discussed in the previous section, three layers are defined by the Cisco SONA framework. Let us understand all the three layers along with the services they provide:

1. **Networked Infrastructure Layer**

   This layer intends to interconnect all IT resources such as clients, servers, storages, etc. anywhere, anytime. These resources might be located at different physical locations in the network. The resources might exist on different campuses, branches, data centres, enterprise edges, MANs, WANs or can be teleworkers. It links all network devices on a converged network foundation.

2. **Interactive Services Layer**

   This is the middle layer and deals with services for application networking as well as infrastructure. Networked infrastructure, achieved through the previous layer, makes the resources available. These resources are efficiently allocated to applications and business processes by this layer. Many services provided by this layer include:

   - Adaptive Network Management Services
   - Compute Services
   - Content Networking Services
   - High Availability
   - IP Multicast
   - Mobility Services
   - Network Infrastructure Virtualisation
   - Storage Services
   - Security and Identity Services
   - Quality of Services
   - Voice and Collaboration Services
   - Wireless Services

The services provided by Cisco SONA are shown in Figure 34

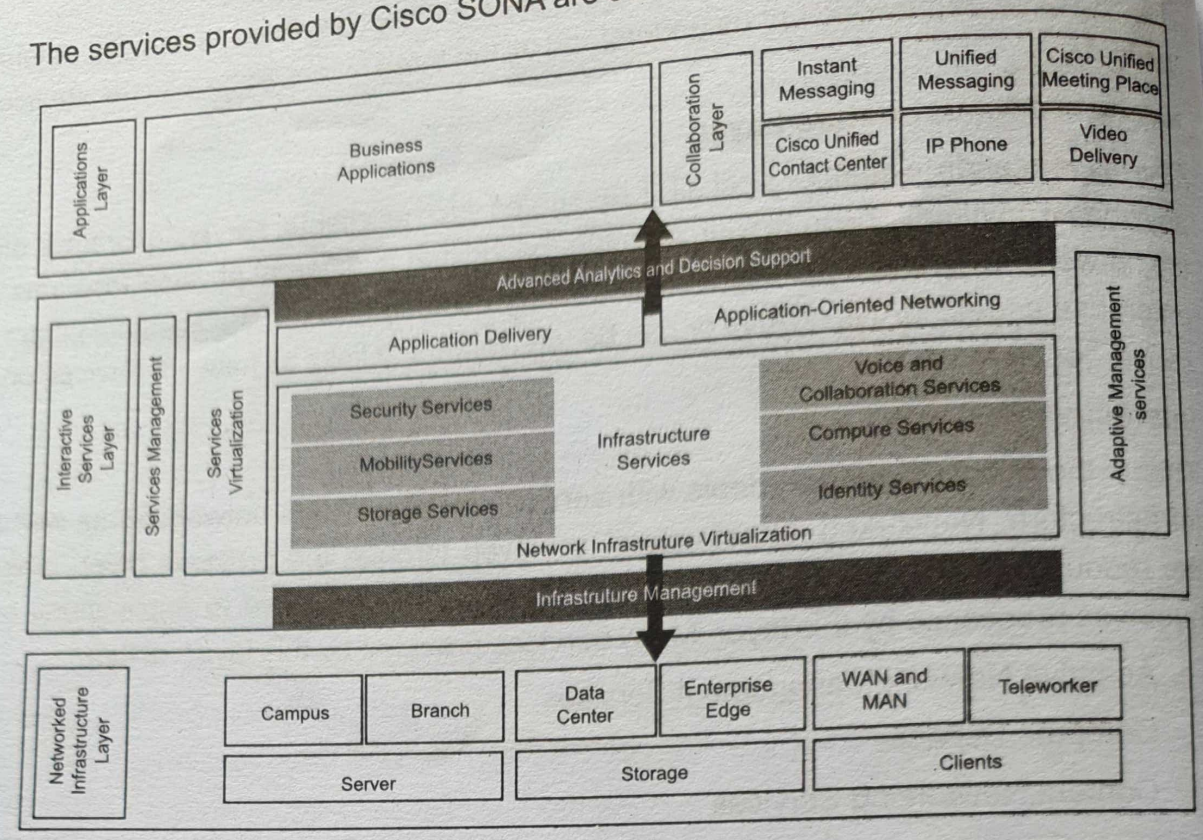


Figure 34: Cisco SONA Offerings

3. **Application Layer**

This is the topmost layer in the Cisco SONA framework. It leverages the interactive service layer to efficiently meet business requirements. It deals with both business applications as well as collaboration applications. Following collaborative applications are a part of this layer:

- Cisco IP Communicator and Cisco Unified IP Phones
- Cisco Unified Contact Centre
- Cisco Unified Meeting Place
- Cisco Unity
- Instant Messaging
- IP telephony
- Video delivery using Cisco Digital Media System

The Cisco SONA Framework has several advantages as listed below:

- **Availability**: Reliable services are made available anywhere, anytime through the networked infrastructure layer.
- **Efficiency**: Leads to a path of intelligent network services and infrastructure

- **Functionality**: Business requirements are met through the efficient use of available IT resources over the intelligent network.
- **Manageability**: The network is easily manageable through control, fault detection and performance monitoring.
- **Performance**: Application-specific business requirements such as throughput, utilisation, etc, are met by the optimal use of the network infrastructure and uninterrupted services.
- **Scalability**: The network can easily expand to accommodate new organisational tasks as functions and products are already separated into different layers.
- **Security**: It protects assets, resources and infrastructure from internal as well as external threats.

BASIS FOR COMPARISON	TOP-DOWN APPROACH	BOTTOM-UP APPROACH
Basic	Breaks the massive problem into smaller subproblems.	Solves the fundamental low-level problem and integrates them into a larger one.
Process	Submodules are solitarily analysed.	Examine what data is to be encapsulated, and implies the concept of information hiding.
Communication	Not required in the top-down approach.	Needs a specific amount of communication.
Redundancy	Contain redundant information.	Redundancy can be eliminated.
Programming languages	Structure/procedural oriented programming languages (i.e. C) follows the top-down approach.	Object-oriented programming languages (like C++, Java, etc.) follows the bottom-up approach.
Mainly used in	Module documentation, test case creation, code implementation and debugging.	Testing

Top-down Approach	Bottom-up Approach
A top-down approach is essentially the breaking down of a program to gain insight into its compositional small program (or module) in a reverse engineering fashion.	A bottom-up approach is the piecing together of module (or small program) to give rise to more complex program, thus making the original modules of the emergent program.
Structure / procedure oriented programming languages like C programming language follows top-down approach.	Object oriented programming languages like C++ and JAVA programming language follows bottom-up approach.
A top-down approach begins with high level design and ends with low level design or development.	A bottom-up approach begins with low level design or development and ends with high level design.
In top-down approach, main function is written first and all sub functions are called from main function thus, sub-functions are written based on the requirement	In bottom-up approach, code is developed from modules and then these modules are integrated with main function

1.	In this approach We focus on breaking up the problem into smaller parts.	In bottom up approach, we solve smaller problems and integrate it as whole and complete the solution.
2.	Mainly used by structured programming language such as COBOL, Fortran, C, etc.	Mainly used by object oriented programming language such as C++, C#, Python.
3.	Each part is programmed separately therefore contain redundancy.	Redundancy is minimized by using data encapsulation and data hiding.
4.	In this the communications is less among modules.	In this module must have communication.
5.	It is used in debugging, module documentation, etc.	It is basically used in testing.
6.	In top down approach, decomposition takes place.	In bottom up approach composition takes place.
7.	In this top function of system might be hard to identify.	In this sometimes we can not build a program from the piece we have started.
8.	In this implementation details may differ.	This is not natural for people to assemble.

External Threats

Outside attacks penetrate the network from the Enterprise Edge module. Hence, potential security attacks should be stopped at this module.

Figure 16 displays external threats:

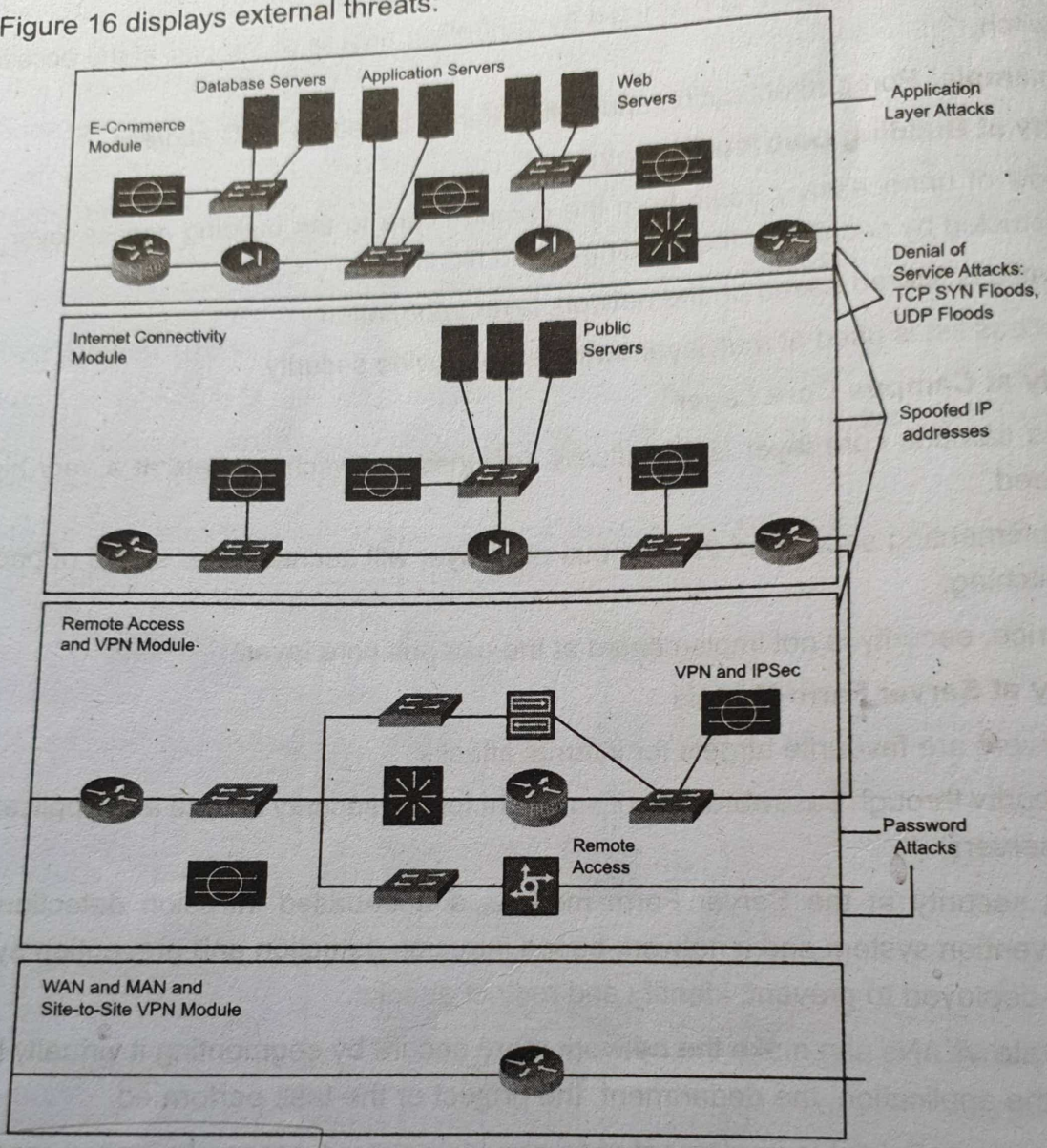


Figure 16: External Threats

Possible outside attacks at Enterprise Edge, as represented in Figure 16, are described as follows:

- **Application Layer Attacks**
  - It is performed at the E-Commerce module of Enterprise Edge which consists of application servers, database servers, web servers, etc.
  - Access to hosts is gained by exploiting well-known vulnerabilities of commonly used software.

- Since administrators are advised publicly to use a patch to handle existing flaw in the software, hackers readily get the knowledge of the existing vulnerability in the software.
- Example: Weakness in SMTP Servers
- Access to the privileged system level account having all permissions is acquired through such attacks.
- Attack at the application layer is through a port that is being commonly used to access application services. Traffic through such ports is allowed by a firewall.
- Example: Port 80 is the default port to get services from a web server. An attacker uses port 80 to exploit a vulnerability in a web server as traffic by port 80 is allowed by a firewall.

- **DoS Attack**
  - DoS stands for Denial of Service attack.
  - It is performed at the E-Commerce module or Internet Connectivity module of Enterprise Edge.
  - The aim is to make the service unavailable for genuine users.
  - It exploits weaknesses in the overall network architecture.
  - It exhausts network resources, application resources or OS to keep the network busy.
  - It floods the network with undesired packets to consume the available bandwidth.
  - Example: TCP SYN floods, UDP floods
  - It provides false information about network resources.
  - No intention to gain information or access to data or network.
  - TCP, ICMP are generally used to implement DoS attacks.
  - Many systems may simultaneously perform the DoS attack on a system; this is referred as Distributed Denial of Service Attack.
- **IP Spoofing**
  - It is performed at the E-Commerce module or Internet Connectivity module or Remote Access and VPN module of Enterprise Edge.
  - A trusted computer is used for IP spoofing attack.
  - This attack can be performed from inside the network or outside the network.
  - In any case, the IP address used for the attack is in the list of trusted IP addresses (either internal or external) by the network.
  - It serves as a gateway to perform other attacks such as DoS attack.

