ENTERPRISE NETWORK DESIGN

STAREDU SOLUTIONS

Neeraj Khairwal

Trupti Lotlikar

Scanned by CamScanner

Contents

1. APPLYING A METHODOLOGY TO NETWORK DESIGN 1

1.1. Network 2

→ Local Area Network (LAN) 3

→ Metropolitan Area Network (MAN) 3

→ Wide Area Network (WAN) 4

1.2. Network Components and OSI Layer 4

1.3. Network Topology 6

→ Point to Point Topology 6

→ Bus Topology 7

→ Star Topology 7

→ Ring Topology 8

→ Mesh Topology 9

→ Tree Topology 10

→ Daisy Chain Topology 11

→ Hybrid Topology 12

1.4. Transmission Technologies 12

Scanned by CamScanner

→ Token Ring 12
→ FDDI 12
→ Ethernet 13
1.5. Transmission Media 13
→ Coaxial Cable 14
→ Twisted Pair 14
→ Fibre Optics 15
1.6. CSMA/CD and CSMA/CA 16
→ Carrier Sense Multiple Access/Collision Detect (CSMA/CD) 16
→ Wireless LAN and CSMA/CA 17
1.7. Collision Domain and Broadcast Domain 17
→ Collision Domain 17
→ Broadcast Domain 18
1.8. Internetworking Devices 18
→ Repeaters 20
→ Hubs 20
→ Bridges 21
→ Switches 25
→ Routers 26
1.9. Addresses 27
→ Physical Address 27
→ Logical Address 28
1.10. Routing and Network Layer Addresses 28
→ IP Addresses 28
→ Private and Public IP Address 29
→ Subnet 30
1.11. Virtual Lans 31
→ STP and VLANs 32
→ INTERVLAN ROUTING 32
1.12. Old Network vs Current Network 33
1.13. Overview of Network Analysis, Architecture and Design Process 34
1.14. Hierarchy and Diversity 35

Scanned by CamScanner

1.15. Network Services, Characteristics and Metrics 36
→ Network Services and Metrics 36
→ Performance Characteristics 37
1.16. Cisco Service-Oriented Network Architecture 37
→ Evolution of Network Architecture 38
→ Intelligent Network 39
→ Cisco SONA Framework 40
1.17. Network Design Methodology 43
→ PPDIOO Methodology 43
→ Benefits of PPDIOO on Network Design Methodology 45
→ Design Methodology 47
1.18. Identifying Customer Requirements 48
→ Assessing the Scope of a Network Design Project 48
→ Identifying Required Information 49
→ Planned Applications and Network Services 51
→ Organisational Goals 53
→ Organisational Constraints 53
→ Technical Goals 54
→ Technical Constraints 55
1.19. Characterising the Existing Network and Sites 56
→ Sample Site Contact Information 57
→ Sample High-Level Network Diagram 58
→ Auditing or Assessing the Existing Network 59
→ Analysing Network Traffic and Applications 60
→ Network Health Checklist 61
→ Summary Report 62
→ Creating a Draft Design Document 62
1.20. Using the Top-Down Approach to Network Design 63
→ Bottom-Up Approach to Network Design 63
→ Top-Down Approach to Network Design 63
→ Decision Tables in Network Design 64
→ Structured Design 66

Scanned by CamScanner

1.21. Design Implementation Process 67
→ Planning a Design Implementation 68
→ Implementing and Verifying the Design 69
→ Monitoring and Redesigning the Network 69
1.22. Summary 70

2. STRUCTURING AND MODULARISING THE NETWORK 71
2.1. Network Hierarchy 72
→ Hierarchical Network Model 72
2.2. Using A Modular Approach To Network Design 80
→ Cisco SONA Framework 81
→ Functional Areas of Cisco Enterprise Architecture 81
→ Guidelines for Creating an Enterprise Network 84
→ Enterprise Campus Modules 85
→ Enterprise Edge Modules 88
→ Service Provider Modules 92
→ Remote Enterprise Modules 93
2.3. Services within Modular Networks 94
→ Interactive Services 94
→ Security Services in Modular Network Design 96
→ High-Availability Services in a Modular Network Design 100
→ Voice Services in a Modular Network Design 104
→ Wireless Services in a Modular Network 107
→ Application Networking Services in a Modular Network Design 108
2.4. Network Management Protocols and Features 109
→ Simple Network Management Protocol (SNMP) 112
→ MIB 115
→ RMON 116
→ Syslog Accounting 118
2.5. Summary 120

3. DESIGNING BASIC CAMPUS AND DATA CENTRE NETWORKS 121
3.1. Campus Design Considerations 122

Scanned by CamScanner

→ Application Considerations 122
→ Environmental Considerations 126
→ Infrastructure Considerations 129
3.2. Enterprise Campus Design 132
→ Building Access Layer Design Considerations 132
→ Building Distribution Layer Design Considerations 133
→ Campus Core Design Considerations 135
→ Server Placement 138
3.3. Enterprise Data Centre Design Considerations 141
→ The Enterprise Data Centre 141
→ Enterprise Data Centre Infrastructure 144
3.4. Summary 146

4. **DESIGNING REMOTE CONNECTIVITY 147**
4.1. Enterprise Edge Wan Technologies 148
→ Introduction to WANs 148
→ WAN Interconnections 148
→ Traditional WAN Technologies 149
→ WAN Transport Technologies 151
4.2. WAN Design 160
→ Application Requirements 161
→ Technical Requirements 163
→ WAN Ownership 166
→ Bandwidth Optimisation 166
4.3. Using WAN Technologies 168
→ Remote Access Network Design 168
→ VPN Design 168
→ WAN Backup Strategies 170
→ The Internet as a WAN Backup Technology 173
4.4. Enterprise Edge WAN and MAN Architecture 173
→ Enterprise WAN Architecture Technologies 174
4.5. Selecting Enterprise Edge Components 178
4.6. Enterprise Branch and Teleworker Design 179

Scanned by CamScanner

→ Enterprise Branch Architecture 179
→ Enterprise Branch Design 181
→ Enterprise Teleworker Design 185
4.7. Summary 186

5. **DESIGNING IP ADDRESSING IN THE NETWORK & SELECTING ROUTING PROTOCOLS** 187
5.1. Designing an IP Addressing Plan 188
→ Determine the Size of the Network 188
→ IP address Hierarchy and Routing 188
→ Route Summarisation– Route Supernetting 188
→ Benefit of Hierarchical Addressing for large networks 189
→ Summarisation Groups in Multilevel Hierarchical Network 190
→ Disadvantages of Poorly Designed IP Addressing 190
→ Fixed and Variable length Subnet mask and Routing Protocol Consideration . 191
→ Classful Routing protocols uses following rules while updating the routing tables and which help in achieving automatic route summarisation 192
→ Method of Assigning IP addresses 193
5.2. Introduction To IPV6 195
→ IPV6 Features 195
→ Types of IPv6 Addresses 196
→ IPV6 Address Notation and Header Format 196
→ Address Assignment Strategies 197
→ IPv6 Name Resolution 198
→ IPv4-to-IPv6 Transition Strategies and Deployments 199
5.3. Routing Protocols 202
→ Types of Routes 202
→ Routing Protocol Features 202
5.4. Routing Protocols for Enterprise 209
5.5. Routing Protocol Deployment 214
5.6. Route Redistribution 216
5.7. Route Filtering 218

Scanned by CamScanner

5.8. Redistributing And Filtering With Bgp. 218
5.9. Route Summarisation. 220
5.10. Summary 221

6. **SOFTWARE DEFINED NETWORKING 223**
6.1. Understanding Software Defined Networking [SDN] 224
→ Networking the Traditional Way: 224
→ Networking the SDN Way 225
→ SDN Architecture 226
6.2. SDN Building Blocks 228
6.3. Open Flow Protocol 229
6.4. Openflow Message Types 230
→ Controller-to-Switch Messages: 230
→ Asynchronous Messages 231
→ Symmetric Messages: 231
6.5. Implementing Openflow Switch 232
→ OpenFlow Reference Switch: 232
→ Structure of a Flow-table. 233
→ Open Flow Operation 234
→ Flow Table Entry Field 235
→ SDN OpenFlow Laboratory Implementation 236
6.6. Openflow Controllers 244
6.7. NOX 247
6.8. POX 248
→ Running POX Application 249
6.9. Open Flow in Cloud Computing 252
→ OpenStack and Neutron 252
→ OpenStack Process Workflow 254
→ Neutron Plugins 256
6.10. Case Study: How Sdn Changed Traditional Enterprise Network Design 256
→ Effect of SDN on Traditional Enterprise Network Design 256

Scanned by CamScanner

→ The Features considered in case study 257
→ Use Cases: 259
6.11. Summary 260

Scanned by CamScanner

Applying a Methodology to Network Design

1

OBJECTIVES

After reading this chapter, the student will be able to:

- To learn networking fundamentals
- To introduce network design methodology
- To build an effective network design solution
- To understand the design implementation process

Scanned by CamScanner

The main discussion area in this book is about network design. As Information and Communication Technology (ICT) is going to be the main pillar for any organisation, the business success of an organisation is driven by the successful implementation of ICT. Here ICT includes not only the development of software for various activities of an organisation, but the underlying support of the computer network. The software helps the organisation to process information and will help with strategic decisions. When software, like ERP, processes huge data to give various insights into information, the main concern is the storage of this large data. Also, there is a need to think about designing a disaster recovery site. The success of ICT implementation is when commuting and communication go hand in hand. Twenty years back, computer networking was about connecting computers so that users were able to share files or printing devices or other network resources. Computer networking is not limited to connection, rather it extends to networking application, bandwidth and reliability of network. This chapter is about a recap of basic networking concepts keeping in mind about the design perspective of the networks. Later sections cover the network design methodology.

1.1. Network

Based on the area covered by the network, the network can be classified into Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN). They differ from each other based on three categories viz. size, transmission technology and topology. Figure 1 shows different types of the network as a part of a single corporate office in multiple sites:

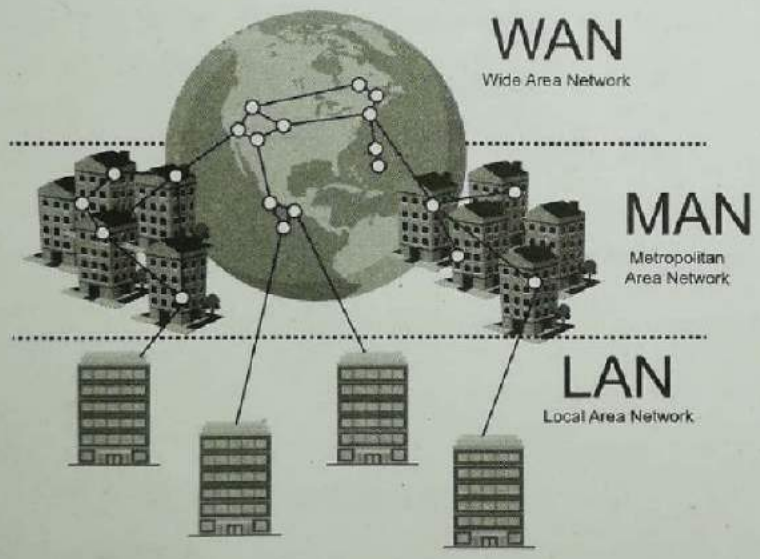


Figure 1: LAN, WAN, MAN as part of a single corporate office in multiple sites

Let us discuss each one of them with respect to the design perspective.

Scanned by CamScanner

Local Area Network (LAN)

Local Area Network (LAN) refers to the network spread across a building or a campus. It is used to share resources and exchange information across less than 500 interconnected devices. Sharing of information, resources and network services reduces the cost of the network. Information can be easily exchanged across an organisation using LAN. Since LANs are restricted in size, transmission time across the network can be known well in advance. Knowing this limitation makes the network management simpler and easier.

The transmission technology used for LANs may be a Token Ring network, Fiber Distributed Data Interface (FDDI) network or Ethernet. Star, bus and ring are commonly used topologies for designing LAN. IEEE 802.3 defines LAN access methods using CSMA/CD.

The design of LAN is for an organisation within a single building or within a single campus. In a broad sense, only one transmission technology will be considered for the entire LAN or utmost two will be considered. For example, Ethernet IEEE 802.3 or IEEE 802.11x. More focus will be on designing a network to support application requirement, centralised storage of files, access of cloud-based applications and design of Demilitarised zone to protect public servers of the organisation.

Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) refers to the network across a metropolitan city such as Delhi, Mumbai, etc. It spans across a city and has a larger area than LAN. MAN connects two or more local area networks situated in the same city. For example, MAN might be used to connect various branches of an organisation in a single city. MAN can be completely owned and operated by a private company. Thus, it proves to be the backbone for large networks. MAN uses Distributed Queue Dual Bus (DQDB) or the IEEE 802.6 standard which enables data transmission in both directions simultaneously. MAN is widely used to connect banks, universities and colleges. Therefore, designing of MAN is extending the private network across multiple sites of an organisation. Here, all design considerations of LAN need to be considered along with the design of the backbone network to support multiple sites. A strategy for designing reliable backup and storage site is also created. As multiple sites of an organisation in a city are working on different administrative aspects of an organisation, heterogeneous connectivity at the operating system level also needs to be considered. For example, single sign-on mechanism across sites or access of data from servers of different OSs etc. Also, the network should support the integration of various applications across multiple sites seamlessly.

Scanned by CamScanner

Wide Area Network (WAN)

Wide Area Network (WAN) refers to the network spanning across multiple cities, countries or continents. It uses long distance carriers whereas the protocols and equipment are the same as used in MAN. Internet is the best example of WAN. International banks across several countries are connected through WAN. It might be a group of MANs, LANs or both. If a WAN is specifically owned by a large, private company, it is better known as Enterprise Network. One or more Internet Service Providers can be used to offer network services such as the Internet, asynchronous transfer mode and frame relay. It is slower and less reliable than LAN. WAN utilises many media for communication, such as cables, fibre, telephone lines, satellite and airwaves. Since it covers a large geographical area, setting up a WAN is an expensive, time-consuming and complicated task. Once a WAN is set up, network supervisors and technicians are required to maintain the network. Security is undoubtedly a major concern when people from different verticals access information from devices connected through WAN. Security against hackers and viruses, apart from malicious users, is much required. For a mid-sized organisation, the design of efficient and secure Virtual Private Network (VPN) to connect multiple offices across the city is a challenging task. For that, the Routing strategy for implementation of Software Defined Network across multiple sites needs to be considered. Prioritisation of application-specific traffic is also a part of the critical design strategy.

1.2. Network Components and OSI Layer

In today's era, working in a networking environment is very common and has become pervasive in our life. Anyone can easily identify various networking components involved while working on a network-based application. For example, for a mobile to access a website, end devices easily identifiable include wireless access point or another wired media, LAN card, Operating system, etc. As shown in Figure 2, a user accesses a website hosted on the server based in the US, using the Chrome browser from his/her Android mobile. Here information is transferred from the client (mobile) side to server side having different Operating systems, and different NIC cards through different transmission media. And this is possible due to the Open Systems Interconnections (OSI) reference model created by the International Organization for Standardization (ISO). Figure 2 shows using a mobile browser to access the content from a web server.

Scanned by CamScanner

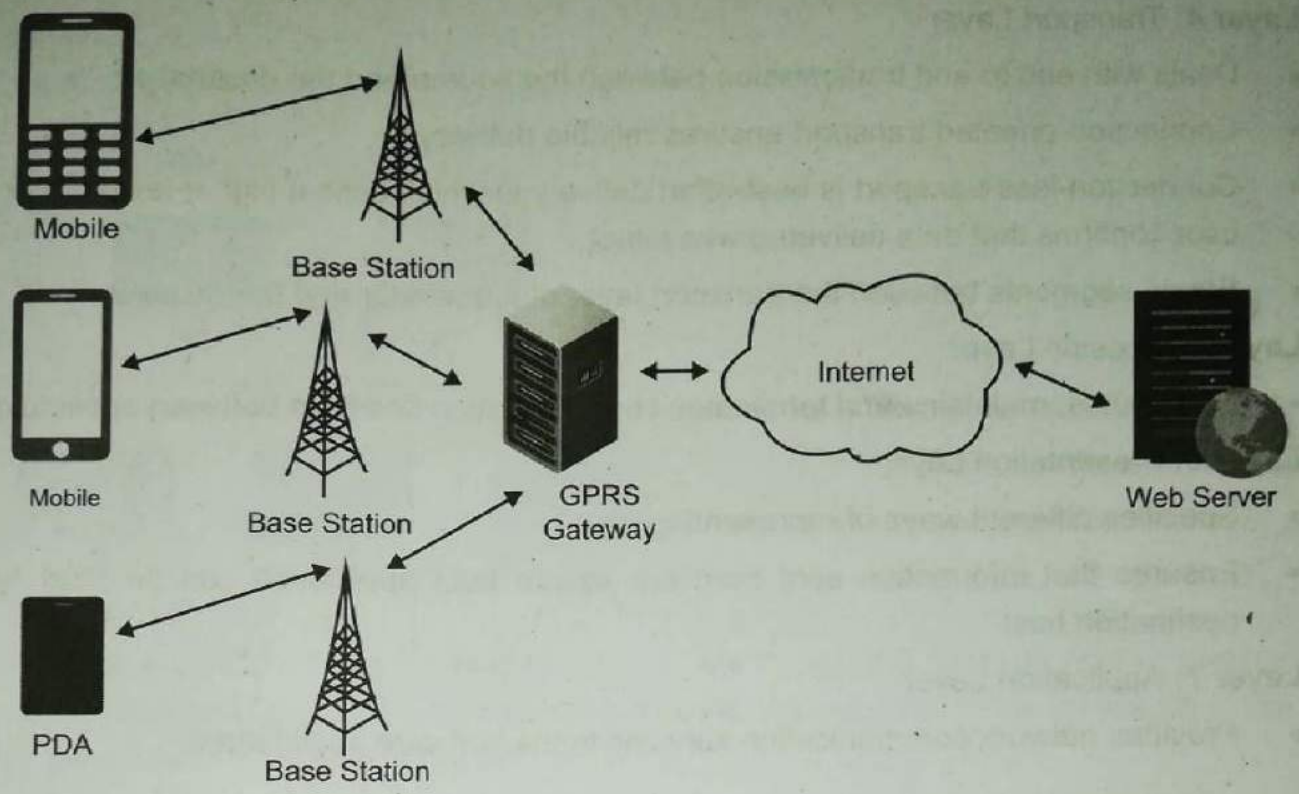


Figure 2: Mobile Browser to Access Content from Web Server

The OSI seven-layer model is designed based on the network functions required for communication. The model specifies what needs to be done and not how to do it. The functionality required by each layer can be implemented in varied ways by different protocols. For example, network layer implementation is done by the open standard Internet Protocol (IP) as well as Novell's Internetwork Packet Exchange (IPX) protocol. Let us have a quick overview of seven layers of the OSI reference model:

Layer 1: Physical Layer

- Deals with physical and mechanical specifications
- Supports binary transmission of data

Layer 2: Data Link Layer

- Deals with physical addressing, error control and flow control across the physical network
- Transmits frames between network devices

Layer 3: Network Layer

- Deals with data forwarding across the logical internetwork that might consist of multiple physical networks
- Fragments datagram into packets if the amount of data to be transmitted is more than the network can handle at a time and reassembles at the destination

Scanned by CamScanner

Layer 4: Transport Layer

- Deals with end to end transmission between the source and the destination
- Connection-oriented transport ensures reliable delivery
- Connection-less transport is best-effort delivery in which case a higher level protocol or user confirms that data delivered was intact
- Sends segments between the transport layer of the sender and the receiver

Layer 5: Session Layer

- Establishes, maintains and terminates communication sessions between applications

Layer 6: Presentation Layer

- Specifies different ways of representing data
- Ensures that information sent from the source host application can be read by the destination host

Layer 7: Application Layer

- Provides network communication services to the software applications

1.3. Network Topology

Network topology refers to the arrangement of network components in the communication network. And it is an important part of designing the network. Network topology is differentiated as logical topology and physical topology. Actually, devices are connected in physical topology but appear to the user in logical topology. Understanding VLAN will give a clear picture of this concept which is covered later in this chapter. There are eight different network topologies viz. point to point, bus, star, ring, mesh, tree, daisy chain and hybrid. Let us discuss each one in detail.

Point to Point Topology

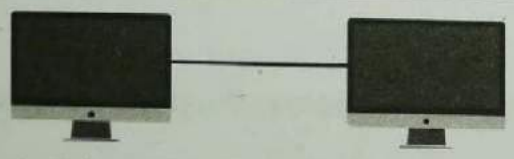


Figure 3: Point to Point Topology

As the name suggests, in point to point topology, exactly two hosts are directly connected to each other with a dedicated link.

Advantage:

- High performance

Scanned by CamScanner

Disadvantage:

- Failure of a node disconnects the network

Bus Topology

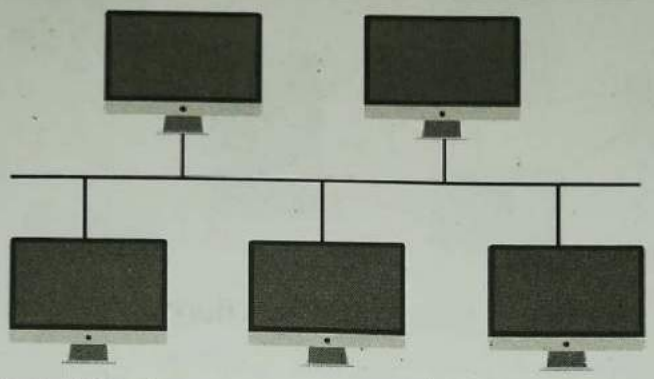


Figure 4: Bus Topology

In this topology, each node is connected only to one cable and thus, all nodes share a single communication line i.e. the central cable. The central cable being the backbone of the network serves as the single point of failure.

Advantages:

- Cost effective
- Easily expandable

Disadvantages:

- Central Cable failure leads to network failure.
- Performance degrades as network traffic or nodes increases.

Star Topology

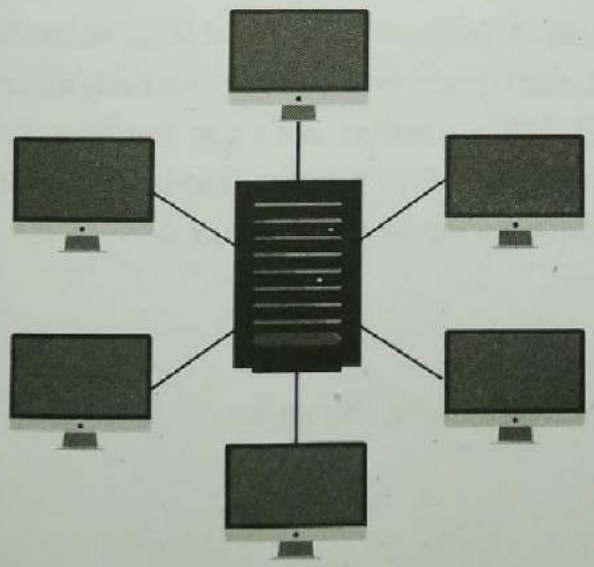


Figure 5: Star Topology

Scanned by CamScanner

All nodes are connected to a single, central hub using point to point connection. Communication among any two nodes is through the hub. Thus, the hub acts as a repeater. A new node can be easily added and configured. Being the most common Ethernet network topology, it is the most popular topology in business today. 10Base-T is an example of the star topology.

Advantages:

- Better scalability
- Easier to manage

Disadvantages:

- Failure of the hub results in network failure.
- Since all communication is through the hub, it can be a bottleneck during heavy traffic.

Ring Topology

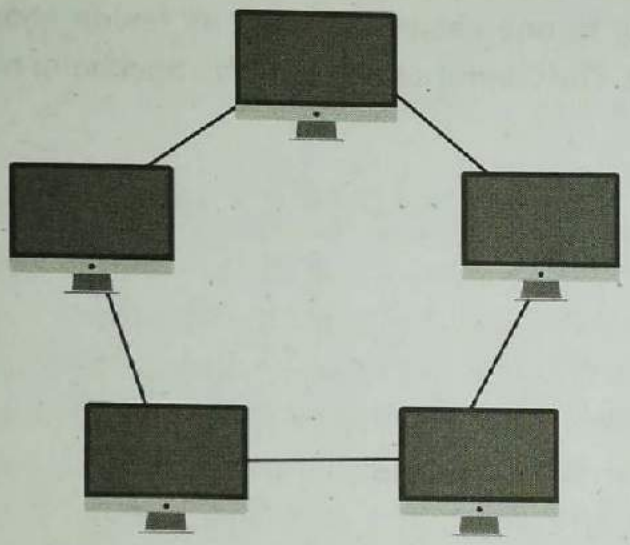


Figure 6: Ring Topology

Ring topology derives its name from the fact that each node is connected to another node and the last node connecting to the first one. Thus, each node has exactly two neighbours. It is a bus topology in a closed loop. For a larger network, repeaters are used to prevent data loss. This topology is preferred for a token ring environment. In a token ring environment, a token is sent with data from one node to another until the destination is found.

