END MODULE 1

Q1) Explain CISCO Service Oriented Network Architecture (SONA) Framework in detail.

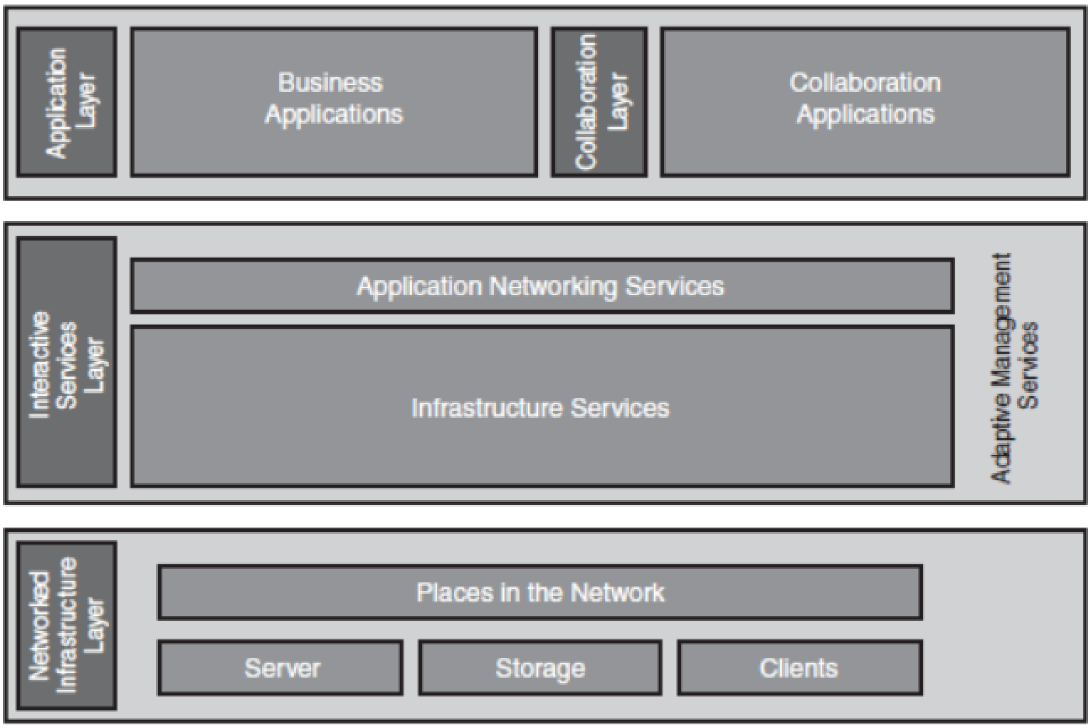
Ans)

SONA stands for Service Oriented Network Architecture. The Cisco SONA is an architectural framework that illustrates how to build integrated systems and guides the evolution of enterprises toward more intelligent networks. Using the SONA framework, enterprises can improve flexibility and increase efficiency by optimizing applications, business processes, and resources to enable IT to have a greater effect on business.

The SONA framework leverages the extensive product-line services, proven architectures, and experience of Cisco and its partners to help enterprises achieve their business goals.

In the SONA framework, the network is the common element that connects and enables all components of the IT infrastructure.

The SONA framework, shows how integrated systems can allow a dynamic, flexible architecture and provide for operational efficiency through standardization and virtualization.


Application Layer
Business Applications
Collaboration Layer
Collaboration Applications
Interactive Services Layer
Application Networking Services
Infrastructure Services
Adaptive Management Services
Networked Infrastructure Layer
Places in the Network
Server
Storage
Clients

igure 1.1: Cisco SONA (Service Oriented Network Architecture) Framework

The SONA framework defines the following three layers:

Networked Infrastructure layer: Where all the IT resources are interconnected across a converged network foundation. The IT resources include servers, storage, and clients. The Networked Infrastructure layer represents how these resources exist in different places in the network, including the campus, branch, data center, enterprise edge, WAN, metropolitan-area network (MAN), and with the teleworker. The objective of this layer is to provide connectivity, anywhere and anytime. The Networked Infrastructure layer includes the network devices and links to connect servers, storage, and clients in different places in the network.

Interactive Services layer: Includes both application networking services and infrastructure services. This layer enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure. This layer includes the following services:

- Voice and collaboration services
- Mobility services
- Wireless services
- Security and identity services
- Storage services
- Compute services
- Application networking services (content networking services)
- Network infrastructure virtualization
- Adaptive network management services
- Quality of service (QoS)
- High availability
- IP multicast

Application layer: This layer includes business applications and collaboration applications. The objective of this layer is to meet business requirements and achieve efficiencies by leveraging the interactive services layer. This layer includes the following collaborative applications:

- Instant messaging
- Cisco Unified Contact Center
- Cisco Unity (unified messaging)
- Cisco IP Communicator and Cisco Unified IP Phones
- Cisco Unified MeetingPlace
- Video delivery using Cisco Digital Media System
- IP telephony.

The benefits of SONA include the following:

- Functionality: Supports the organizational requirements.

- Scalability: Supports growth and expansion of organizational tasks by separating functions and products into layers; this separation makes it easier to grow the network.
- Availability: Provides the necessary services, reliably, anywhere, anytime.
- Performance: Provides the desired responsiveness, throughput, and utilization on a perapplication basis through the network infrastructure and services.
- Manageability: Provides control, performance monitoring, and fault detection.
- Efficiency: Provides the required network services and infrastructure with reasonable operational costs and appropriate capital investment on a migration path to a more intelligent network, through step-by-step network services growth.
- Security: Provides for an effective balance between usability and security while protecting information assets and infrastructure from inside and outside threats.

Q2) Compare the top-down vs bottom-up network design approach.

Ans)

Bottom-Up Approach to Network Design

One of the ways to design a network is to start from the bottom of the OSI model i.e. physical, data link and network layer requirements. In this, the focus is on selecting network devices and technologies to be used rather than applications and services to be provided. Mostly, experienced designers have the expertise to design a network using the bottom-up approach. This is the preferred approach for quick response to a design request. There remains a possibility that business requirements are not always met through the bottom-up approach network design which results in costly network design.

Top-Down Approach to Network Design

As the name suggests, in this approach, the focus is on the big picture. In this, designing starts from the top OSI model. Initially, requirements of upper layers (application, presentation and session layers) are worked upon and then lower layers are designed to support functionalities of the upper layer. That is, customer requirements are thoroughly analysed to determine the services and applications expected from the network to be designed. To fulfil the network services required by the application, the decision is made regarding the network infrastructure which includes type, spreed, cost, capacity, etc. of routers, switches and media. Network Infrastructure is also influenced by scalability requirements, protocol behaviour and many other factors. All these factors needed to be considered while designing the network. Thus, in the top-down approach network design, applications and services required to drive the design of the physical infrastructure.

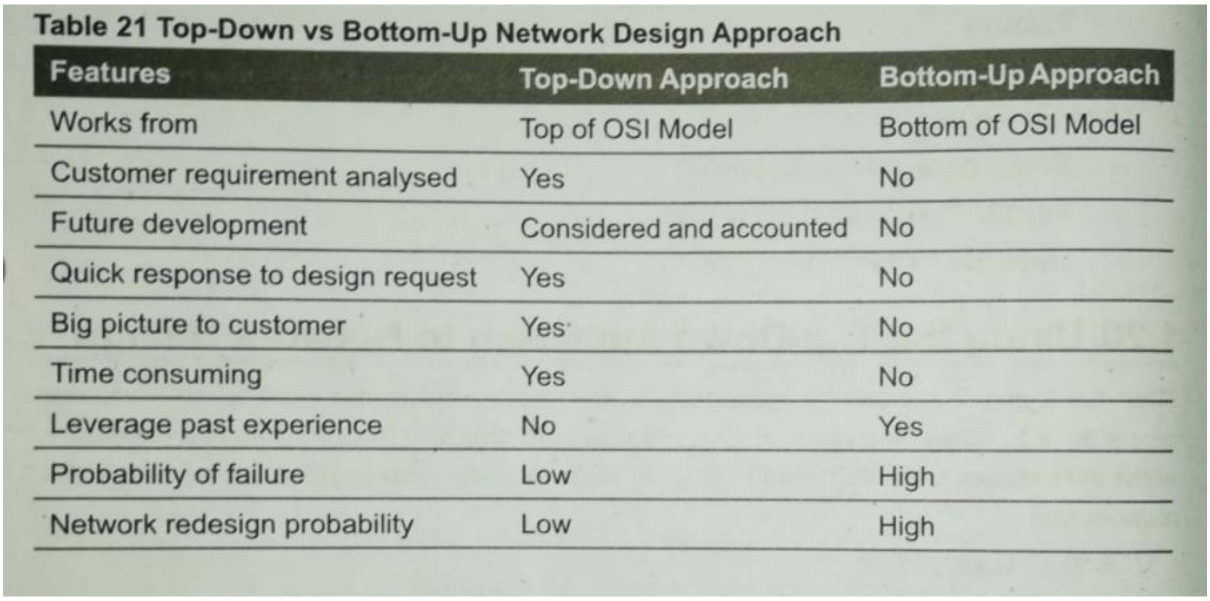
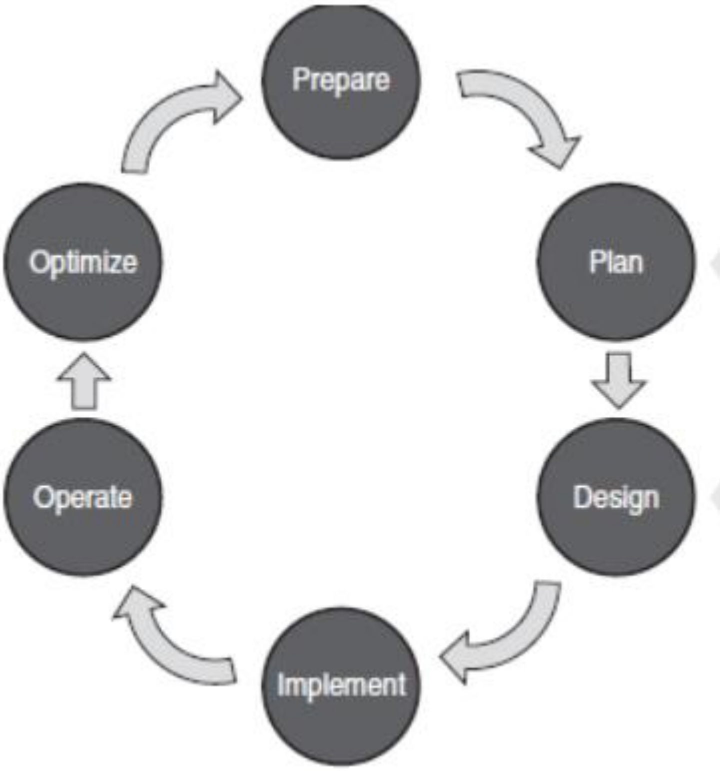


Table 21 Top-Down vs Bottom-Up Network Design Approach

Features	Top-Down Approach	Bottom-Up Approach
Works from	Top of OSI Model	Bottom of OSI Model
Customer requirement analysed	Yes	No
Future development	Considered and accounted	No
Quick response to design request	Yes	No
Big picture to customer	Yes	No
Time consuming	Yes	No
Leverage past experience	No	Yes
Probability of failure	Low	High
Network redesign probability	Low	High

Q3) Explain different phases in PPDIOO Network Lifecycle.

Ans)



igure: PPDIOO Network Lifecycle Influences Design

The above diagram depicts the phases in the network’s lifecycle which are part of PPDIOO methodology. All six phases are closely related to each other.

1. **Prepare Phase**

- Establish business requirements
- Develop a network strategy
- Propose a high level conceptual architecture
- Identify technologies that support 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 requirement.
- 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 additional required 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.

Benefits of PPDIOO on Network Design Methodology

- Lowering the total cost of network ownership
- Identifying and validating technology requirements
- Planning for infrastructure changes and resource requirements
- Accelerating successful implementation
- Increasing network availability
- Assessing the state of the network’s security and its ability to support the proposed design
- Specifying the correct set of hardware and software releases and keeping them operational and current
- Producing a sound operational design and validating network operation

- Improving business agility
- Establishing business requirements and technology strategies
- Readying sites to support the system to be implemented
- Expertly installing, configuring, and integrating system components
- Accelerating access to applications and services
- Assessing and improving operational preparedness to support current and planned network technologies and services
- Improving service-delivery efficiency and effectiveness by increasing availability, resource capacity, and performance

Q4) List and explain network design methodology steps.

Ans)

Design methodology refers to a systematic way of designing the network even in tight time constraints. A better approach is to follow well-defined framework to deliver network design deliverables.

Three simple steps for the design methodology are as listed below -

1. **Identify customer requirements**

In this step, which is typically completed during the PPDIOO Prepare phase, key decision makers identify the initial requirements. Based on these requirements, a high-level conceptual architecture is proposed.

2. Characterize the existing network and sites

The Plan phase involves characterizing sites and assessing any existing networks, and performing a gap analysis to determine whether the existing system infrastructure, sites, and operational environment can support the proposed system.

Characterization of the existing network and sites includes site and network audit and network analysis. During the network audit, the existing network is thoroughly checked for integrity and quality. During the network analysis, network behavior (traffic, congestion, and so forth) is analyzed.

3. Design the network topology and solutions

In this step, the detailed design of the network is created. Decisions are made about networked infrastructure, infrastructure services, and applications. The data for making these decisions is gathered during the first two steps.

When the design is complete, the design implementation process is executed; this process includes the following steps:

1. **Plan the implementation**

During this step, the implementation procedures are prepared in advance to expedite and clarify the actual implementation. Cost assessment is also undertaken at this time. This step is performed during the PPDIOO Design phase.

2. **Implement and verify the design**

The actual implementation and verification of the design take place during this step by building a network. This step maps directly to the Implement phase of the PPDIOO methodology.

3. **Monitor and optionally redesign**

The network is put into operation after it is built. During operation, the network is constantly monitored and checked for errors. If troubleshooting problems become too frequent or even impossible to manage, a network redesign might be required; this can be avoided if all previous steps have been completed properly. This step is, in fact, a part of the Operate and Optimize phases of the PPDIOO methodology.

END MODULE 2

Network Hierarchy

Page Number 81 | Ques10

This section explains the hierarchical network model, which is composed of the access, distribution, and core layers. The functions generally associated with each of these layers are discussed, as is the most common approach to designing a hierarchical network. Historically used in the design of enterprise local-area network and wide-area network data networks, this model works equally well within the functional modules of the Cisco Enterprise Architecture. These modules are discussed later in this chapter, in the section “Using a Modular Approach to Network Design.”

Hierarchical Network Model

The hierarchical network model provides a framework that network designers can use to help ensure that the network is flexible and easy to implement and troubleshoot. Hierarchical Network Design Layers As shown in below Figure, the hierarchical network design model consists of three layers:

1. The access layer provides local and remote workgroup or user access to the network.
2. The distribution layer provides policy-based connectivity.
3. The core (or backbone) layer provides high-speed transport to satisfy the connectivity and transport needs of the distribution layer devices.

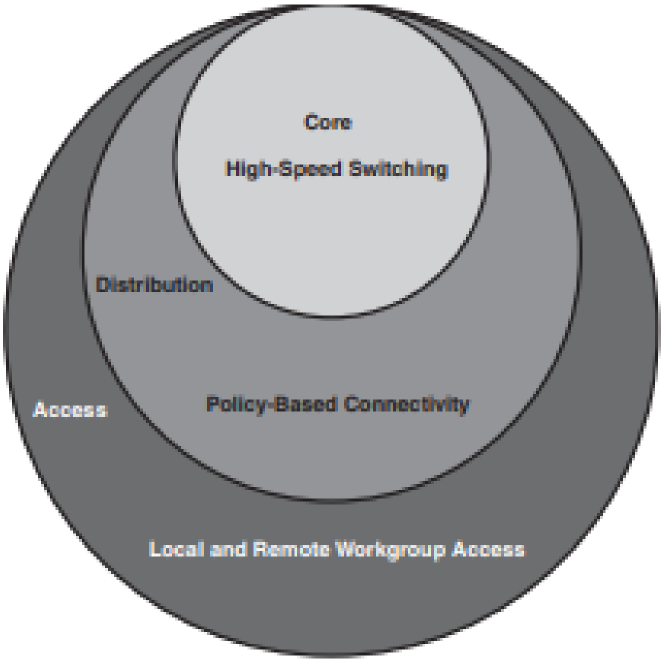


Figure: Hierarchical Model's Three Layers

Each hierarchical layer focuses on specific functions, thereby allowing the network designer to choose the right systems and features based on their function within the model. This approach helps provide more accurate capacity planning and minimize total costs. Below Figure illustrates a sample network showing the mapping to the hierarchical model's three layers.

Sample Network Designed Using the Hierarchical Model

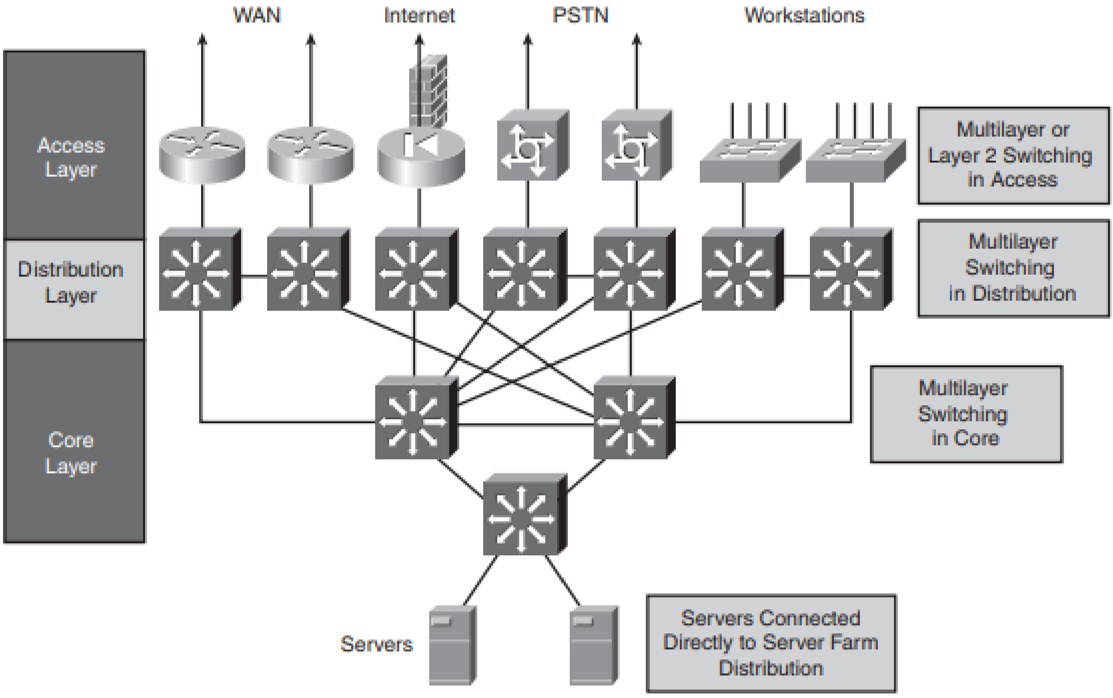

WAN
Internet
PSTN
Workstations
Access Layer
Distribution Layer
Core Layer
Multilayer or Layer 2 Switching in Access
Multilayer Switching in Distribution
Multilayer Switching in Core
Servers
Servers Connected Directly to Server Farm Distribution

Figure: Sample Network Designed Using the Hierarchical Model

Access Layer Functionality

This section describes the access layer functions and the interaction of the access layer with the distribution layer and local or remote users.

The Role of the Access Layer

The access layer is the concentration point at which clients access the network. Access layer devices control traffic by localizing service requests to the access media. The purpose of the access layer is to grant user access to network resources.

Following are the access layer's characteristics:

1. In the campus environment, the access layer typically incorporates switched LAN devices with ports that provide connectivity for workstations and servers.
2. In the WAN environment, the access layer for teleworkers or remote sites provides access to the corporate network across some wide-area technology, such as Frame Relay, Multiprotocol Label Switching (MPLS), Integrated Services Digital Network, leased lines, Digital Subscriber Line (DSL) over traditional telephone copper lines, or coaxial cable.
3. So as not to compromise network integrity, access is granted only to authenticated users or devices (such as those with physical address or logical name authentication). For example, the devices at the access layer must detect whether a telecommuter who is dialing in is legitimate, yet they must require minimal authentication steps for the telecommuter.

Layer 2 and Multilayer Switching in the Access Layer

Access can be provided to end users as part of either a Layer 2 (L2) switching environment or a multilayer switching environment.

Using Layer 2 Switching in the Access Layer

Access to local workstations and servers can be provided using shared or switched media LANs; VLANs may be used to segment the switched LANs. Each LAN or VLAN is a single broadcast domain.

The access layer aggregates end-user switched 10/100 ports and provides Fast Ethernet, Fast EtherChannel, and Gigabit Ethernet uplinks to the distribution layer to satisfy connectivity requirements and reduce the size of the broadcast domains. You can deploy multiple VLANs, each with its own IP subnet and its own instance of Spanning Tree Protocol (STP) providing alternative paths in case of failure. In this case, Layer 2 trunking (typically using the Institute for Electrical and Electronic Engineers [IEEE] 802.1Q trunking protocol) is used between the access layer switches and the distribution layer switches, with per-VLAN STP on each uplink for load balancing and redundancy, and with a distribution layer multilayer switch providing the inter- VLAN communication for the access layer.

In small networks, the access layer is often collapsed into the distribution layer; in other words, one device might handle all functions of the access and distribution layers.

Using Multilayer Switching in the Access Layer

The most common design for remote users is to use multilayer switches or routers. A multilayer switch, or router, is the boundary for broadcast domains and is necessary for communicating between broadcast domains (including VLANs). Access routers provide access to remote office environments using various wide-area technologies combined with multilayer features, such as route propagation, packet filtering, authentication, security, Quality of Service (QoS), and so on. These technologies allow the network to be optimized to satisfy a particular user's needs. In a dialup connection environment, dial-on-demand routing (DDR) and static routing can be used to control costs.

Below Figure illustrates a sample network in which the campus access layer aggregates end users and provides uplinks to the distribution layer. The access layer switches are dual-attached to the distribution layer switches for high availability.

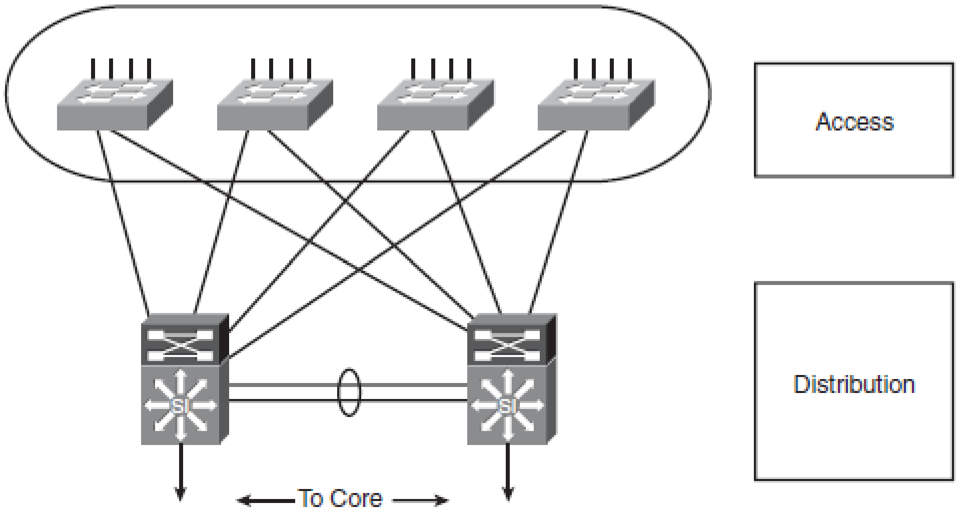


Figure: Access Layer Connectivity in a Campus LAN

The access layer can support convergence, high availability, security, QoS, and IP multicast. Some services found at the access layer include establishing a QoS trust boundary, broadcast suppression, and Internet Group Management Protocol (IGMP) snooping.

Distribution Layer Functionality

This section describes distribution layer functions and the interaction of the distribution layer with the core and access layers.

The Role of the Distribution Layer

The distribution layer represents both a separation between the access and core layers and a connection point between the diverse access sites and the core layer. The distribution layer determines department or workgroup access and provides policy-based connectivity.

Following are the characteristics of the distribution layer:

1. Distribution layer devices control access to resources that are available at the core layer and must therefore use bandwidth efficiently.
2. In a campus environment, the distribution layer aggregates wiring closet bandwidth by concentrating multiple low-speed access links into a high-speed core link and using switches to segment workgroups and isolate network problems to prevent them from affecting the core layer.

3. Similarly, in a WAN environment, the distribution layer aggregates WAN connections at the edge of the campus and provides policy-based connectivity.
4. This layer provides redundant connections for access devices. Redundant connections also provide the opportunity to load-balance between devices.
5. The distribution layer represents a routing boundary between the access and core layers and is where routing and packet manipulation are performed.
6. The distribution layer allows the core layer to connect diverse sites while maintaining high performance. To maintain good performance in the core, the distribution layer can redistribute between bandwidth-intensive access-layer routing protocols and optimized core routing protocols. Route filtering is also implemented at the distribution layer.
7. The distribution layer can summarize routes from the access layer to improve routing protocol performance. For some networks, the distribution layer offers a default route to access-layer routers and runs dynamic routing protocols only when communicating with core routers.
8. The distribution layer connects network services to the access layer and implements policies for QoS, security, traffic loading, and routing. For example, the distribution layer addresses different protocols' QoS needs by implementing policy-based traffic control to isolate backbone and local environments. Policy-based traffic control prioritizes traffic to ensure the best performance for the most time-critical and time-dependent applications.
9. The distribution layer is often the layer that terminates access layer VLANs (broadcast domains); however, this can also be done at the access layer.
10. This layer provides any media transitions (for example, between Ethernet and ATM) that must occur.