- **Password Attacks**
  - It is performed at Remote Access and VPN module of Enterprise Edge.
  - The aim is to determine username and password to access network resources, applications or information.
  - Examples of password attacks are:
    - Brute-force
    - Packet sniffer
    - Trojan horse
  - IP spoofing can be used by a hacker, along with a method to bypass password authentication, to access information on username basis.

High-Availability Services in a Modular Network Design

DoS Attacks

DoS attacks are different from most other attacks because they are not generally targeted at gaining access to a network or its information. Rather, these attacks focus on making a service unavailable for normal use. They are typically accomplished by exhausting some resource limitation on the network or within an operating system or application.

When involving specific network server applications, such as a web server or an FTP server, these attacks focus on acquiring and keeping open all the available connections supported by that server, thereby effectively locking out valid users of the server or service. DoS attacks are also implemented using common Internet protocols, such as TCP and Internet Control Message Protocol (ICMP).

Rather than exploiting a software bug or security hole, most DoS attacks exploit a weakness in the overall architecture of the system being attacked. However, some attacks compromise a network's performance by flooding the network with undesired and often useless network packets and by providing false information about the status of network resources. This type of attack is often the most difficult to prevent, because it requires coordinating with the upstream network provider. If traffic meant to consume the available bandwidth is not stopped there, denying it at the point of entry into your network does little good, because the available bandwidth has already been consumed. When this type of attack is launched from many different systems at the same time, it is often referred to as a *distributed denial of service attack*.

This information was derived from the *SAFE Blueprint for Small, Midsize, and Remote-User Networks*, available at http://www.cisco.com/go/safe/.

Application Layer Attacks

Hackers perform application layer attacks using several different methods. One of the most common methods is exploiting well-known weaknesses in software commonly found on servers, such as SMTP, HTTP, and FTP. By exploiting these weaknesses, hackers gain access to a computer with the permissions of the account that runs the application—usually a privileged system-level account. These application layer attacks are often widely publicized in an effort to allow administrators to rectify the problem with a patch. Unfortunately, many hackers also subscribe to these same informative mailing lists and therefore learn about the attack at the same time (if they have not discovered it already).

The primary problem with application-layer attacks is that they often use ports that are allowed through a firewall. For example, a hacker who executes a known vulnerability against a web server often uses TCP port 80 in the attack. A firewall needs to allow access on that port because the web server serves pages to users using port 80. From a firewall's perspective, the attack appears as merely standard port 80 traffic.

1.17. Network Design Methodology

All the phases of the network's lifecycle are covered by Cisco Prepare, Plan, Design, Implement, Operate and Optimize (PPDIOO) methodology. Hence, the network design methodology described in the subsequent section is derived from the PPDIOO methodology. All the phases of PPDIOO are explained in detail along with their significance in the network design. Further, network design methodology has also been covered in detail.

PPDIOO Methodology

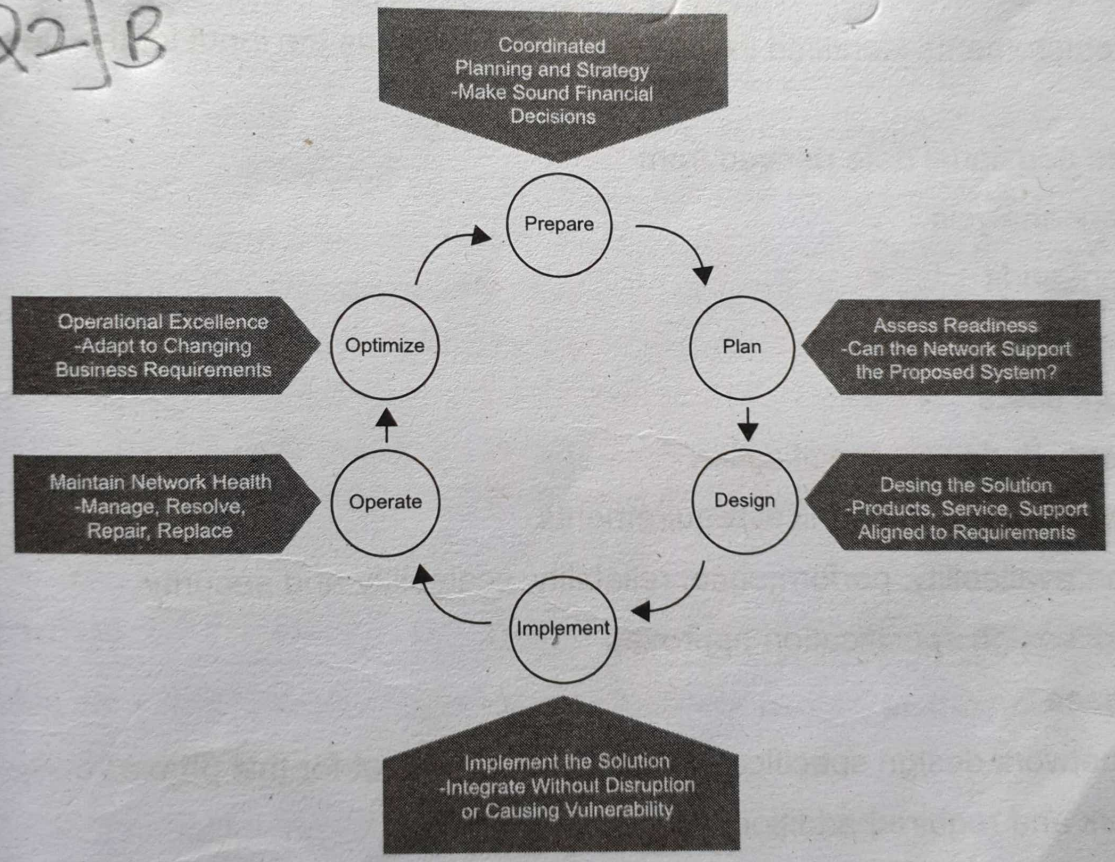


Figure 35: PPDIOO Methodology

The above diagram depicts the phases in the network's life cycle which are part of PPDIOO methodology. All six phases are closely related to each other. Let us understand the significance of each phase.

1. **Prepare Phase**
   - Establish business requirements
   - Develop a network strategy
   - Propose a high-level conceptual architecture
   - Identify technologies that support proposed conceptual architecture
   - Assess business case for proposed conceptual architecture
   - Establish financial justification for the network strategy
2. **Plan Phase**
   - Identify network requirements
   - Perform gap analysis to determine whether the existing network infrastructure has the capability to support proposed architecture
   - Manage the resources, responsibilities, tasks and critical milestones
   - Align with scope, cost and other constraints defined in original business requirements
   - Network requirements are the output of the Plan Phase.
3. **Design Phase**
   - Network requirements identified in the Plan Phase serve as the input for the Design phase
   - Incorporate additional data derived from
     - Network analysis
     - Network audit
     - Network managers
     - Network users
   - Prepare network design specification
     - Meet business and technical requirements
     - Support availability, performance, reliability, scalability and security
   - Get network design specification approved
4. **Implement Phase**
   - Approved network design specification serves as the input for this phase.
   - Built network and required additional components
   - Integrate network devices

- Do not disrupt existing network
- Do not create points of vulnerability

5. **Operate Phase**
   - Test appropriateness of design
   - Maintain network health during day-to-day operations
   - Maintain high availability
   - Reduce expenses
   - Detect and correct faults, if any
   - Monitor performance
6. **Optimise Phase**
   - Fault detection and correction report along with the performance monitoring report serves as the input for the Optimise phase
   - Proactive network management
   - Identify and resolve issues before real issues arise and affect the organisation
   - Predict and mitigate faults
   - Reactive fault detection and correction
   - May lead to network redesign if
     - Too many faults are detected
     - Performance does not meet business requirements
     - Business and technical requirements meet through the new application

Design is one of the six phases of PPDIOO. All other phases closely interact with the Design phase. Prepare and Plan phases gives network requirements as the output which serve as the input for the Design phase. Network Design Specification which is the output of the Design phase serves as the input for the Implementation phase. It verifies the design on the actual network. Network analysis and performance monitoring, done during Operate and Optimise phases, help evaluate the appropriateness of the design. To correct any fault or to meet the business requirement, the network might have to be redesigned. Thus, undeniably all other phases influence the Design phase.

Benefits of PPDIOO on Network Design Methodology

Various benefits of PPDIOO approach on Network Design Methodology is as under:

1. Reduces total cost of network ownership
   - Technology requirements are identified and validated.
   - Any change in the infrastructure or any new resource requirements is planned in advance.

- All the business and technical requirements are included in the design.
- Smooth and successful implementation of the new system
- Efficiency of the network is improved. Improved efficiency of the operation process and tools
- Reduced operation costs

2. **Increases network availability**
   - Network security is continuously evaluated.
   - Handy availability of the correct set of hardware and software releases
   - Keeps the hardware and software operational and current.
   - Validates network operation based on appropriate network design.
   - Pre-deployment testing
   - Monitoring the system ensures high availability.
   - Remedial plans are prepared for security breaches identified during proactive monitoring.
3. **Improves business agility**
   - Business requirements and strategies are created.
   - Existing site is upgraded to support the implementation of the new system.
   - Demonstrate that the network is meeting business and technical requirements specified in the network design.
   - Installation, configuration and integration of network components without any downtime or interrupt.
   - Enhanced performance
4. **Provides speedy access to applications and services**
   - Continuous support for the existing network services as well as planned network services
   - Increased availability, performance and resources capacity of the system resulting in improved service-delivery efficiency
   - Improved availability, stability and reliability of network and network applications
   - Problems affecting the system are managed and resolved efficiently

Before moving ahead, let us have a quick glimpse of network management architecture.

Network Management Architecture

Q3] A [SNMP Role]

Figure 24 shows a simplified network management architecture:

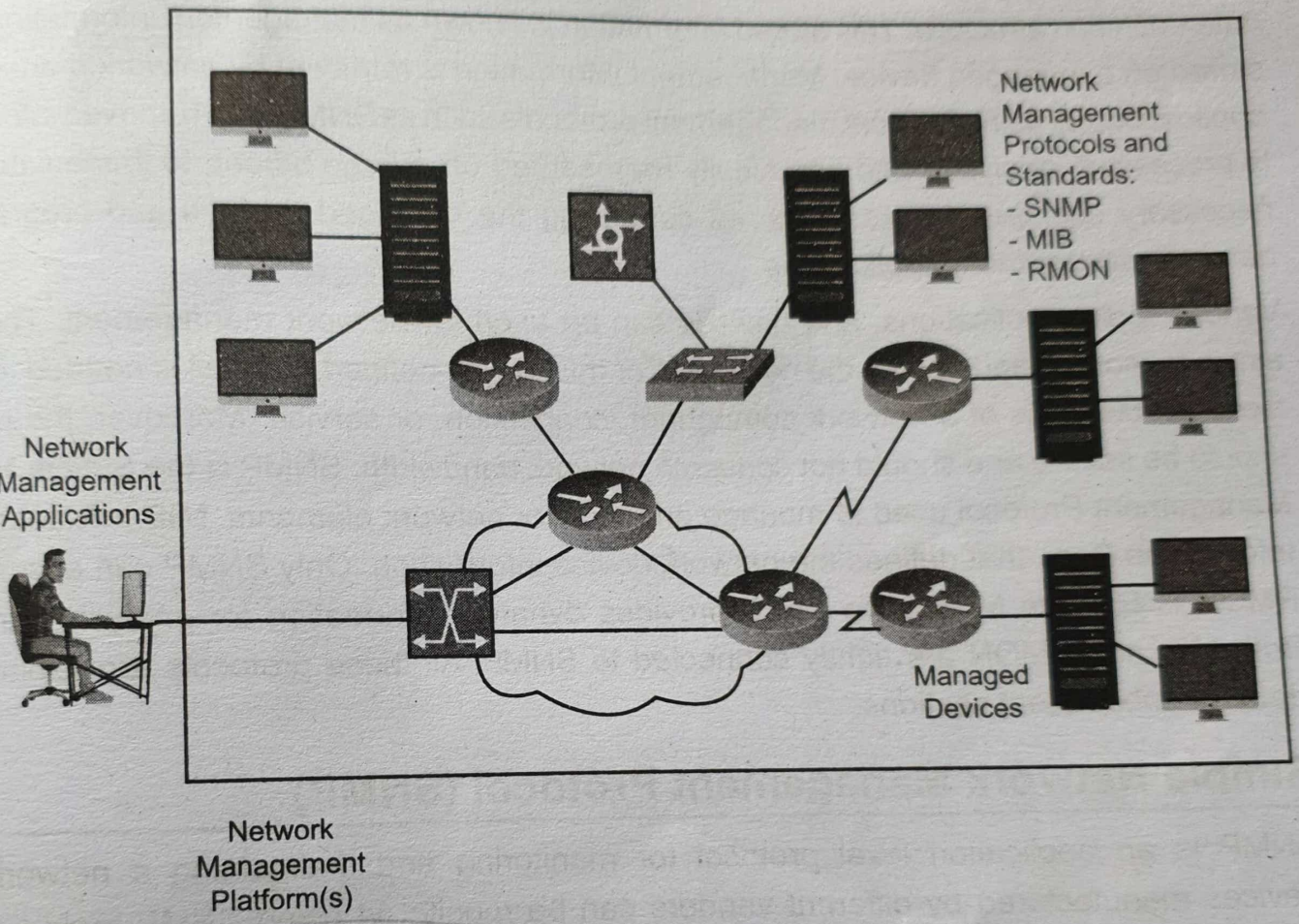


Figure 24: Network Management Architecture

Components of a network management architecture are listed as follows:

- **Network management system** is a system having enough processing and memory resources to run applications that monitor and control managed devices.
- **Network management protocol** is a protocol to exchange network management information among the network management system and managed devices.