Advantages:

- Easy to install and expand
- Performance better than bus topology when network traffic increases.

Disadvantage:

- Each node acts as a single point of failure.

Scanned by CamScanner

Mesh Topology

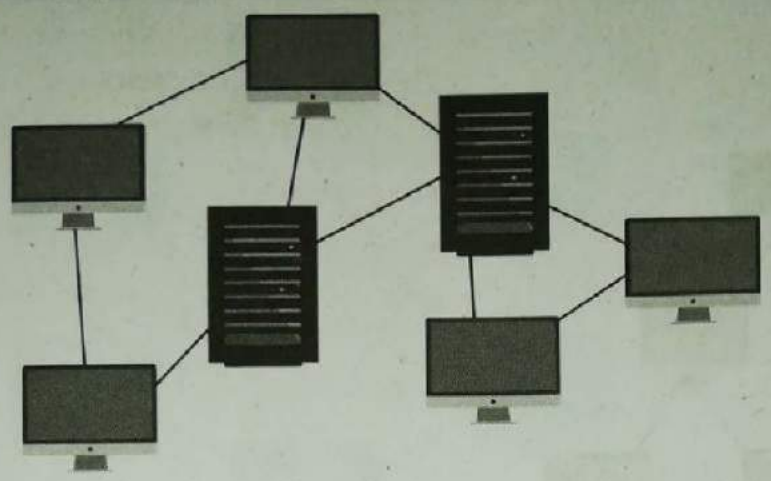


Figure 7: Mesh Topology

In the mesh topology, there is a point to point connection between two nodes. All the nodes are connected to other nodes in the network. To have a direct connection between n nodes, n(n-1)/2 physical connections are required. In the partial mesh topology, all nodes are not directly connected to each other. In full mesh topology, each node has a point to point connection to every other node in the network. This topology is preferred for networks demanding high availability.

Advantages:

- Secure, private, robust and highly reliable
- No single point of failure
- Easy fault detection

Disadvantages:

- Requires network connection to all other devices
- Expensive installation and configuration

Scanned by CamScanner

Tree Topology

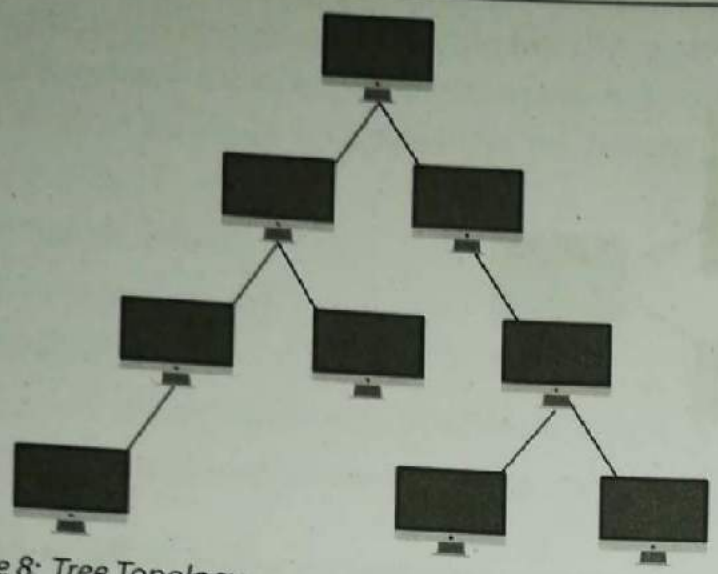


Figure 8: Tree Topology

This topology consists of a root node where all other nodes are connected in a hierarchy. Hence, it is also known as hierarchical topology. It is an extended star topology which inherits features of bus topology. The structure of the tree topology easily divides the network into multiple layers.

Advantages:

- Easily expandable and manageable
- Easy fault detection

Disadvantages:

- Entire network fails if root node fails
- Costly as it is heavily cabled.

Daisy Chain Topology

Figure 9: Daisy Chain Topology

In this topology, all nodes are connected to each other in a series, one after another, in a linear fashion. Except for the end node, all nodes are connected to exactly two nodes.

Advantages:

- Simplicity and scalability

Disadvantages:

- Each link or node acts as a single point of failure.

Scanned by CamScanner

Hybrid Topology

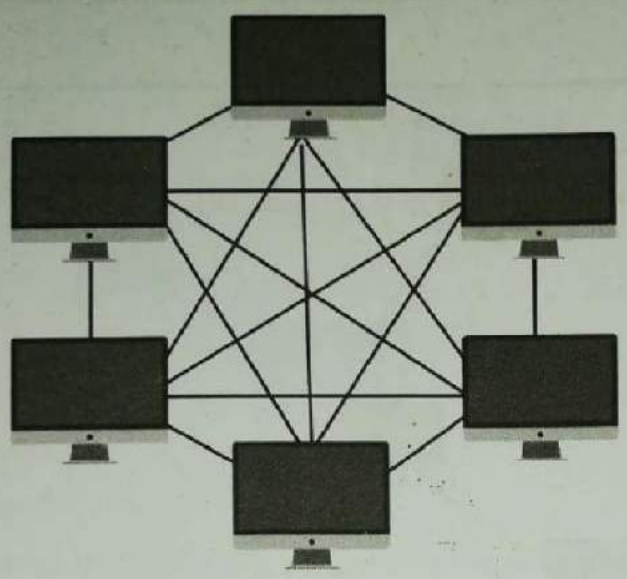


Figure 10: Hybrid Topology

Hybrid topology is a combination of two or more standard topologies where the resulting network does not exhibit any standard topology. Tree topology is a typical example of hybrid topology where star networks are interconnected through the bus network. Other examples of hybrid topologies include:

- Star-ring network
- Star network of star networks
- Hybrid mesh network
- Hierarchical star network

Advantages:

- Scalable and flexible
- Reliable

Disadvantages:

- Network design is complex
- Costly

Scanned by CamScanner

1.4. Transmission Technologies

Token Ring

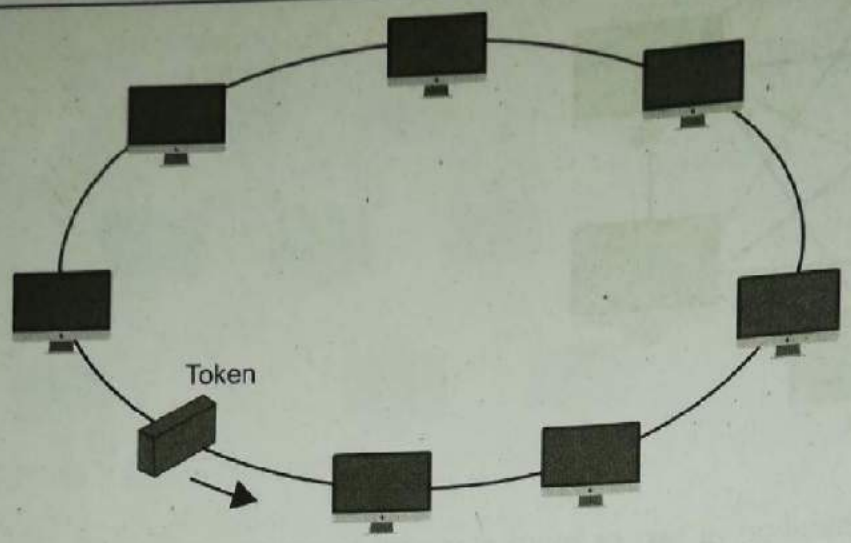


Figure 11: Token Ring

Token Ring is IBM's LAN technology which typically uses twisted pair wires. It gives high throughput for networks having deterministic nature of medium access. 16 Mbps data rate is supported by a token ring network. A token ring is depicted in Figure 11.

FDDI

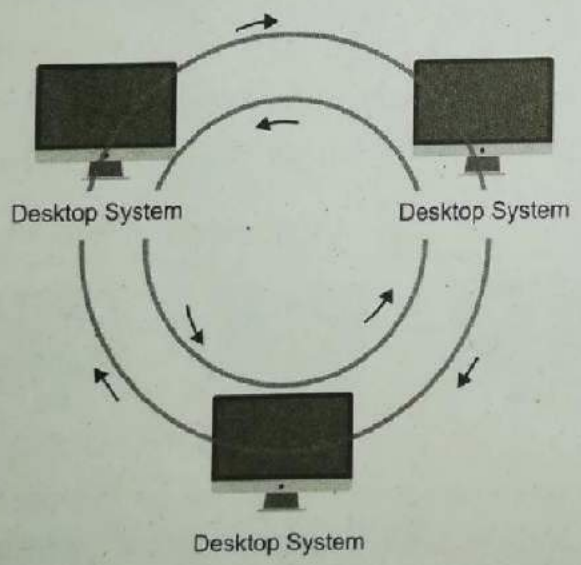


Figure 12: FDDI

FDDI is a standard developed by the American National Standards Institute (ANSI). It transmits data on optical fibres at transmission rates up to 200 Mbps. Generally, a dual ring network is used where the first ring is used to carry data whereas the second ring is for backup. FDDI is shown in Figure 12.

Scanned by CamScanner

Ethernet

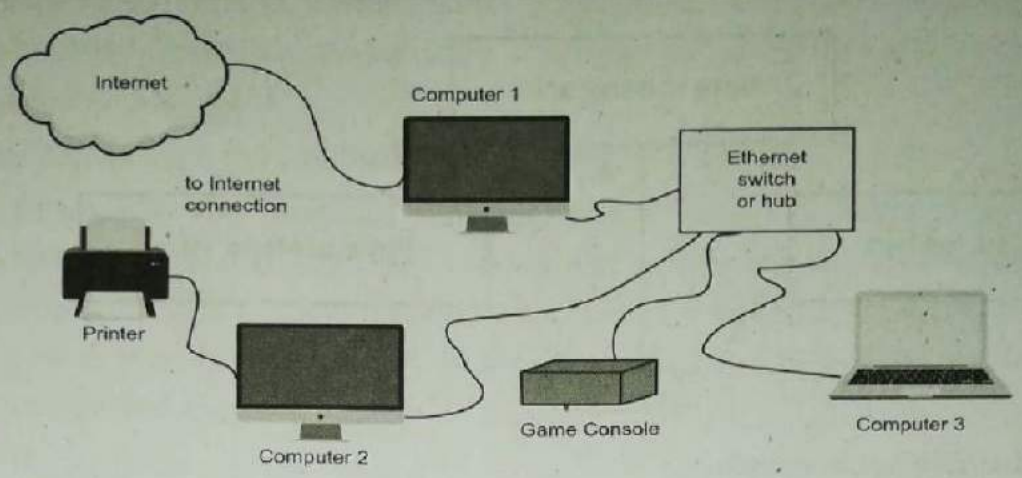


Figure 13: Ethernet

Ethernet is the transmission technology that is established in the IEEE 802.3 standard. The data rate in the range of 10 Mbps-10 Gbps is supported by Ethernet. Ethernet speed has been raised from 10Mbps to 100Mbps for Fast Ethernet and to 1000Mbps for Gigabit Ethernet. Being fast and reliable, Ethernet is the most widely used LAN standard. Generally, star and bus topologies are used with Ethernet. Ethernet has evolved through four generations as depicted in Table1

Table 1 Evolution of Ethernet

ETHERNET	SPEED
Standard Ethernet	10 Mbps
Fast Ethernet	100 Mbps
Gigabit Ethernet	1 Gbps
Ten-Gigabit Ethernet	10 Gbps

1.5. Transmission Media

Today we use different media like coaxial cable, twisted pair and fibre optic in the physical layer of the network as represented in Table 2

Table 2 Transmission Media

Coaxial Cable	Twisted Pair	Fibre Optic
Thick wire 10Base-5	10Base-T	10Base-F
Thin wire 10Base-2	100Base-T	1000Base-X
	1000Base-T	

Let us discuss each one in detail.