Distribution Layer Example

Below Figure shows a sample network with various features of the distribution layer highlighted.

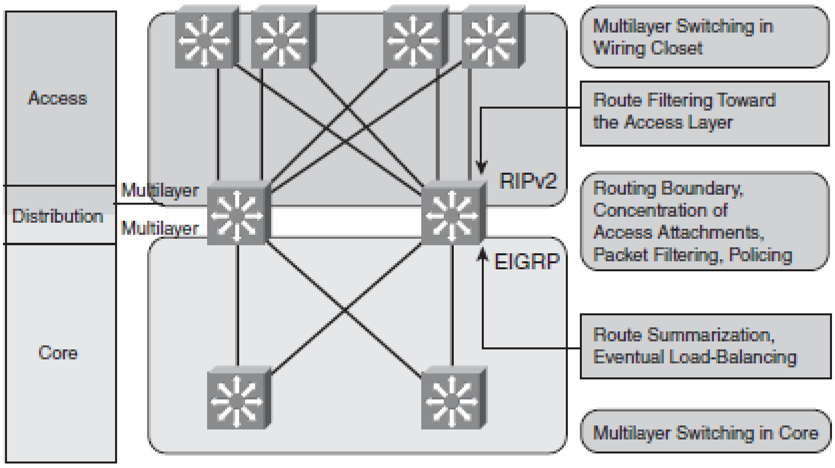

Access
Distribution
Core
Multilayer
Multilayer
RIPv2
EIGRP
Multilayer Switching in Wiring Closet
Route Filtering Toward the Access Layer
Routing Boundary, Concentration of Access Attachments, Packet Filtering, Policing
Route Summarization, Eventual Load-Balancing
Multilayer Switching in Core

Figure: Example of Distribution Layer Features

Multilayer switching is used toward the access layer (and, in this case, within the access layer).

1. Multilayer switching is performed in the distribution layer and extended toward the core layer.
2. The distribution layer performs two-way route redistribution to exchange the routes between the Routing Information Protocol version 2 (RIPv2) and Enhanced Interior Gateway Routing Protocol (EIGRP) routing processes.
3. Route filtering is configured on the interfaces toward the access layer.
4. Route summarization is configured on the interfaces toward the core layer.
5. The distribution layer contains highly redundant connectivity, both toward the access layer and toward the core layer.

Core Layer Functionality

This section describes core layer functions and the interaction of the core layer with the distribution layer.

The Role of the Core Layer

1. The function of the core layer is to provide fast and efficient data transport. Characteristics of the core layer include the following:
2. The core layer is a high-speed backbone that should be designed to switch packets as quickly as possible to optimize communication transport within the network.
3. Because the core is critical for connectivity, core layer devices are expected to provide a high level of availability and reliability. A fault-tolerant network design ensures that failures do not have a major impact on network connectivity. The core must be able to accommodate failures by rerouting traffic and responding quickly to changes in network topology. The core must provide a high level of redundancy. A full mesh is strongly suggested, and at least a well connected partial mesh with multiple paths from each device is required.
4. The core layer should not perform any packet manipulation, such as checking access lists or filtering, which would slow down the switching of packets.
5. The core layer must be manageable.
6. The core devices must be able to implement scalable protocols and technologies, and provide alternative paths and load balancing.

Switching in the Core Layer

Layer 2 switching or multilayer switching (routing) can be used in the core layer. Because core devices are responsible for accommodating failures by rerouting traffic and responding quickly to network topology changes, and because performance for routing in the core with a multilayer switch incurs no cost, most implementations have multilayer switching in the core layer. The core layer can then more readily implement scalable protocols and technologies, and provide alternate paths and load balancing.

Below Figure shows an example of Layer 2 switching in the campus core.

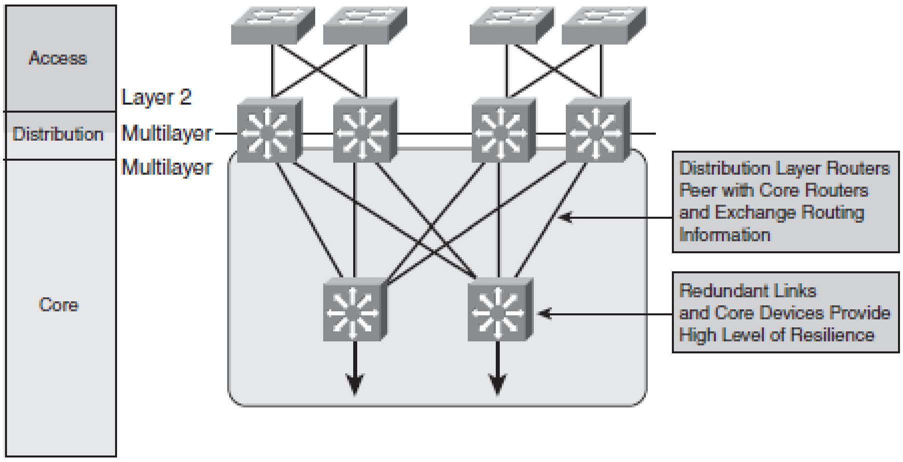

Access
Layer 2
Distribution
Multilayer
Multilayer
Core
Distribution Layer Routers Peer with Core Routers and Exchange Routing Information
Redundant Links and Core Devices Provide High Level of Resilience

Figure: Layer 2 Switching in the Campus Core

In Figure, a typical packet between access sites follows these steps:

1. The packet is Layer 2–switched toward a distribution switch.
2. The distribution switch performs multilayer switching toward a core interface.
3. The packet is Layer 2–switched across the LAN core.
4. The receiving distribution switch performs multilayer switching toward an access layer LAN.
5. The packet is Layer 2–switched across the access layer LAN to the destination host.

Figure shows an example of multilayer switching in the campus core.

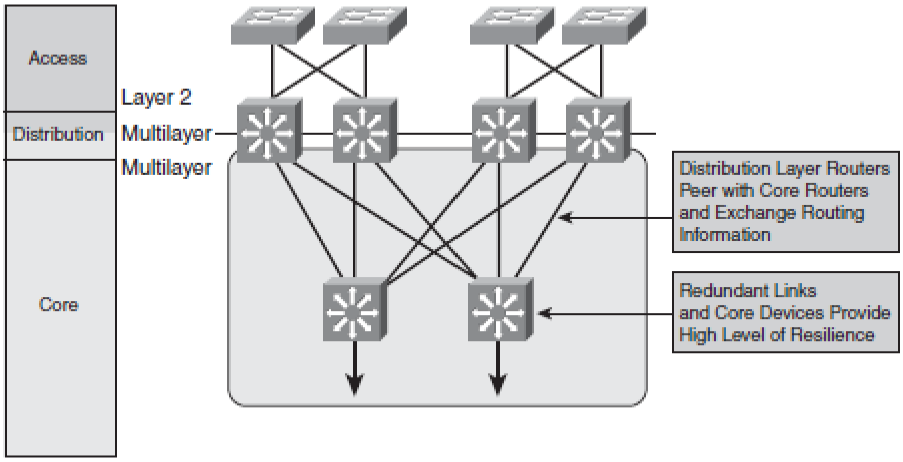

Access
Layer 2
Distribution
Multilayer
Multilayer
Core
Distribution Layer Routers Peer with Core Routers and Exchange Routing Information
Redundant Links and Core Devices Provide High Level of Resilience

Figure: Multilayer Switching in the Campus Core

In figure, A typical packet between access sites follows these steps:

1. The packet is Layer 2–switched toward a distribution switch.
2. The distribution switch performs multilayer switching toward a core interface.
3. The packet is multilayer-switched across the LAN core.
4. The receiving distribution switch performs multilayer switching toward an access LAN.

5. The packet is Layer 2–switched across the access layer LAN to the destination host.

Modular Approach

Cisco SONA Framework

Page Number 90 | Ques10

The Cisco SONA is an architectural framework that illustrates how to build integrated systems and guides the evolution of enterprises toward more intelligent networks. Using the SONA framework, enterprises can improve flexibility and increase efficiency by optimizing applications, business processes, and resources to enable IT to have a greater effect on business.

The SONA framework leverages the extensive product-line services, proven architectures, and experience of Cisco and its partners to help enterprises achieve their business goals.

In the SONA framework, the network is the common element that connects and enables all components of the IT infrastructure.

The SONA framework, shown in Figure 1.1, shows how integrated systems can allow a dynamic, flexible architecture and provide for operational efficiency through standardization and virtualization.

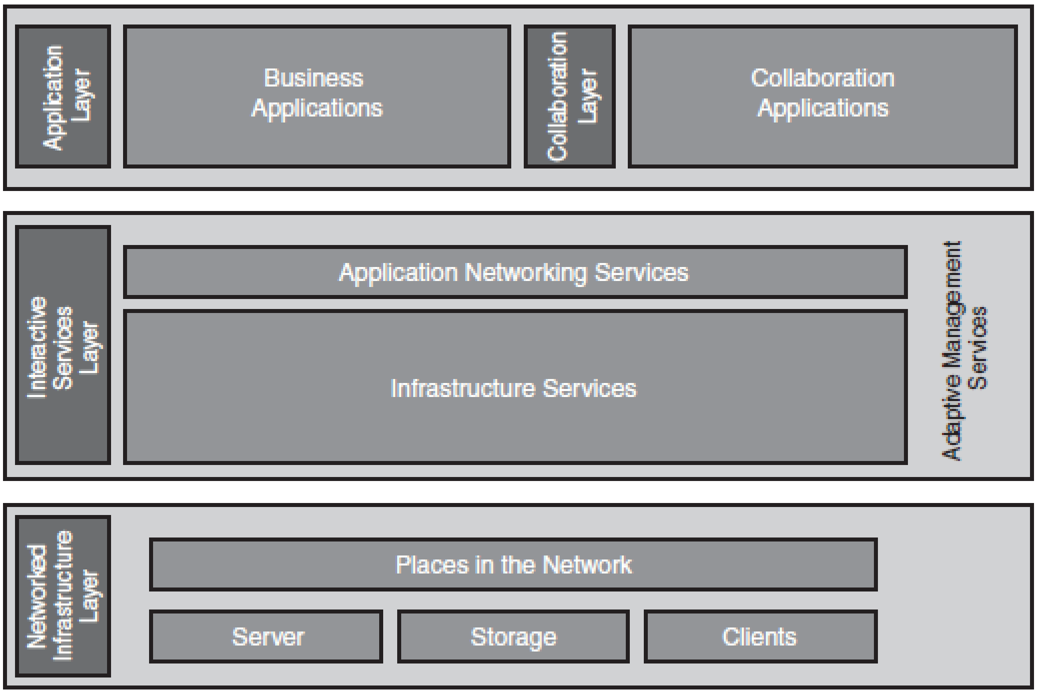

Application Layer
Business Applications
Collaboration Layer
Collaboration Applications
Interactive Services Layer
Application Networking Services
Infrastructure Services
Adaptive Management Services
Networked Infrastructure Layer
Places in the Network
Server
Storage
Clients

Figure 1.1: Cisco SONA (Service Oriented Network Architecture) Framework

The SONA framework defines the following three layers:

Networked Infrastructure layer

Where all the IT resources are interconnected across a converged network foundation. The IT resources include servers, storage, and clients.

The Networked Infrastructure layer represents how these resources exist in different places in the network, including the campus, branch, data center, enterprise edge, WAN, metropolitan-area network (MAN), and with the teleworker. The objective of this layer is to provide connectivity, anywhere and anytime.

The Networked Infrastructure layer includes the network devices and links to connect servers, storage, and clients in different places in the network.

Interactive Services layer

Includes both application networking services and infrastructure services. This layer enables efficient allocation of resources to applications and business processes delivered through the networked infrastructure.

This layer includes the following services:

1. Voice and collaboration services
2. Mobility services
3. Wireless services
4. Security and identity services
5. Storage services
6. Compute services
7. Application networking services (content networking services)
8. Network infrastructure virtualization
9. Adaptive network management services
10. Quality of service (QoS)
11. High availability
12. IP multicast

Application layer

This layer includes business applications and collaboration applications. The objective of this layer is to meet business requirements and achieve efficiencies by leveraging the interactive services layer.

This layer includes the following collaborative applications:

1. Instant messaging
2. Cisco Unified Contact Center
3. Cisco Unity (unified messaging)
4. Cisco IP Communicator and Cisco Unified IP Phones
5. Cisco Unified MeetingPlace

6. Video delivery using Cisco Digital Media System
7. IP telephony.

The benefits of SONA include the following:

1. Functionality: Supports the organizational requirements.
2. Scalability: Supports growth and expansion of organizational tasks by separating functions and products into layers; this separation makes it easier to grow the network.
3. Availability: Provides the necessary services, reliably, anywhere, anytime.
4. Performance: Provides the desired responsiveness, throughput, and utilization on a per application basis through the network infrastructure and services.
5. Manageability: Provides control, performance monitoring, and fault detection.
6. Efficiency: Provides the required network services and infrastructure with reasonable operational costs and appropriate capital investment on a migration path to a more intelligent network, through step-by-step network services growth.
7. Security: Provides for an effective balance between usability and security while protecting information assets and infrastructure from inside and outside threats.

Cisco Enterprise Architecture

Detailed Explanation on Page Number 90

Enterprise Campus

Enterprise Edge

Enterprise Data Centre

Enterprise Branch

Enterprise Teleworker

Service Provider

Guidelines for Creating an Enterprise Network

Detailed Explanation on Page Number 93

Enterprise Campus

1. Campus Infrastructure Module

a. Building Access Layer

b. Building Distribution Layer

c. Campus Core Layer

2. Server Farm Module

Enterprise Edge

1. Ecommerce Module

a. Application Servers

b. Database Servers

c. Firewalls

d. Host-based intrusion protection system

e. Network intrusion detection

f. Web Server

2. Internet Connectivity Module

. SMTP Mail Servers

a. DNS Servers

b. Public Servers

c. Firewalls

d. Edge Routers

3. Remote Access and VPN Module

. Dial-in Access Concentrators

a. Firewalls

b. Network intrusion detection system

4. WAN and MAN and Site to Site VPN Module

Detailed Explanation on Page Number 101

Service Provider

1. Internet Service Provider Module
2. PSTN Module
3. Frame Relay ATM Module

Remote Enterprise

1. Enterprise Branch
2. Enterprise Data Center
3. Enterprise Teleworker

END MODULE 3

1. What are the various factors to design an Enterprise Campus? Explain each one in detail.

(FIRST PART OF THE ANSWER)

The Enterprise Campus network is the foundation for enabling business applications, enhancing productivity, and providing a multitude of services to end users. The following three characteristics should be considered when designing the campus network:

- Network application characteristics
- Environmental characteristics
- Infrastructure device characteristics

(SECOND PART OF THE ANSWER)

Environmental characteristics:

A campus may include one building or many buildings. The count of buildings as well as to distance between these buildings matters while designing the network. Also, the number of end users, location of the end users and distance among them influence the network design .The same holds true for hosts and network devices. Apart from geographical conditions, transmission media used to connect nodes also influence the network design. Distance and bandwidth are a major deciding factor to select transmission media. Additionally, the selected transmission media should have the capability to support emerging technologies so that no infrastructure changes are required to deploy emerging technologies in the existing network.

NETWORK PHYSICAL STRUCTURE

1) Network Structure: Intrabuilding
   If all nodes are located the same building along with the server, then both building access layer and building distribution layer are located in the same building. Nodes are connected to the access layer either through twisted-pair copper wires or wireless LAN. Optical fibre being resilient to environmental disturbances, are used to connect building access layer switches to building distribution layer switches.

Figure 5 displays the intrabuilding network structure:

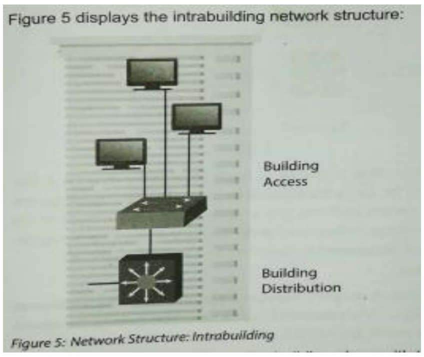


Figure 5: Network Structure: Intrabuilding

2) Network Structure: Intrabuilding
   If all nodes are located the same building along with the server, then both building access layer and building distribution layer are located in the same building. Nodes are connected to the access layer either through twisted-pair copper wires or wireless LAN. Optical fibre being resilient to environmental disturbances, are used to connect building access layer switches to building distribution layer switches.

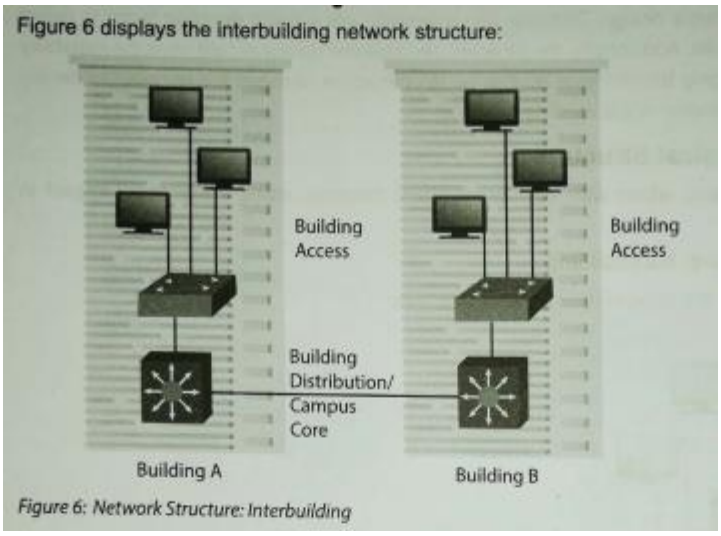


Figure 6 displays the interbuilding network structure:

Figure 6: Network Structure: Interbuilding

2. Detailed Enterprise Data Centre design.

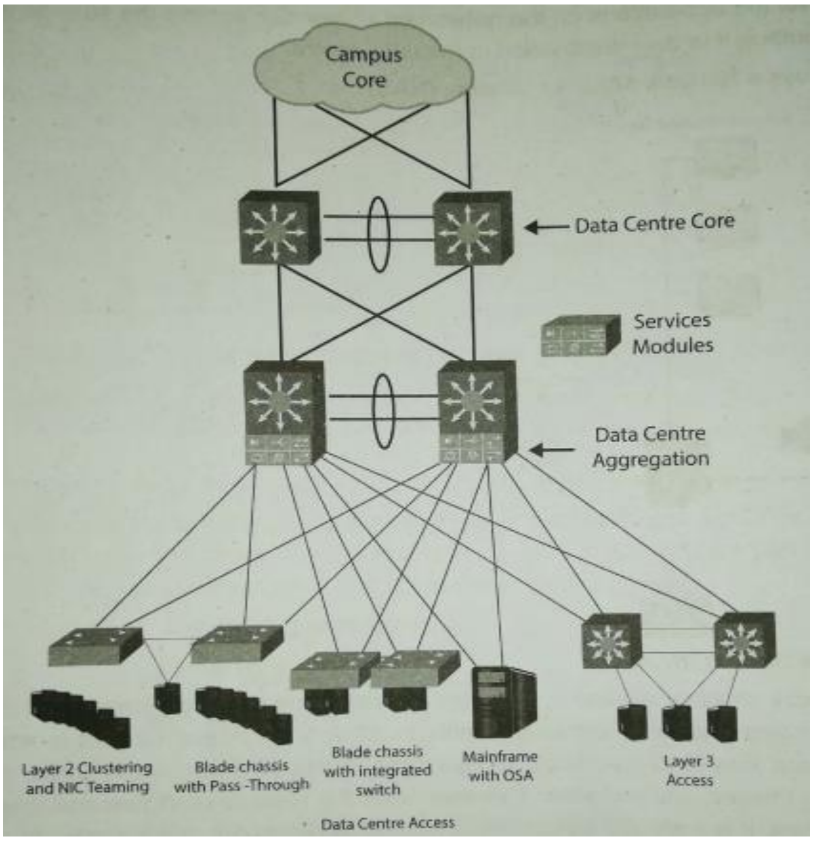


Figure 1- DATA CENTER INFRASTRUCTURE DESIGN

As shown in Figure, data centre infrastructure design consists of three layers, i.e. core layer, aggregation layer and access layer.

Data Centre Access Layer

Layer 2, Layer 3 and mainframe connectivity are provided by the data centre access layer. Layer 2 or Layer 3 access switches may be used in the data centre. Layer 2 access switches allow the sharing of services among multiple servers as well as clustering since they have low latency and high performance. Default server gateways can be implemented at the data centre access layer or data centre aggregation layer. To provide better availability, servers can have dual-attached NICs. The two-server links are connected to two separate redundant access switches. To have a single IP address for the two-server links, a better design option is to either have a VLAN or a trunk between the two redundant access switches. In this case, the default gateway for the server is at the data centre access layer. Both Layer 2 and Layer 3 switches can be used in the data centre access layer using the one rack unit (1 RU) approach. 1 RU opens a way for flexible yet optimal solutions for different applications.

Data Centre Aggregation Layer

The data centre aggregation layer is the intermediate layer between the data centre access layer and the data centre core layer. It aggregates the uplinks from the data centre access layer to the data centre core layer. Layer 2 connectivity at the data centre aggregation layer is generally avoided since it would demand for STP to manage physical loops in the network topology. Layer 3 connectivity is used at the data centre aggregation layer. This layer provides security services by the use of security service devices such as Firewalls, Intrusion Detection System, load balancing devices, and SSL offloading devices. These security service devices are implemented as modules in the data centre aggregation layer. Since the security service devices are deployed at the data centre aggregation layer, it is possible to share security services across all the servers. Deployment of security service devices at the data centre access layer would have restricted the service to the directly attached server. Thus, deployment of security service devices at the data centre aggregation layer reduces the total cost of ownership and complexity to configure and manage security service devices.

Data Centre Core Layer

Large Data Centres need a separate data centre core layer. Various factors that determine the need for a separate data centre core layer are listed as follows:
Capability of the campus core switch pair to support both the building distribution layer and the data centre aggregation layer
Availability of sufficient 10-Gigabit Ethernet ports on Campus Core
Isolation of the building distribution layer from the data centre aggregation layer for administrative, troubleshooting and maintenance purposes facilitated by the separation of the campus core and data centre core layer.
Layer 3 connectivity is used to connect the data centre core layer to the data centre. It has a distributed forwarding architecture with 10-Gigabit Ethernet connectivity and low latency switching. It supports IP multicast and is scalable.

Density and Scalability of Servers

The number of servers keeps growing in an Enterprise Data Centre. Multiple challenges are faced as the number of servers increases. To a single server, three or more interfaces may be attached. And many servers are placed in a rack. Therefore, cable routing and management becomes a tedious task as the number of interfaces connected to servers grows. A large number of cables on the floor and in the cabinet block the airflow to the rack and thus, equipment in the rack does not get cool.

Moreover, due to the high server density in the rack, comparatively more cooling is required. Also, as server density in a rack increases, a large power feed is required to the rack. These challenges are tackled by moving to alternatives. One of them is to avoid having a high density of servers in a rack. Another option is to modify cabinet routes or space the cabinets. A rack-based switching solution can also be used to cater to server density issues. In this, cables interfacing to the server are not on the floor, rather they are in the cabinet of 1 RU top of rack switches. This way, the problem of cooling and cabling management can be overcome.

END MODULE 4

Enterprise Edge WAN Technologies

-Introduction to WAN

A WAN is a data communications network that covers a relatively broad geographic area. A WAN typically uses the transmission facilities provided by service providers (SP) (also called carriers), such as telephone companies.