  Example: SNMP, MIB, RMON.
- **Managed devices** are devices managed by the network management system.

  Example: router, firewall, servers.

- **Management agents** are software that collect and store network management information from managed devices.

  Example: SNMP agents, RMON agents.

- **Management information** is the information of a managed device that can be used for network management.

  Example: Information regarding the number of packets received and forwarded by a router can be used to check if the router is congested.

A management agent collects the network-related data and stores it in MIB, i.e. a standardised data definition structure. This stored information is known as management information and is stored on a managed device. Management information is retrieved by network management applications by using network management protocols such as SNMP. The retrieved information is processed, analysed and graphically represented on a large screen to immediately take necessary countermeasures such as controlling the managed devices and programming network management applications.

Various tools, applications, and devices can be used for network management. The basic aim is to monitor and control the network. For this, a well-defined protocol is needed to check the characteristics of a network component, connection, or service. Moreover, the protocol should be secure and should not consume network bandwidth. SNMP is the Simple Network Management Protocol used to manage and monitor network elements. MIB is Management Information Base that defines the network device information. Only SNMP can access MIB. RMON is Remote Monitoring which provides dynamic information for analysis purposes. Both MIB and RMON are tightly connected to SNMP. All these protocols are explained in detail in subsequent sections.

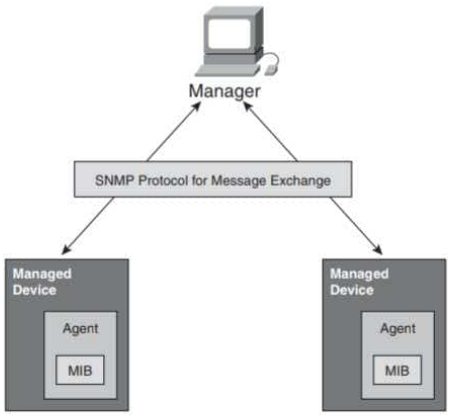
SNMP

SNMP has become the de facto standard for network management. SNMP is a simple solution that requires little code to implement, which enables vendors to easily build SNMP agents for their products. In addition, SNMP is often the foundation of the network management architecture. SNMP defines how management information is exchanged between network management applications and management agents. Figure 3-26 shows the terms used in SNMP; they are described as follows:

- **Manager**: The manager, a network management application in an NMS, periodically polls the SNMP agents that reside on managed devices for the data, thereby enabling information to be displayed using a GUI on the NMS. A disadvantage of periodic SNMP polling is the possible delay between when an event occurs and when it is collected by the NMS; there is a trade-off between polling frequency and bandwidth usage.
- **Protocol**: SNMP is a protocol for message exchange. It uses the User Datagram Protocol (UDP) transport mechanism to send and retrieve management information, such as MIB variables.
- **Managed device**: A device (such as a router) managed by the manager.
- **Management agents**: SNMP management agents reside on managed devices to collect and store a range of information about the device and its operation, respond to the manager's requests, and generate traps to inform the manager about certain events. SNMP traps are sent by management agents to the NMS when certain events occur. Trap notifications could result in substantial network and agent resource savings by eliminating the need for some SNMP polling requests.

- **MIB**: The management agent collects data and stores it locally in the MIB, a database of objects about the device. Community strings, which are similar to passwords, control access to the MIB. To access or set MIB variables, the user must specify the appropriate read or write community string; otherwise, access is denied.

Figure 3-26 *NMP Is a Protocol for Management Information Exchange*

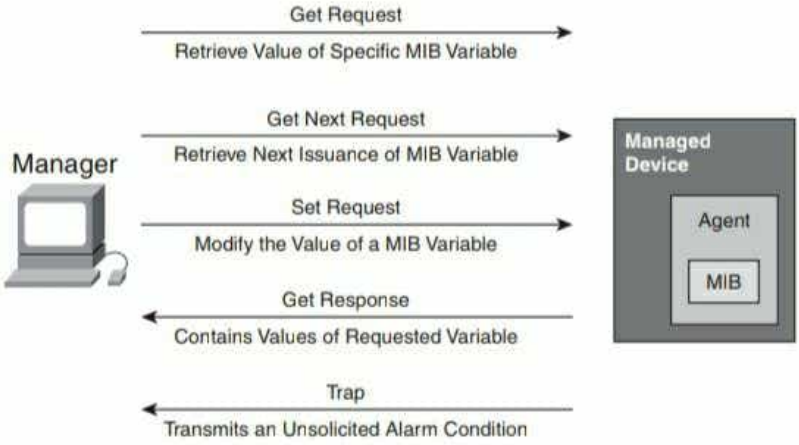


SNMPv1

The initial version of SNMP, SNMPv1 is defined in RFC 1157, *Simple Network Management Protocol (SNMP)*. The protocol's simplicity is apparent by the set of operations that are available. Figure 3-27 shows the basic SNMP messages, which the manager uses to transfer data from agents that reside on managed devices. These messages are described as follows:

- **Get Request**: Used by the manager to request a specific MIB variable from the agent.
- **Get Next Request**: Used after the initial get request to retrieve the next object instance from a table or list.
- **Set Request**: Used to set a MIB variable on an agent.
- **Get Response**: Used by an agent to respond to a manager's Get Request or Get Next Request message.
- **Trap**: Used by an agent to transmit an unsolicited alarm to the manager. A Trap message is

Figure 3-27 *SNMPv1 Message Types*



SNMPv2

SNMPv2 is a revised protocol that includes performance and manager-to-manager communication improvements to SNMP. SNMPv2 was introduced with RFC 1441, *Introduction to version 2 of the Internet-standard Network Management Framework*, but members of the IETF subcommittee could not agree on several sections of the SNMPv2 specification (primarily the protocol's security and administrative needs). Several attempts to achieve acceptance of SNMPv2 have been made by releasing experimental modified versions, commonly known as SNMPv2*, SNMPv2, SNMPv2u, SNMPv1+, and SNMPv1.5, which do not contain the disputed parts.

Community-based SNMPv2 (or SNMPv2c), which is defined in RFC 1901, *Introduction to Community-based SNMPv2*, is referred to as SNMPv2 because it is the most common implementation. The "c" stands for *community-based security* because SNMPv2c uses the same community strings as SNMPv1 for read and write access. SNMPv2 changes include the introduction of the following two new message types:

- **GetBulk message type**: Used for retrieving large amounts of data, such as tables. This message reduces repetitive requests and replies, thereby improving performance.
- **InformRequest**: Used to alert the SNMP manager of a specific condition. Unlike unacknowledged trap messages, InformRequest messages are acknowledged. A managed device sends an InformRequest to the NMS; the NMS acknowledges the receipt of the message by sending a Response message back to the managed device.

SNMPv3

SNMPv3 is the latest SNMP version to become a full standard. Its introduction has moved SNMPv1 and SNMPv2 to historic status. SNMPv3, which is described in RFCs 3410 through 3415, adds methods to ensure the secure transmission of critical data to and from managed devices. Table 3-2 lists these RFCs. Note that these RFCs make RFCs 2271 through 2275 and RFCs 2570 through 2575 obsolete.

Table 3-2 *SNMPv3 Proposed Standards Documents*

RFC Number	Title of RFC
3410	Introduction and Applicability Statements for Internet-Standard Management Framework
3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
3413	Simple Network Management Protocol (SNMP) Applications
3414	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

SNMPv3 introduces the following three security levels:

- **NoAuthNoPriv**: Without authentication and without privacy (encryption).
- **AuthNoPriv**: With authentication but without privacy. Authentication is based on Hash-Based Message Authentication Code-Message Digest 5 or HMAC-Secure Hash Algorithm algorithms.
- **AuthPriv**: With authentication as described earlier and privacy using the 56-bit Cipher-Block Chaining-Data Encryption Standard encryption standard.

design layers of the hierarchical model are explained in the subsequent sections.

Hierarchical Network Model

The hierarchical network model is a network design framework for network designers. This framework specifies three network design layers, each having a specific role and functionality. Such a framework adds flexibility to a designed network. Implementation and troubleshooting of the designed network become easier.

Hierarchical Network Design Layers

Figure 1 displays the three layers of the hierarchical network design model:

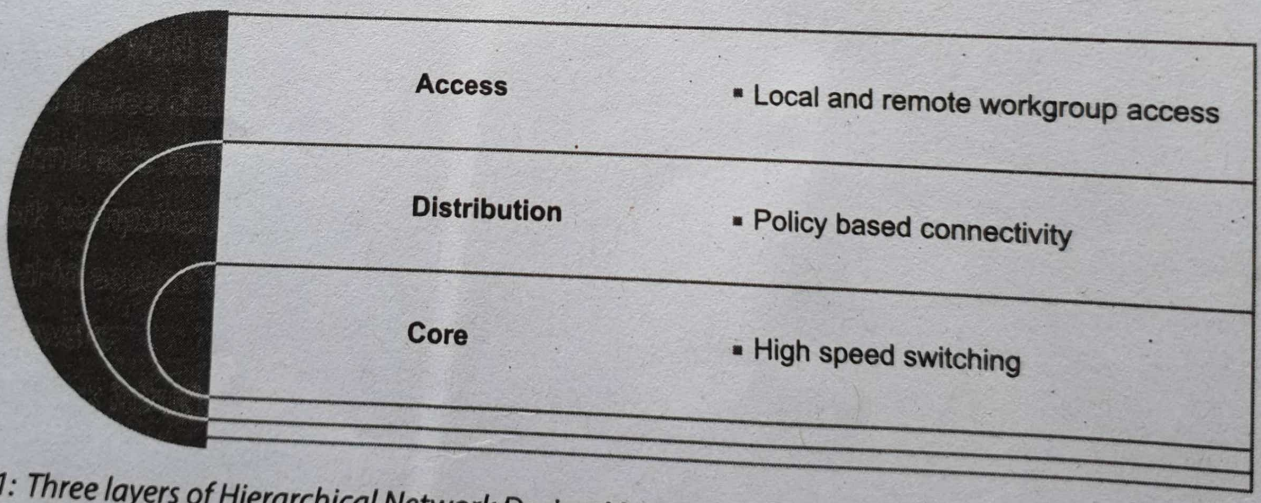


Figure 1: Three layers of Hierarchical Network Design Model

The three layers of the hierarchical network design model are listed as follows:

1. Access Layer: Provides access to the network to users and/or workgroup
2. Distribution Layer: Provides policy-based connectivity
3. Core Layer: Provides high-speed connectivity and switching

The hierarchical network design model helps in performing efficient capacity planning at a minimal cost. A network can be mapped to three layers of the hierarchical network model, as depicted in Figure 2:

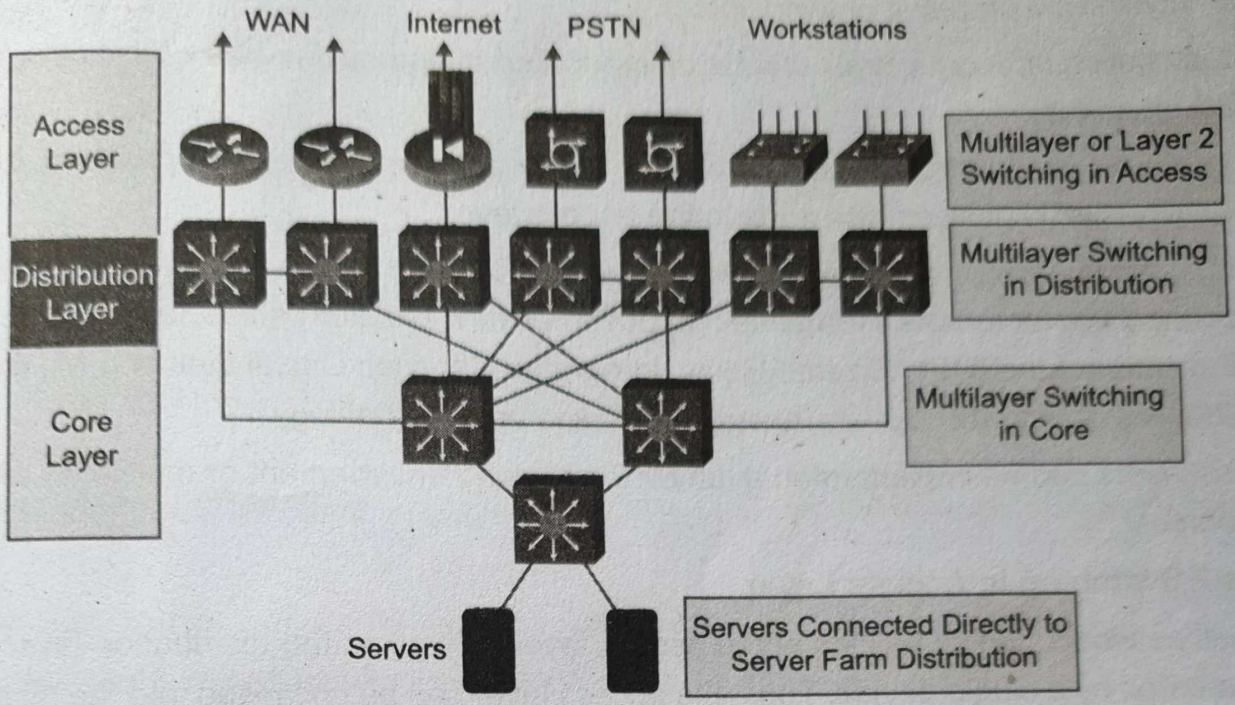


Figure 2: Sample Network Using Hierarchical Network Design

Hierarchical layers represent the functionality of each layer which might not be physically distinct. Subsequent sections explain each layer along with their functionality and implementation.