Scanned by CamScanner

Coaxial Cable

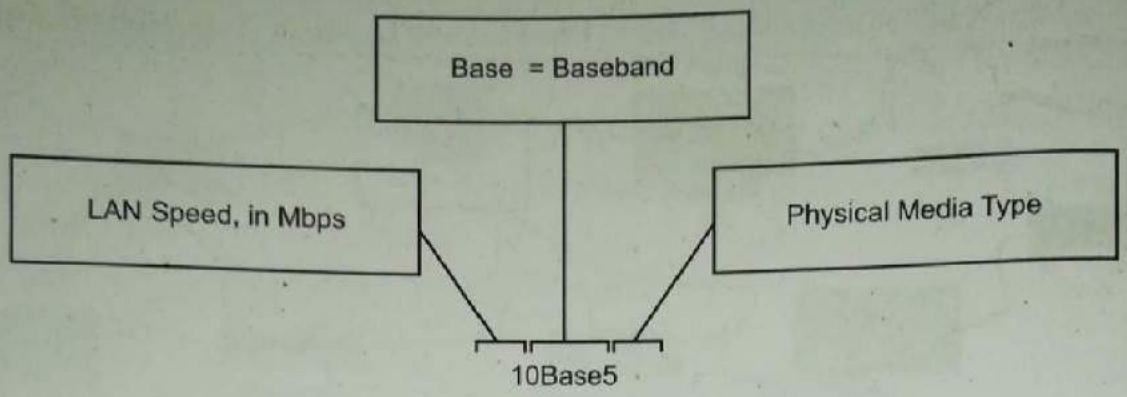


Figure 14: Coaxial Cable Naming Convention

The name coaxial cable is derived from the physical characteristics of the cable. Generally, it is represented as:

[bandwidth/data rate in Mbps][Signalling method]-[Maximum segment length or cable type]

10Base-5 coaxial cable can be interpreted as-

10: Mbps bandwidth of signal

Base: Baseband signalling

5: 500 metres is the segment length, that is, the longest distance to which a cable can carry the signal.

Media standards in the coaxial cable technology are:

1. **10Base-5**: was used in standard Ethernet. It is also known as thick Ethernet or thicknet. Length of the coaxial cable is maximum 500 metres in the network. 100 nodes can be connected using 10Base-5 using the RG-8 connector. Thick wire 10Base-5 coaxial cable was expensive. Therefore, the thick wire was replaced by comparatively cheaper thin wire 10Base-2 cable.
2. **10Base-2**: Thin wire is also referred to as thinnet, thin Ethernet and cheapernet. Thin wire can carry signal up to 185 metres. It has been rounded up to 200 metres for the name of the cable i.e. 10Base-2. Due to this, a maximum of only 30 nodes can be connected with a minimum distance of 50 cm between two devices. It uses the coaxial cable that is terminated with BNC connectors. This media is ideal for small networks having only two or three nodes.

Twisted Pair

UTP stands for Unshielded Twisted Pair and is the most commonly used wiring in Ethernet. It has several categories and performance level. Several limitations of the previous standard could be overcome using twisted pair cabling in the star topology for Ethernet. For example, overall cost of the Ethernet network was reduced as telephone services were using twisted

Scanned by CamScanner

pair cables in office premises. Since star topology was already in use for telephone services and is easier to manage, it was a preferred approach than the bus topology. Troubleshooting was simplified using the star topology. The networks could be easily upgraded by the use of advanced switching hubs.

Media standards in the twisted pair technology are:

1. **10Base-T**: The family of Ethernet over twisted pair technologies is referred to as 10Base-T where T is for twisted pair. This standard specifies certain physical characteristics a cable must meet. Some of these characteristics include attenuation, characteristics impedance, propagation delay, timing jitter, etc. 10Base-T can be interpreted as-

   10: 10 Mbps

   Base: Baseband signalling

   T: Twisted pair cable

   For 10Base-T electric signals, Cat 3 to Cat 5 UTPs are preferred. 10Base-T media is used for low power, low-bandwidth applications. Network interface cards in Wake-on-LAN use this media for transmission.

2. **100Base-T**: It is also referred to as Fast Ethernet. For 100Base-T electric signals, Cat 3 to Cat 5 UTPs are preferred. Maximum cable length can be 100 metres for 100Base-T. LAN using 100Base-T are built in star topology by the use of hub and switches. Fast Ethernet devices are backward compatible to support 10base-T nodes. It works in full duplex mode and CSMA/CD is used for media access control.

3. **1000Base-T**: It is Gigabit Ethernet which demands Cat 5 or higher grade. The network segment in 1000Base-T network can have a maximum cable length of 100 metres.

Fibre Optics

Coaxial cable as well as Twisted pair cables get affected due to environmental conditions. Fibre optics, even though expensive, are unaffected. There are two types of fibre optics: Simple Mode Fibre (SMF) and Multimode Fibre(MMF). SMF is used for long distance communication whereas MMF is preferred for 500 m or shorter distances.

1. **10Base-F** is the generic term used for the family of Ethernet standards using optical fibre. Most popular among them is 10Base-FL where FL stands for Fibre optic Link.

2. **1000Base-X** is the Gigabit Ethernet transmission over fibre which is the largest Ethernet networking configuration. It supports 1000Mbps, that is, 10 Gbps transmission rate. It operates in the half duplex as well as full duplex mode.

Scanned by CamScanner

Various Fibre optics Gigabit Ethernet implementations are as under:

1. **1000Base-SX**: It is the Gigabit Ethernet standard for Short wavelength (SX). It operates on multimode fibre using near-infrared light wavelength. Based on the core size of multimode fibre and its modal bandwidth, maximum length of the segment is defined. For example, 550 m is the maximum length for a multimode fibre having 50 μm core size and 500 MHz×km modal bandwidth.
2. **1000Base-LX**: It is the Gigabit Ethernet standard for Long wavelength (LX). It operates on single mode fibre of core size 10 μm for up to 5 km distance. It can also operate on multimode fibre for a maximum segment length of 550m.

Thus, various transmission media and their standards can be summarised as given in Table 3

Table 3 Various Transmission Media and their Standards

Transmission	Media	Cable	Connector	IEEE Standard
10Base-5	Thick Ethernet	Thick-wire cable	RG-8	802.3
10Base-2	Thin Ethernet	Thin-wire cable	BNC	802.3a
10Base-T	Unshielded Twisted Pair	UTP Cat. 3	RJ 45	802.3i
100Base-T	UTP and Fibre Optics	UTP Cat. 3 and Cat. 5	RJ-45, FC, ST, SC, LC	802.3u
1000Base-T	UTP	UTP Cat. 5 or greater	RJ-45	802.3ab
1000Base-X	Short or Long Wavelength	SMF or MMF	FC, ST, SC, LC	802.3ae

1.6. CSMA/CD and CSMA/CA

Carrier Sense Multiple Access/Collision Detect (CSMA/CD)

Each device senses whether the line is available for use. If the line is idle, the device starts data transmission in the form of frames. In case another device has sent frames at the same time, a collision occurs and the frames get discarded. Each device is required to wait for a random amount of time and retry for data transmission until successful.

Scanned by CamScanner

Wireless LAN and CSMA/CA

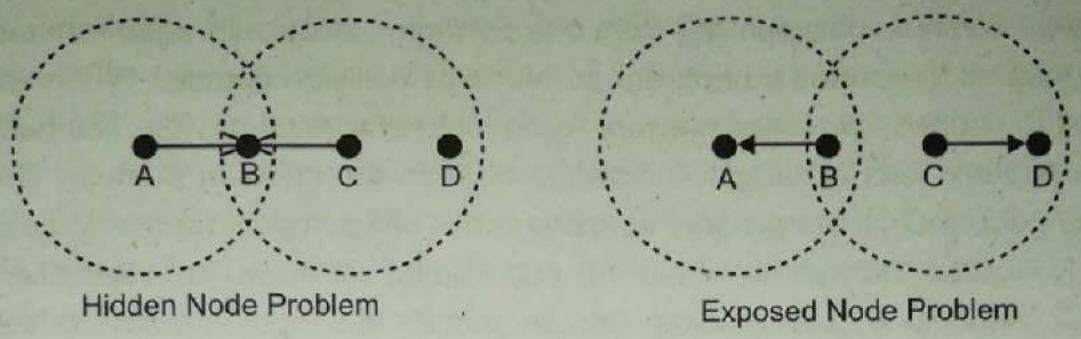


Figure 15: Hidden Terminal and Exposed Terminal

In wireless LAN, the collision detection mechanism fails. It is due to the hidden terminal and exposed terminal problem. So, there is a need for avoidance of collision. To avoid collisions, a device will use Ready-to-Send (RTS) and Clear-to-Send (CTS) signals. When a device is ready to transmit, it first senses the airwaves for the current signal. If there is none, it generates an RTS signal, indicating that it is about to send data. It then sends its data and finishes by sending a CTS signal, indicating that another wireless device can now transmit. Figure 15 shows the hidden terminal and the exposed terminal.

1.7. Collision Domain and Broadcast Domain

As covered in previous sections, CSMA/CD, used by Ethernet, creates the problem of the collision domain. Before we move further, let us try to understand the collision domain and the broadcast domain and their significance while designing a network.

Collision Domain

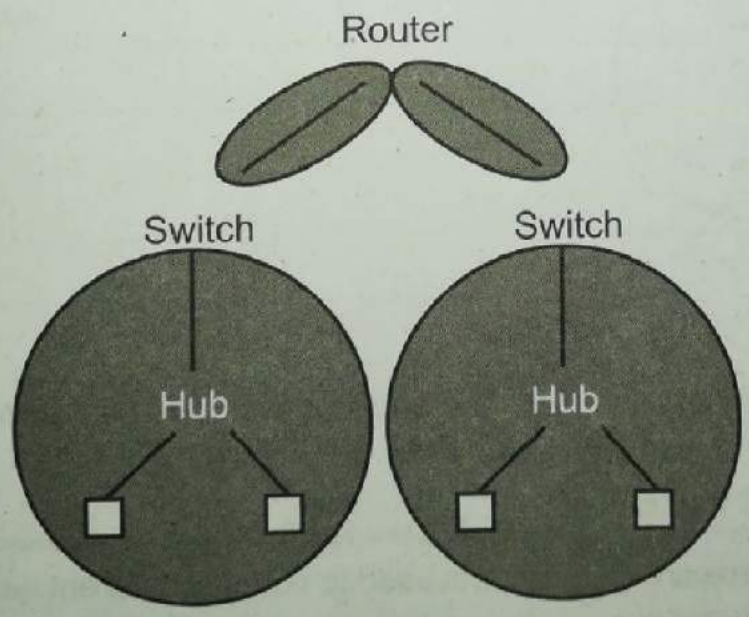


Figure 16: Collision Domain

Scanned by CamScanner

The logical part of a network where packets can collide with each other is known as the collision domain. If a hub receives data, it will be forwarded to all the devices connected to other ports in the hub. Thus, data arriving from one port can collide with data from another port. Hence, we say all the ports in a hub are in the same collision domain. When Layer 1 devices are used to connect two small network using internetworking devices like hub (star topology) and repeaters (bus topology), it actually extends the collision domain. This will directly affect the performance of networks as more nodes will compete for media as all will use CSMA/CD to access the media. Hence for optimisation of networks, internetworking devices at Layer2 (switches for star topology and bridges for bus topology) were developed which split the collision domain. When a switch receives a frame, it is forwarded only to the port of the intended device and not to other ports on the switch. Hence, data from different ports do not collide. Same holds true for bridges and routers. Therefore, all the ports in a switch, bridge or router are in different collision domains. Figure 16 shows four collision domain.

Broadcast Domain

The broadcast domain is the logical part of a network where devices receive broadcasts (data for all) and multicast (data for a group). Hub, bridges and switches broadcast the data to all the ports if they receive any broadcast frame. Therefore, all ports on a hub, bridge, and switch are in the same broadcast domain. Routers discard the broadcast packet if they receive any. That is, routers do not forward the broadcast packet to other ports on the network. Hence, all ports on a router are in different broadcast domain. Figure 17 shows the broadcast domain.

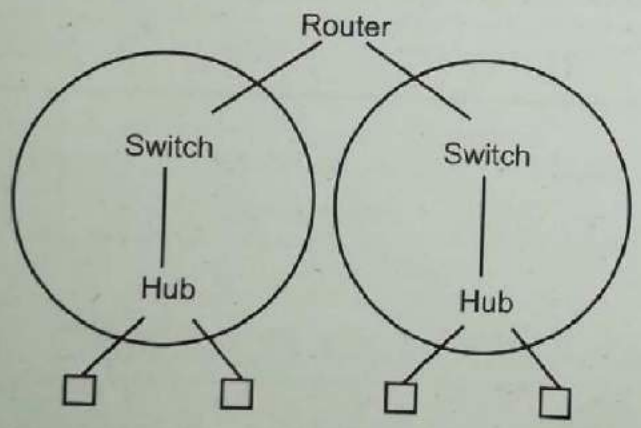


Figure 17: Broadcast domain

In the above figure, there are two broadcast domains, one each for two ports on the router.