-Types of WAN interconnections

Figure 5-1 *Different Types of WAN Connections Are Appropriate for Different Uses*

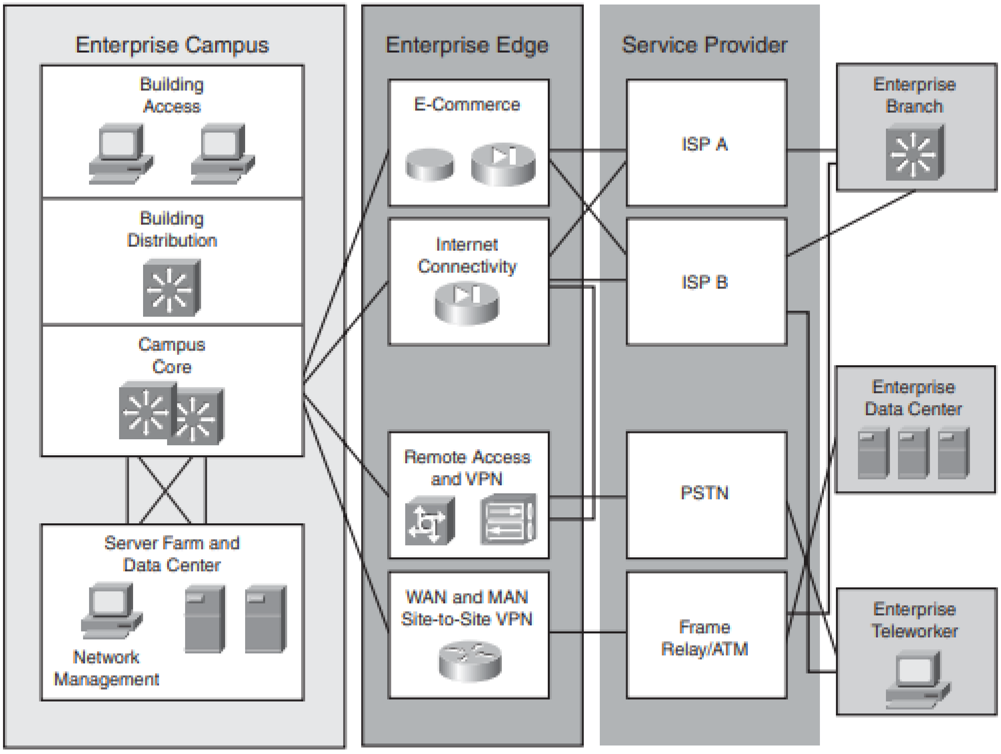


Figure illustrates the three ways that WAN technologies connect the Enterprise Edge modules with the outside world, represented by the service provider network. Typically, the intent is to provide the following connections:

■ Connectivity between the Enterprise Edge modules and the Internet Service Provider (ISP) Edge module

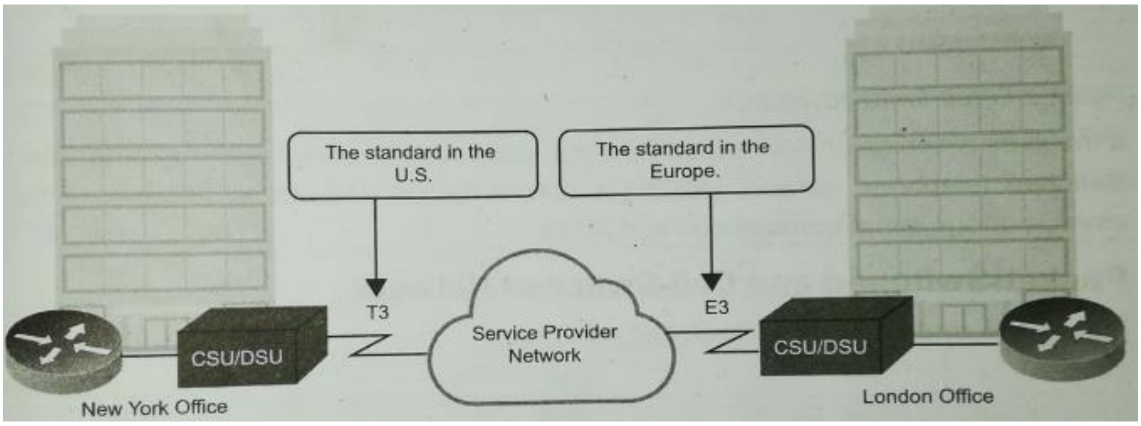
■ Connectivity between Enterprise sites across the ISP network

■ Connectivity between Enterprise sites across the SP or public switched telephone network (PSTN) carrier network

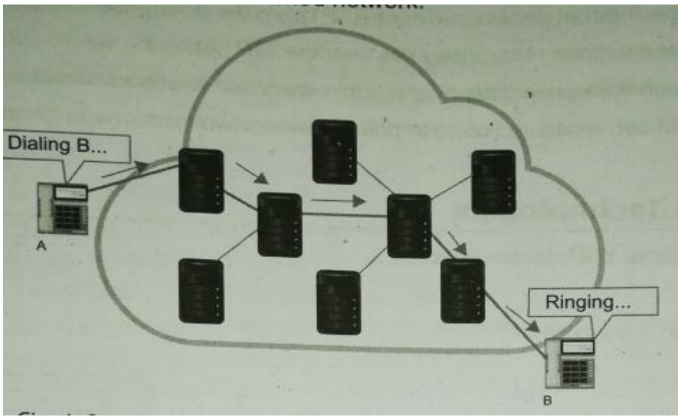
WAN connections can be point-to-point between two locations or connections to a multipoint WAN service offering, such as a Frame Relay or Multiprotocol Label Switching (MPLS) network.

-Traditional WAN Technologies

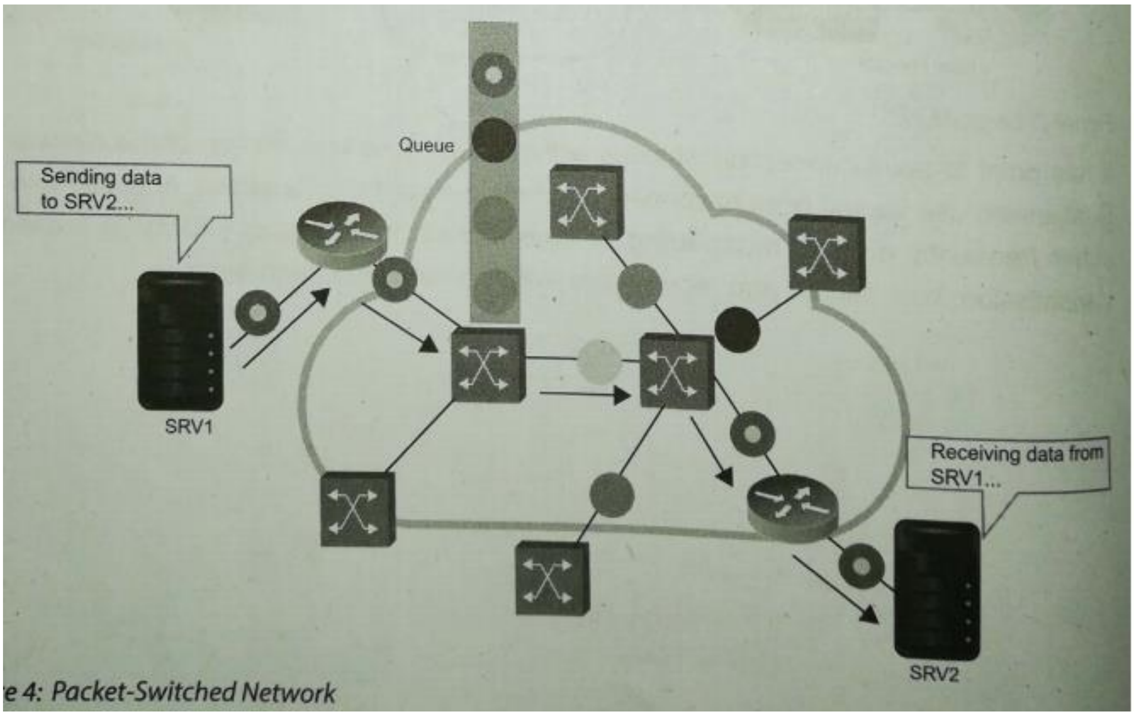
1) Leased lines: Point-to-point connections indefinitely reserved for transmissions, rather than used only when transmission is required. The carrier establishes the connection either by dedicating a physical wire or by delegating a channel using frequency division multiplexing or time-division multiplexing (TDM). Leased-line connections usually use synchronous transmission.



2) Circuit-switched networks: A type of network that, for the duration of the connection, obtains and dedicates a physical path for a single connection between two network endpoints. Ordinary voice phone service over the PSTN is circuit-switched; the telephone company reserves a specific physical path to the number being called for the call's duration. During that time, no one else can use the physical lines involved. Other circuit-switched examples include asynchronous serial transmission and ISDN.



3)Packet-switched and cell-switched networks: A carrier creates permanent virtual circuits (PVC) or switched virtual circuits (SVC) that deliver packets of data among customer sites. Users share common carrier resources and can use different paths through the WAN (for example, when congestion or delay is encountered). This allows the carrier to use its infrastructure more efficiently than it can with leased point-to-point links. Examples of packet-switched networks include X.25, Frame Relay, and Switched Multimegabit Data Service.



e 4: Packet-Switched Network

-WAN Transport Technologies

Question - list and explain any 5 WAN transport technologies?

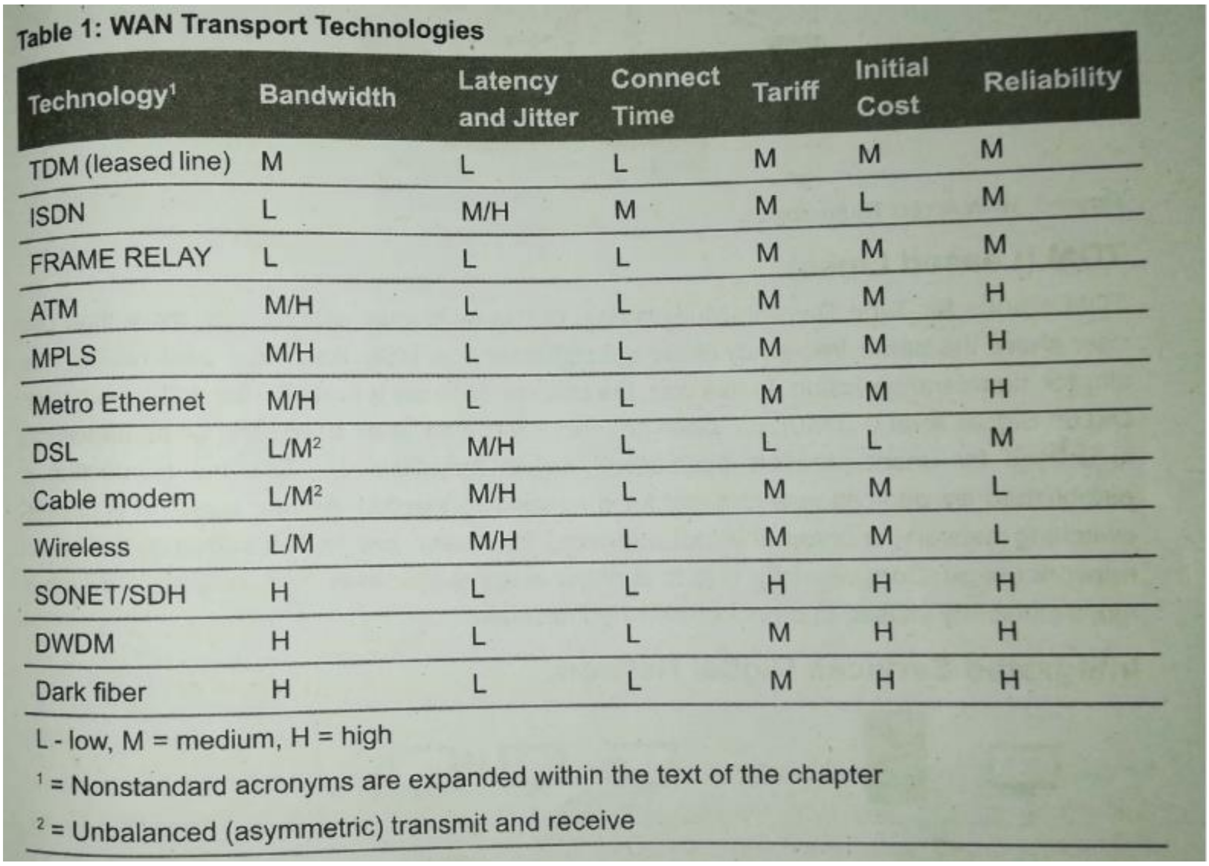


Table 1: WAN Transport Technologies

Technology[1]	Bandwidth	Latency and Jitter	Connect Time	Tariff	Initial Cost	Reliability
TDM (leased line)	M	L	L	M	M	M
ISDN	L	M/H	M	M	L	M
FRAME RELAY	L	L	L	M	M	M
ATM	M/H	L	L	M	M	H
MPLS	M/H	L	L	M	M	H
Metro Ethernet	M/H	L	L	M	M	H
DSL	L/M[2]	M/H	L	L	L	M
Cable modem	L/M[2]	M/H	L	M	M	L
Wireless	L/M	M/H	L	M	M	L
SONET/SDH	H	L	L	H	H	H
DWDM	H	L	L	M	H	H
Dark fiber	H	L	L	M	H	H

L - low, M = medium, H = high

[1] = Nonstandard acronyms are expanded within the text of the chapter

[2] = Unbalanced (asymmetric) transmit and receive

Table compares various WAN technologies, based on the main factors that influence technology selection. This table provides typical baseline characteristics to help you compare the performance and features offered by different technologies

TDM (Leased Lines)

TDM is a type of digital multiplexing in which pulses representing bits from two or more channels are interleaved, on a time basis. Rather than using bandwidth only as required, TDM indefinitely reserves point-to-point connection bandwidth for transmissions.

In this technique, the signals from more than one user share the same frequency channel in different time slots.Each user uses his/her time slot for signal transmission . In this way the channel capacity is partially utilised by each user.The base channel bandwidth is 64 kilobits per

second (kbps), also known as digital signal level 0 (DS0).

In TDMA carrier establishes a connection in a TDM network by dedicating a channel for a specific connection.n. In contrast, packet-switched networks traditionally offer the service provider more flexibility and use network bandwidth more efficiently than TDM networks because the network resources are shared dynamically and subscribers are charged on the basis of their network use.

ISDN

Analog modem dialup, also called plain old telephone service (POTS), provides data connectivity over the PSTN using analog modems.Integrated Services Digital Network (ISDN) is a circuit-switched technology that digitally transmits voice and data simultaneously over PSTN. The PSTN connection carries TDM digital signals for ISDN.

More than one TDM signal can be transmitted in a single communication channel. It has a call setup time of less than a second. The 64 kbps bearer channel provides greater capacity than an analogous modem connection.Hence ISDN connectivity offers increased bandwidth, reduced call setup time, reduced latency, and lower signal-to-noise ratios, compared to analog dialup.

Frame Relay

Frame Relay is a Layer-2 packet switched technology that is used to interconnect Enterprise LANs. This technology handles multiple circuits simultaneously ,which may be permanent or temporary. Permanent Virtual Circuits (PVCs) use a router interface to connect multiple sites where data and voice are carried at a rate of 4mbps or higher. Switched Virtual Circuits (SVCs) are temporary connections.in SVCs, when data is to be transferred, a connection is established . As soon as the data transfer is complete, the established connection is terminated.PVCs are widely used as compared to SVCs PVCs are uniquely identified by the data Link Connection Identifier (DLCI).

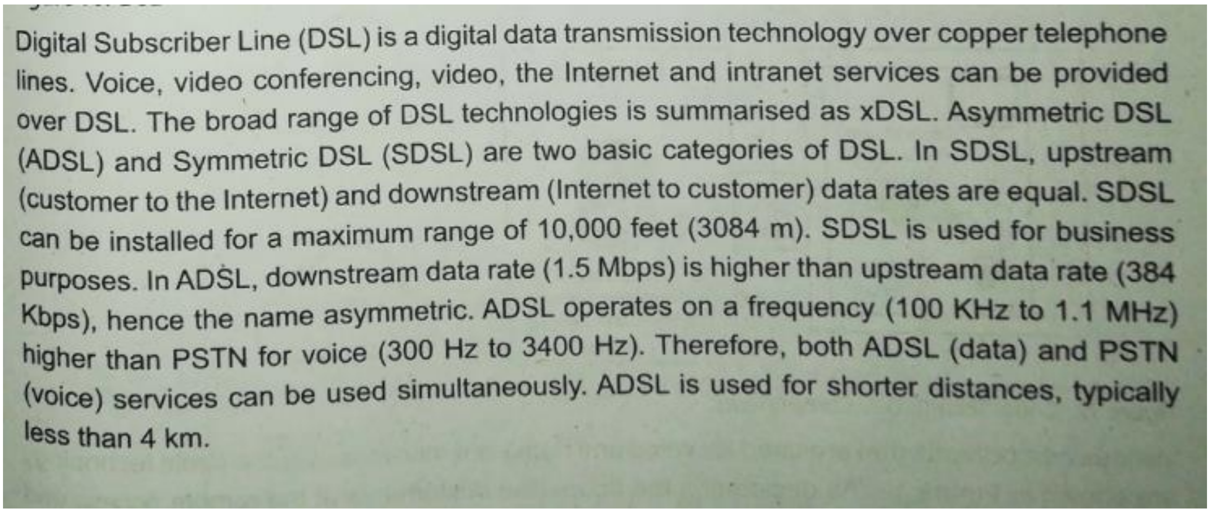
Asynchronous Transfer Mode

The Asynchronous Transfer Mode(ATM) is a cell-switched technology that is capable of transferring data,voice and video over private and public networks. It transmits fixed-size ATm cells of 53 bytes which are processed asynchronously to other related cells.Due to fixed-length cells,small voice, or video,the data gets transmitted to every cell. Network traffic does not need to wait for large packet transmission. Hence an ATM is suitable for business and networks having stringent Qos criteria for delay and loss

Metro Ethernet

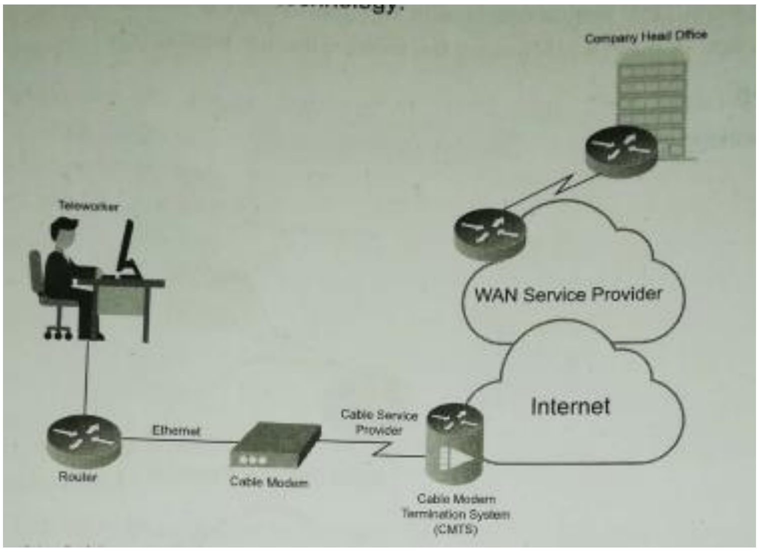
Metro Ethernet is a favourable technology for enterprises using Ethernet on their LAN. It provides high-speed connectivity with a scalable bandwidth for WAN and MAN applications . Enterprise can easily meet Qos requirements with high-performance network delivering converged data, voice and video in a MAN using metro Ethernet Technology

DSL Technologies



Digital Subscriber Line (DSL) is a digital data transmission technology over copper telephone lines. Voice, video conferencing, video, the Internet and intranet services can be provided over DSL. The broad range of DSL technologies is summarised as xDSL. Asymmetric DSL (ADSL) and Symmetric DSL (SDSL) are two basic categories of DSL. In SDSL, upstream (customer to the Internet) and downstream (Internet to customer) data rates are equal. SDSL can be installed for a maximum range of 10,000 feet (3084 m). SDSL is used for business purposes. In ADSL, downstream data rate (1.5 Mbps) is higher than upstream data rate (384 Kbps), hence the name asymmetric. ADSL operates on a frequency (100 KHz to 1.1 MHz) higher than PSTN for voice (300 Hz to 3400 Hz). Therefore, both ADSL (data) and PSTN (voice) services can be used simultaneously. ADSL is used for shorter distances, typically less than 4 km.

Cable Technology



Cable Technology uses coaxial cables to transmit data over a cable distribution system . both analogue and digital services are supported by the technology.It is used for residential as well as commercial purposes.

WAN Design

Based on Prepare-Plan-Design-ImplementOperate-Optimize (PPDIOO) methodology following are design steps for an Enterprise WAN:

1 Analyzing customer requirements: The initial step in the design methodology is to analyze the requirements of the network and its users, including the type of applications, the traffic volume, and traffic patterns. User needs continually change in response to changing business conditions and changing technology. For example, as more voice and video-based network applications become available, there is pressure to increase network bandwidth.

2 Characterizing the existing network and sites: The second step is to analyze the existing networking infrastructure and sites, including the technology used and the location of hosts, servers, terminals, and other end nodes. Together with the network's physical description, the analysis should evaluate the possibility of extending the network to support new sites, new features, or the reallocation of existing nodes. For example, the future integration of data and telephone systems requires considerable changes in the network's configuration. In this case, a detailed evaluation of current options is important.

3 Designing the network topology and solutions: The final step in the design methodology is to develop the overall network topology and its appropriate services, based on the availability of technology, and taking into account the projected traffic pattern, technology performance constraints, and network reliability. The design document describes a set of discrete functions performed by the Enterprise Edge modules and the expected level of service provided by each selected technology, as dictated by the SP.Q--explain the application and technical requirements of WAN design?

-Application Requirements of WAN Design

(staredu_pdf pg 171)

Application requirements highly influence the Enterprise WAN design as they influence Enterprise Campus design.Different applications have different requirements in terms of speed, bandwidth,memory , data storage etc.All these along with high availability,throughput,reliability and security requirements, highly influence the ENterprise WAN design

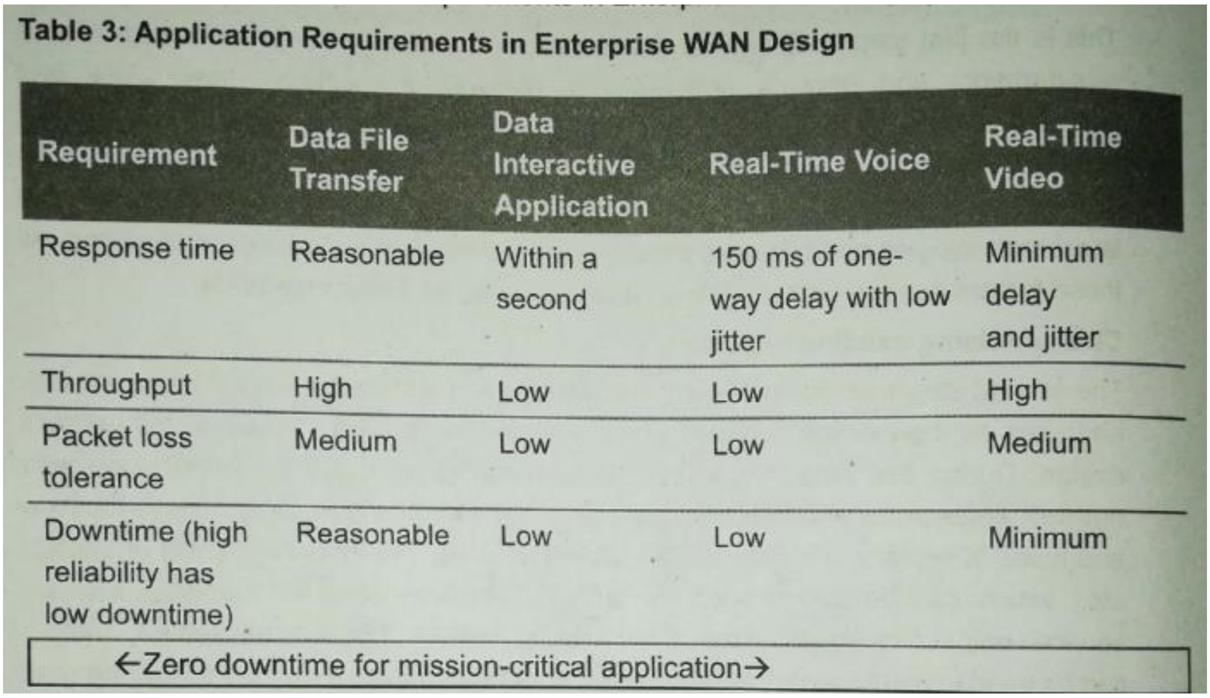


Table 3: Application Requirements in Enterprise WAN Design

Requirement	Data File Transfer	Data Interactive Application	Real-Time Voice	Real-Time Video
Response time	Reasonable	Within a second	150 ms of one-way delay with low jitter	Minimum delay and jitter
Throughput	High	Low	Low	High
Packet loss tolerance	Medium	Low	Low	Medium
Downtime (high reliability has low downtime)	Reasonable	Low	Low	Minimum

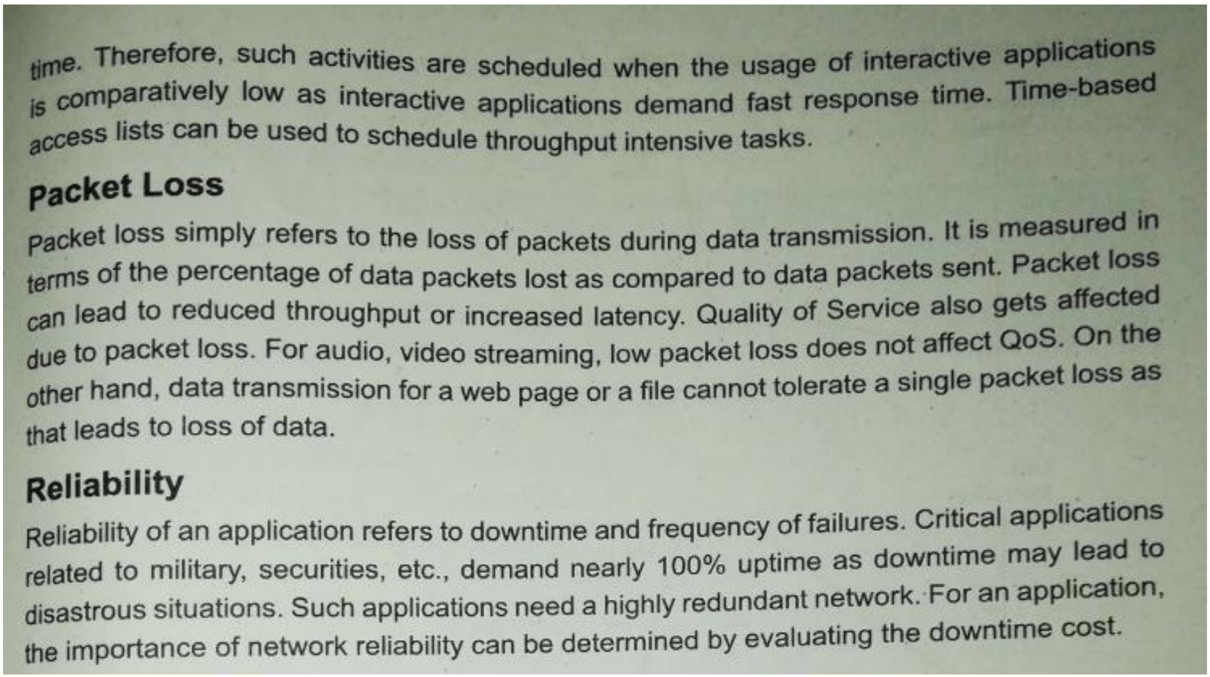
←Zero downtime for mission-critical application→

1 Response Time

2 Throughput

3 Packet Loss

4 Reliability



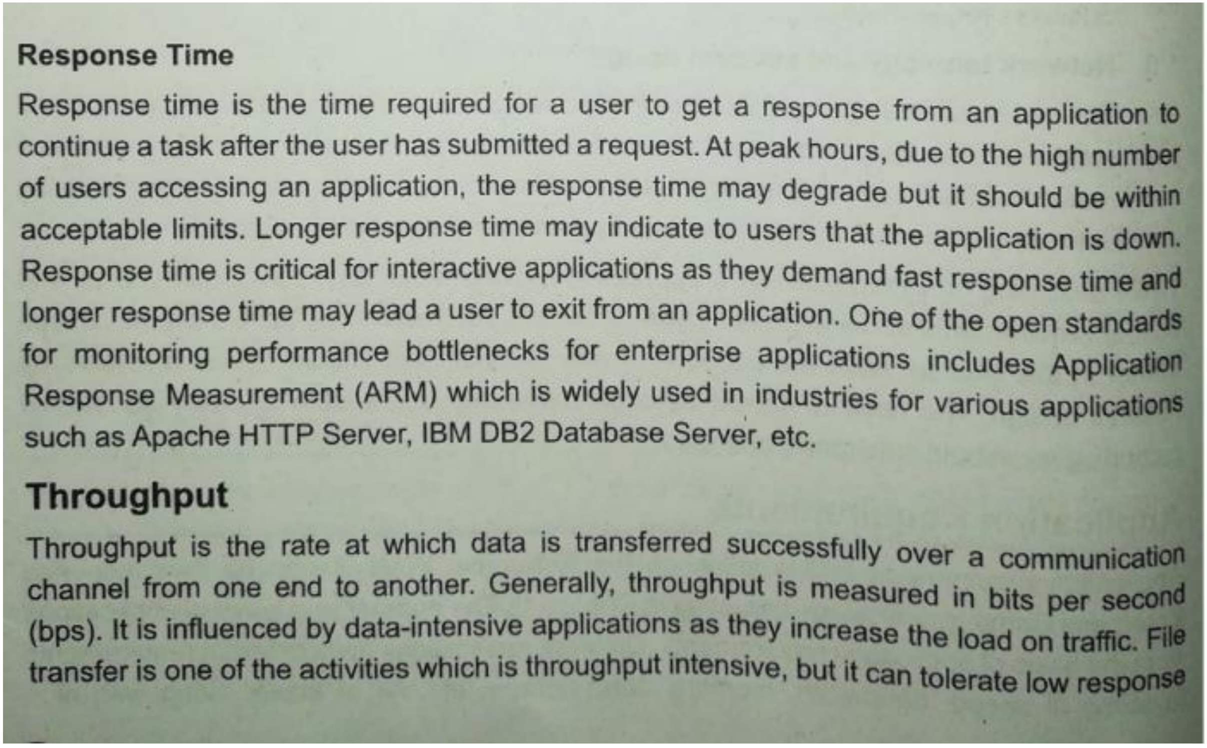
time. Therefore, such activities are scheduled when the usage of interactive applications is comparatively low as interactive applications demand fast response time. Time-based access lists can be used to schedule throughput intensive tasks.