Taking the example of a college network, network design has been explained. Nowadays, engineering colleges across the country keep at least 800 to 1500 computers and that too in a single building or campus. Every college has various departments based on branches. So, here you may think of one multilayer higher-end switch at the core layer which is connected to various department level switches at the distribution layer. Every department has many computer laboratories. Then, at the access layer, laboratory-wise switches are connected to corresponding department switches. It is advisable to visualise this case study while reading the entire book.

Access Layer Functionality

The role of access layer and its interaction with users and the distribution layer is described in this section along with an example.

Role of Access Layer

Clients access network resources through the access layer. This layer grants access only to authenticated users (logical name authentication) or authenticated devices (physical address authentication) to preserve network integrity.

Characteristics of access layer can be differentiated based on the size of the network they are designed for.

- In a LAN environment, connectivity for users and workstations is provided by using switched LAN devices with ports in the access layer.
- In a WAN environment, wide area technology is used in the access layer to provide connectivity for remote sites to the corporate network. Coaxial cables, leased lines, Digital Subscriber Line (DSL), Frame Relay, Integrated Services Digital Link and Multiprotocol Label Switching (MPLS) are examples of wide area technology.

Access layers can be implemented at Layer 2 switching environment or multilayer switching environment.

Layer 2 Switching in Access Layer

In small networks, functionalities of the access layer as well as the distribution layer can be implemented by a single device. Thus, the access layer can be collapsed into the distribution layer.

For large networks:

- Shared or switched media LANs can be used to provide access to local users, workgroups or servers.
- Switched LANs can be segmented using VLAN.
- Each LAN or VLAN is a single broadcast domain.
- 10/100/1000 Ethernet ports are aggregated by the access layer.
- Fast Ethernet, Fast EtherChannel and Gigabit Ethernet uplinks are used to connect access layer to distribution layer.
- Multiple VLANs can be configured.
- Each VLAN has its own:
  - IP subnet
  - Instance of Spanning Tree Protocol
- Layer 2 Trunk is used to connect access layer switches to distribution layer switches:
  - For load balancing and redundancy, per-VLAN STP is used on each uplink.
  - For inter VLAN communication at the access layer, a distribution layer multilayer switch is used.

- Implement one VLAN per access switch.
- Use Layer 3 links instead of Layer 2 trunks to connect access layer switches to distribution layer switches.
- Use Rapid Spanning Tree Protocol (RSTP) for enterprises.

Multilayer Switching in Access Layer

- A multilayer switch is better known as Router.
- A router defines the boundary of broadcast domain.
- A router is required to communicate across different broadcast domains as well as across different VLANs.
- A router provides functions such as authentication, packet filtering, route propagation, QoS, security, etc.
- Wide area technologies along with the router optimise the network to meet customer requirements.

Access Layer Example

Figure 3 displays an example of the access layer:

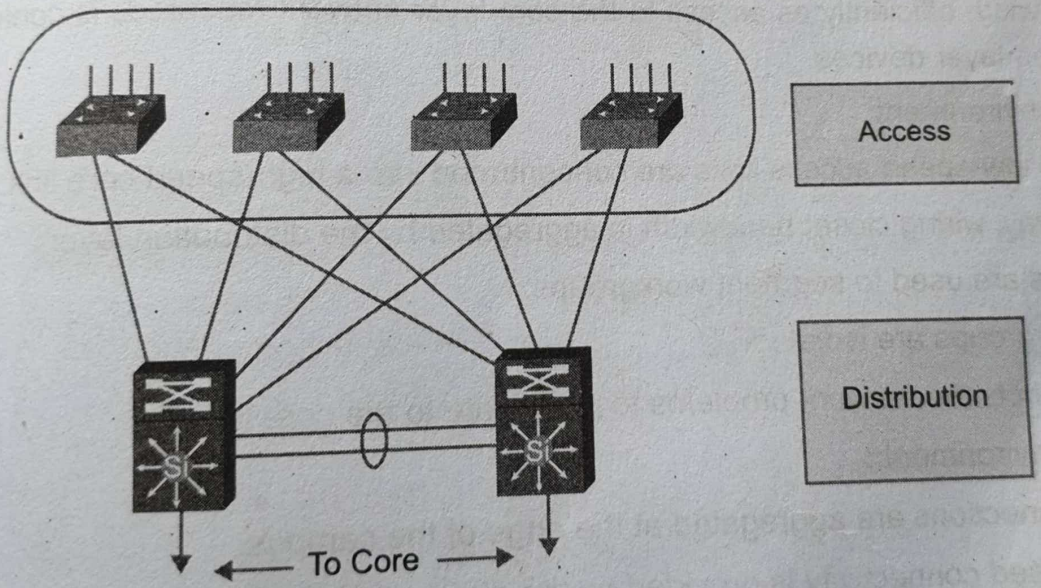


Figure 3: Access Layer Example

In Figure 3, the network of a campus is depicted. At the access layer, end-users are aggregated and uplink is provided to the distribution layer. As noticed from the figure, each access layer switch is connected to two distribution layer switches. This is done to achieve high availability. Apart from high availability, other features supported by the access layer includes convergence, IP multicast, QoS, and security.

Distribution Layer Functionality

The role of distribution layer and its interaction with the access layer and the core layer described in this section along with an example.

Role of Distribution Layer

The distribution layer separates the access layer from the core layer. It also serves as connection point between several access sites and the core layer. At this layer, policies of the organisation are implemented. This is referred to as Policy-based connectivity.

Various examples of implementing policies are given as follows:

- Based on input or output ports, filters can be applied.
- Based on the source or destination address, filters can be applied.
- Restriction of certain packets to a specific part of the network can be applied for security purposes.
- Route filters are applied to hide internal networks.
- Static routes can be specified using policy.
- Traffic can be prioritised using queuing mechanisms at routers to maintain QoS.

Characteristics of distribution layer are stated as follows:

- Utilise bandwidth efficiently as access to the core layer network resources is controlled by distribution layer devices.
- In the LAN environment:
  - Multiple low-speed access links are concentrated into a high-speed core link.
  - In this way, wiring closet bandwidth is aggregated by the distribution layer.
  - Switches are used to segment workgroups.
  - Network groups are isolated.
  - This restricts the network problems to propagate to the core layer.
- In the WAN environment:
  - WAN connections are aggregated at the edge of the campus.
  - Policy-based connectivity is provided by the distribution layer.
  - Media transition is supported by the distribution layer; for example, between ATM and Ethernet.
  - The routing boundary between the access layer and the core layer is defined.
  - The distribution layer has the capability to terminate a broadcast domain for VLAN even though this can be done at the access layer.
  - The distribution layer implements route filtering.
  - A default route can be set for routers of the access layer by the distribution layer.

- Dynamic routing protocols can be configured to communicate with core layers by the distribution layer.
- The distribution layer provides high performance even though diverse sites are connected to the core layer.
- The distribution layer uses bandwidth-intensive access layer routing protocols.
- The distribution layer uses optimised core routing protocols.
- Policies for load balancing, routing, QoS and security are implemented by the distribution layer to provide network services to the access layer.
- Routing protocol performance can be improved by summarising routes from the access layer.
- To balance load among network devices, redundant connections to access devices are provided by the distribution layer.
- Traffic can be wisely controlled by the distribution layer by prioritising traffic for mission-critical applications.

Distribution Layer Example

Figure 4 displays an example of distribution layer connectivity:

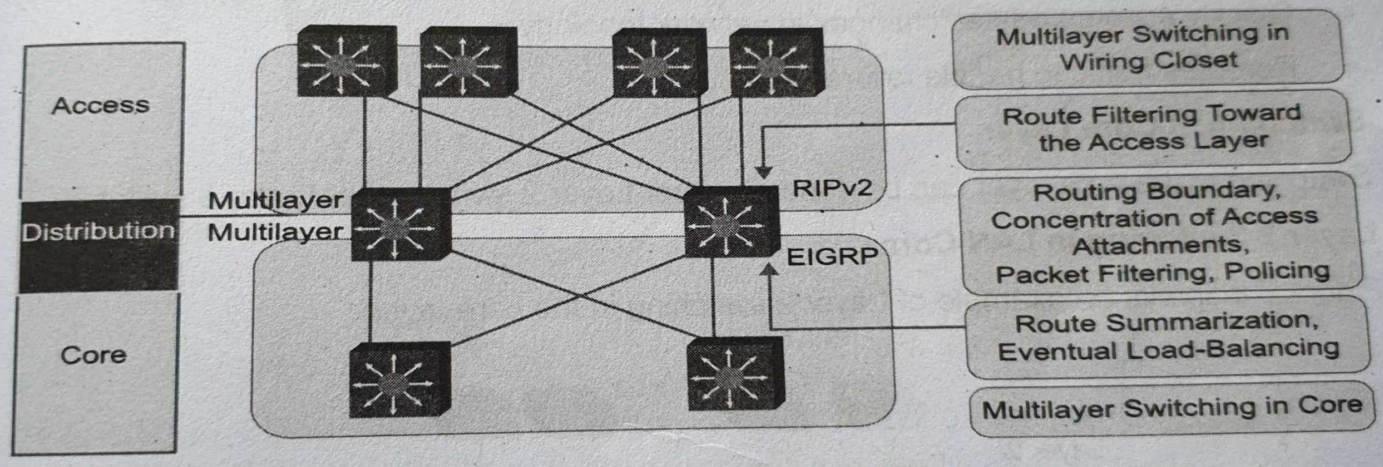


Figure 4: Distribution Layer Connectivity

Characteristics of distribution layer in a LAN are stated as follows:

- Multilayer switches at the distribution layer have redundant connectivity towards the access layer as well as towards the core layer.
- Multilayer switching is used towards the access layer in the wiring closet as well as towards the core layer.
- Routing Information Protocol version 2 (RIPv2) is used for route filtering towards the access layer.
- Enhanced Interior Gateway Routing Protocol (EIGRP) is used for route summarisation and load balancing towards the core layer.

- Distribution layer exchanges routes between RIPv2 and EIGRP.

Core Layer Functionality

The role of core layer and its interaction with the distribution layer is described in this section along with an example.

Role of Core Layer

Characteristics of core layer are stated as follows:

- Avoids packet filtering or any other manipulation to avoid slowdown of switching of packets
- Possesses high-speed backbone
- Implements scalable protocols and technologies
- Provides fast and efficient data transport
- Provides high availability and reliability
- Provides load balancing
- Provides redundancy through fully mesh or partially mesh connectivity
- Quickly switches a packet to optimise data transport within the network
- Quickly accommodates changes in network topology
- Reroutes traffic to handle failures

Switching in Core Layer

Switching in the core layer can be done by either Layer 2 switching or Layer 3 switching.

Layer 2 Switching in LAN Core

Figure 5 displays an example of Layer 2 switching in the core layer:

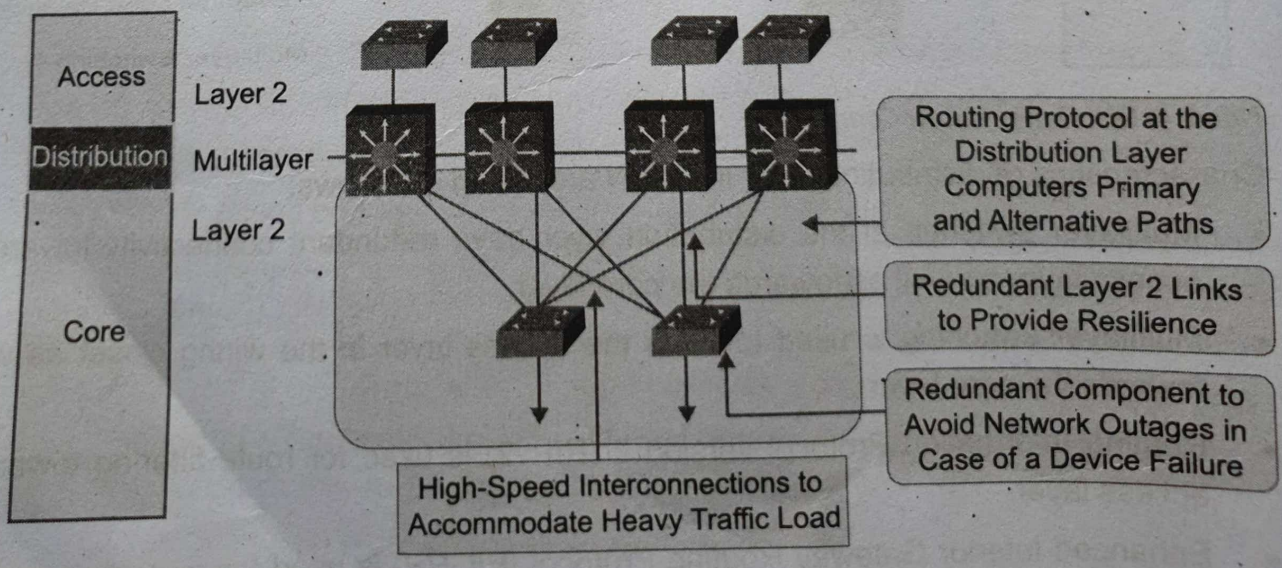


Figure 5: Layer 2 Switching in Core Layer

VPN

- VPN stands for virtual private network that creates a safe and encrypted connection over a less secure network,
- VPN also ensures security by providing an encrypted tunnel between client and vpn server
- Using VPN we can Anonymously browse because it hides your ip address.

How can a VPN help protect against identity theft?