1.8. Internetworking Devices

Internetworking devices refer to the hardware components used to connect different network resources. Size and complexity of a network may demand internetworking. Simply adding new nodes and cables in the network does not help in expanding the network. Internetworking

Scanned by CamScanner

devices are used to expand the network. In order to connect a LAN to another LAN or a WAN, internetworking devices will be required. Similarly, internetworking devices can be used to link two LANs via a WAN i.e. for a LAN-WAN-LAN internetwork. This allows a greater number of nodes to be connected in a network that can be expanded and extended over a large distance. On the other hand, internetworking devices help localise the traffic on the network which makes fault detection easier, faster and simpler. Therefore, in a network experiencing heavy traffic, internetworking devices can be used to break a LAN into segments and manage network traffic efficiently. Also, they can be used for security among different types of users. In this section, we will discuss various internetworking devices in detail and give a brief insight into which, when, where and why the internetworking device should be used.

Different internetworking devices in their increasing order of power and complexity are:

- Repeaters (Bus Topology)
- Hubs (star Topology)
- Bridges (Bus topology)
- Switches (Star Topology)
- Routers

Repeaters and Hubs are Layer 1 devices. Bridges and Switches are Layer 2 devices. Routers are Layer 3 devices. Therefore, within a LAN, different network segments are connected using repeaters and hubs. In order to connect segments on two different networks i.e. for a LAN to LAN connection, bridges and switches are used. Routers are used to link a LAN with WAN. Table 4 shows Internetworking devices and their corresponding OSI Layers.

Table 4 Internetworking Devices with Corresponding OSI Layers

INTERNETWORKING DEVICE	OSI LAYER	OSI LAYER NAME
Repeater	Layer 1	Physical Layer
Hub	Layer 1	Physical Layer
Bridge	Layer 2	Data Link Layer
Switch	Layer 2	Data Link Layer
Router	Layer 3	Network Layer

Scanned by CamScanner

Repeaters

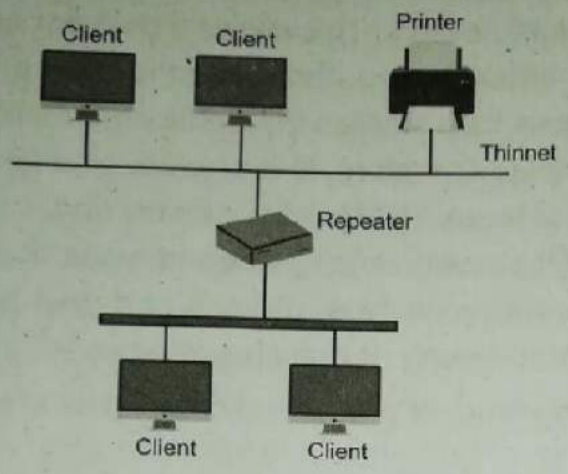


Figure 18: Repeater Expanding Network Span

Repeaters are the internetworking devices used at the OSI layer 1, i.e. physical layer. Repeaters are used to connect different segments in a LAN and pass data as bits in both directions of the network segment. It thus helps to expand a network. As discussed earlier, in 10Base-5 thicknet, a single network segment can have a maximum length of 500 metres whereas in 10base-2 thinnet, the maximum length of a single network segment is limited to 185 metres. To increase the length of the network, a repeater may be used to connect network segments. An Ethernet network can span up to 2.5 km as Ethernet allows cascading of five network segments. However, as the length of the network segment increases, the signal weakens and deteriorates. Repeaters amplify and regenerate the signal while passing the signal to the other end. Also, repeaters do not separate one network segment from another. Therefore, collision at one segment is regenerated and transmitted to the other network segment. All the devices connected to the repeater have the same collision domain and the broadcast domain.

Hubs

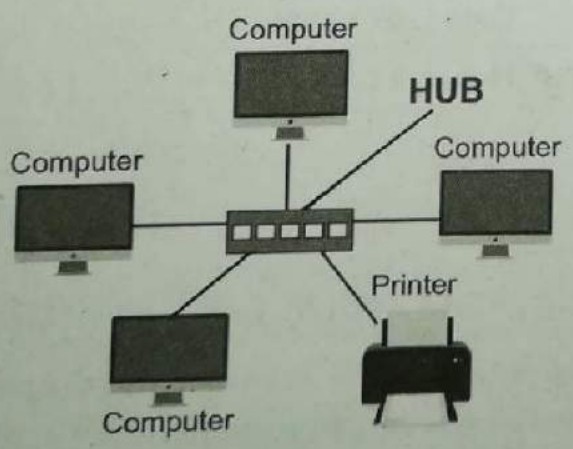


Figure 19: Hub Star topology/hierarchical manner

Scanned by CamScanner

A hub is an internetworking device with multiple ports. Multi-port repeaters are better known as a Hub. It simply passes data received in the bit format to all other ports. Multiple levels of the hierarchy of nodes can be created by using the hub to realise a larger single LAN with a greater number of nodes. RJ-45 is used to connect a node to the hub.

Hubs do not have the brain; they do not apply any logic nor do they filter network traffic. Therefore, data received by a hub is passed to all other network segments connected to the hub irrespective of whether the data is required or not. Implicitly it adds unnecessary traffic onto the network. Similar to the repeater, the collision in one segment is passed on to all other network segments by the hub. Devices connected through a hub are in the same collision domain and broadcast domain. A hub cannot connect unlike segments. Also, network segments working on different access methods cannot be joined using a hub.

Bridges

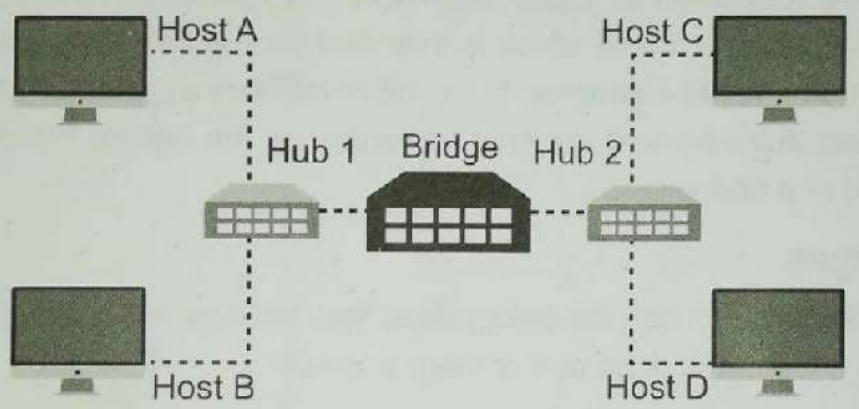


Figure 20: Bridge Connecting Different LANs

The bridge is an OSI Layer-2 device operating at the MAC sub layer of Data Link layer. It is used to connect two different LANs. The two LANs can be similar or dissimilar. It is protocol independent and is designed to store and forward frames. The bridge has the intelligence to isolate network traffic. It has the ability to examine source and destination addresses of the incoming packet and filter traffic based on MAC address. Also, a bridge has addressing and routing capability. Thus, a large geographic area can be connected using bridges. Each port has a different collision domain but the same broadcast domain. It provides high reliability and performance. But a bridge can match the QoS requirement of only one LAN. Availability, frame size and priority, frame lifetime, frame mishaps, transit delay, undetected bit errors are all examples of QoS parameters. Let us understand how a bridge works.

Scanned by CamScanner

Working of Bridge

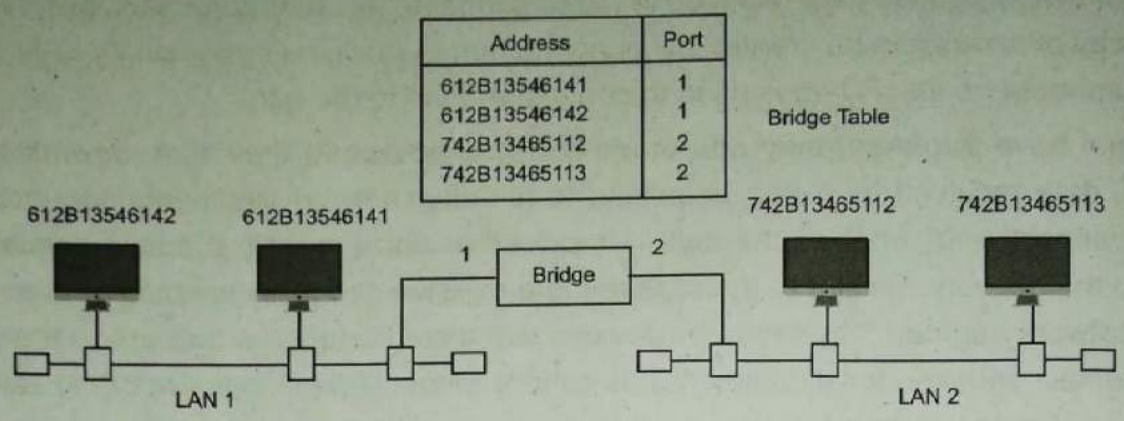


Figure 21: Selective Forwarding

Bridge maintains a table for filtering/routing. In the table, it stores the MAC address of both the network segments. Bridges may span to many segments. All segments receive the broadcast frames. If a bridge receives a frame which is intended for the MAC address on the local side of a bridge, the frame is not forwarded to the other network segment. Frames containing MAC address of the other segment are only forwarded by the bridge. Figure 21 shows the selective forwarding of a bridge:

Different Types of Bridges

Based on the routing capability, bridges can be categorised into transparent bridges and source routing bridges. Let us understand each one of them in detail:

1. **Transparent bridge**

   Transparent bridges are applicable to all IEEE 802 LANs. As the name suggests, the nodes are unaware of the presence of the transparent bridge. Two main functions of transparent bridge include forwarding the frames to the destination address and learning to create a forwarding database. It, thus, works on two processes:

   – Bridge forwarding
   – Bridge learning

   Bridge Forwarding:

   Transparent bridges maintain a forwarding database in the form of a table that contains the MAC address and port number of all hosts. If the entry for destination address exists in the database, then the frame is forwarded to the respective port number. If the entry for the destination address is missing in the database, then the frame is forwarded to all port numbers. This is known as flooding. The entire process is referred to as bridge forwarding.

Scanned by CamScanner

Bridge Learning:

During the installation of the transparent bridge, the forwarding database is empty. Whenever a frame arrives at the database, the source address of the frame gives detail as to where the particular host is located. In this way, the bridge learns where to forward frames if they are destined for this address. This process is called bridge learning.

Loop Problem

If there is no redundant bridge in the system, bridge forwarding and bridge learning work absolutely fine. But failing of a bridge should not lead to disconnection of the network. Hence, for having high reliability, redundant bridges are desirable in the network. Presence of a redundant bridge introduces loop problem. Let us understand this with the help of an example.