Packet Loss

Packet loss simply refers to the loss of packets during data transmission. It is measured in terms of the percentage of data packets lost as compared to data packets sent. Packet loss can lead to reduced throughput or increased latency. Quality of Service also gets affected due to packet loss. For audio, video streaming, low packet loss does not affect QoS. On the other hand, data transmission for a web page or a file cannot tolerate a single packet loss as that leads to loss of data.

Reliability

Reliability of an application refers to downtime and frequency of failures. Critical applications related to military, securities, etc., demand nearly 100% uptime as downtime may lead to disastrous situations. Such applications need a highly redundant network. For an application, the importance of network reliability can be determined by evaluating the downtime cost.



Response Time

Response time is the time required for a user to get a response from an application to continue a task after the user has submitted a request. At peak hours, due to the high number of users accessing an application, the response time may degrade but it should be within acceptable limits. Longer response time may indicate to users that the application is down. Response time is critical for interactive applications as they demand fast response time and longer response time may lead a user to exit from an application. One of the open standards for monitoring performance bottlenecks for enterprise applications includes Application Response Measurement (ARM) which is widely used in industries for various applications such as Apache HTTP Server, IBM DB2 Database Server, etc.

Throughput

Throughput is the rate at which data is transferred successfully over a communication channel from one end to another. Generally, throughput is measured in bits per second (bps). It is influenced by data-intensive applications as they increase the load on traffic. File transfer is one of the activities which is throughput intensive, but it can tolerate low response

-Cost-Effectiveness of WAN Ownership

In the WAN environment, the following usually represent fixed costs:

■ Equipment purchases, such as modems, channel service unit/data service units, and router interfaces

■ Circuit and service provisioning

■ Network-management tools and platforms Recurring costs include the monthly circuit fees from the SP and the WAN’s support and maintenance, including any network management center personnel. From an ownership perspective, WAN links can be thought of in the following three categories:

1) Private: A private WAN uses private transmission systems to connect distant LANs. The owner of a private WAN must buy, configure, and maintain the physical layer connectivity (such as copper, fiber, wireless, and coaxial) and the terminal equipment required to connect locations. This makes private WANs expensive to build, labor-intensive to maintain, and difficult to reconfigure for constantly changing business needs. The advantages of using a private WAN might include higher levels of security and transmission quality.

2)Leased: A leased WAN uses dedicated bandwidth from a carrier company, with either private or leased terminal equipment. The provider provisions the circuit and provides the maintenance. However, the company pays for the allocated bandwidth whether or not it is used, and operating costs tend to be high. Some examples include TDM and SONET circuits.

3)Shared: A shared WAN shares the physical resources with many users. Carriers offer a variety of circuit- or packet-switching transport networks, such as MPLS and Frame Relay. The provider provisions the circuit and provides the maintenance. Linking LANs and private.WANs into shared network services is a trade-off among cost, performance, and security. An ideal design optimizes the cost advantages of shared network services with a company's performance and security requirements.

-Optimizing Bandwidth in a WAN

Q--various techniques to optimise bandwidth?

It is expensive to transmit data over a WAN. Therefore, one of many different techniques—such as data compression, bandwidth combination, tuning window size, congestion management (queuing and scheduling), congestion avoidance, and traffic shaping and policing—can be used to optimize bandwidth usage and improve overall performance

Data Compression

Compression enables more efficient use of the available WAN bandwidth, which is often limited and is generally a bottleneck. Compression allows higher throughput because it squeezes packet size and therefore increases the amount of data that can be sent through a transmission resource in a given time period. Compression can be of an entire packet, of the header only, or of the payload only. Payload compression is performed on a Layer 2 frame's payload and therefore compresses the entire Layer 3 packet. You can easily measure the success of these solutions using compression ratio and platform latency. However, although compression might seem like a viable WAN bandwidth optimization feature, it might not always be appropriate.

Data compression algorithms use **two types of encoding techniques**,

1) Statistical compression, which uses a fixed, usually nonadaptive encoding method, is best applied to a single application where the data is relatively consistent and predictable. Because the traffic on internetworks is neither consistent nor predictable, statistical algorithms are usually not suitable for data compression implementations on routers.

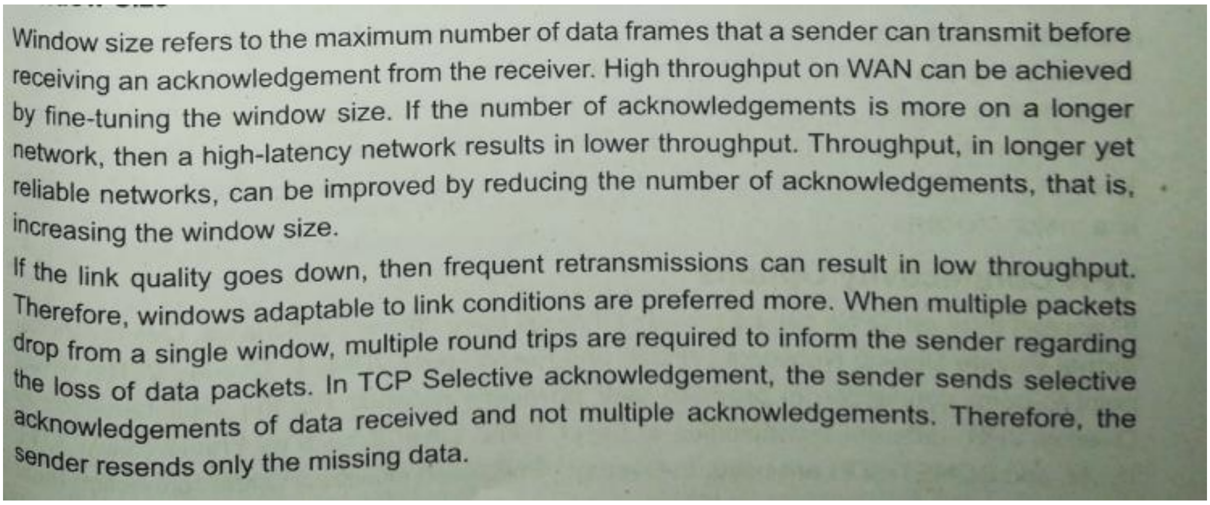
2) An example of **dictionary compression** is the Lempel-Ziv algorithm, which is based on a dynamically encoded dictionary that replaces a continuous stream of characters with codes. The symbols represented by the codes are stored in memory in a dictionary-style list. This approach is more responsive to variations in data than statistical compression.

Real-Time Transport Protocol (RTP) is used for carrying packetized audio and video traffic over an IP network. RTP is not intended for data traffic, which uses TCP or User Datagram Protocol. RTP provides end-to-end network transport functions intended for applications that have real-time transmission requirements such as audio, video, or simulation data over multicast or unicast network services. Because RTP header compression (cRTP) compresses the voice headers from 40 bytes to 2 or 4 bytes.Hardware-assisted data compression achieves the same goal as software-based data compression, except that it accelerates compression rates by offloading the task from the main CPU to specialized compression circuits. Compression is implemented in compression hardware that is installed in a system slot.

Combined Bandwidth

Point to point protocol (PPP) is a protocol used for establishing a direct connection between two nodes. There are no network devices in between. Phone lines connecting two computers or trunk lines connecting two computers are an example of PPP. customer dial-up access to the internet service is provided by the Internet Service Providers by using PPP. Similarly for DSL internet service ,PPPoE or PPPoA is used . When extra bandwidth is required between two computers multiple physical communication links are established using multilink PPP(MLP) . The bandwidth of three multiple links is logically aggregated which results in extra bandwidth and increased throughput

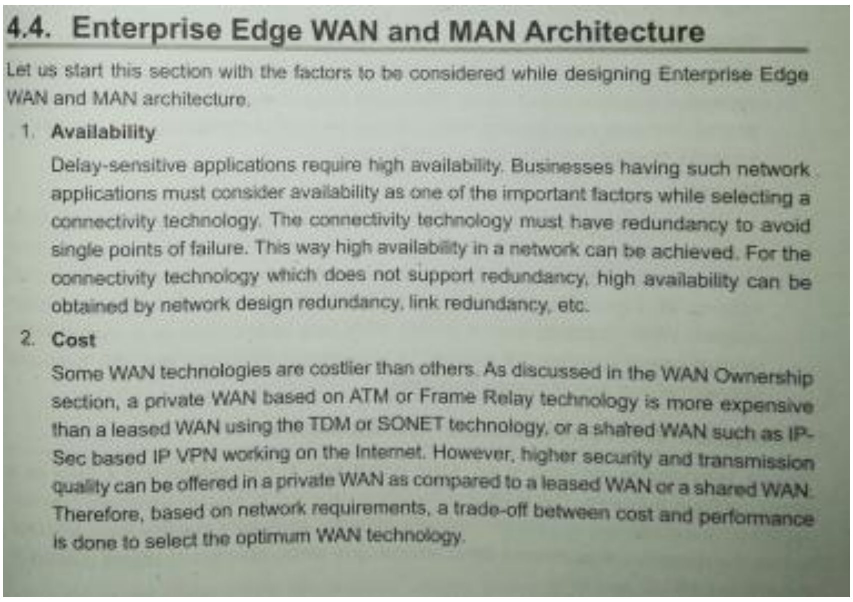
Window size



Window size refers to the maximum number of data frames that a sender can transmit before receiving an acknowledgement from the receiver. High throughput on WAN can be achieved by fine-tuning the window size. If the number of acknowledgements is more on a longer network, then a high-latency network results in lower throughput. Throughput, in longer yet reliable networks, can be improved by reducing the number of acknowledgements, that is, increasing the window size.

If the link quality goes down, then frequent retransmissions can result in low throughput. Therefore, windows adaptable to link conditions are preferred more. When multiple packets drop from a single window, multiple round trips are required to inform the sender regarding the loss of data packets. In TCP Selective acknowledgement, the sender sends selective acknowledgements of data received and not multiple acknowledgements. Therefore, the sender resends only the missing data.

Q-explain enterprise WAN and MAN architecture?



4.4. Enterprise Edge WAN and MAN Architecture

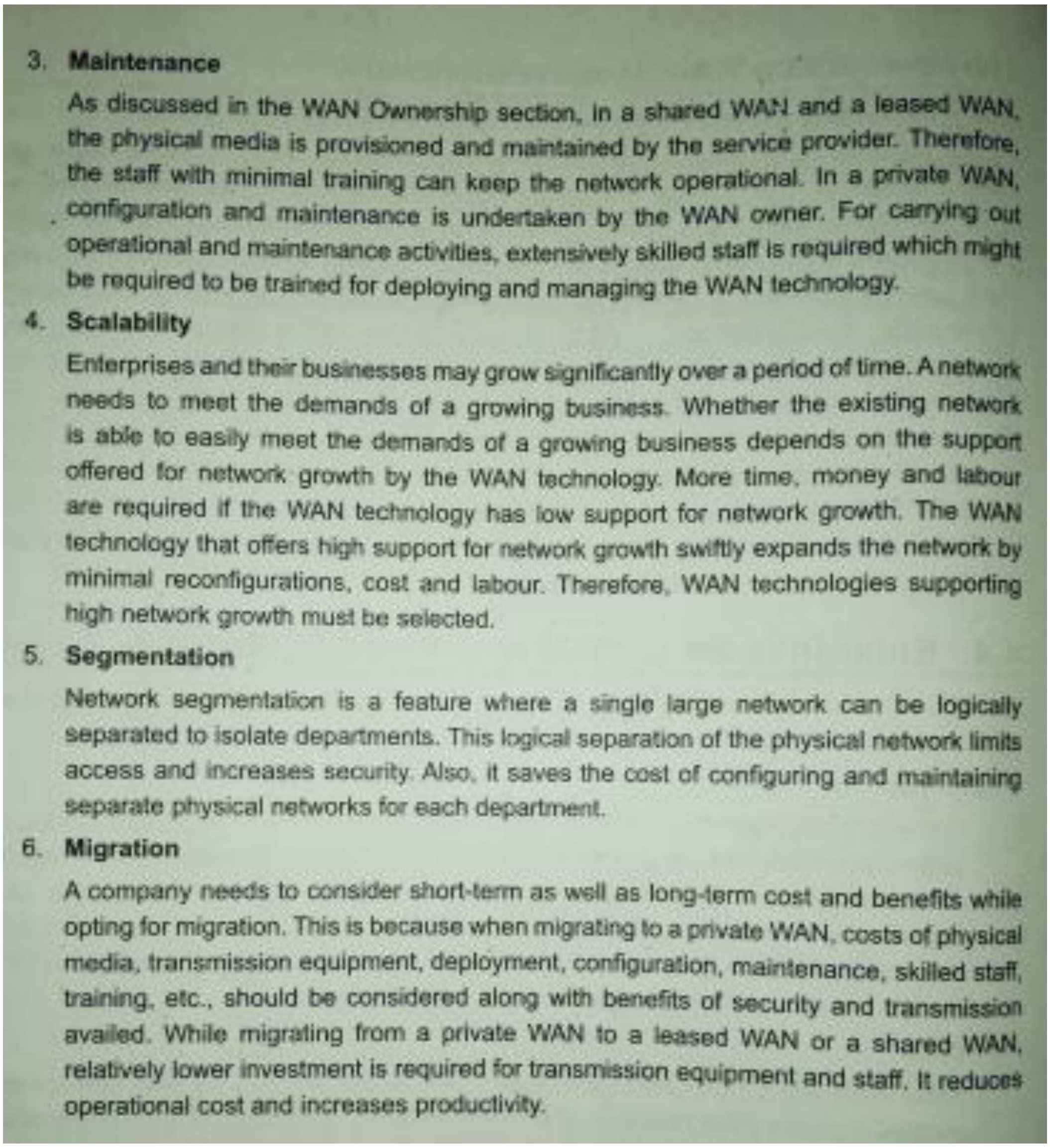
Let us start this section with the factors to be considered while designing Enterprise Edge WAN and MAN architecture.

1. **Availability**

   Delay-sensitive applications require high availability. Businesses having such network applications must consider availability as one of the important factors while selecting a connectivity technology. The connectivity technology must have redundancy to avoid single points of failure. This way high availability in a network can be achieved. For the connectivity technology which does not support redundancy, high availability can be obtained by network design redundancy, link redundancy, etc.

2. **Cost**

   Some WAN technologies are costlier than others. As discussed in the WAN Ownership section, a private WAN based on ATM or Frame Relay technology is more expensive than a leased WAN using the TDM or SONET technology, or a shared WAN such as IP-Sec based IP VPN working on the Internet. However, higher security and transmission quality can be offered in a private WAN as compared to a leased WAN or a shared WAN. Therefore, based on network requirements, a trade-off between cost and performance is done to select the optimum WAN technology.



3. **Maintenance**

   As discussed in the WAN Ownership section, in a shared WAN and a leased WAN, the physical media is provisioned and maintained by the service provider. Therefore, the staff with minimal training can keep the network operational. In a private WAN, configuration and maintenance is undertaken by the WAN owner. For carrying out operational and maintenance activities, extensively skilled staff is required which might be required to be trained for deploying and managing the WAN technology.

4. **Scalability**

   Enterprises and their businesses may grow significantly over a period of time. A network needs to meet the demands of a growing business. Whether the existing network is able to easily meet the demands of a growing business depends on the support offered for network growth by the WAN technology. More time, money and labour are required if the WAN technology has low support for network growth. The WAN technology that offers high support for network growth swiftly expands the network by minimal reconfigurations, cost and labour. Therefore, WAN technologies supporting high network growth must be selected.

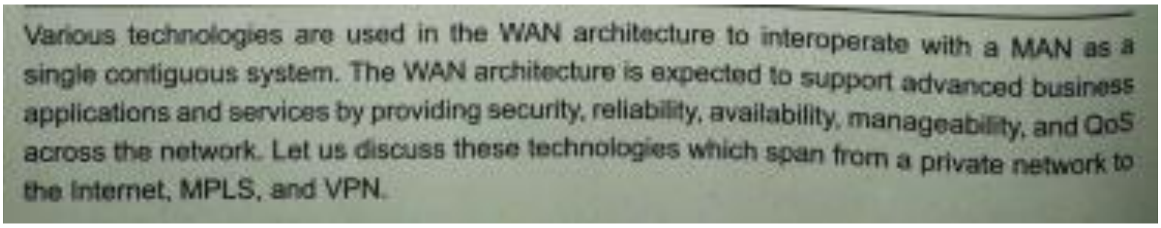
5. **Segmentation**

   Network segmentation is a feature where a single large network can be logically separated to isolate departments. This logical separation of the physical network limits access and increases security. Also, it saves the cost of configuring and maintaining separate physical networks for each department.

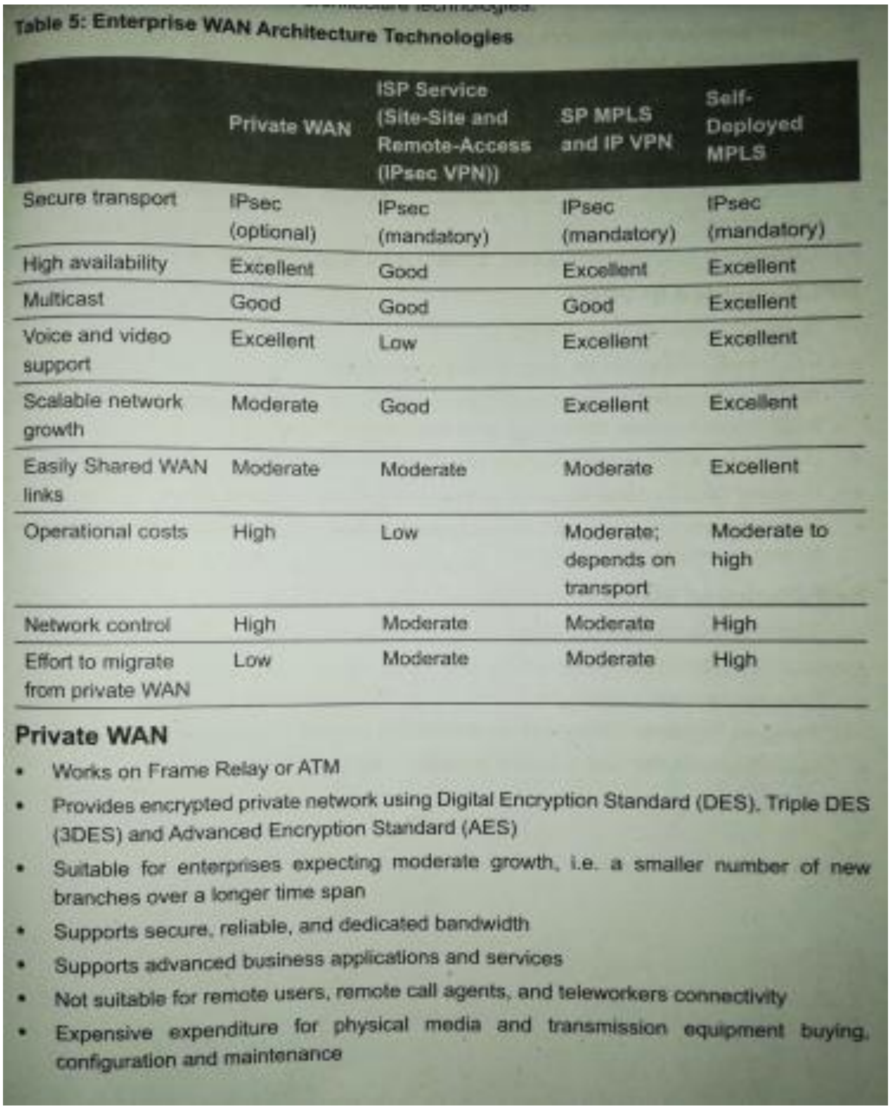
6. **Migration**

   A company needs to consider short-term as well as long-term cost and benefits while opting for migration. This is because when migrating to a private WAN, costs of physical media, transmission equipment, deployment, configuration, maintenance, skilled staff, training, etc., should be considered along with benefits of security and transmission availed. While migrating from a private WAN to a leased WAN or a shared WAN, relatively lower investment is required for transmission equipment and staff. It reduces operational cost and increases productivity.

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.



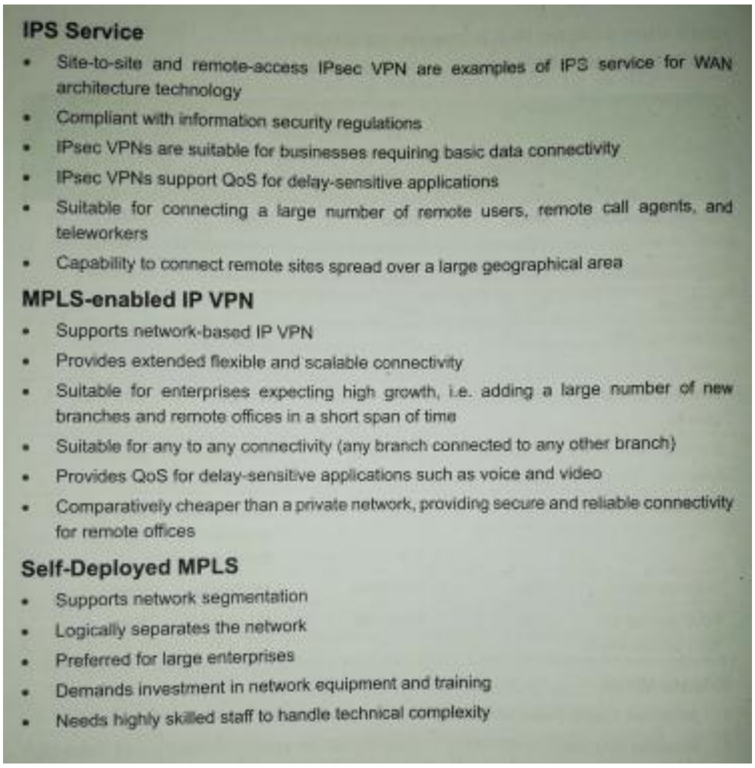
architecture technologies.