1. It creates an encrypted tunnel for the data you send and receive that's out of reach of cyberthieves.
2. disguises your IP address when you use the internet, making its location invisible to everyone

What does a VPN hide?

1. Your IP address and location
2. Your devices
3. Your location for streaming
4. Your browsing history

VPN Connectivity Options

- Overlay VPNs
- Virtual private dial-up networks (VPDN)
- Peer-to-peer VPNs

There are six types of protocols used in VPN.

1. Internet Protocol Security or IPSec
2. Layer 2 Tunnelling Protocol (L2TP)
3. Point – to – Point Tunnelling Protocol (PPTP)
4. Secure Sockets Layer (SSL),
5. Secure Shell (SSH).

VPN stands for Virtual Private Network (VPN), that allows a user to connect to a private network over the Internet securely and privately. VPN creates an encrypted connection that is called VPN tunnel, and all Internet traffic and communication is passed through this secure tunnel.

Virtual Private Network (VPN) is basically of 2 types:

1. **Remote Access VPN:**
   Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.
   An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

2. **Site to Site VPN:**
   A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

- **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
- **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

Types of Virtual Private Network (VPN) Protocols:

(implementation techniques of vpn)

1. **Internet Protocol Security (IPSec):**
   Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.
   IPSec runs in 2 modes:

   - (i) Transport mode
   - (ii) Tunneling mode

   The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system.

2. **Layer 2 Tunneling Protocol (L2TP):**
   L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

3. **Point-to-Point Tunneling Protocol (PPTP):**
   PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

4. **SSL and TLS:**
   SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have "https" in the initial of the URL instead of "http".

5. **OpenVPN:**
   OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.
6. **Secure Shell (SSH):**
   Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel.

- Enhanced Interior Gateway Routing Protocol -

EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP is a Cisco-proprietary Hybrid routing protocol, incorporating features of both Distance-Vector and Link-State routing protocols.

EIGRP adheres to the following Hybrid characteristics:

- EIGRP uses **Diffusing Update Algorithm (DUAL)** to determine the best path among all "feasible" paths. DUAL also helps ensure a loop-free routing environment.
- EIGRP will form **neighbor** relationships with adjacent routers in the same **Autonomous System (AS)**.
- EIGRP traffic is either sent as unicasts, or as multicasts on address **224.0.0.10**, depending on the EIGRP packet type.
- Reliable Transport Protocol (RTP) is used to ensure delivery of most EIGRP packets.
- EIGRP routers **do not** send periodic, full-table routing updates. Updates are sent when a change occurs, and include *only* the change.
- EIGRP is a classless protocol, and thus supports VLSMs.

Other characteristics of EIGRP include:

- EIGRP supports IP, IPX, and Appletalk routing.
- EIGRP applies an Administrative Distance of **90** for routes originating *within* the local Autonomous System.
- EIGRP applies an Administrative Distance of **170** for external routes coming from *outside* the local Autonomous System
- EIGRP uses **Bandwidth** and **Delay of the Line,** by default, to calculate its distance metric. It also supports three other parameters to calculate its metric: **Reliability**, **Load**, and **MTU.**
- EIGRP has a maximum hop-count of **224**, though the default maximum hop-count is set to **100**.

EIGRP, much like OSPF, builds three separate tables:

- **Neighbor table** – list of all neighboring routers. Neighbors must belong to the same **Autonomous System**
- **Topology table** – list of *all* routes in the Autonomous System
- **Routing table** – contains the *best* route for each known network

EIGRP Neighbors

EIGRP forms neighbor relationships, called **adjacencies,** with other routers in the same AS by exchanging **Hello** packets. Only after an adjacency is formed can routers share routing information. Hello packets are sent as multicasts to address 224.0.0.10.

By default, on LAN and high-speed WAN interfaces, EIGRP Hellos are sent every **5 seconds**. On slower WAN links (T1 speed or slower), EIGRP Hellos are sent every **60 seconds** by default.

EIGRP Neighbors (continued)

A **neighbor table** is constructed from the EIGRP Hello packets, which includes the following information:

- The IP address of the neighboring router.
- The local interface that received the neighbor's Hello packet.
- The Hold timer.
- A sequence number indicating the order neighbors were learned.

Adjacencies will not form unless the **primary IP addresses** on connecting interfaces are on the same subnet. Neighbors *cannot* be formed on secondary addresses.

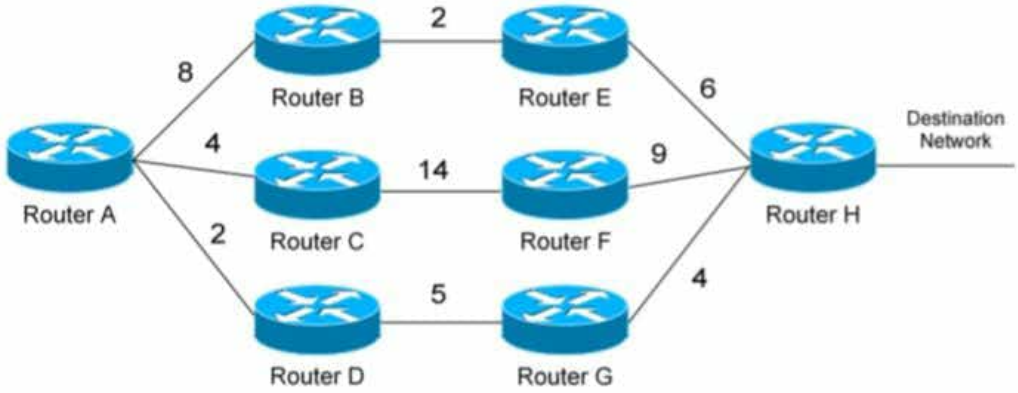
The EIGRP Topology Table

Once EIGRP neighbors form adjacencies, they will begin to share routing information. Each router's update contains a list of all routes known by that router, and the respective metrics for those routes.

All such routes are added to an EIGRP router's topology table. The route with the lowest metric to each network will become the **Feasible Distance (FD)**. The Feasible Distance for each network will be installed into the routing table.

The Feasible Distance is derived from the **Advertised Distance** of the router *sending* the update, and the local router's metric to the advertising router.

Confused? Consider the following example:



EIGRP Packet Types

EIGRP employs five packet types:

- **Hello packets -** *multicast*
- **Update packets –** *unicast* or *multicast*
- **Query packets** – *multicast*
- **Reply packets** – *unicast*
- **Acknowledgement packets -** *unicast*

Hello packets are used to form neighbor relationships, and were explained in detail previously. Hello packets are always multicast to address 224.0.0.10.

Update packets are sent between neighbors to build the topology and routing tables. Updates sent to *new* neighbors are sent as unicasts. However, if a route's metric is changed, the update is sent out as a multicast to address 224.0.0.10.

Query packets are sent by a router when a Successor route fails, and there are no Feasible Successors in the topology table. The router places the route in an **Active state**, and queries its neighbors for an alternative route. Query packets are sent as a multicast to address 224.0.0.10.

Reply packets are sent in response to Query packets, assuming the responding router has an alternative route (feasible successor). Reply packets are sent as a unicast to the querying router.

Recall that EIGRP utilizes the **Reliable Transport Protocol** (**RTP**) to ensure reliable delivery of most EIGRP packets. Delivery is guaranteed by having packets *acknowledged* using…..**Acknowledgment packets!**

EIGRP Metrics

EIGRP can utilize 5 separate metrics to determine the best route to a destination:

- **Bandwidth** (K1) – Slowest link in the route path, measured in kilobits
- **Load** (K2) – Cumulative load of all outgoing interfaces in the path, given as a fraction of 255
- **Delay of the Line** (K3) – Cumulative delay of all outgoing interfaces in the path in tens of microseconds
- **Reliability** (K4) – Average reliability of all outgoing interfaces in the path, given as a fraction of 255
- **MTU** (K5) – The smallest Maximum Transmission Unit in the path. The MTU value is actually *never* used to calculate the metric

By default, only **Bandwidth** and **Delay of the Line** are used. This is identical to IGRP, except that EIGRP provides a more granular metric by multiplying the bandwidth and delay by 256. Bandwidth and delay are determined by the interfaces that lead towards the destination network

EIGRP Authentication

EIGRP supports authentication to secure routing updates.

The first step is creating a shared authentication *key* that must be identical on both routers. This is accomplished in global configuration mode:

IPv4-to-IPv6 Transition

Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. The transition from IPv4 to IPv6 will take several years because of the high cost of upgrading the equipment. In the meantime, IPv4 and IPv6 must coexist. To overcome this drawback, we have the following few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6:

- Dual stack
- Tunneling
- Translation

- Dual Stack Mechanism

A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme. A dual stack node enables both IPv4 and IPv6 stacks and enables communication between applications with both IPv4 and IPv6 stacks.

Figure 11 depicts the dual stack mechanism:

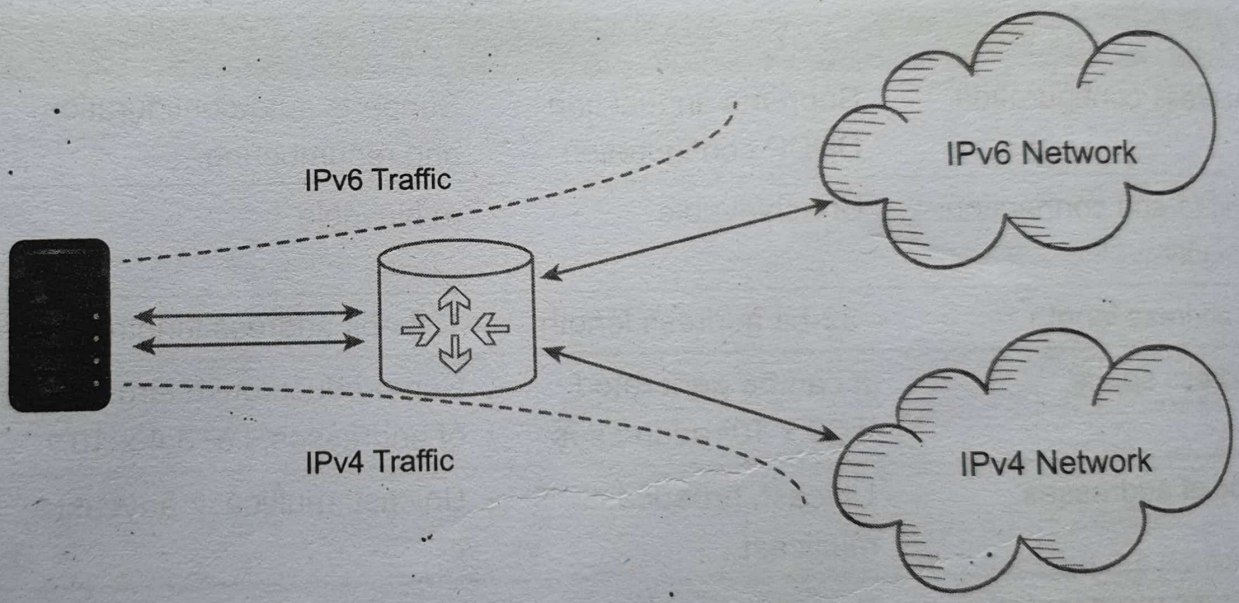


Figure 11: Dual Stack Mechanism

In the given diagram, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a dual stack router. The dual stack router can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.

- **Tunneling Mechanism**

The purpose of tunneling is to encapsulate packets of one type in packets of another type. When

transitioning to IPv6, tunneling encapsulates IPv6 packets in IPv4 packets, to minimise any dependencies during the transition, all the routers in the path between two IPv6 nodes do not need to support IPv6. This mechanism is called tunneling. Basically, IPv6 packets are placed inside IPv4 packets, which are routed through the IPv4 routers. The Figure 12 illustrates the tunneling mechanism through IPv4 routers:

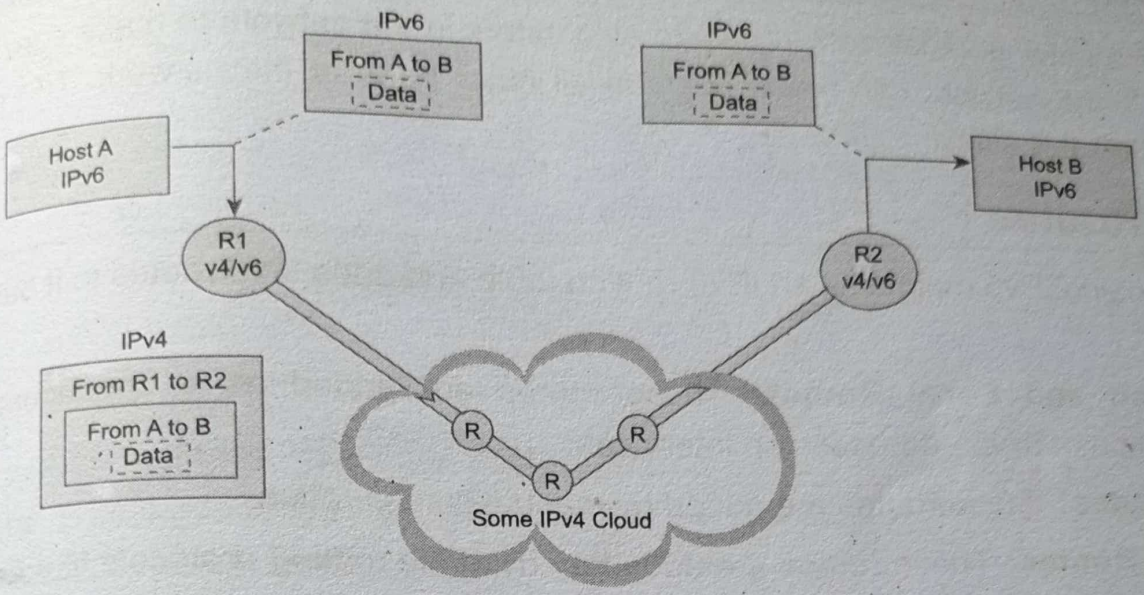


Figure 12: Tunneling Mechanism

The different uses of tunneling in the transition are as follows:

- Configured tunnels between two routers
- Automatic tunnels that terminate at the dual hosts

NAT Protocol Translation

A mechanism that translates one protocol to the other to facilitate communication between the two networks. This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. Figure 13 depicts the translation procedure:

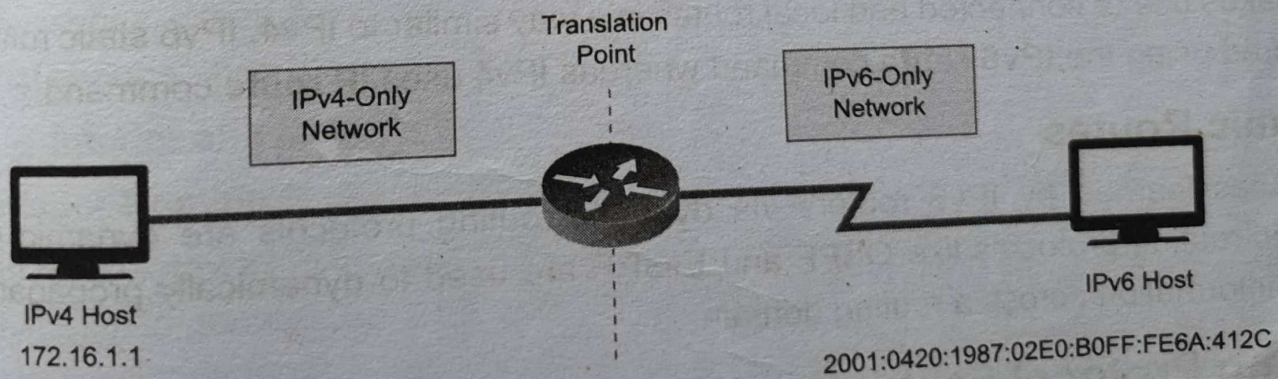


Figure 13: NAT Protocol Translation

A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router

Characteristics	IPV4	IPV6
Address configuration	Supports annual and DHCP configuration	Supports auto-configuration and renumbering
End-to-end connection integrity	Unachievable	Achievable
IP address length	32-bit address length	128 –bit address length
Address space	It can be generated 4.29×10^9 addresses	Can produce quite large number of addresses, i.e. 3.4×10^{38}
Type of addresses	Unicast, broadcast, multicast	Unicast, multicast, anycast
Address representation	Decimal	hexadecimal
Checksum field	Not available	Available
Fragmentation	Fragmentation is done by sending and forwarding routes	Fragmentation is done by the senders

Difference Between IPv4 and IPv6:

IPv4	IPv6
IPv4 has 32-bit address length	IPv6 has 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
In IPv4 Packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In IPv4 checksumfield is available	In IPv6 checksumfield is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed

5.4. Routing Protocols for Enterprise

All routing protocols support different features, including VLSM, summarisation, scalability, and fast convergence. The choice depends on many factors, and hence we choose the optimal out of the options. This section discusses the most common routing protocols for use within the enterprise and evaluates their suitability for given network requirements. Initially, the interior routing protocols EIGRP, OSPF, and Integrated IS-IS are discussed, followed by a description of BGP.

The topology of the network design are the deciding factors of routing protocols decided. Running multiple routing protocols might be necessary in large enterprise networks, for example, when a network is upgraded, the old routing protocol is backward compatible with the new one during the transition period. All routing protocols behave differently. Some attributes such as exchange of routing information, convergence times, metrics used for optimal route determination, required amount of processing power and memory, and availability of a routing protocol can determine whether a routing protocol is suitable for a particular network or not.

EIGRP (Enhanced Interior Gateway Routing Protocol)

Enhanced Interior Gateway Routing Protocol (EIGRP) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers. EIGRP is used on a router to share routes with other routers within the same autonomous system. Unlike other well-known routing protocols, such as RIP, EIGRP, etc. it only sends incremental updates, reducing the workload on the router and the amount of data that needs to be transmitted. EIGRP replaced the Interior Gateway Routing Protocol (IGRP) in 1993. One of the major reasons for this was the change to classless IPv4 addresses in the Internet Protocol, which IGRP could not support. EIGRP is a dynamic routing protocol by which routers automatically share route information. This eases the workload on a network administrator who does not have to configure changes to the routing table manually.

In addition to the routing table, EIGRP uses the following tables to store information:

- **Neighbour Table:** The neighbour table keeps a record of the IP addresses of routers that have a direct physical connection with this router. The routers that are connected to this router indirectly, through another router, are not recorded in this table as they are not considered neighbours.
- **Topology Table:** The topology table stores routes that it has learned from neighbour routing tables. Unlike a routing table, the topology table does not store all routes, but only those routes that have been determined by EIGRP. The topology table also records the metrics for each of the listed EIGRP routes, the feasible successor and the successors.

EIGRP supports the following features:

- Support for Classless Inter-Domain Routing (CIDR) and variable length subnet masking
- The ability to use different authentication passwords at different times
- Provides MD5 and SHA-2 authentication
- Support for load balancing on parallel links between sites
- Backwards compatibility with the IGRP routing protocols
- Sends topology changes, rather than sending the entire routing table, when a route is changed
- Periodically checks if a route is available, and propagates routing changes to neighbouring routers if any changes have occurred

EIGRP Metrics

EIGRP uses the minimum bandwidth on the path to a destination network and the total delay to compute routing metrics. Although you can configure other metrics, we do not recommend it, as it can cause routing loops in your network. The bandwidth and delay metrics are determined from values configured on the interfaces of routers in the path to the destination network.

Figure 19, Router One is computing the best path to Network A:

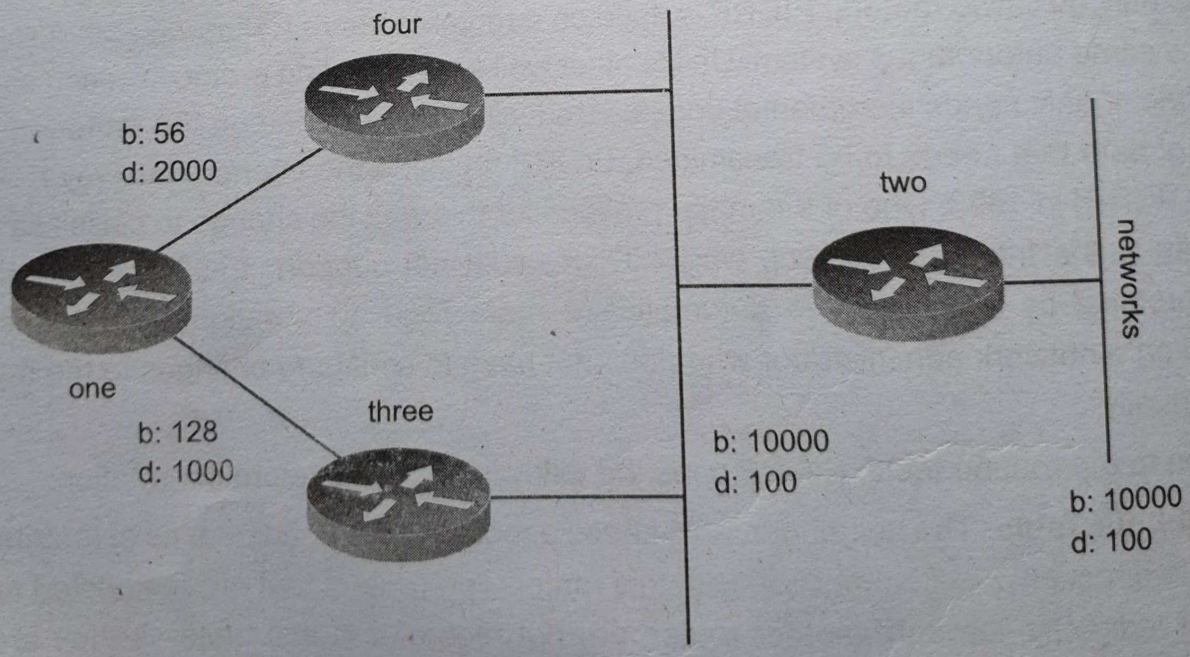


Figure 19: Example of EIGRP Network

...the two advertisements for this network: one through Router Four, with a

OSPF (Open Shortest Path First)

As discussed in the earlier part of this chapter, OSPF is an interior gateway protocol which uses link-state routing. It is used to allow routers to dynamically learn routes from other routers and to advertise routes to other routers. Advertisements containing routes are referred to as Link-State Advertisements (LSAs) in OSPF. OSPF router keeps track of the *state* of all the various network connections *(links)* between itself and a network it is trying to send data to. This makes it a *link-state* routing protocol. OSPF supports the use of classless IP address ranges and is very efficient. OSPF selects the best routes by finding the lowest cost paths to a destination. All router interfaces (links) are given a cost. The cost of a route is equal to the sum of all the costs configured on all the outbound links between the router and the destination network, plus the cost configured on the interface that OSPF received the Link-State Advertisement.

Figure 20 depicts the example of OSPF network:

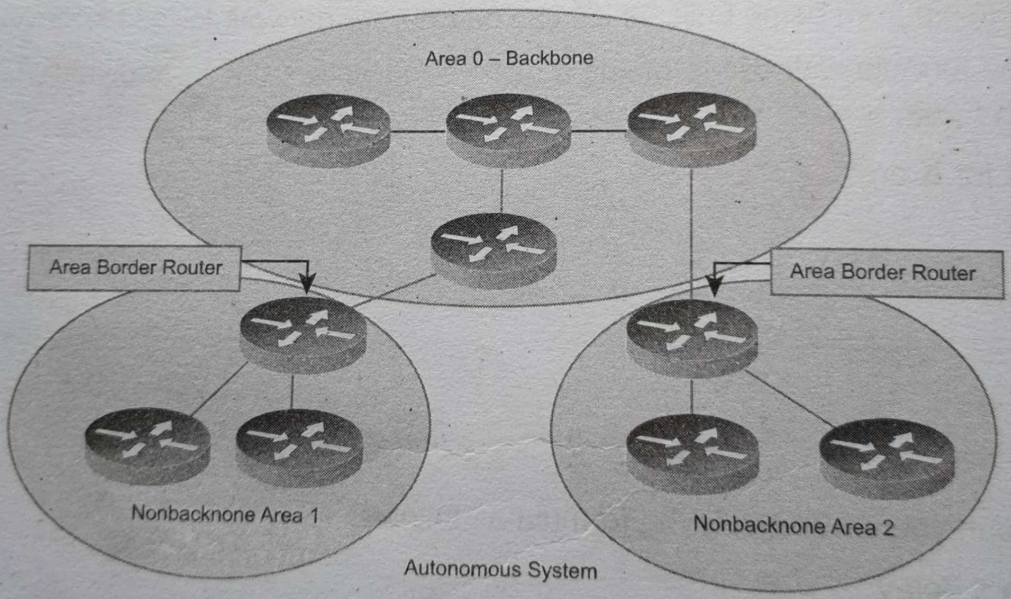


Figure 20: Example of OSPF Network

OSPF has the following features:

- It is effectively loop-free, having a maximum hop metric of 65,535.
- It can load balance network traffic between multiple paths of the same metric value.
- It supports authentication using passwords and other methods.
- It converges quicker than RIP since routing updates are sent immediately instead of periodically.

It uses less bandwidth since transmission take place only when routing changes occur.
It supports the logical grouping of network segments into areas.
It announces routes outside of an autonomous system within the autonomous system so that it can calculate costs to reach outside networks.
Since OSPF announces subnet masks, it supports CIDR, VLSM (Variable Length Subnetting), Supernetting (used to aggregate Class C networks) and non-contiguous network segments.

Intermediate System to Intermediate System (IS-IS)

Intermediate System to Intermediate System (IS-IS) is defined in ISO 10589. The IS-IS protocol is one of a family of IP Routing protocols and is an Interior Gateway Protocol (IGP) for the Internet, used to distribute IP routing information throughout a single Autonomous System (AS) in an IP network.IS-IS is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbours. The topology information is flooded throughout the AS, so that every router within the AS has a complete picture of the topology of the AS. This picture is then used to calculate end-to-end paths through the AS, normally using a variant of the Dijkstra's algorithm. Therefore, in a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.