Figure 22 shows the loop problem:

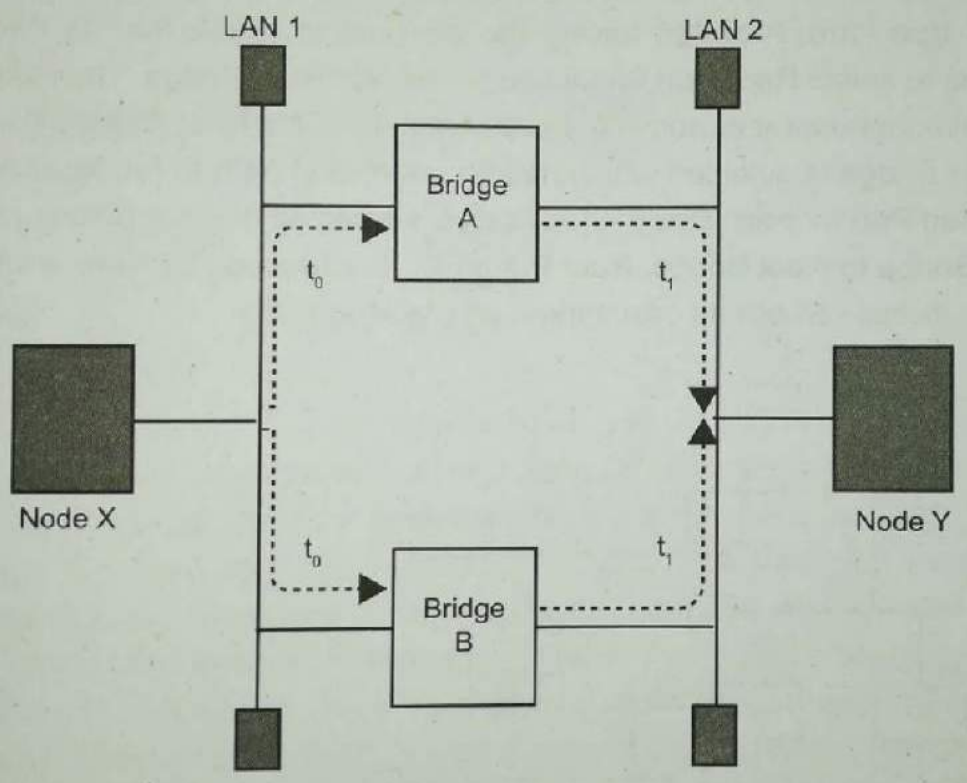


Figure 22: Loop Problem

As shown in Figure 22, two LANs viz. LAN 1 and LAN 2, each containing Node X and Node Y, respectively, are connected through two bridges viz. Bridge A and Bridge B. Initially forwarding database of both the bridges is empty.

i. Node X sends a frame to Node Y.

ii. As the forwarding database does not contain any entry, Bridge A updates its forwarding database with the source address of Node X and forwards the frame to LAN 2. Bridge B does exactly the same thing. At this point of time, LAN 2 has two copies of frame.

Scanned by CamScanner

iii. Bridge B now receives the frame copy sent by Bridge A and vice-versa.

iv. Since none of the bridges has any information about Node Y, both the bridges forward the frame to LAN 1. At this point of time, LAN 1 has two copies of frame.

v. Bridge B now receives the frame copy sent by Bridge A and vice-versa.

vi. Since none of the bridges has any information about Node Y, both the bridges forward the frame to LAN 2. At this point of time, LAN 2 has two copies of frame.

vii. Now, steps (iii) to (vi) will be repeated indefinitely in the two LANs and the frame will loop.

Spanning Tree

To overcome the loop problem, IEEE specifies that the bridges should use spanning tree topology. Spanning tree is a graph which has no loop. In other words, there is only one path between any two bridges. Spanning tree algorithm creates a logical topology of a network in a tree form. A bridge having the smallest id is selected as the Root Bridge. Next step is to select Root Port for all bridges except Root Bridge. The Root Port should have a minimum number of hops i.e. least cost path to the Root Bridge. For each LAN, a Designated Bridge is selected which has the least cost path to the Root Bridge. Similarly, Designated Port for each Designated Bridge is selected that has minimum hops from Designated Bridge to Root Bridge. Root Ports and Designated Ports are termed as Forwarding Ports whereas all others are marked as Blocking Ports.

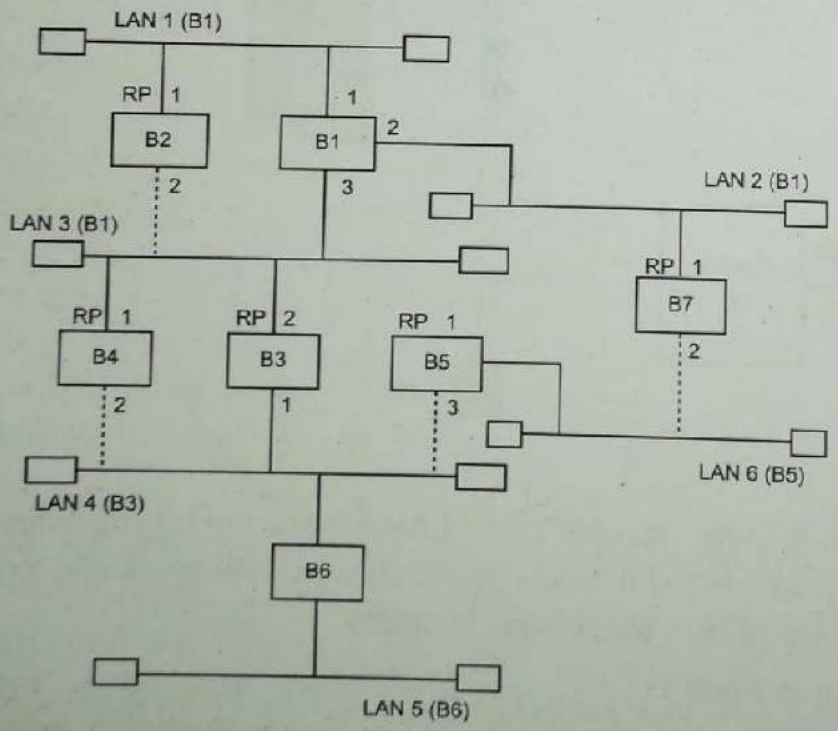


Figure 23: Spanning Tree

In Figure 23, B1 is the Root Bridge. Root Ports and Designated Ports that act as forwarding ports are in solid lines. Dashed lines represent Blocking Ports.

Scanned by CamScanner

2. **Source Routing bridge**

   Source routing bridges have been specifically developed for IEEE 802.5 token rings. As the name suggests, the source node specifies the route to be followed by the frame. The route to the destination is determined by the source node by sending a discovery frame. Discovery frame reaches the destination from all possible paths in the network, thus, implicitly adding traffic on the network. Based on the response from the destination, the source selects the best possible path. A route with a minimum number of hop counts can be the criteria for choosing the best path. A field for routing information is added to the frame by the source routing bridge.

Switches

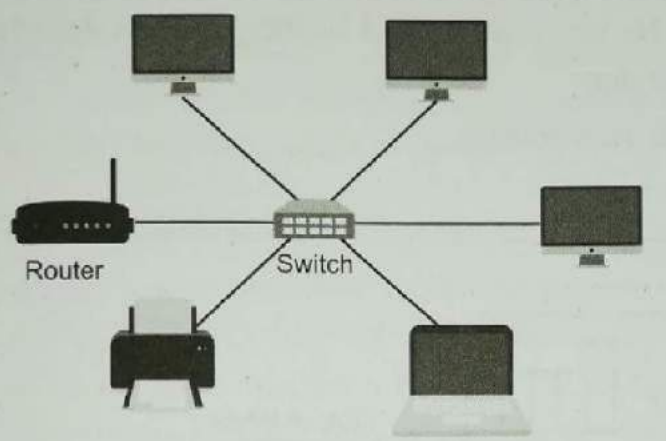


Figure 24: Switches

LAN Switch is an OSI Layer-2 device working at Data Link Layer. A switch allows a network to be segmented into smaller isolated LANs, i.e. different collision domains. This is because switches have intelligence. They can read source MAC address and destination MAC address. They forward the frame to a port only if it is needed to go there. Thus, a port receives only those frames that are intended for the device connected to it and it does not receive any frame addressed to devices connected to other ports. This, thus, helps in reducing the traffic experienced by a device. But, if the frames contain a broadcast address (frames intended for all) or multicast address (frames intended for a group), switch forwards it to all ports except from the one which it was received.

Devices connected to a port are all in the same collision domain whereas devices connected to different ports are in different collision domains. But all the devices connected to a switch, even though on different ports, are in a single broadcast domain.

Ports on switches have a buffer. A collision can occur if two devices try to send frames on a segment at the same time. This can be avoided by buffering the frame of one of them for later access.

Let us have a look at how different is a switch from a hub:

1. In a physical star topology, hubs work like logical bus whereas switches work like a

Scanned by CamScanner

logical star.

2. All ports of a hub are in the same collision domain whereas all ports of a switch are in different collision domains.
3. All ports share the bandwidth in the hub whereas each port has dedicated bandwidth in the switch.
4. Ports in the hub do not have buffer whereas, in the switch, each port has a buffer.

Even though logically equivalent, there are some significant differences between bridges and switches:

1. Switches are faster than bridges.
2. Bridges cannot connect unlike bandwidth whereas switches can support more than one type of media. For example, two LANs viz. 10Mbps and 100Mbps Ethernet LANs, can be connected using switch but not bridge.
3. Generally, switches have more ports than bridges.

Routers

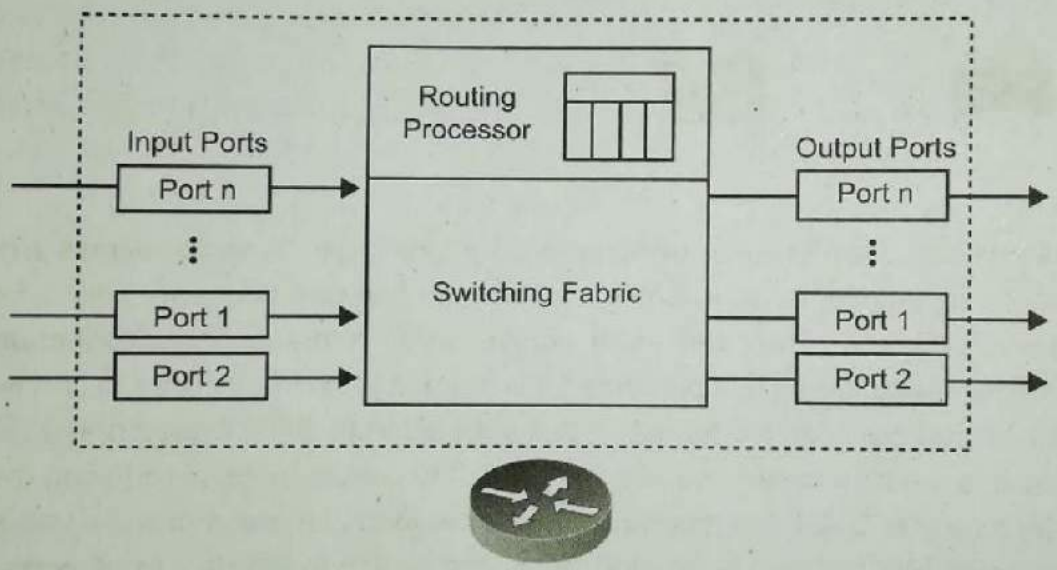


Figure 25: Routers

A router is an OSL Layer 3 device working on Network Layer. Different networks can be connected using a router. Devices on different LANs can communicate with each other through router even though they may be physically over a long distance. Routers have more intelligence than a hub and a switch. Routers have the ability to forward packets to the best path on the network for delivery to the destination. They can listen to a network to identify whether the network is busy and transmit the data through the most cost-effective path. The IP address of the destination is used along with the routing tables in order to determine the best path. Hence, packets are forwarded only where they need to go.

Scanned by CamScanner

Broadcast messages and multicast messages are blocked by routers. They only support unicast messages. The collision domain is the same for all the devices connected through a single router port. The collision domain is different for devices connected through different router ports. Similarly, the broadcast domain is the same for all the devices connected through one router port. The broadcast domain is different for devices connected through different router ports.

Broadcast might be required by some protocols, for say, routing protocol advertisement. But such broadcast is required only on local LAN and not on other LANs. Moreover, for the advertisement of routing protocols, routers can generate and broadcast packets, if necessary, but can avoid broadcasting received packets. This helps in reducing traffic on the network.

1.9. Addresses

A device in a network has two types of address i.e. physical address and logical address. Let us understand both addresses in detail.

Physical Address

MAC address is also known as a physical address. It is specified by the MAC sublayer which is a part of OSI Layer-2 Data Link Layer. MAC address uniquely identifies each device on the network. Each frame contains a MAC address of the source as well as the destination. Only the destination should receive and process the frame.

MAC address is analogous to an Aadhar Card number which is unique for every Indian citizen. Aadhar Card number of an individual does not change even if one moves from one house to another or a city to another.

Each Network Interface Card (NIC) gets a Burned-In Address (BIA) during manufacturing. It is a permanent address that does not change even when the NIC is moved from one device to another or from one network to another. A MAC address might be assigned to a device or to a router's interface. MAC address does not reveal any information about where or which network it is connected to. Therefore, the MAC address cannot be used by a router to determine the best path to deliver the packet to the destination. Rather a router needs logical address which is assigned when a device is connected to a network. If the device is moved to another network, the logical address of the device changes.