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

Selecting Enterprise Edge components

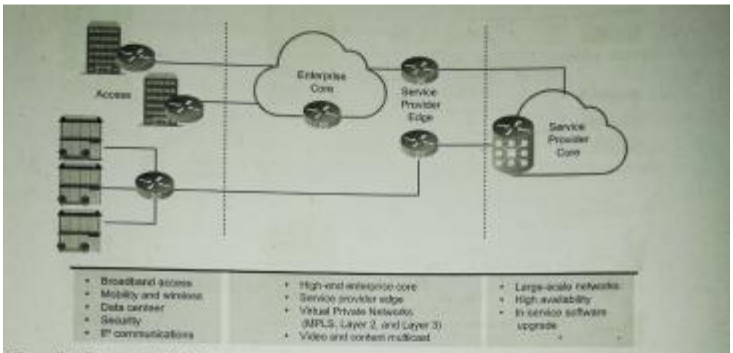


Figure 24: Enterprise WAN Software

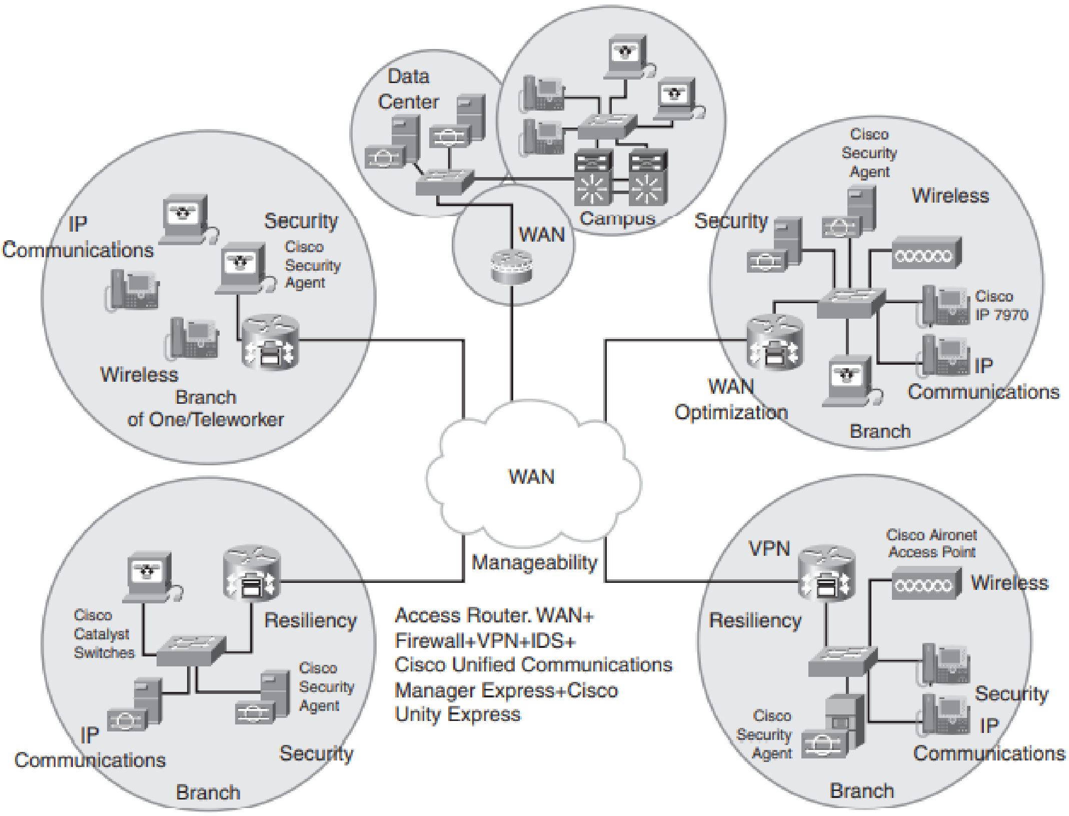
Enterprise Edge components are selected after identifying requirements and determining the architecture of the WAN. Both hardware and software for Enterprise Edge components must be judiciously selected. Initially, the hardware selection must be made followed by the software selection. Vendor documents must be referred to while evaluating and selecting any hardware component. A basic check should be made to ensure that the required functionalities are provided by the selected hardware. Examples of hardware features and functionalities include expanding capabilities, redundant connections, throughput, port density, etc. Based on the selected hardware, the appropriate corresponding software must be selected. The software must have the capability to support functionalities required by various businesses at different levels. Software programs are customised for IP data, converged voice and data, advanced security and VPN, Layer 3 routing protocols, service provider services, such as ATM, VoATM, MPLS, SSH, NetFlow, etc., IPv6, advanced security, service provider services, advanced enterprise services, etc.

Enterprise Branch Design and Teleworker Design.

-Enterprise branch architecture

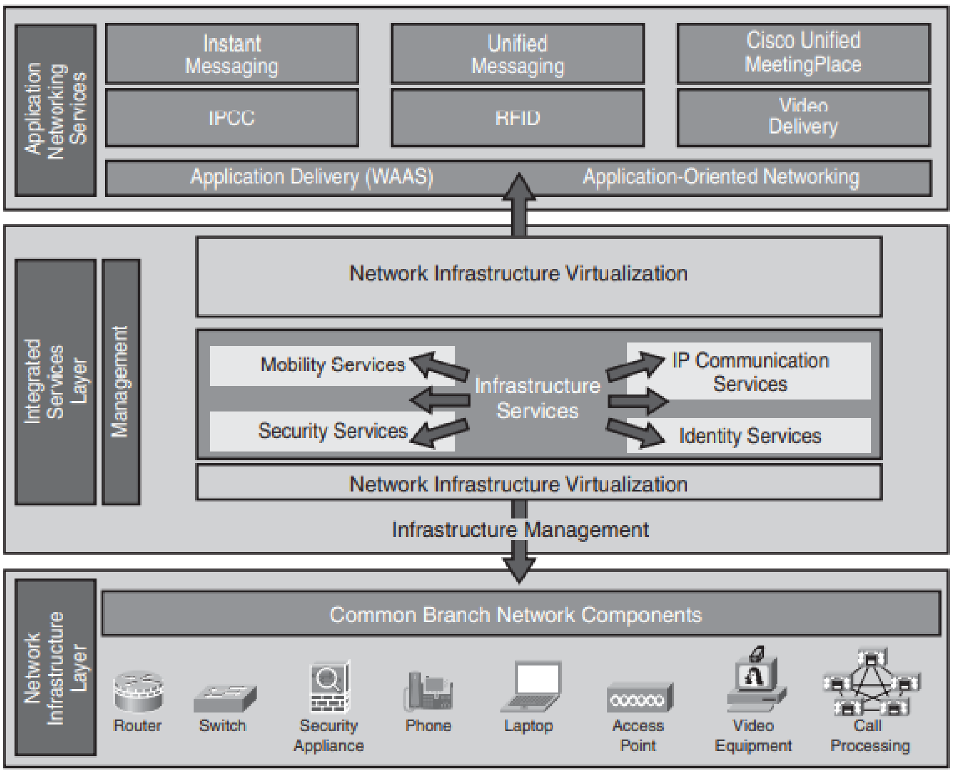
Enterprises are seeking opportunities to protect, optimize, and grow their businesses by increasing security; consolidating voice, video, and data onto a single IP network; and investing in applications that will improve productivity and operating efficiencies. These services provide enterprises with new opportunities to reduce costs, improve productivity, and safeguard information assets in all their locations. The Cisco Enterprise Branch architecture takes into account the services that enterprises want to deploy at their endpoints, no matter how far away the endpoints are or how they are connected.

Figure 5-23 *Enterprise Branch Services*



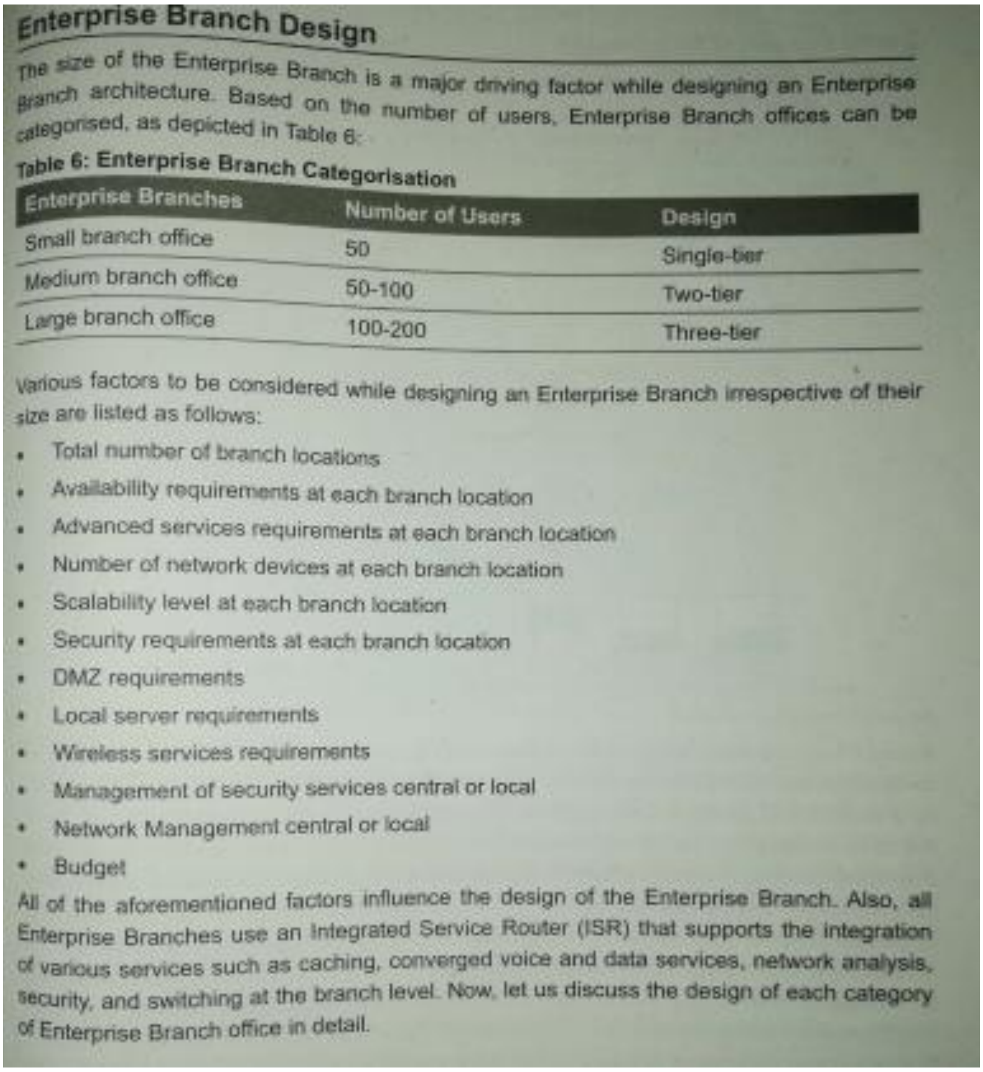
The Cisco Enterprise Branch Architecture, illustrated in Figure 5-24, is an integrated, flexible, and secure framework for extending headquarters applications in real time to remote sites. The Cisco Enterprise Branch Architecture applies the SONA framework to the smaller scale of a branch location.

Figure 5-24 *Enterprise Branch Architecture*


Application Networking Services
Instant Messaging
Unified Messaging
Cisco Unified MeetingPlace
IPCC
RFID
Video Delivery
Application Delivery (WAAS)
Application-Oriented Networking
Integrated Services Layer
Management
Network Infrastructure Virtualization
Mobility Services
Infrastructure Services
IP Communication Services
Security Services
Identity Services
Network Infrastructure Virtualization
Infrastructure Management
Network Infrastructure Layer
Common Branch Network Components
Router
Switch
Security Appliance
Phone
Laptop
Access Point
Video Equipment
Call Processing

-Enterprise branch Design

Refer to staredu_pdf pg 190



Enterprise Branch Design

The size of the Enterprise Branch is a major driving factor while designing an Enterprise Branch architecture. Based on the number of users, Enterprise Branch offices can be categorised, as depicted in Table 6:

Table 6: Enterprise Branch Categorisation

Enterprise Branches	Number of Users	Design
Small branch office	50	Single-tier
Medium branch office	50-100	Two-tier
Large branch office	100-200	Three-tier

Various factors to be considered while designing an Enterprise Branch irrespective of their size are listed as follows:

- Total number of branch locations
- Availability requirements at each branch location
- Advanced services requirements at each branch location
- Number of network devices at each branch location
- Scalability level at each branch location
- Security requirements at each branch location
- DMZ requirements
- Local server requirements
- Wireless services requirements
- Management of security services central or local
- Network Management central or local
- Budget

All of the aforementioned factors influence the design of the Enterprise Branch. Also, all Enterprise Branches use an Integrated Service Router (ISR) that supports the integration of various services such as caching, converged voice and data services, network analysis, security, and switching at the branch level. Now, let us discuss the design of each category of Enterprise Branch office in detail.

Small Branch Office Design

Figure 27 shows a Small Branch office:

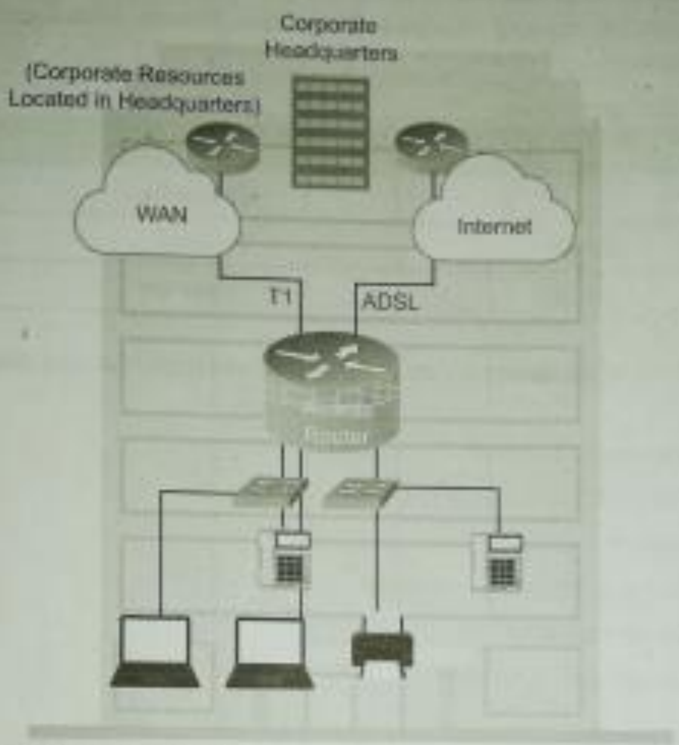


Figure 27: Small Branch Office

Figure 27 depicts the design of a Small Branch office. Layer 2 switches and end-user devices of an Enterprise Branch are connected to an ISR. ISR can be connected to Layer 2 switches by a multiservice router, trunked network interface, or logical EtherChannel interface. In all the three connectivity options, end devices can get power from access switches using Power over Ethernet (PoE). A trunked network interface does not provide link redundancy between ISR and Layer 2 switches. On the other hand, a logical EtherChannel has the capability to provide link redundancy over an EtherChannel. The EtherChannel is also preferable for Enterprise Branch offices requiring high-bandwidth and advanced services. While designing an Enterprise Branch, loop in the Layer 2 of Branch offices network are avoided. To protect the Enterprise Branch network from an accidental loop, Rapid Per-VLAN Spanning Tree Plus is enabled and configured at Layer 2. For each VLAN configured in the Enterprise Branch network, ISR is the default gateway. T1 primary link is used to provide WAN services. For the WAN backup, the Internet is utilised. The EIGRP protocol is used for network services. A static route over an ADSL Internet connection is used to provide high availability in a Small Branch office. Traffic shaping and policing along with the scavenger class of traffic is used to provide QoS.

Medium Branch Office Design

Figure 28 displays a Medium Branch office:

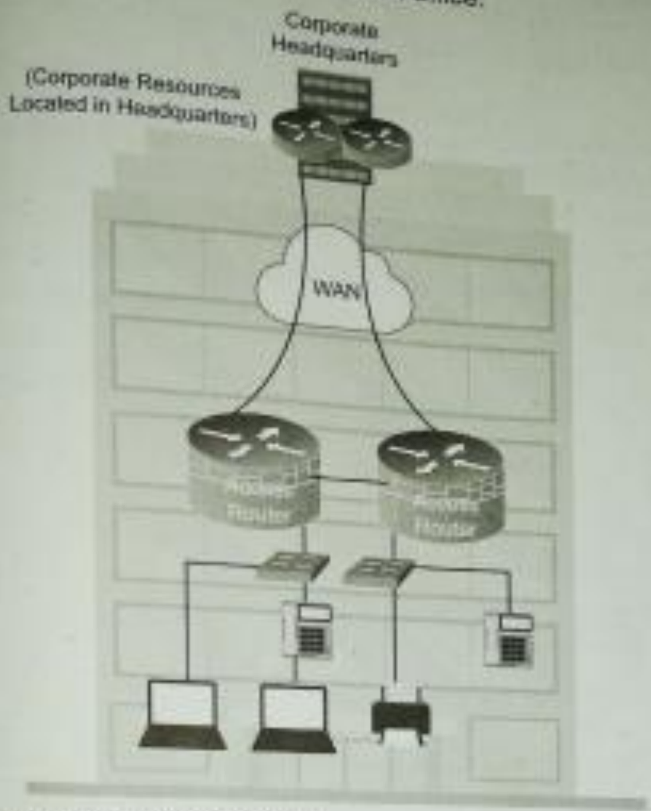
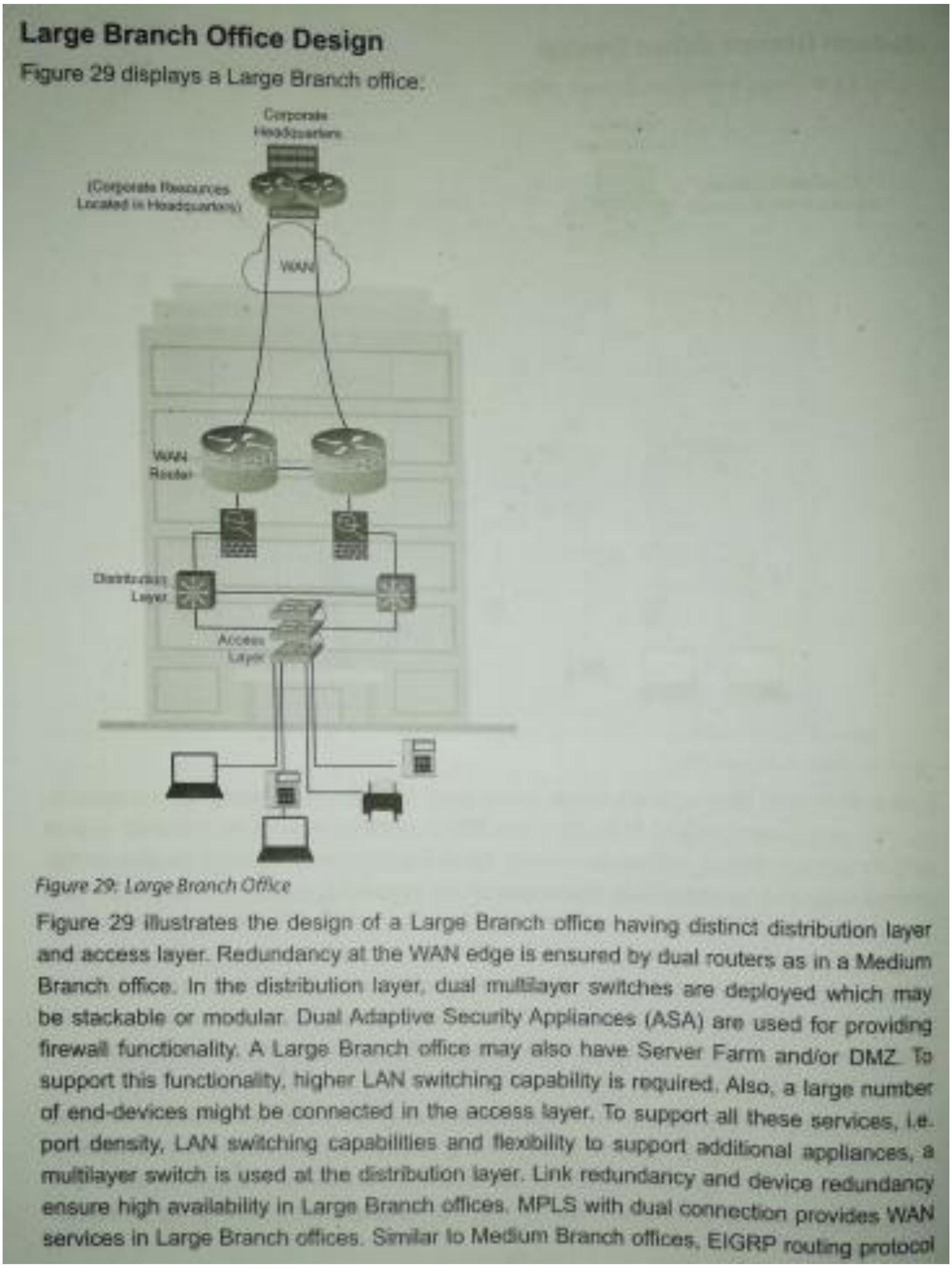


Figure 28: Medium Branch Office

A Medium Branch office's design differs from a Small Branch office's design in two aspects, viz. ISR and access switch. More than one ISR is required to support switched access ports for Medium Branch offices connectivity. Layer 2 access switches are high port density external stackable switches. Both these features are required to support 100 users. For link redundancy from ISR to access switches, EtherChannel interface is used. In order to have the flexibility to access switches, integrated 10/100/1000 interfaces on the ISRs are used as Layer 3 trunks. Frame Relay links are typically used to provide WAN services in Medium Branch offices. Similar to Small Branch offices, EIGRP routing protocol is used to provide network services and traffic shaping; policing along with scavenger class of traffic is used to provide QoS in Medium Branch offices.

Instead of using a static route on an ADSL Internet connection, high availability is ensured in a Medium Branch office by configuring routing redundancy protocols on dual routers. Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load-Balancing Protocol (GLBP) are all examples of routing redundancy protocols.



Large Branch Office Design

Figure 29 displays a Large Branch office.

Corporate Headquarters
(Corporate Resources Located in Headquarters)
WAN
WAN Router
Distribution Layer
Access Layer

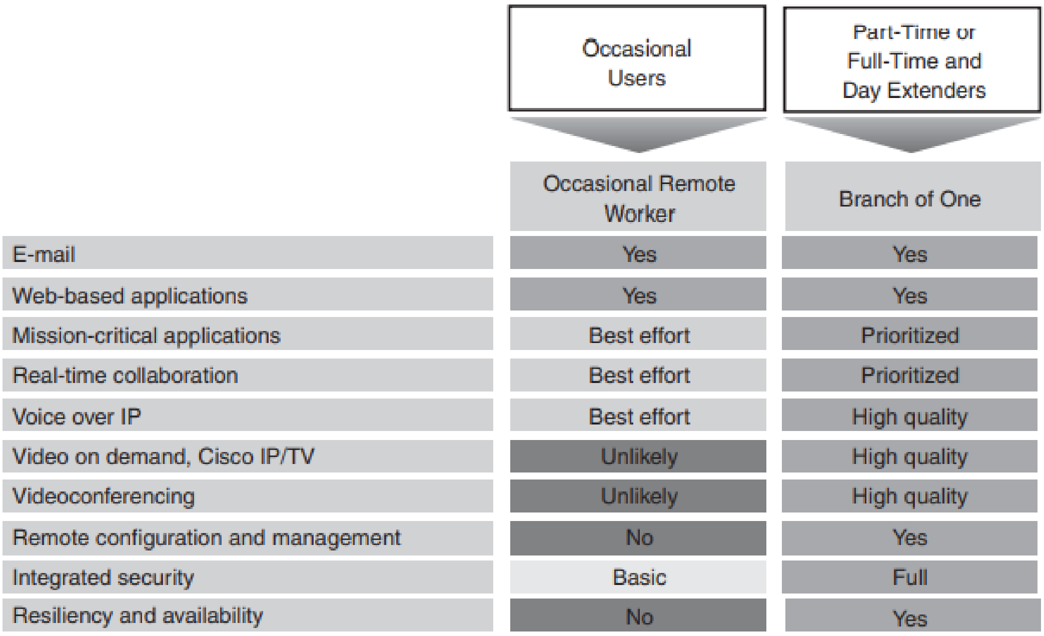
Figure 29: Large Branch Office

Figure 29 illustrates the design of a Large Branch office having distinct distribution layer and access layer. Redundancy at the WAN edge is ensured by dual routers as in a Medium Branch office. In the distribution layer, dual multilayer switches are deployed which may be stackable or modular. Dual Adaptive Security Appliances (ASA) are used for providing firewall functionality. A Large Branch office may also have Server Farm and/or DMZ. To support this functionality, higher LAN switching capability is required. Also, a large number of end-devices might be connected in the access layer. To support all these services, i.e. port density, LAN switching capabilities and flexibility to support additional appliances, a multilayer switch is used at the distribution layer. Link redundancy and device redundancy ensure high availability in Large Branch offices. MPLS with dual connection provides WAN services in Large Branch offices. Similar to Medium Branch offices, EIGRP routing protocol

-Enterprise Teleworker Design

Organizations are constantly striving to reduce costs, improve employee productivity, and retain valued employees. These goals can be furthered by allowing employees to work from home with quality, function, performance, convenience, and security similar to that available in the office. With a work environment in the residence, employees can optimally manage their work schedules, allowing for higher productivity (less affected by office distractions) and greater job satisfaction (flexibility in schedule). This transparent extension of the enterprise to employee homes is the objective of the Cisco Enterprise Teleworker architecture.

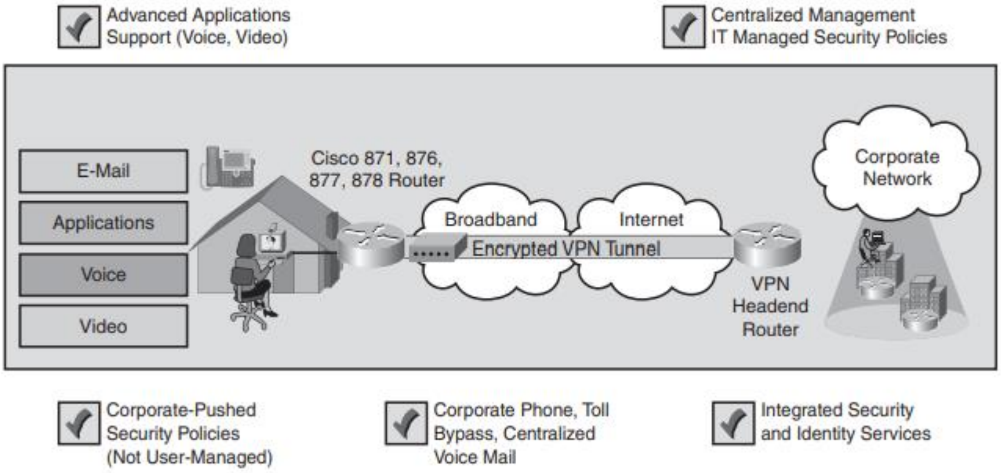
Figure 5-28 *Comparison of Teleworking Options*



	Occasional Users	Part-Time or Full-Time and Day Extenders
	Occasional Remote Worker	Branch of One
E-mail	Yes	Yes
Web-based applications	Yes	Yes
Mission-critical applications	Best effort	Prioritized
Real-time collaboration	Best effort	Prioritized
Voice over IP	Best effort	High quality
Video on demand, Cisco IP/TV	Unlikely	High quality
Videoconferencing	Unlikely	High quality
Remote configuration and management	No	Yes
Integrated security	Basic	Full
Resiliency and availability	No	Yes

In contrast, Enterprise teleworkers can be differentiated from other forms of work-at-home or telecommuting scenarios in that the emphasis is on delivering seamless, managed accessibility to the full range of applications and services critical to the operational effectiveness of enterprises, as illustrated in Figure 5-28. The Cisco Enterprise Teleworker architecture is part of the overall secure Cisco Enterprise architecture infrastructure. It companies the capability to integrate and securely manage their remote workers within the corporate network while simultaneously providing a high-quality end-user experience supporting a full range of enterprise applications for the enterprise teleworker.