In an IS-IS network, there are End Systems, Intermediate Systems, Areas and Domains. The end systems are user devices and the intermediate systems are routers. Routers are organised into local groups called 'areas' and several areas are grouped together into a 'domain'. IS-IS places area routers into Layer 1, and routers that interconnect the areas into Layer 2. IS-IS uses its own addressing scheme. The figure 21 shows the IS-IS Network:

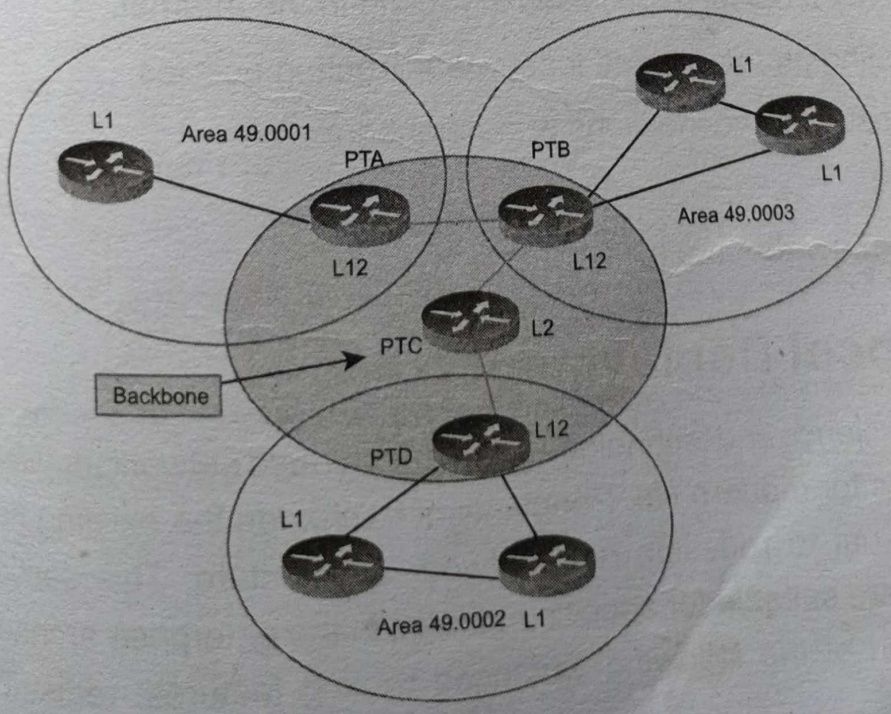


Figure 21: IS-IS Network

BGP (Border Gateway Protocol)

BGP is an interdomain routing protocol which means that you can use BGP to exchange routing information between autonomous systems. The primary function of BGP is to provide and exchange network-reachability information between domains or autonomous systems. BGP is a path vector protocol that is suited for setting routing policies between the autonomous systems. In the enterprise campus architecture, BGP is used in the Internet connectivity module. BGP is usually configured between two directly connected routers that belong to different autonomous systems. Each autonomous system is under different technical administration. BGP is frequently used to connect the enterprise to service providers and to interconnect service providers as shown in the figure 22:

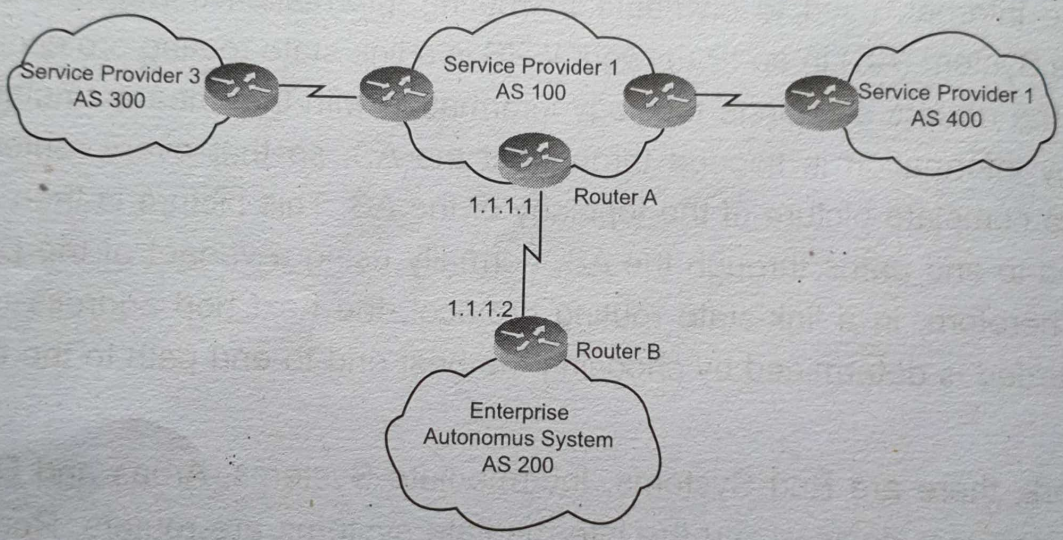


Figure 22: Example of BGP Network

The characteristics of BGP are as follows:

- BGP is an exterior gateway protocol (EGP) used in routing in the Internet.
- BGP is a path vector routing protocol suited for strategic routing policies.
- It uses TCP port 179 to establish connections with neighbours.
- BGPv4 implements CIDR.
- eBGP is used for external neighbours.

SDN 06 A

6.1. Understanding Software Defined Networking [SDN]

Software defined networking is a network technology where the control plane logic is decoupled from the forwarding plane and has the ability to control, change and manage the network behaviour dynamically through the software via open interfaces. Software defined networking (SDN) provides a different approach in network designing and its management. The nature of the conventional networking is static, even a small change in networking conditions would exact a high cost of re-configuring large number of switches, routers and other network resources . SDN Features

SDN focuses on the key features are listed as follows:

1. Separation of the control plane from the data plane
2. A centralised controller and view of the network
3. Open interfaces between devices in the control plane (controllers) and those in the data plane.

The advent in technology has created new trends and is causing the network providers and users to reconsider the traditional approaches for networking advancements.

SDN Architecture

The SDN architecture consists of three layers, the application layer, the control layer and the data or forwarding layer. Apart from this the fundamental SDN building blocks are the SDN switch (i.e. OpenFlow switch), the SDN controller, and the interfaces present on the controller for communication with forwarding devices, i.e. southbound interface (OpenFlow) and network applications interface (northbound interface)

SDN Application Plane: SDN application plane includes a variety of applications that interact with SDN controllers, programs that communicate behaviours and needed resources with the SDN Controller via application programming interface (APIs). In addition, the applications can build an abstract view of the network by collecting information from the controller for decision-making purposes. These applications can include networking management, analytics, or business applications which are used to run large data centers.

- **SDN Control Plane:** The SDN controller plane is a logical entity that receives instructions or requirements from the SDN application layer and relays them to the networking components. The controller also extracts information about the network from the hardware devices and communicates back to the SDN Applications with an abstract view of the network, including statistics and events about what is happening.
- **SDN Data Plane:** The SDN data plane consists of physical switches and virtual switches. In both the cases, the switches are responsible for forwarding packets. The SDN networking devices control the forwarding and data processing capabilities for the network. This includes forwarding and processing of the data path.

Figure 2 illustrates the communication path between the application, control and data layers:

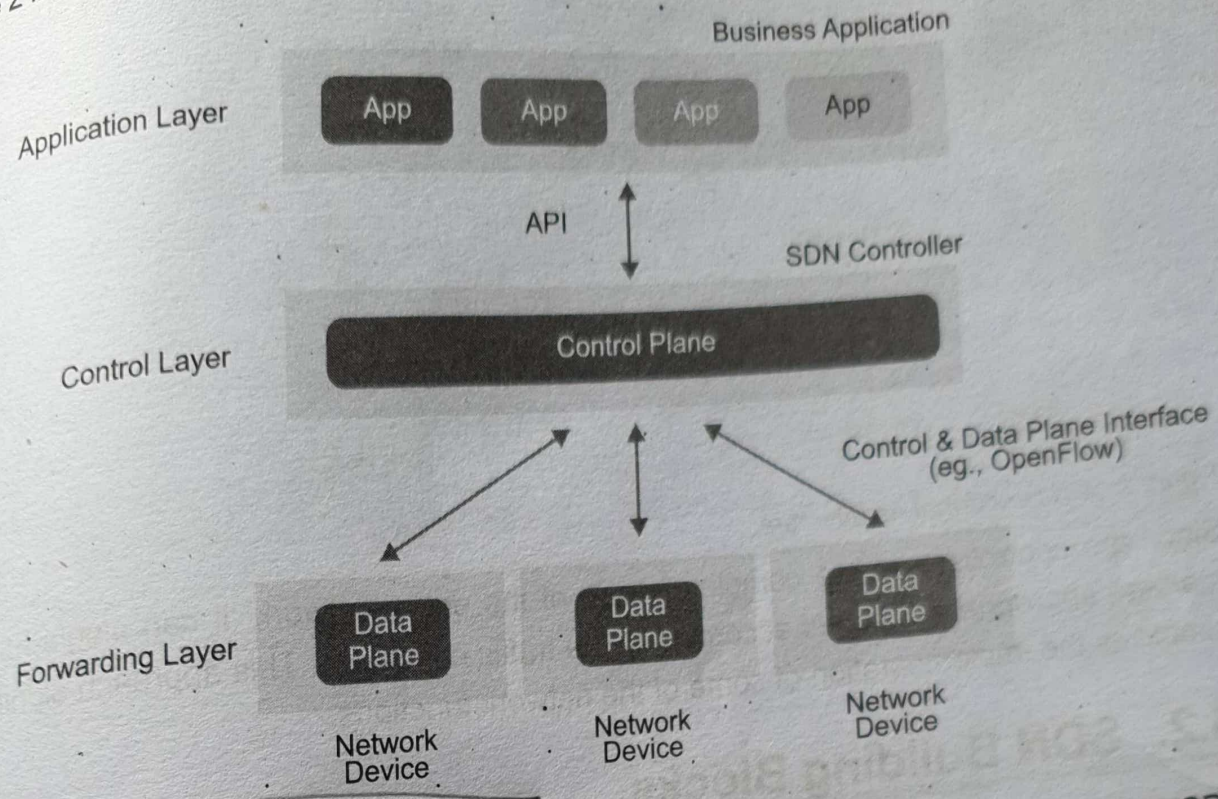


Figure 2: Software-Defined Network Architecture

Control plane applications such as load balancing at the application layer of the SDN architecture interact with the data plane through application programming interfaces (APIs). Both the application and control layers are implemented at the controller while the data layer which is implemented is distributed by the networking devices such as routers and switches. APIs are utilized to implement network services that are customized as per based on the application layer requirements (quality of service, access control, bandwidth management, energy management and etc.)

Figure 3 shows the SDN functional architecture:

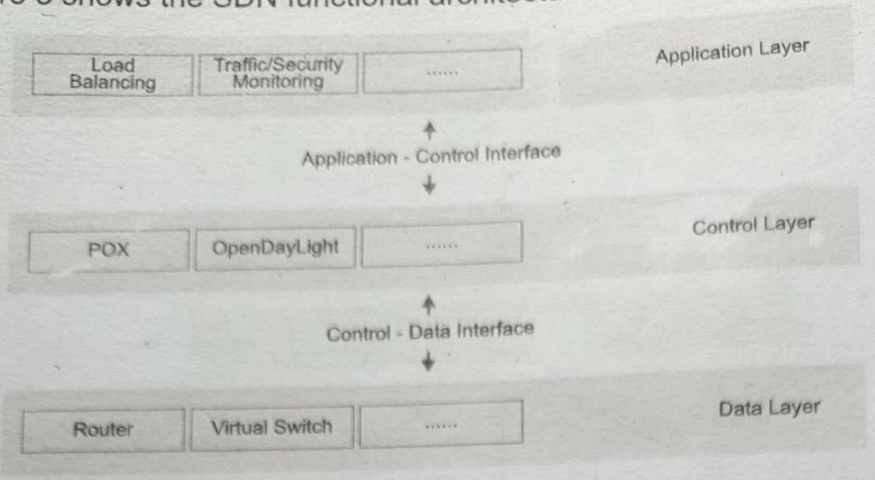


Figure 3: SDN Functional Architecture

Since the controller gains a complete vision of the entire network, it can single-handedly manage appropriate changes according to the traffic conditions. This approach significantly simplifies the implementation of some of the network functions.

6.2. SDN Building Blocks

As mentioned earlier the fundamental SDN building blocks are the SDN switch (i.e. OpenFlow switch), the SDN controller, and the interfaces present on the controller for communication with forwarding devices, i.e. southbound interface (OpenFlow) and network applications interface (northbound interface).

Figure 4 describes the building blocks of SDN:

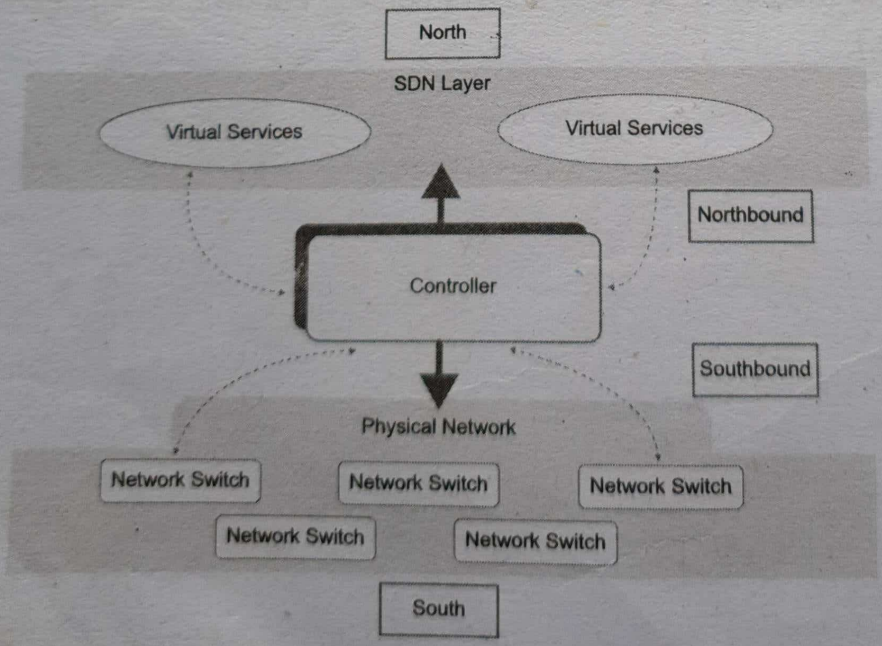


Figure 4: SDN Building Blocks and Interfaces

SDN architectures generally has three components or groups of functionalities which are as follows:

- **SDN Applications and Interfaces**: SDN applications are programs that communicate behaviors and needed resources with the SDN controller via application programming interfaces (APIs). The SDN architecture APIs are often referred to as the northbound and the southbound interfaces, defining the communication amongst the applications, the controllers, and the networking systems. The northbound interface is defined as the connection between the controller and the applications, whereas the Southbound interface is the connection between the controller and the physical networking hardware. Since SDN is a virtualised architecture, these elements do not have to be physically located at the same place. In addition, the applications can build an abstracted view of the network by collecting information from the controller for decision-making purposes. These applications could include networking management, analytics, or business applications used to run large data centers.
- **SDN Controller**: The SDN controller is a logical entity that receives instructions or requirements from the SDN application layer and relays them to the networking components. The controller also extracts information about the network from the hardware devices and communicates back to the SDN applications with an abstract view of the network, including statistics and events about what is happening.
- **SDN Networking Devices (OpenFlow Switch):** The SDN networking devices control the forwarding and data processing capabilities for the network. This includes forwarding and processing of the data path.