Scanned by CamScanner

Logical Address

A logical address is also known as the network layer address. It is similar to a postal address. A postal address is unique all over the world. No two houses can have the same postal address. Moreover, the postal address is logical and hierarchical. It contains country, state, district, city, sector, building and flat number. All houses in a building will have the same address till building name but each one will have a different flat number.

Similarly, the network layer address of a device consists of the network address and the host address. The network address is common for all the devices on a single network whereas the host address is unique for each device. Thus, network layer address is hierarchical as well as logical. It might be defined by the administrator or automatically assigned by the server.

Data Link layer uses Address Resolution Protocol to get MAC address from the network layer address.

1.10. Routing and Network Layer Addresses

Network portion of the destination address is used by the router to determine which interface the packet should be forwarded to. For this, the router compares the network portion of the destination address with the entries in the routing table. If the network portion of the destination address is same as the network portion of the source address i.e. the packet is intended for the device on the same network, the router uses Address Resolution Protocol to determine MAC address of device from network layer address. This destination MAC address is used while creating the frame and the frame is forwarded to the destined device.

IP Addresses

An IP address is a 32-bit number represented in dotted decimal notation. This 32-bit number is grouped into four octets. Each octet is separated by a dot and is represented in the decimal format. The eight bits in the octet can have binary 0 or 1 value. Thus, each octet in the IP address can have minimum decimal value 0 and maximum decimal value 255.

Example: 192.168.0.4 is represented in binary as 11000000.10101000.00000000.00000100

Five classes of IPv4 addressing include A, B, C, D and E. For devices connected on the network, Class A, B and C addresses are used. Class D addresses are used for multicast whereas Class E is reserved for experimental purpose. Class of the IP address can be determined from the higher order bits. And the class of the IP address determines how many bits are for network ID and how many for host ID as shown in Table 5

Scanned by CamScanner

Table 5 IP Addresses

Class	Format	Higher Order bits	Address From	Address To
A	Network.Host.Host.Host	0	1.0.0.0	126.0.0.0
B	Network.Network.Host.Host	10	128.0.0.0	191.255.0.0
C	Network.Network.Network.Host	110	192.0.0.0	223.255.255.0
D	Network.Network.Network.Host	1110	224.0.0.0	239.255.255.255
E	Network.Network.Network.Host	1111	240.0.0.0	255.255.255.255

Thus, as reflected from Table 5, Class A addresses have a higher order bit as 0. Network address 0.0.0.0 is reserved and network 127.0.0.0 is used for loopback functionality. Class A addresses can have a maximum of 126 networks and each network can have 16,777,214 hosts. Similarly, based on higher order bits, network bits and host bits, address range for each Class can be determined. For example, 192.168.0.4 is a Class C address where 192.168.0 is network ID and 4 is the host ID. The number of networks and the number of hosts in each network for a class are shown in Table 6:

Table 6 Number of Networks and Hosts

Class	Number of networks	Number of hosts per network
A	126	16,777,214
B	16,386	65,534
C	2,097,152	254

Private and Public IP Address

RFC 1918 Address Allocation for Private Internets have defined the private IPv4 addresses that can be used in an organisation network. To interact with the Internet, these private IP addresses need to be mapped to organisation's registered external address. Thus, IP addresses are divided into private and public IP addresses. The reserved private IP addresses for each class are as listed in Table 7. The remaining are public addresses.

Scanned by CamScanner

Table 7 Private IP Addresses

Class	Address From	Address To
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

Subnet

Class A address can have 16,777,214 hosts on a single network which might not be a desirable feature for an organisation. For the efficient use of IP addressing of different classes, the concept of subnetworks or subnets was introduced. Subnetworks help to configure a larger number of networks, each having comparatively fewer hosts. Bits from the host ID are borrowed to create a subnetwork. The borrowed bits can be identified from the subnet mask. Subnet mask consists of network bits, subnetwork bits and host bits. Thus, a three-level hierarchy is created by subnet masks i.e. network, subnetwork and host. In an IP address, network bit or subnet bit in the subnet mask is represented by subnet mask bit as 1 whereas the host bit in subnet mask is represented by subnet mask bit as 0. The IP address of default subnet masks are given in Table 8

Table 8 IP Address Default Subnet Masks

Class	Default Subnet Mask in Binary Format	Default Subnet Mask in Decimal Format
A	11111111.00000000.00000000.00000000	255.0.0.0
B	11111111.11111111.00000000.00000000	255.255.0.0
C	11111111.11111111.11111111.00000000	255.255.255.0

In Table 8, all host bits are 0 which represent the subnet address. If all the host bits would have been 1, it would represent the broadcast address for the subnetwork.

Example: Class A address 12.0.0.0 has 8 network bits and 24 host bits. It has default subnet mask as 255.0.0.0. To create subnetwork, if 8 bits of host id are borrowed then the subnet mask would be 11111111.11111111.00000000.00000000, that is, 255.255.0.0 in decimal. From 8 bits of subnet, 2^8, that is, 256 subnetworks can be created. Since now 16 bits are left for hosts, each subnetwork can have 2^{16}, that is, 65,534 hosts.

Subnet mask 255.255.192.0 can also be represented in another format using a prefix. The prefix represented by slash (/) is followed by network bits plus subnetwork bits in the IP address. 255.255.192.0 in the binary format is 11111111.11111111.11000000.00000000. It has 18 1s followed by 14 0s. Therefore, the subnet mask can be represented as 255.255.192.0/18 indicating 18 bits are for the subnet.

Scanned by CamScanner

All machines in a single LAN should have the same NetworkID. Only then two machines can communicate to each other. If machines have separate NetworkID, then the router will be required for communication between the two.

1.11. Virtual Lans

Virtual LAN i.e. VLAN is a network of a group of devices that are on different physical LANs but communicate as if they are on a single network. Even though on different physical LANs, devices on a VLAN have a single broadcast domain. Thus, VLAN is a logical construct which includes segments from different physical LANs. This logical connection provides flexibility to the VLAN. The concept of VLAN is depicted in Figure 26:

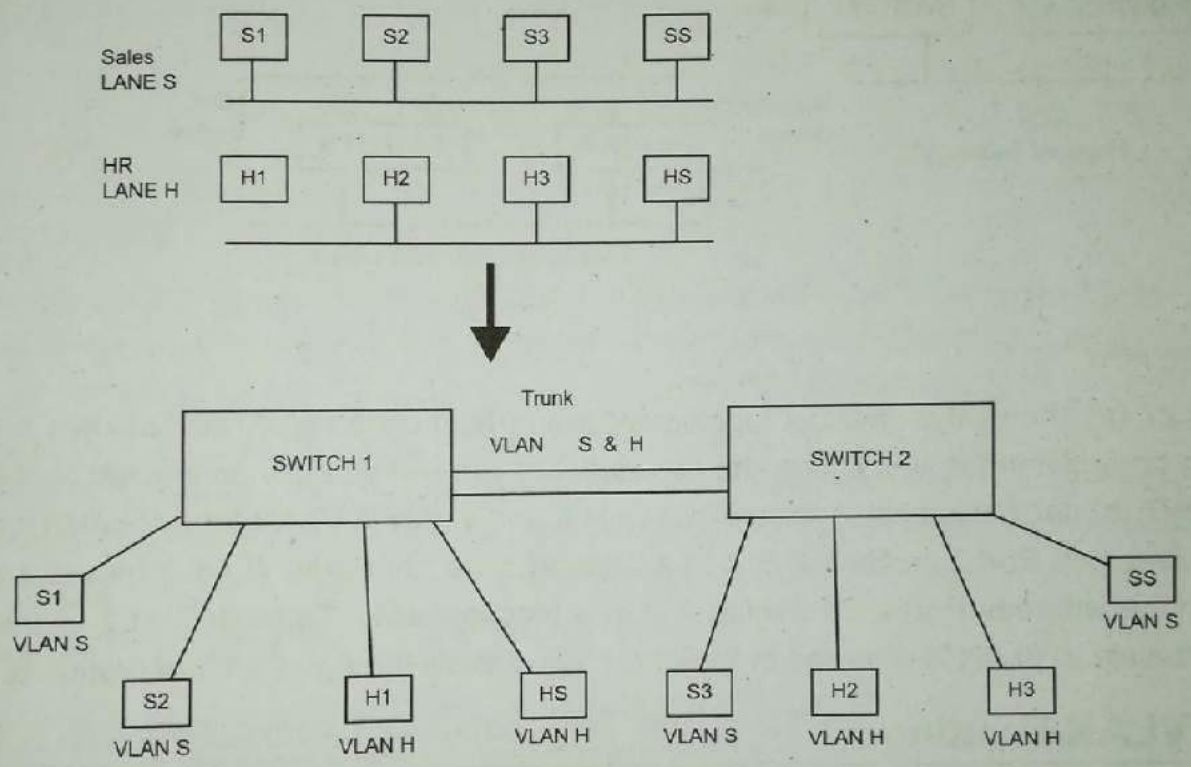


Figure 26: VLAN

Two VLANs, one each for Sales and HR is shown in the upper part of Figure 26. S1, S2, S3, H1, H2, H3 are workstations on the LANs whereas SS and HS are the servers. For better efficiency, the enterprise can create Virtual LANs as depicted from the right side of the diagram. Even though members of the same department are located at different physical locations, they are connected to their workgroup. VLAN S has all the devices of the Sales department connected to it logically and VLAN H has all the devices of HR department connected logically. VLAN S has a different broadcast domain from VLAN H. Thus, there are two broadcast domains, one separate for each department. VLAN can span multiple switches. The link connecting two switches in Figure 26 is referred to as Trunk. Trunk carries traffic from both VLANs. A trunk can connect multiple switches, routers or servers to carry data from multiple VLANs.

Scanned by CamScanner

STP and VLANs

Redundant physical links on the network can be used for different VLANs. This results in reducing the traffic on individual links. For this, only one instance of STP should run on switches for a VLAN. To achieve this, Cisco developed per-VLAN Spanning Tree (PVST). It is shown in Figure 27:

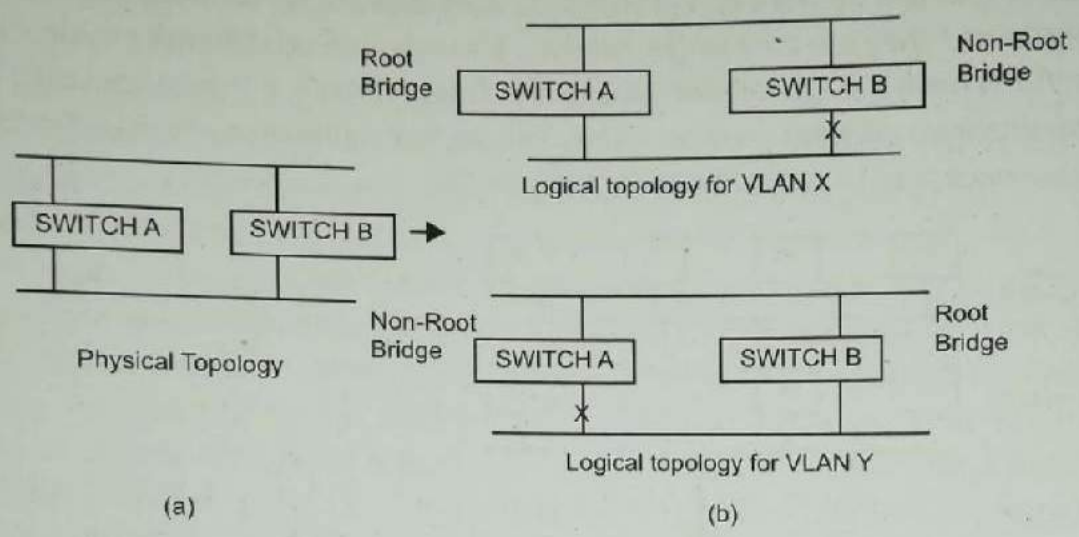


Figure 27: PVST

Figure 27 (a) shows the physical topology of the LAN. It consists of two switches A and B. As can be observed in this figure, the two switches are redundantly connected to the LAN. Figure 27 (b) depicts logical topology for VLAN X and VLAN Y. VLAN X has Switch A as root bridge whereas Port 2 on Switch B is in a blocked state. Similarly, VLAN Y has switch B as root bridge whereas Port 2 on Switch A is in a blocked state. Through Port 2 of Switch A, traffic travels in VLAN X whereas in VLAN Y traffic travels through Port 2 of Switch B.

InterVLAN Routing

When a device from a VLAN wants to communicate with a device on another VLAN, the need for router or Layer 3 switch arises. This is similar to the concept used in communication among different LANs. There are two ways to connect a Layer 3 internetworking device to a switched network.