Figure 5-29 *Teleworker (Branch of One) Architecture*


Advanced Applications Support (Voice, Video)
Centralized Management IT Managed Security Policies
E-Mail
Applications
Voice
Video
Cisco 871, 876, 877, 878 Router
Broadband
Internet
Encrypted VPN Tunnel
Corporate Network
VPN Headend Router
Corporate-Pushed Security Policies (Not User-Managed)
Corporate Phone, Toll Bypass, Centralized Voice Mail
Integrated Security and Identity Services

END MODULE 5

Q1) State and explain IPv4-IPv6 transition strategies.

Ans)

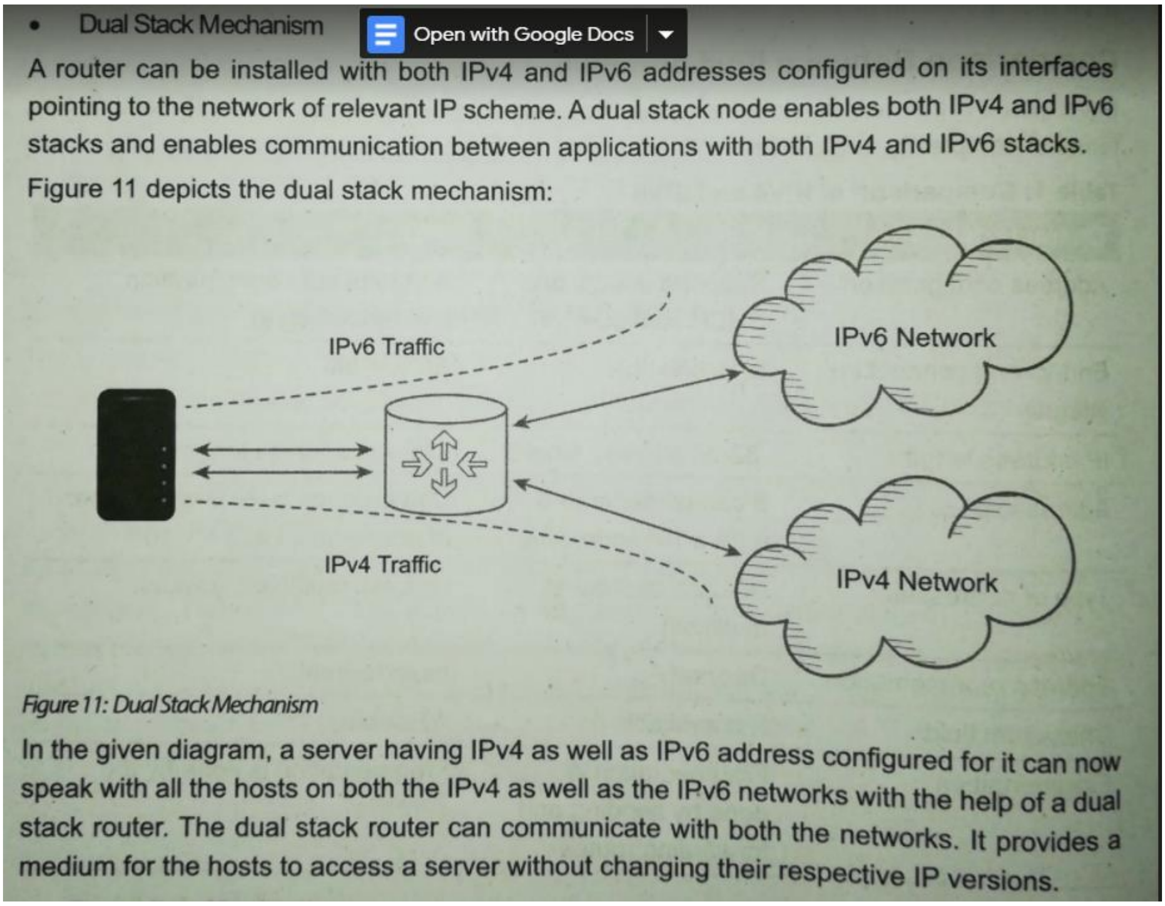
There is no automatic transition from IPv4 to IPv6.

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
- Tunnelling
- Translation

1. **Dual Stack**


Open with Google Docs
IPv6 Traffic
IPv6 Network
IPv4 Traffic
IPv4 Network

- Dual Stack Mechanism

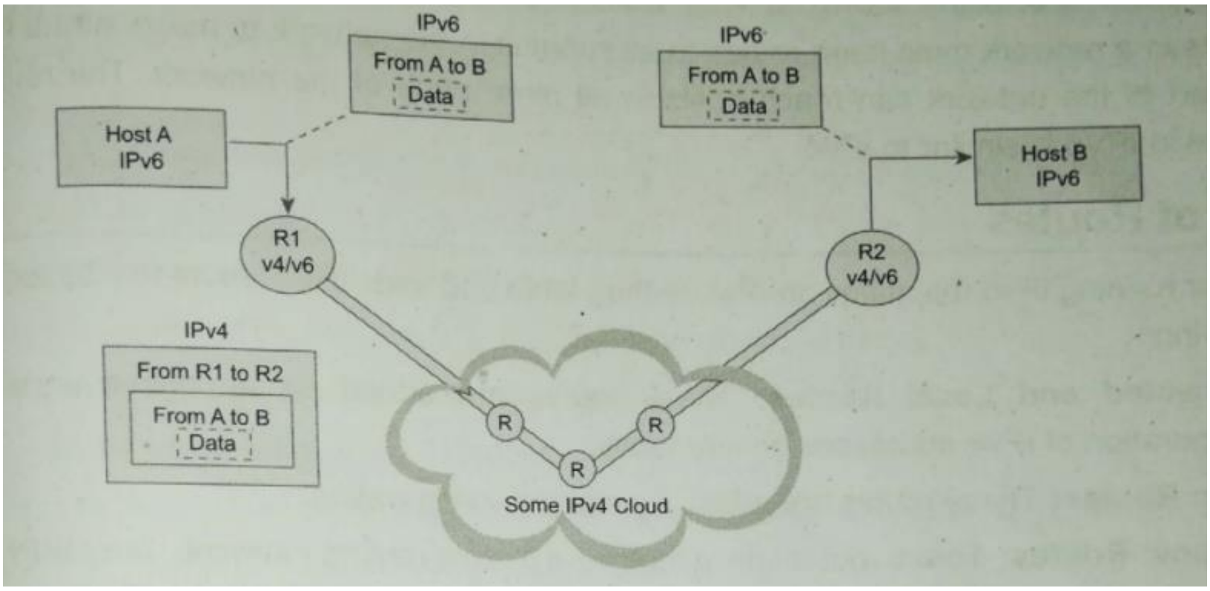
A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme. A dual stack node enables both IPv4 and IPv6 stacks and enables communication between applications with both IPv4 and IPv6 stacks. Figure 11 depicts the dual stack mechanism:

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.

2. **Tunneling Mechanism**

The purpose of the tunneling mechanism 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.

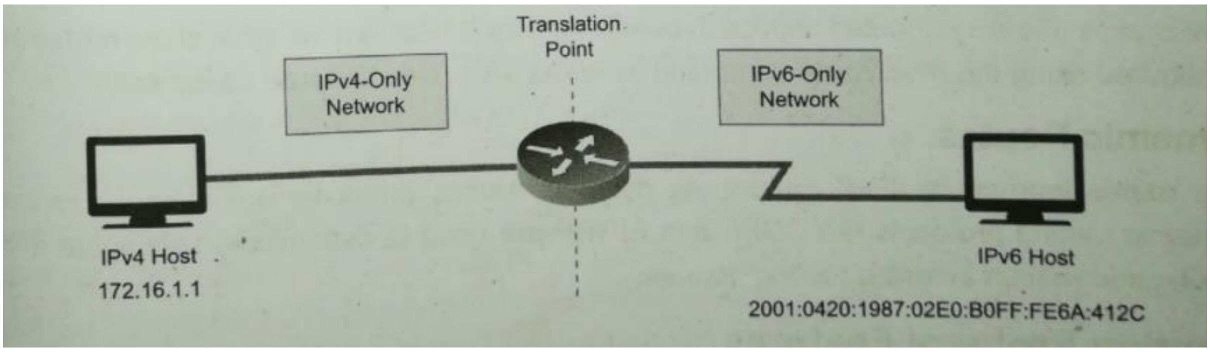


The different uses of tunneling in the transition are as follows:

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

3. 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.



A host with the IPv4 address sends a request to an IPv6 enabled server on the 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 strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the internet. When a response from the IPv6 server comes to the IPv4 host, the router does vice versa.

Q2) Comparison between IPv4 and IPv6.

Ans)

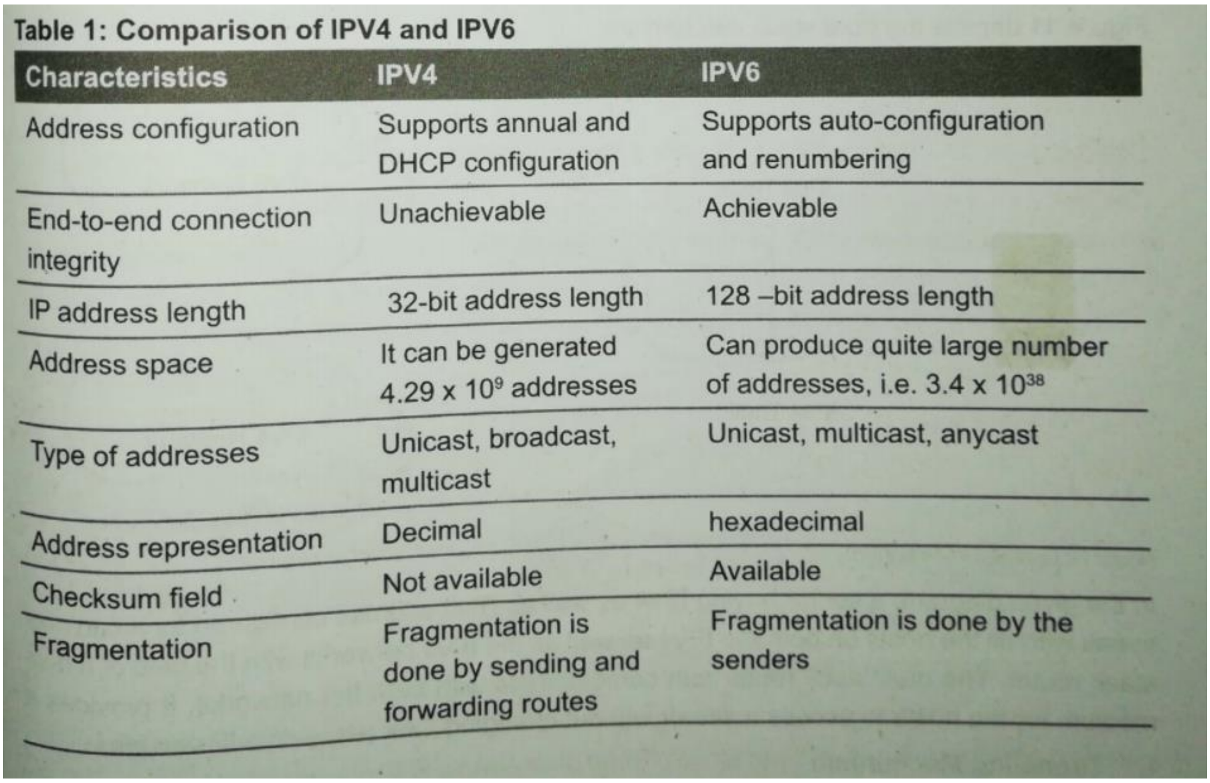


Table 1: Comparison of IPV4 and IPV6

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 x 10^9 addresses	Can produce quite large number of addresses, i.e. 3.4 x 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

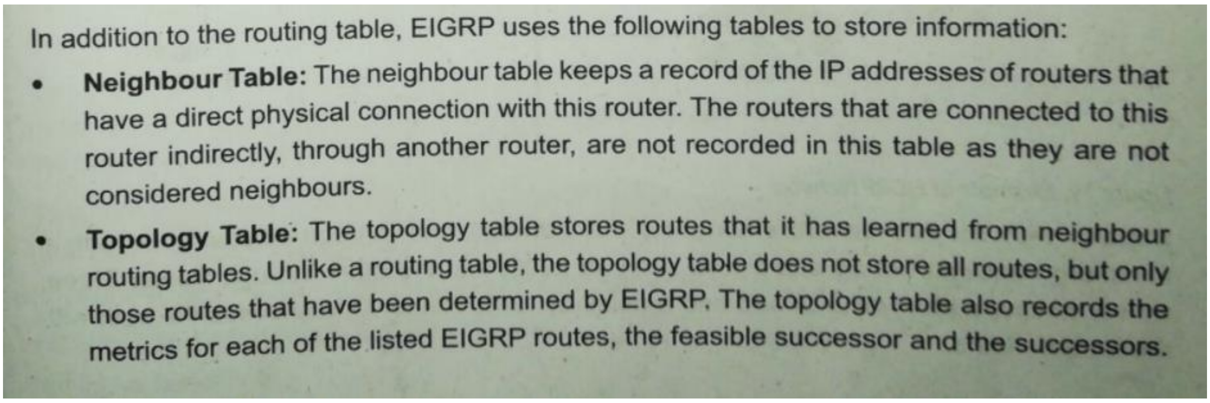
Q3) Explain EIGRP.

Ans)

Stands for Enhanced Interior Gateway Routing Protocol.

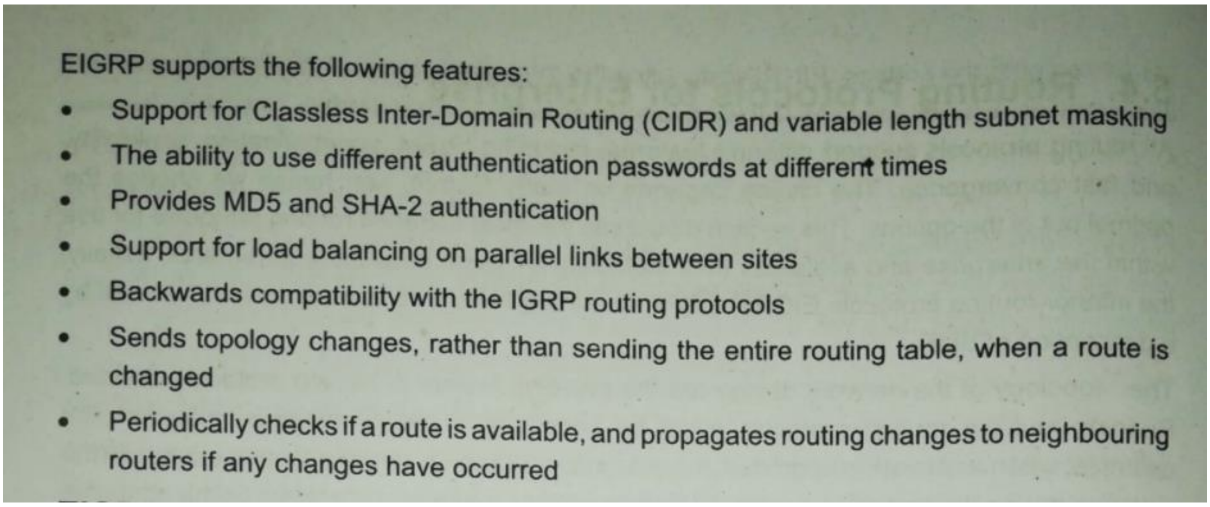
It is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. The protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers. EIGRP is used on a router to share routes with other routers 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 the 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 Characteristics

The characteristics that make EIGRP suitable for deployment in enterprise networks include the following:

■ Fast convergence: One advantage of EIGRP is its fast-converging DUAL route calculation mechanism. This mechanism allows backup routes (the feasible successors) to be kept in the topology table for use if the primary route fails. Because this process occurs locally on the router, the switchover to a backup route (if one exists) is immediate and does not involve action in any other routers.

■ Improved scalability: Along with fast convergence, the ability to manually summarize also improves scalability. EIGRP summarizes routes on classful network boundaries by default. Automatic summarization can be turned off, and manual summarization can be configured at any point in the network, improving scalability and network performance because the routing protocol uses fewer resources.

■ Use of VLSM: Because EIGRP is a classless routing protocol, it sends subnet mask information in its routing updates and therefore supports VLSM.

■ Reduced bandwidth usage: Because EIGRP does not send periodic routing updates as other distance vector protocols do, it uses less bandwidth—particularly in large networks that have a large number of routes. On the other hand, EIGRP uses the Hello protocol to establish and maintain adjacencies with its neighbors. If many neighbors are reachable over the same physical link, as might be the case in NBMA networks, the Hello protocol might create significant routing traffic overhead. Therefore, the network must be designed appropriately to take advantage of EIGRP's benefits.

■ Multiple network layer protocol support: EIGRP supports multiple network layer protocols through Protocol-Dependent Modules (PDM). PDMs include support for IPv4, IPv6, IPX, and AppleTalk.

Q4) IPv6 Header.

Ans)

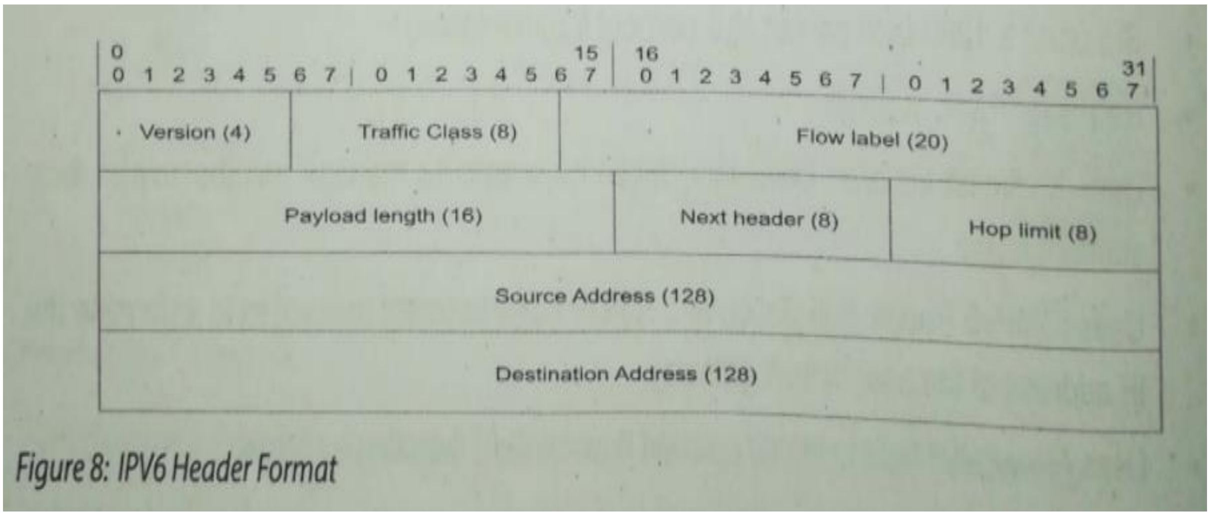


Figure 8: IPV6 Header Format

The IPv6 header has 40 octets, in contrast to the 20 octets in the IPv4 header. IPv6 has fewer fields, and the header is 64-bit-aligned to enable fast, efficient, hardware-based processing. The IPv6 address fields are four times larger than in IPv4. IPv6 contains fields similar to 7 of the 12 IPv4 basic header fields (5 plus the source and destination address fields) but does not require the other fields. The IPv6 header contains the following fields:

■ Version: A 4-bit field, the same as in IPv4. For IPv6, this field contains the number 6; for IPv4, this field contains the number 4.

■ Traffic class: An 8-bit field similar to the type of service (ToS) field in IPv4. This field tags the packet with a traffic class that it uses in differentiated services (DiffServ) QoS. These functions are the same for IPv6 and IPv4.

■ Flow label: This 20-bit field is new in IPv6. It can be used by the source of the packet to tag the packet as being part of a specific flow, allowing multilayer switches and routers to handle traffic on a per-flow basis rather than per-packet, for faster packet-switching performance. This field can also be used to provide QoS.

■ Payload length: This 16-bit field is similar to the IPv4 total length field.

■ Next header: The value of this 8-bit field determines the type of information that follows the basic IPv6 header. It can be transport-layer information, such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), or it can be an extension header. The next header field is similar to the protocol field of IPv4.

■ Hop limit: This 8-bit field specifies the maximum number of hops that an IPv6 packet can traverse. Similar to the time to live (TTL) field in IPv4, each router decreases this field by 1. Because there is no checksum in the IPv6 header, an IPv6 router can decrease the field without recomputing the checksum; in IPv4 routers, the recomputation costs processing time. If this field ever reaches 0, a message is sent back to the source of the packet, and the packet is discarded.

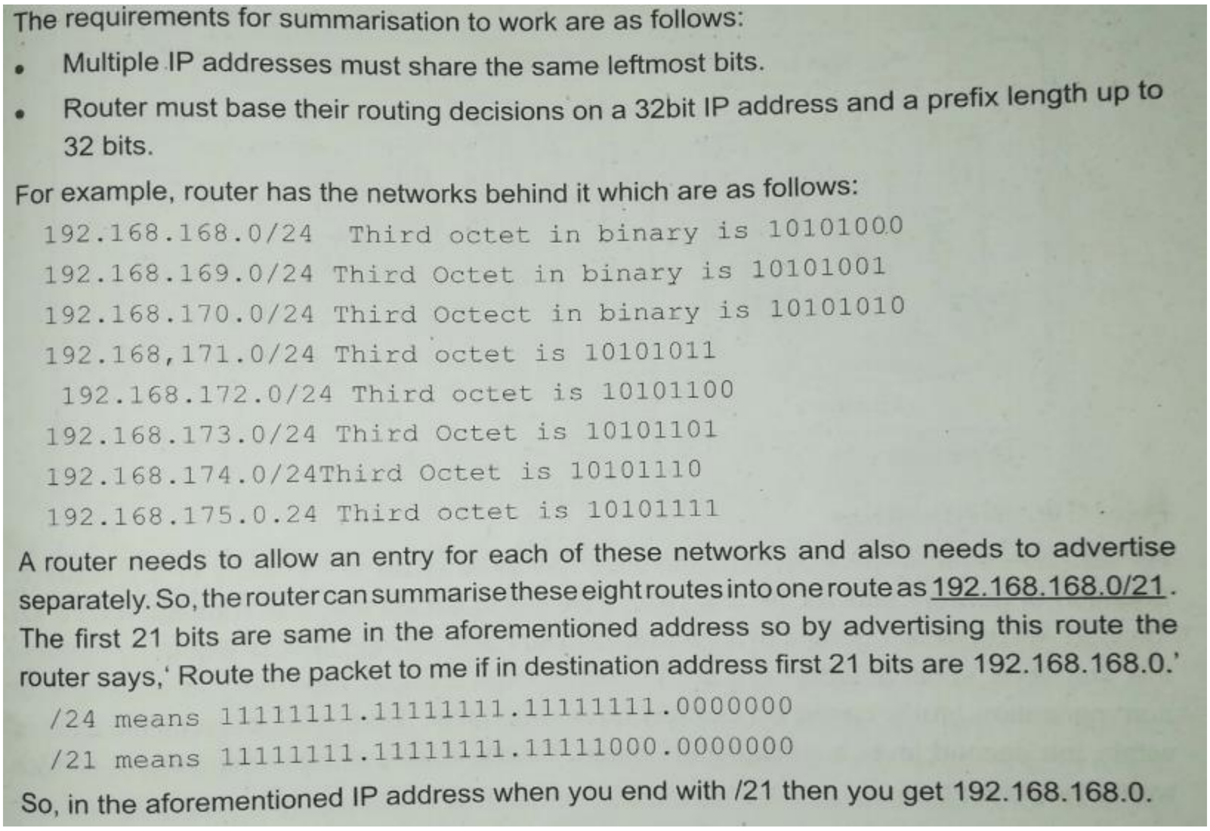
■ Source address: This field has 16 octets (128 bits). It identifies the source of the packet.

■ Destination address: This field has 16 octets (128 bits). It identifies the destination of the packet.

Routing

Over the internet, the router uses Network ID (prefix part of IP address) to reach the next hop in the best path, not worried about how to reach the end node. So, all routers in between do indirect delivery of packets. Once it reaches the destination IP address, the last router (one where the local host is present whose IP has been followed for decision of packet forwarding) does direct delivery of the packet.

Route Summarisation/Route Supernetting

- Summarisation results in smaller entries on routing tables, thereby reducing routing update traffic which reduces number of routes in routing tables which in turn reduces overall overhead of the router.
- This is done with CIDR (classless interdomain routing). CIDR combines blocks of multiple addresses into a larger classless set of IP addresses.
- 

The requirements for summarisation to work are as follows:

- Multiple IP addresses must share the same leftmost bits.
- Router must base their routing decisions on a 32bit IP address and a prefix length up to 32 bits.