Multi Protocol Label Switching (MPLS) is an IP packet routing technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers. This feature helps in increasing the delivery rate of IP packets.

MPLS uses layer 3 service i.e, Internet Protocol, and uses router as forwarding device. The traffic of different customers is separated from each other because MPLS works somewhat like VPN. It does not work like regular VPN that encrypts the data but it ensures packet from one customer cannot be received by another customer. An MPLS header is added to packet that lies between layers 2 and 3. Hence, it is also considers to be *Layer 2.5 protocol.*

MPLS Header –
The MPLS Header is 32 bit long and is divided into four parts –

1. **Label –** This field is 20 bit long and can take value b/w 0 & $2^{20} - 1$.
2. **Exp –** They are 3 bits long and used for *Quality of Service (QoS)*.
3. **Bottom of stack (S) –** It is of size 1 bit. MPLS labels are stacked one over other. If there is only one label remained in MPLS header, then its value is 1 otherwise 0.
4. **Time to Live (TTL) –** It is 8 bit long and its value is decreased by one at each hop to prevent packet to get stuck in network.

Figure – MPLS Header

Multiprotocol Label Switching (MPLS) Routing :

Forwarding in MPLS :
LSRs receive IP packet CE and add an MPLS header in between layer 3 and layer 2 means it encapsulates the link-layer i.e, layer 2 frames. This feature allows LSRs to support receiving packets containing frames from different protocols like Frame Relay, Metro Ethernet, etc, that's why it is called multi-protocol.

MPLS forwarding is based on label attached to IP packet. This label attachment is regulated by protocol called Label Distribution Protocol(LDP). Each LSR initially learns routes as normal routers do. This learning starts with PE routers. Each PE router learns routes to different subnets from CE router. Suppose PE router PE1 learns route to subnet (say subnet1) from CE router. Now PE1 will add label to packet, forward to its neighboring LSR, and tells them that if you receive packet which destination address to subnet1 then forward it to me.

Again this process is repeated by this LSR. In this way, LSR learns routes and add this information in *Label Forwarding Information Base(LFIB)*. Now if any PE receives packet with destination to subnet1, then looking at labels and LFIB, LSRs can easily forward IP packet.

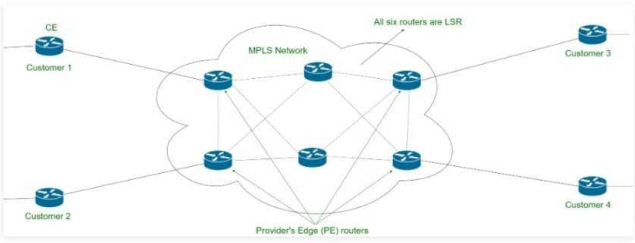


Figure – MPLS Network

Important terms used in MPLS :

Terms	Description
Provider Edge(PE) Router	Router at edge of MPLS network that add or remove label from IP packet.
Customer Edge(CE) Router	Router at edge of customer network that send or receive IP packet from PE.
Label Switch Router(LSR)	Routers used in MPLS network that can understand labels.
Ingress LSR	LSR routers that receive IP packet from CE Routers and add MPLS header.
Intermediate LSR	LSR routers that swap label in MPLS header and assigned for forwarding labeled IP packet.

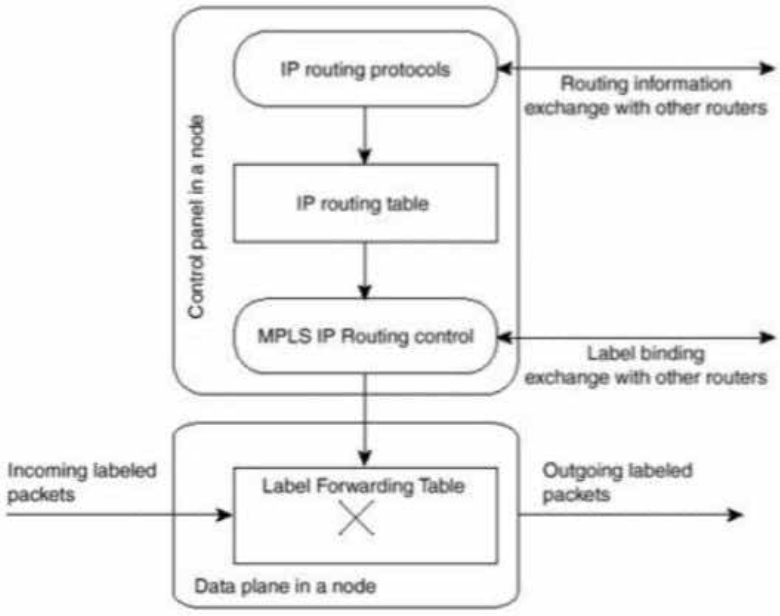
MPLS Services

■ **Traffic engineering:** MPLS allows traffic to be directed through a specific path, which might
be different from the least-cost path determined by the IP routing protocol. This ability to
define routes and resource utilization is known as traffic engineering.

■ **QoS support**: MPLS creates a connection-oriented network for IP traffic, thereby providing
the foundation for QoS traffic controls. For example, it might provide guaranteed bandwidth
to specific traffic between two locations.

■ Fast reroute (FRR): Because FRR allows extremely quick recovery from node or link
failure, it prevents applications from timing out and losing data.

■ MPLS VPNs: MPLS VPNs are much easier to deploy than traditional VPNs. They scale easily with increasing numbers of routes and customers and provide the same



level

Enterprise WAN Architecture Technologies

Various technologies are used in the WAN architecture to interoperate with a MAN as a single contiguous system. The WAN architecture is expected to support advanced business applications and services by providing security, reliability, availability, manageability, and QoS across the network. Let us discuss these technologies which span from a private network to the Internet, MPLS, and VPN.

Table 5 shows Enterprise WAN architecture technologies:

Table 5: Enterprise WAN Architecture Technologies

	Private WAN	ISP Service (Site-Site and Remote-Access (IPsec VPN))	SP MPLS and IP VPN	Self-Deployed MPLS
Secure transport	IPsec (optional)	IPsec (mandatory)	IPsec (mandatory)	IPsec (mandatory)
High availability	Excellent	Good	Excellent	Excellent
Multicast	Good	Good	Good	Excellent
Voice and video support	Excellent	Low	Excellent	Excellent
Scalable network growth	Moderate	Good	Excellent	Excellent
Easily Shared WAN links	Moderate	Moderate	Moderate	Excellent
Operational costs	High	Low	Moderate; depends on transport	Moderate to high
Network control	High	Moderate	Moderate	High
Effort to migrate from private WAN	Low	Moderate	Moderate	High

Private WAN

- Works on Frame Relay or ATM
- Provides encrypted private network using Digital Encryption Standard (DES), Triple DES (3DES) and Advanced Encryption Standard (AES)
- Suitable for enterprises expecting moderate growth, i.e. a smaller number of new branches over a longer time span
- Supports secure, reliable, and dedicated bandwidth
- Supports advanced business applications and services
- Not suitable for remote users, remote call agents, and teleworkers connectivity
- Expensive expenditure for physical media and transmission equipment buying, configuration and maintenance

IPS Service

- Site-to-site and remote-access IPsec VPN are examples of IPS service for WAN architecture technology
- Compliant with information security regulations
- IPsec VPNs are suitable for businesses requiring basic data connectivity
- IPsec VPNs support QoS for delay-sensitive applications
- Suitable for connecting a large number of remote users, remote call agents, and teleworkers
- Capability to connect remote sites spread over a large geographical area

MPLS-enabled IP VPN

- Supports network-based IP VPN
- Provides extended flexible and scalable connectivity
- Suitable for enterprises expecting high growth, i.e. adding a large number of new branches and remote offices in a short span of time
- Suitable for any to any connectivity (any branch connected to any other branch)
- Provides QoS for delay-sensitive applications such as voice and video
- Comparatively cheaper than a private network, providing secure and reliable connectivity for remote offices

Self-Deployed MPLS

- Supports network segmentation
- Logically separates the network
- Preferred for large enterprises
- Demands investment in network equipment and training
- Needs highly skilled staff to handle technical complexity

Figure 23 shows a sample Enterprise WAN architecture:

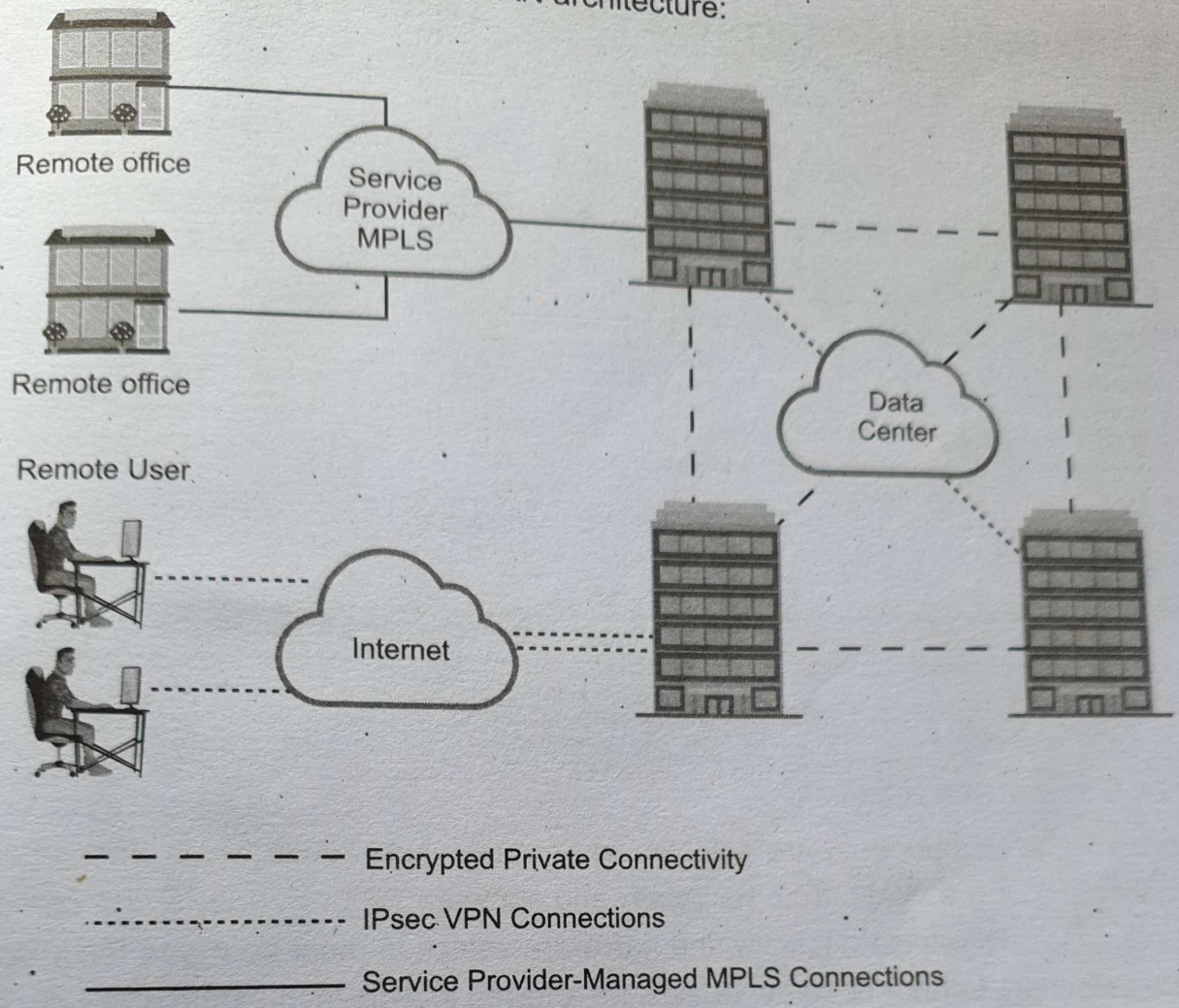


Figure 23: Sample Enterprise WAN Architecture

A combination of the aforementioned WAN technologies is used for connecting various offices, remote users and sites in an Enterprise WAN. As shown in Figure 23, the offices of an enterprise along with its data centre are connected using an encrypted private network. Service provider MPLS is used to connect remote offices with the enterprise offices. Remote users get access to the enterprise by the IPsec VPN connection laid over the Internet.