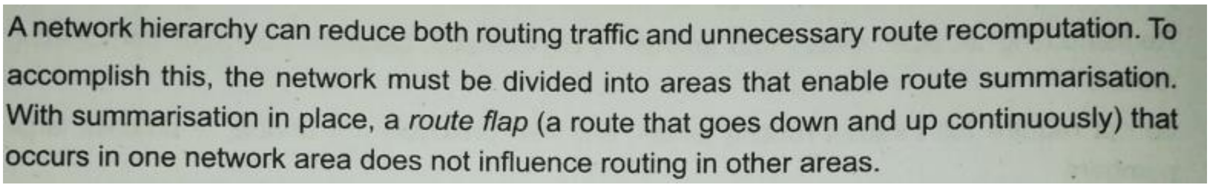
For example, router has the networks behind it which are as follows:

```
192.168.168.0/24  Third octet in binary is 10101000
192.168.169.0/24 Third Octet in binary is 10101001
192.168.170.0/24 Third Octect in binary is 10101010
192.168,171.0/24 Third octet is 10101011
 192.168.172.0/24 Third octet is 10101100
192.168.173.0/24 Third Octet is 10101101
192.168.174.0/24Third Octet is 10101110
192.168.175.0.24 Third octet is 10101111
```

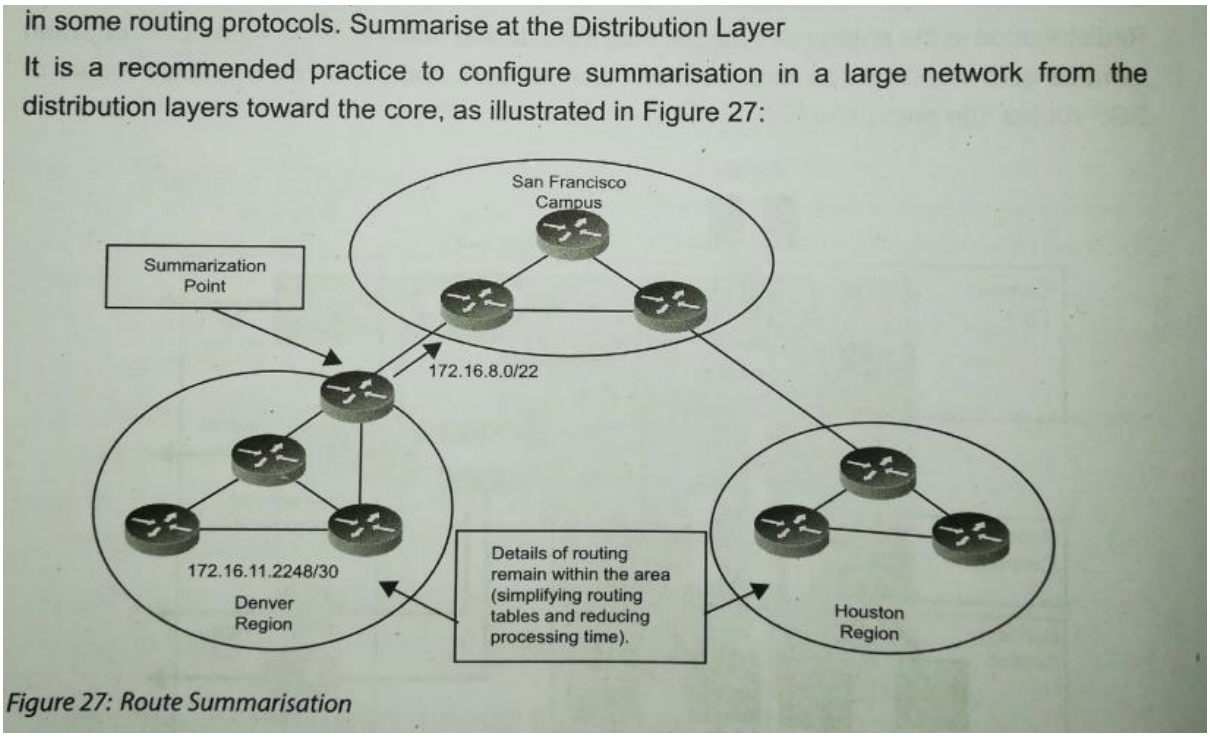
A router needs to allow an entry for each of these networks and also needs to advertise separately. So, the router can summarise these eight routes into one route as 192.168.168.0/21. The first 21 bits are same in the aforementioned address so by advertising this route the router says,‘ Route the packet to me if in destination address first 21 bits are 192.168.168.0.’

```
/24 means 11111111.11111111.11111111.0000000
/21 means 11111111.11111111.11111000.0000000
```

So, in the aforementioned IP address when you end with /21 then you get 192.168.168.0.

- 

  A network hierarchy can reduce both routing traffic and unnecessary route recomputation. To accomplish this, the network must be divided into areas that enable route summarisation. With summarisation in place, a *route flap* (a route that goes down and up continuously) that occurs in one network area does not influence routing in other areas.

- 

  in some routing protocols. Summarise at the Distribution Layer

  It is a recommended practice to configure summarisation in a large network from the distribution layers toward the core, as illustrated in Figure 27:

  San Francisco Campus
Summarization Point
172.16.8.0/22
172.16.11.2248/30
Denver Region
Details of routing remain within the area (simplifying routing tables and reducing processing time).
Houston Region

  Figure 27: Route Summarisation

Disadvantages of poorly designed IP addressing

A poorly designed IP addressing scheme would be to randomly assign IP addresses when required, i.e range of IP addresses with different Network IDs.

- Aggregation or summarisation is difficult to achieve.
- If one link is faulty, the information needs to be broadcasted as all the routers need to update that information about the link is up or down continuously. This leads to unnecessary traffic for updating routing tables of all the routers.

Fixed and Variable length subnet mask (FLSM and VLSM)

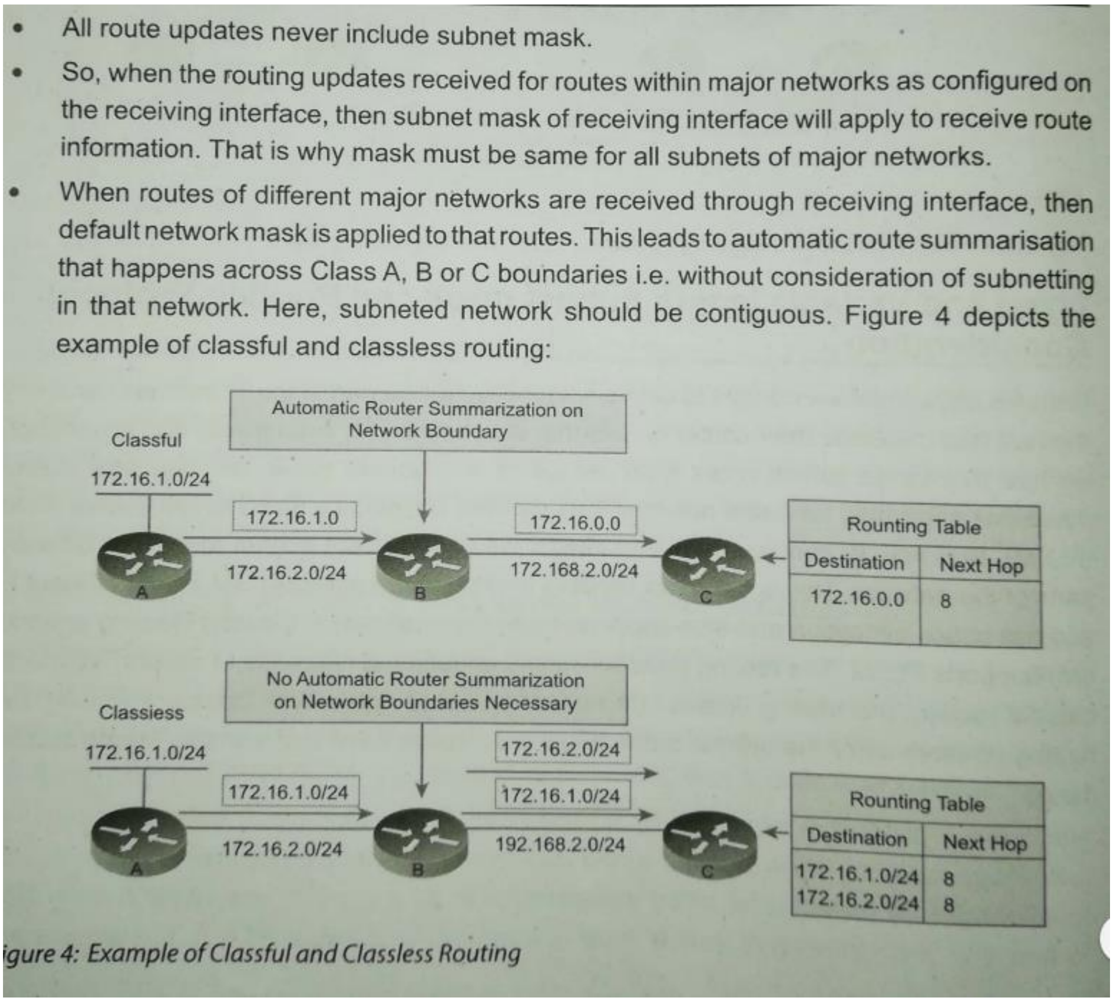
Earlier to create a subnetwork, the number of bits required by subnetwork was decided beforehand and changes to subnet mask from default to new mask needed to be applied to the entire network. This process is called FLSM.

Now to conserve IP addresses, we use different subnet masks for different parts of the network, i.e VLSM.

- VLSM allows efficient IP address space allocation and supports route summarisation.
- Classful Routing protocol only supports FLSM.

- In classful routing, routing updates do not carry the subnet mask. With classless routing, routing updates carry the subnet mask.

Classful routing protocol uses following rules while updating routing table which helps in achieving automatic route summarisation



- All route updates never include subnet mask.
- So, when the routing updates received for routes within major networks as configured on the receiving interface, then subnet mask of receiving interface will apply to receive route information. That is why mask must be same for all subnets of major networks.
- When routes of different major networks are received through receiving interface, then default network mask is applied to that routes. This leads to automatic route summarisation that happens across Class A, B or C boundaries i.e. without consideration of subnetting in that network. Here, subneted network should be contiguous. Figure 4 depicts the example of classful and classless routing:

Rounting Table	
Destination	Next Hop
172.16.0.0	8

Rounting Table	
Destination	Next Hop
172.16.1.0/24 172.16.2.0/24	8 8

igure 4: Example of Classful and Classless Routing

Classless Routing Protocols

- All routing updates including subnet masks are in CIDR form
- Subnetted networks can be discontiguous
- VLSM is possible
- VLSM is used for route summarisation, hence automated route summarisation at network edge is not required as in case of FLSM.

2. Method of assigning IP addresses

In a TCP/IP network, every node/host/server needs to have a unique IP address in the network. To make the host internet ready, Gateway Address and DNS server's address along with IP address need to be assigned.

It is a challenging task for a large network. 2 methods, static and dynamic IP address assignment.

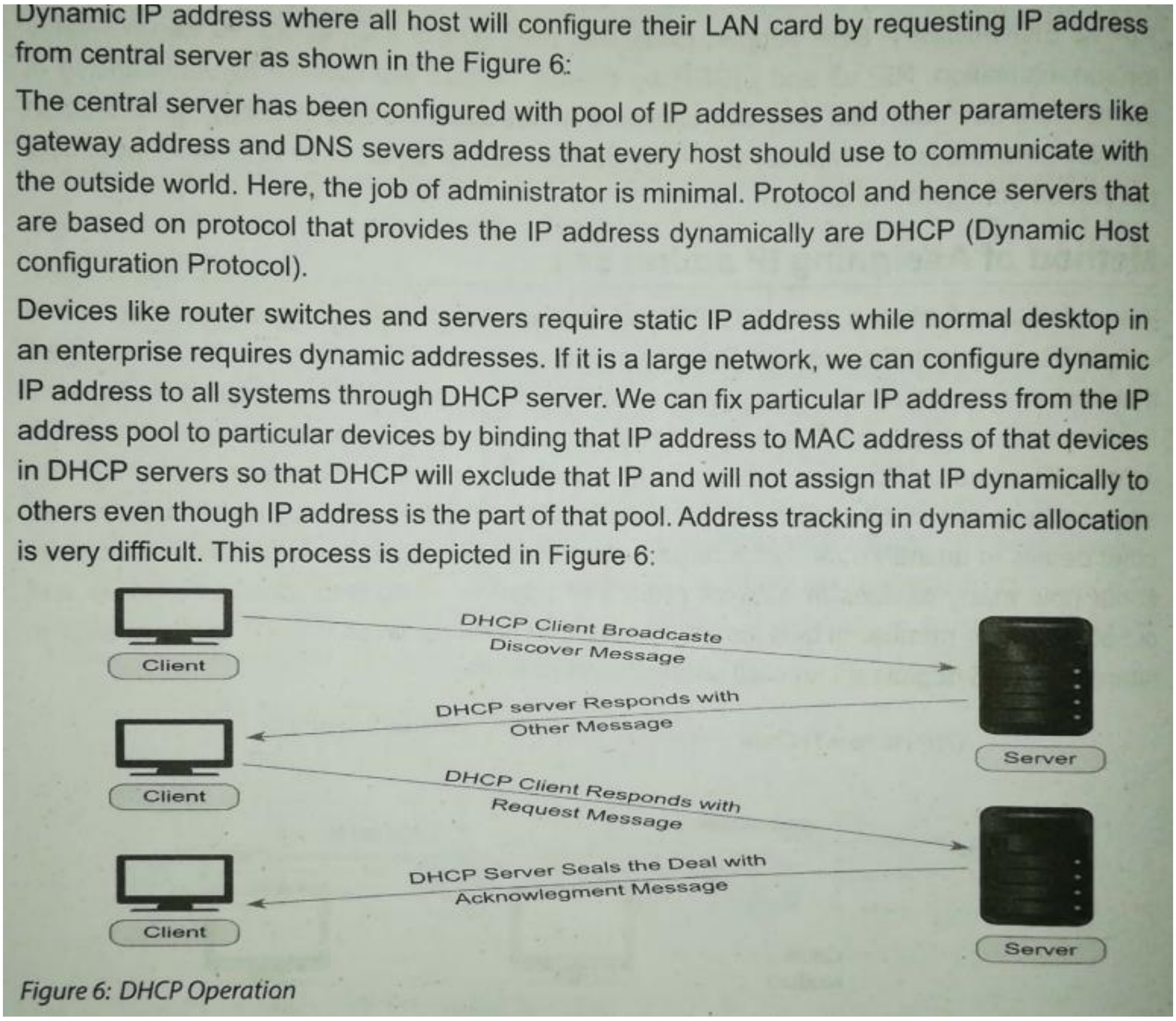
2.1 Static IP address assignment

Network Administrator needs to manually configure LAN card and provide IP address along with gateway address and DNS server address.

Net Admin might assign them room wise, department wise, etc. whatever method which helps in future problem solving.

2.2 Dynamic IP address assignment

Implemented using DHCP (Dynamic Host Configuration Protocol).



Dynamic IP address where all host will configure their LAN card by requesting IP address from central server as shown in the Figure 6:

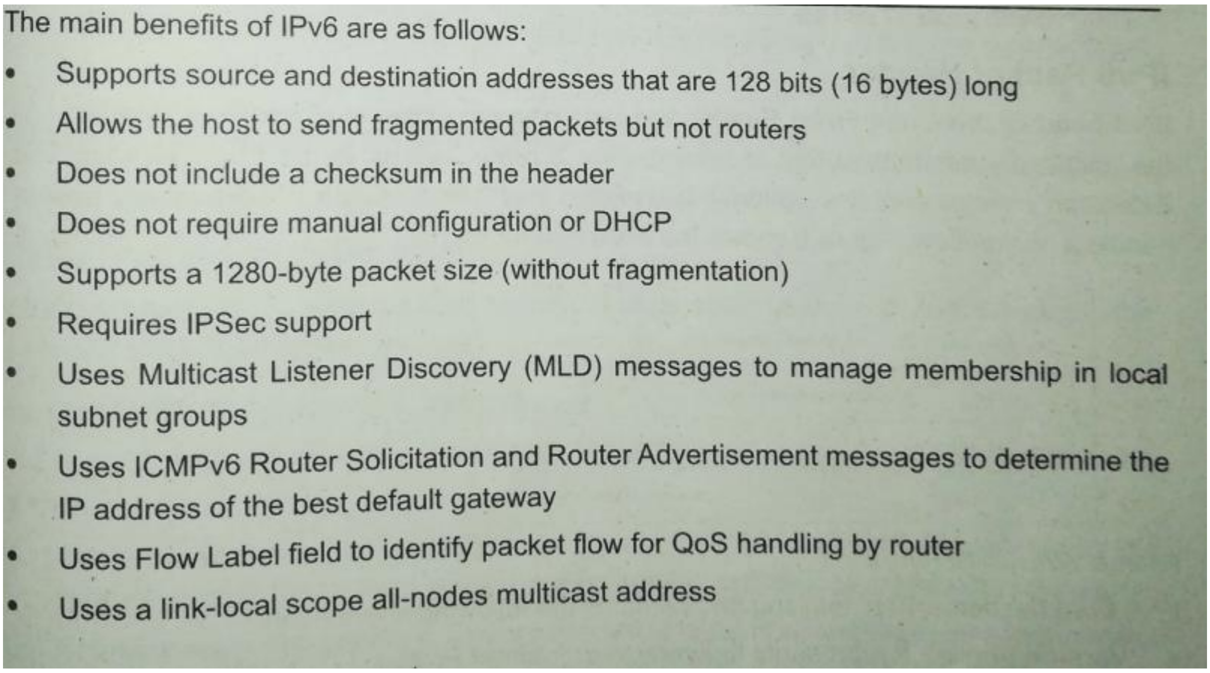
The central server has been configured with pool of IP addresses and other parameters like gateway address and DNS severs address that every host should use to communicate with the outside world. Here, the job of administrator is minimal. Protocol and hence servers that are based on protocol that provides the IP address dynamically are DHCP (Dynamic Host configuration Protocol).

Devices like router switches and servers require static IP address while normal desktop in an enterprise requires dynamic addresses. If it is a large network, we can configure dynamic IP address to all systems through DHCP server. We can fix particular IP address from the IP address pool to particular devices by binding that IP address to MAC address of that devices in DHCP servers so that DHCP will exclude that IP and will not assign that IP dynamically to others even though IP address is the part of that pool. Address tracking in dynamic allocation is very difficult. This process is depicted in Figure 6:

Client
DHCP Client Broadcaste Discover Message
DHCP server Responds with Other Message
Server
Client
DHCP Client Responds with Request Message
DHCP Server Seals the Deal with Acknowlegment Message
Client
Server

Figure 6: DHCP Operation

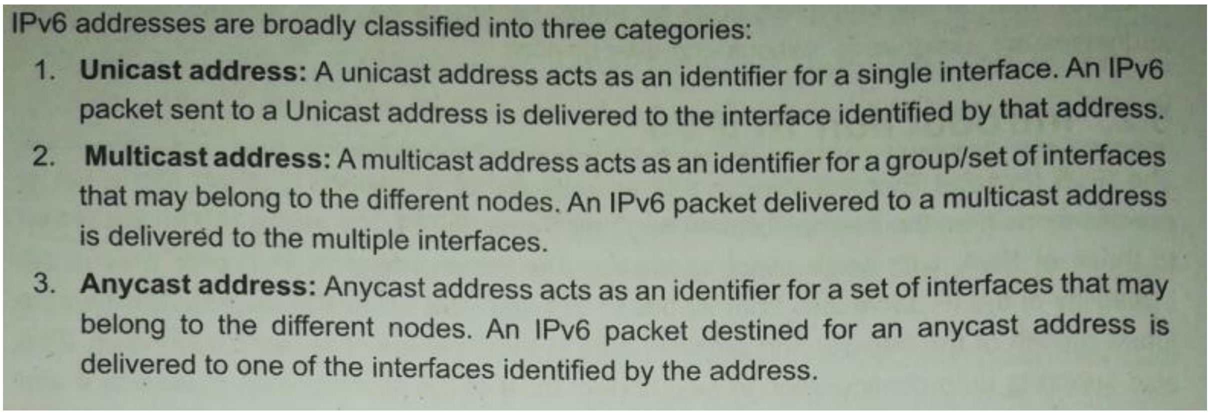
IPv6 Features



The main benefits of IPv6 are as follows:

- Supports source and destination addresses that are 128 bits (16 bytes) long
- Allows the host to send fragmented packets but not routers
- Does not include a checksum in the header
- Does not require manual configuration or DHCP
- Supports a 1280-byte packet size (without fragmentation)
- Requires IPSec support
- Uses Multicast Listener Discovery (MLD) messages to manage membership in local subnet groups
- Uses ICMPv6 Router Solicitation and Router Advertisement messages to determine the IP address of the best default gateway
- Uses Flow Label field to identify packet flow for QoS handling by router
- Uses a link-local scope all-nodes multicast address

Types of IPv6 addresses



IPv6 addresses are broadly classified into three categories:

1. **Unicast address:** A unicast address acts as an identifier for a single interface. An IPv6 packet sent to a Unicast address is delivered to the interface identified by that address.
2. **Multicast address:** A multicast address acts as an identifier for a group/set of interfaces that may belong to the different nodes. An IPv6 packet delivered to a multicast address is delivered to the multiple interfaces.
3. **Anycast address:** Anycast address acts as an identifier for a set of interfaces that may belong to the different nodes. An IPv6 packet destined for an anycast address is delivered to one of the interfaces identified by the address.

IPv6 Address Assignment Strategies

Static

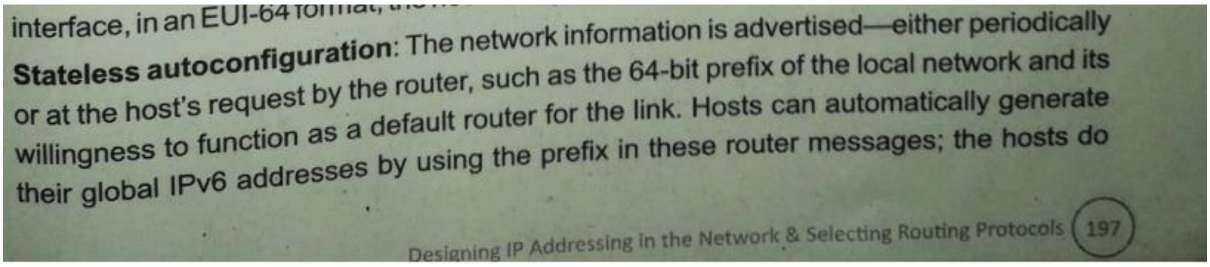
- Admin must enter IPv6 address configuration manually on every device in the network.

Dynamic

This strategy allows dynamic assignment as follows:

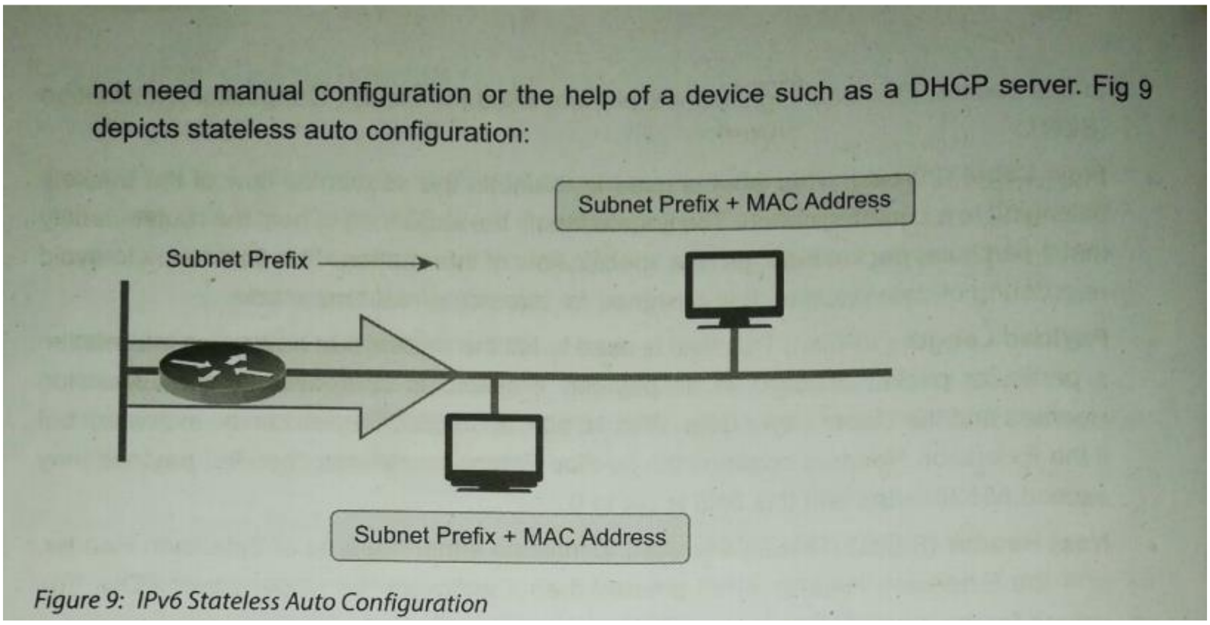
- **Link-local address**: The host configures its own link-local address autonomously using link-local prefix and a 64 bit identifier for the interface in an EUI-64 format.

- **Stateless Autoconfiguration**:



interface, in an EUI-64 format, ...

Stateless autoconfiguration: The network information is advertised—either periodically or at the host's request by the router, such as the 64-bit prefix of the local network and its willingness to function as a default router for the link. Hosts can automatically generate their global IPv6 addresses by using the prefix in these router messages; the hosts do



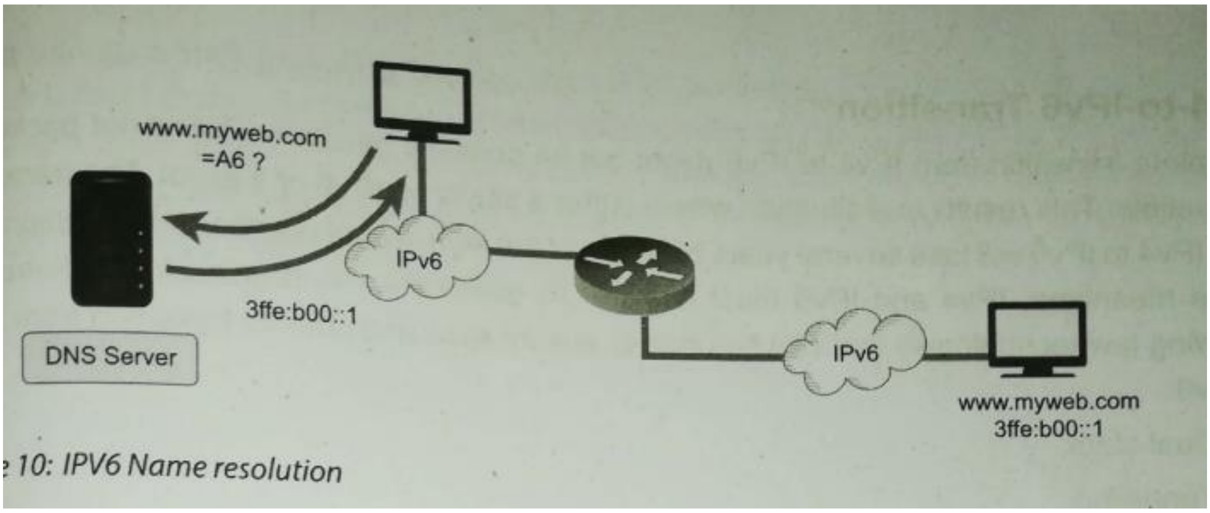
not need manual configuration or the help of a device such as a DHCP server. Fig 9 depicts stateless auto configuration:

Figure 9: IPv6 Stateless Auto Configuration

- **SLAAC (IPv6 Stateless Address Autoconfiguration)**: SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router via router advertisements (RAs).

Dynamic name resolution IPv6

Accomplished using DNS server that supports IPv6, usually along with IPv4 support.



e 10: IPV6 Name resolution

An IPv6-aware application requests destination hostname's IPv6 address from DNS server using a request for A6 record, which contains an address record for an IPv6 host). The network administrator must set up the appropriate DNS server and connect it to IPv6 network with a valid IPv6 address.

3. Routing Protocols

3.1 Types of Routes

3.1.1 Connected and Local routes

- These routes are added as a result of configuration of IPv6 addresses on interfaces.
- Dynamic routing protocols for IPv6 are good but are complex to understand and configure
- Simpler way would be that routers can add IPv6 routes to their routing tables namly, connected, local and static routes.

3.1.2 Static Routes

- IPv6 static routes are configured using ***IPv6 route*** command whereas IPv4 uses ***IP route*** command.

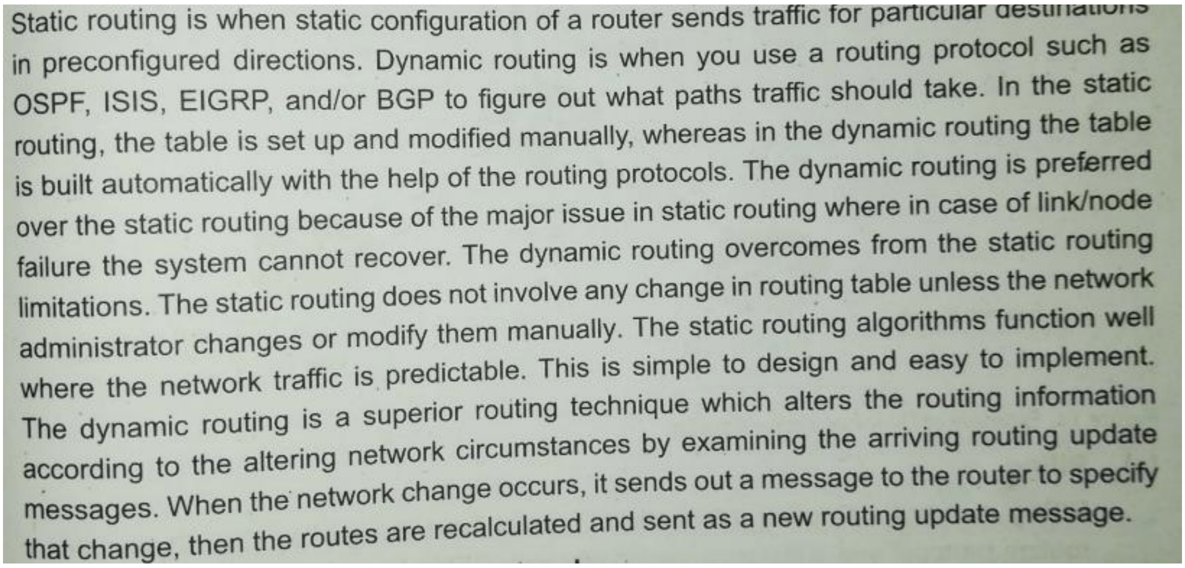
3.1.3 Dynamic Routes

- Routes learnt using dynamic routing protocols (like OSPF and EIGRP) are dynamic routes.

3.2 Routing Protocol Features

- ***Routing*** is the process to forward routable data choosing the best route amongst several available routes or path to the destination.
- A ***routing protocol*** specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network.
- There are many ways to characterize routing protocols as follows:

1. **Static vs Dynamic Routing**



Static routing is when static configuration of a router sends traffic for particular destinations in preconfigured directions. Dynamic routing is when you use a routing protocol such as OSPF, ISIS, EIGRP, and/or BGP to figure out what paths traffic should take. In the static routing, the table is set up and modified manually, whereas in the dynamic routing the table is built automatically with the help of the routing protocols. The dynamic routing is preferred over the static routing because of the major issue in static routing where in case of link/node failure the system cannot recover. The dynamic routing overcomes from the static routing limitations. The static routing does not involve any change in routing table unless the network administrator changes or modify them manually. The static routing algorithms function well where the network traffic is predictable. This is simple to design and easy to implement. The dynamic routing is a superior routing technique which alters the routing information according to the altering network circumstances by examining the arriving routing update messages. When the network change occurs, it sends out a message to the router to specify that change, then the routes are recalculated and sent as a new routing update message.

2. **Interior vs Exterior Routing**

3. **Distance vector vs Link-state vs Hybrid Protocols**

4. **Flat vs Hierarchical Routing**

3.2.2 Interior and Exterior Routing Protocols

3.2.2.1 Interior Routing Protocol

- Handles routing within an Autonomous System (one routing domain)
- 2 forms of IRP:

A. Distance Vector Protocols

In this algo, routes are selected based on the distance between networks. The distance metric is something simple enough to allow consistent values across the domain.

a. **Routing Information Protocol (RIP)**

- RIPng stands for RIP next generation, for IPv6 support
- RIP uses hop count as routing distance metric
- Works on application layer of OSI model
- Disabled by default

b. **Interior Gateway Routing Protocol (IGRP)**

- Created in response to limitations of RIP (RIP handles max hop count of 15), IGRP supports max hop count upto 255.
- One of its primary purposes is to communicate routing info to all connected routers within its boundary or autonomous system.
- Second of which is to continue updating whenever a topological, network or path change occurs

B. Link-State Protocol

- This protocol acknowledges the state of a link and advertises to its neighbours. Info about new links is learnt from peer routers.
- Complete knowledge of topology allows routers to route according to requirements, useful for traffic engineering purposes.
- Disadvantage is that it does not scale well, thus not suitable for routing across the internet at large.
- **OSPF** and **IS-IS** are both link-state routing protocols and both use Dijkstra's Shortest Path First algorithm.

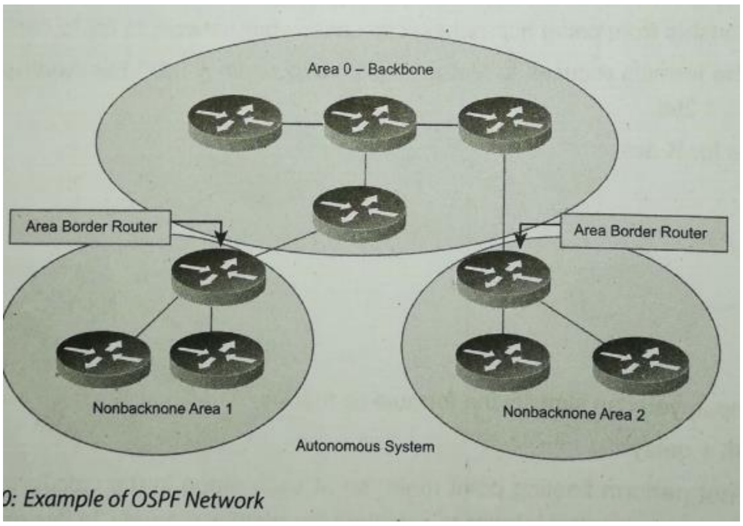
OSPF

- 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.

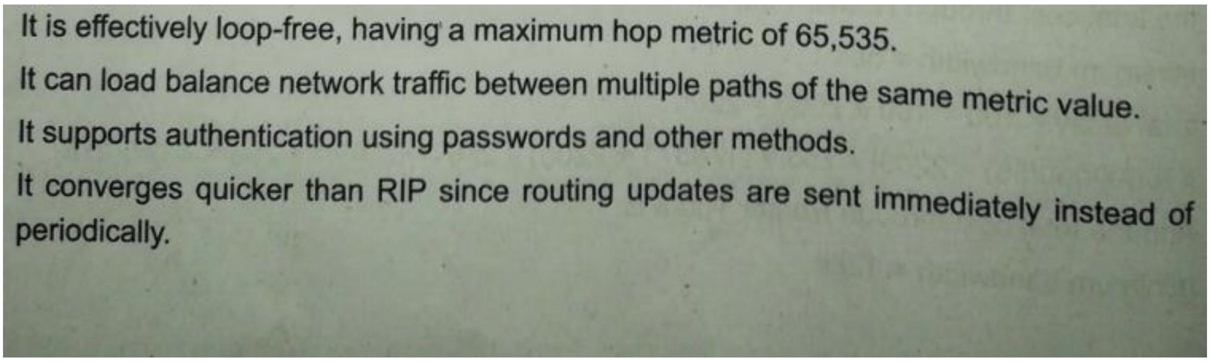
Advertisements containing routes are referred to as Link-State Advertisements (LASs) in OSPF.

- OSPF router, by keeping track of states of all various links between itself and a receiver network, makes itself a link-state routing protocol.
- OSPF selects best routes by finding lowest cost paths to a destination.
- Example:



): Example of OSPF Network

- Features of OSPF:

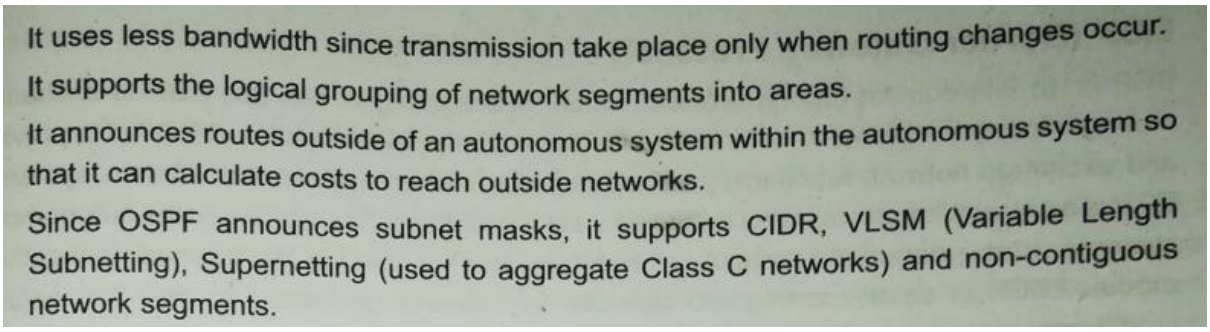


It is effectively loop-free, having a maximum hop metric of 65,535.

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.



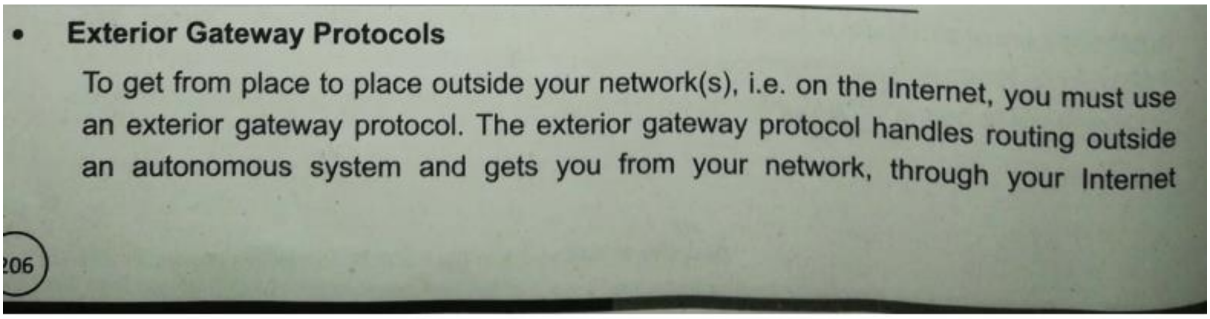
It uses less bandwidth since transmission take place only when routing changes occur.

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.

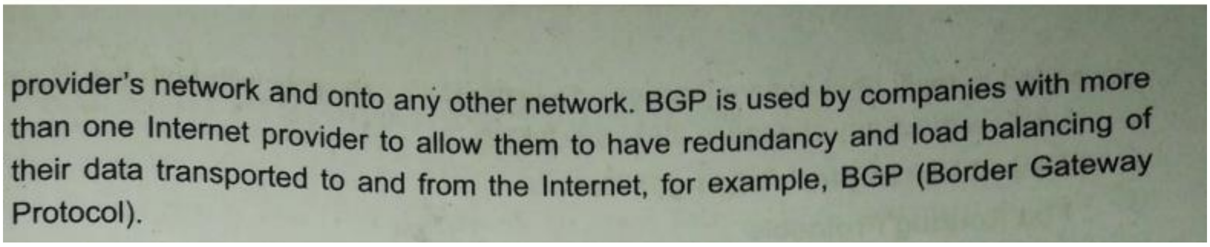
Since OSPF announces subnet masks, it supports CIDR, VLSM (Variable Length Subnetting), Supernetting (used to aggregate Class C networks) and non-contiguous network segments.

3.2.2.2 Exterior Gateway Protocols



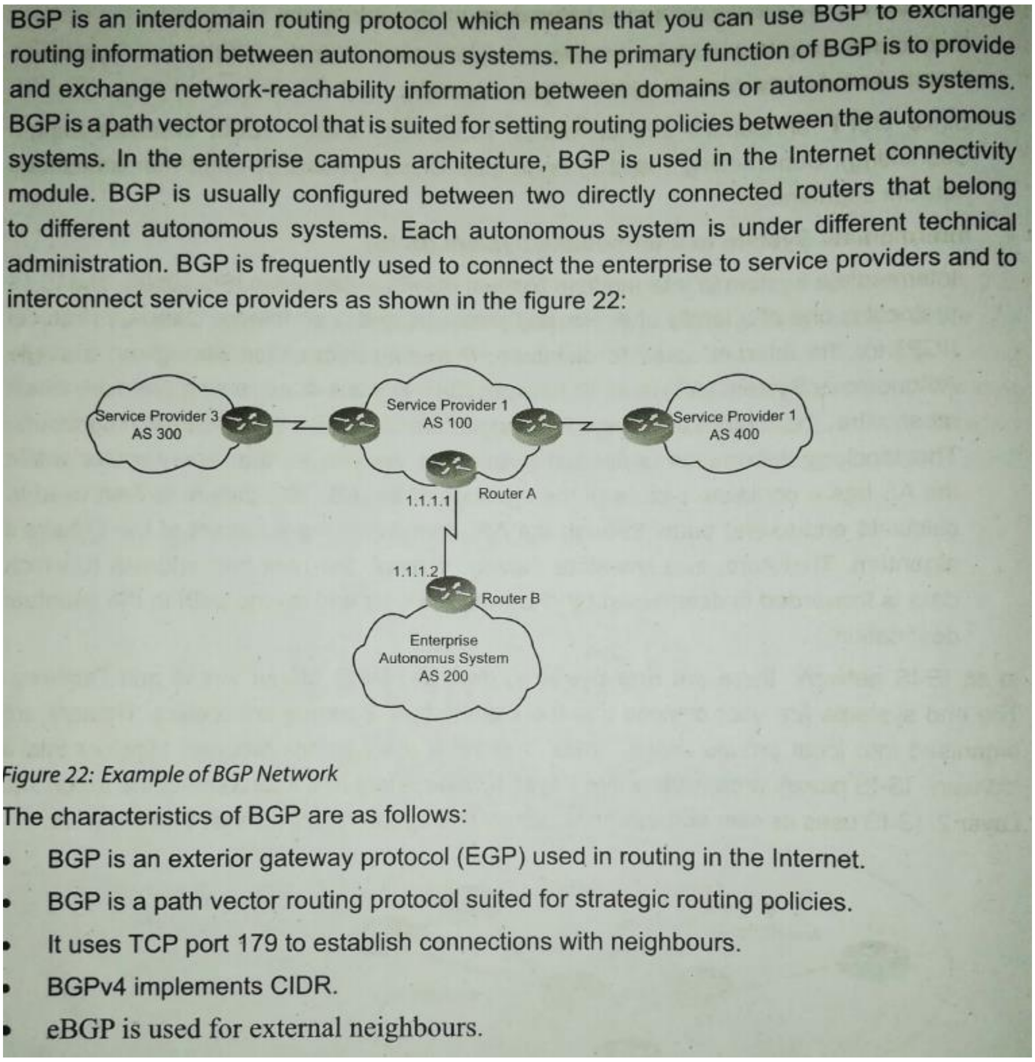
- **Exterior Gateway Protocols**

  To get from place to place outside your network(s), i.e. on the Internet, you must use an exterior gateway protocol. The exterior gateway protocol handles routing outside an autonomous system and gets you from your network, through your Internet



provider's network and onto any other network. BGP is used by companies with more than one Internet provider to allow them to have redundancy and load balancing of their data transported to and from the Internet, for example, BGP (Border Gateway Protocol).

BGP (Border Gateway Protocol)



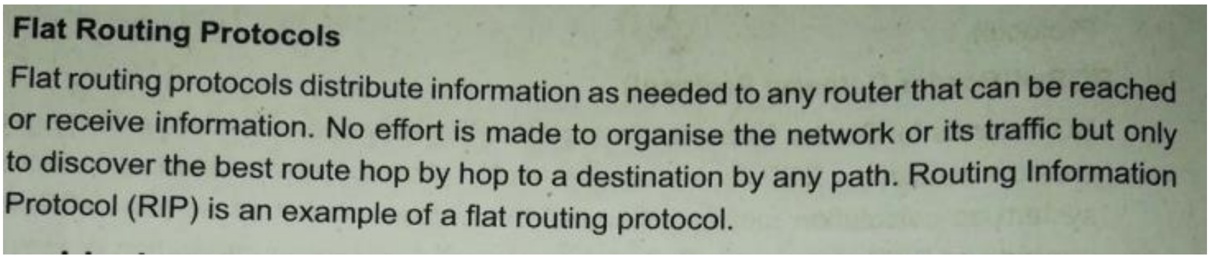
BGP is an interdomain routing protocol which means that you can use BGP to exchange routing information between autonomous systems. The primary function of BGP is to provide and exchange network-reachability information between domains or autonomous systems. BGP is a path vector protocol that is suited 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.

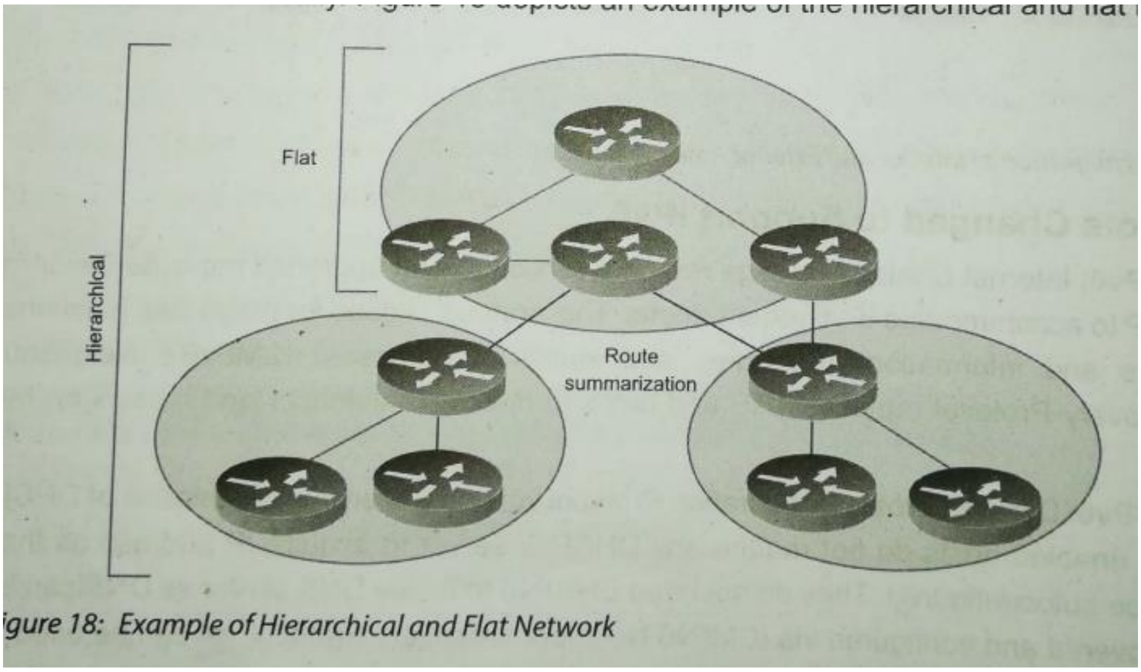
3.2.4 Flat and Hybrid Routing Protocols



Flat Routing Protocols

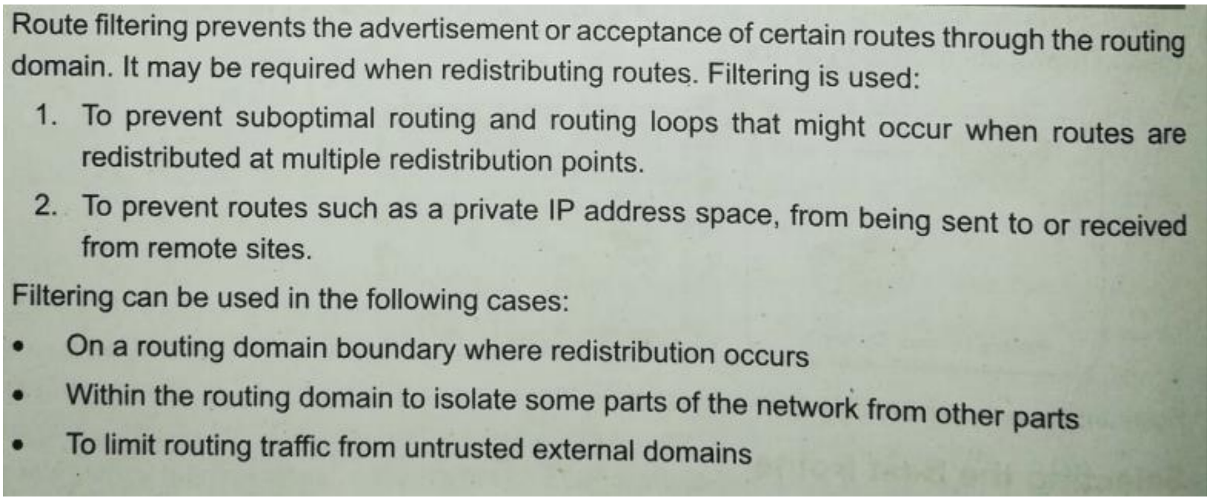
Flat routing protocols distribute information as needed to any router that can be reached or receive information. No effort is made to organise the network or its traffic but only to discover the best route hop by hop to a destination by any path. Routing Information Protocol (RIP) is an example of a flat routing protocol.

y Figure 18 depicts an example of the hierarchical and flat



igure 18: Example of Hierarchical and Flat Network

Route Filtering



Route filtering prevents the advertisement or acceptance of certain routes through the routing domain. It may be required when redistributing routes. Filtering is used:

1. To prevent suboptimal routing and routing loops that might occur when routes are redistributed at multiple redistribution points.
2. To prevent routes such as a private IP address space, from being sent to or received from remote sites.

Filtering can be used in the following cases:

- On a routing domain boundary where redistribution occurs
- Within the routing domain to isolate some parts of the network from other parts
- To limit routing traffic from untrusted external domains

END MODULE 6

Software Defined Networking

Understanding Software Defined Networking Page 233

Networking the Traditional Way

Networking the SDN Way Page 234

Traditional Approach and SDN Approach Diagram

SDN Architecture

SDN Application Plane

SDN Control Plane

SDN Data Plane

SDN Architecture Diagram Page 236

SDN Functional Architecture Diagram Page 237

SDN Building Blocks Page 237

SDN Building Blocks and Interfaces Diagram

SDN Applications and Interfaces

SDN Controller

SDN Networking Devices (OpenFlow Switch)

Open Flow Protocol Page 238

Structural View of Open Flow Protocol Page 239

OpenFlow Message Types

Controller-to-Switch Messages

Features

Configuration

Modify-State

Read-State

Packet-out

Barrier

Role-Request

Asynchronous-Configuration

Asynchronous Messages

Packet-in

Flow-Removed

Port-status

Symmetric Messages

Hello

Echo

Experimenter

Implementing Openflow Switch

OpenFlow Reference Switch Diagram Page 241

Structure of a Flow-table

OpenFlow Table Entry Diagram Page 242

OpenFlow Operation

OpenFlow Flow Processing Procedure Diagram Page 243

OpenFlow Flow Chart Page 244

Components of OpenStack Diagram

OpenStack Process Workflow Diagram Page 263

Neutron Plugins

Case Study How SDN Changed Traditional Enterprise Network Design

Effect of SDN on Traditional Enterprise Network Design

SDN Advantages over Traditional Network Design

Features considered in Case Study

Use Cases

Hospital Use Case

Manufacturing Use Case

Summary