1. Using multiple physical interfaces
2. Using a single interface configured as the trunk

Scanned by CamScanner

Both ways of InterVLAN are depicted in Figure 28

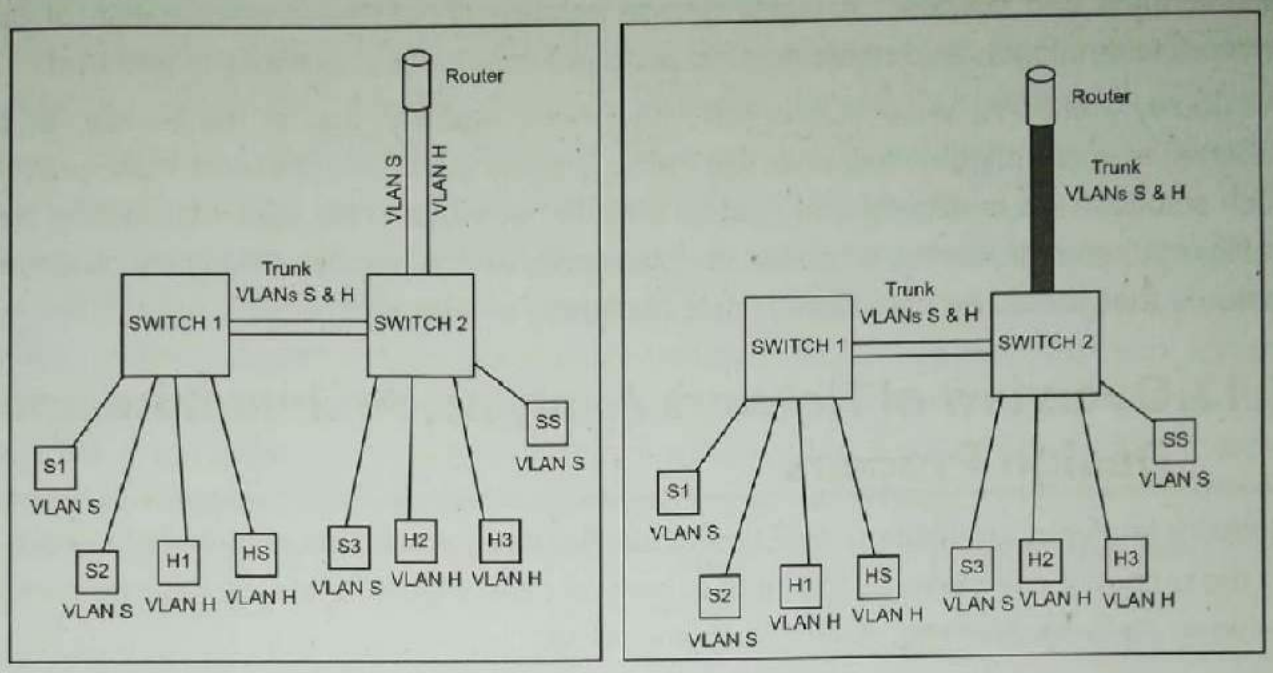


Figure 28: Inter-VLAN Routing

The left side of the figure depicts that there are two physical connections to the switch, one each for Sales and HR. Traffic from only one, that is, respective VLAN is carried by these physical connections. The right side of the figure illustrates a single physical connection between the switch and the router. Interfaces of both switch and router have been configured as trunk. Hence, there exist multiple logical connections between the switch and the router. This scenario is also referred to as 'Router on a stick' since the router is connected to only one interface. Physical interfaces as well as logical interfaces have different VLANs, each having different subnetwork for IP networks.

1.12. Old Network vs Current Network

In the initial days of networking, a network was simply a way to connect devices so that they can share and communicate data. They were not considered as a critical resource. Neither were they counted for revenue generation for a business. But now, a network is not an independent entity. It is a very important part of the system that provides services to end users. Hence, they are critical to the success of an organisation. Nowadays, networks are omnipresent, be it office, home or any outside environment. Also, any information can be accessed across the world in real-time. Therefore, networks must be designed judiciously so that they have rudimentary decision-making capability.

Old networks follow 80/20 rule, that is, 80% network traffic is local and 20% is remote. That is because, most of the communication was among devices connected in an office, campus or LAN. Very less network traffic was for the outside world. It was in sync with the saying, 'bridge when you can, route when you must'. At that time, there was a limited choice of

Scanned by CamScanner

network technologies and services. At present, numerous choices are available for network technologies and services. A viable design solution should be a combination of optimal network technologies and network services to provide the best services to end users.

Previously, networks were concerned only about capacity, that is the bandwidth of the network, to accommodate low and high traffic. But, the increase in network traffic proved that such solutions are inefficient and rigid as they do not adapt to the user's fluctuating network traffic requirements. Delay, reliability, maintainability and availability (RMA) are other network features that should be considered while designing a network.

1.13. Overview of Network Analysis, Architecture and Design Process

Network analysis, architecture and design are the three processes interrelated to each other as the output of one serve as the input to next process. Figure 29 shows the information flow between network analysis, architecture and design:

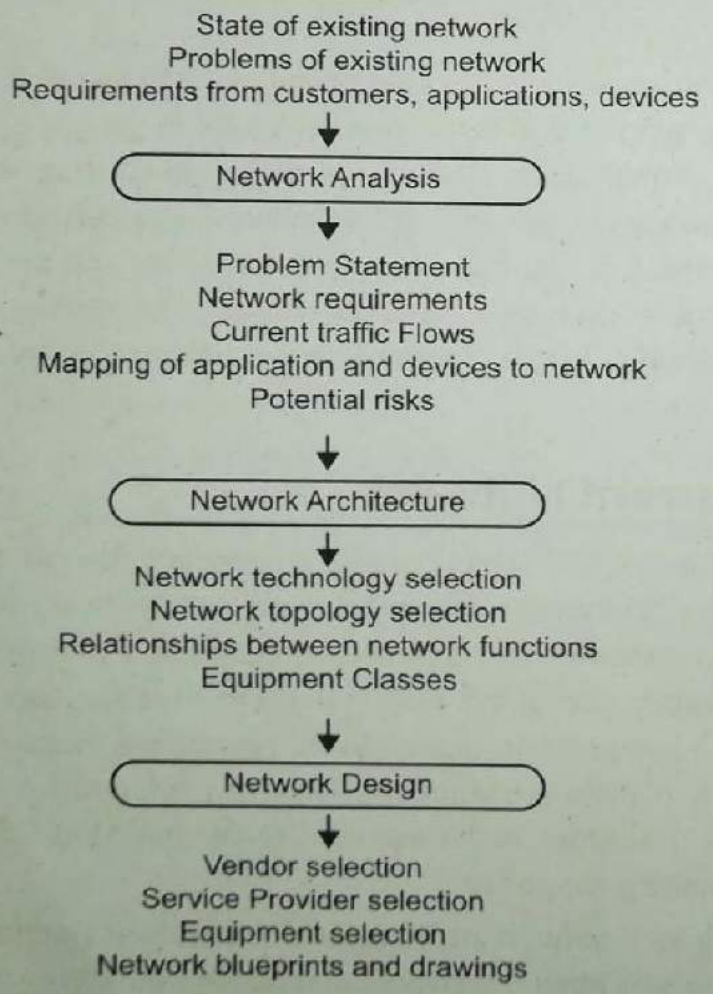


Figure 29: Information Flow Between Network Analysis, Architecture and Design

Scanned by CamScanner

Network analysis is about understanding customer requirements and understanding existing network to perform risk analysis. As a part of customer requirements, all requirements related to network applications and services, expected by customers, are captured. While understanding the existing network, the current state of the existing network is examined along with problems faced by the network. Such an analysis gives better insight regarding the objective of defining a new network and goals to be achieved.

Network architecture is a process of defining high-level, conceptual network infrastructure for the system. It is based on problems identified during network analysis. In this phase, network technology and topology are selected, addressing/routing mechanisms are identified, and the focus is on improving the performance of the system without compromising on the security aspect. This might result in many 'right' network solutions but the best solution is finalised that optimises maximum parameters to meet customer requirements.

The network design is the ultimate target where physical aspects of network architecture are detailed. In this process, a blueprint of design is prepared. Equipment, service providers and vendors are selected. This selection is based on the evaluation done to minimise network cost while maximising network performance.

1.14. Hierarchy and Diversity

As the size of the network grows, the number of devices connected in the network, network applications, network services and network traffic increases. This adds complication in the flat network and the performance of the network is degraded. A better way to handle increasing size of the network is to restructure the organisation in a hierarchical manner. Hierarchy decongests from network traffic. It provides separation points in the network through routing and addressing mechanisms. The network is segmented into several subnetworks or broadcast domains. This helps in handling traffic congestion, scaling the network, improving performance and service levels.

Diversity in the network refers to the redundancy or interconnectivity in the network at different levels. It helps in providing better performance at each level of the network. Both hierarchy and diversity need to be balanced for better performance of the network.

Scanned by CamScanner

A network, represented in the tree structure, has both hierarchy and diversity as shown in Figure 30:

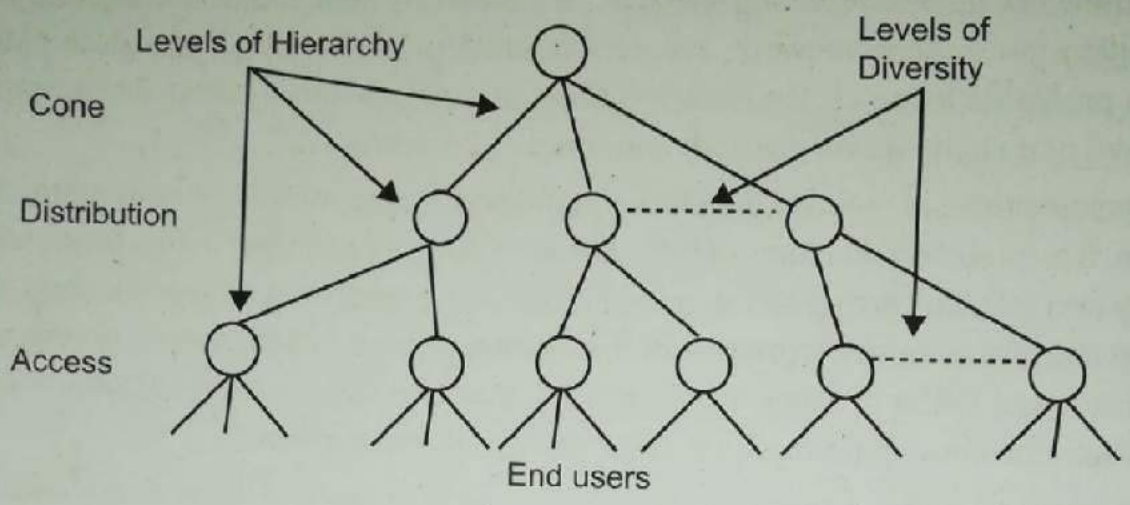


Figure 30: Hierarchy and Diversity in network

Circles signify routers or network devices whereas lines characterise communication path in the network. The core layer, distribution layer and access layer represent three levels of hierarchy in the network. Different network devices at the same level represent the diversity in the network.

1.15. Network Services, Characteristics and Metrics

Network Services and Metrics

Network services refer to the level of performance and functions in the network. Service can be categorised as:

1. **Service Offering**: Network services provided to applications, devices and users
2. **Service Request**: Network services requested by applications, devices and user

Various parameters constituting performance of a network are capacity, delay, reliability, maintainability, availability whereas accounting, billing, management, security, etc. are the functions. These are better known as service characteristics. Service characteristics can be defined for each level, subnetwork, broadcast domain and/or for the entire network. Service characteristics can also be grouped to form the hierarchy of service levels. Service levels can be created based on network delay, capacity, technology, protocol, mechanism, etc. or a combination of these. For example, a service having a capacity 1.5 Mbps and reliability 99.99% can be termed as Premium Service. Customer requirements can thus be described in the form of service characteristics. These network services can be monitored, verified and managed with the help of service metrics. Service metrics is the scale for measuring network services. Service metrics define thresholds and limits of network service.

Scanned by CamScanner

Threshold signifies the conformance level for a service metric. Thus, low-performance level and high-performance level for a service can be defined using the threshold. In either case, both performance levels are adhering to service. If crossed, an action might be taken. For example, sending an alert to the administrator when round-trip delay exceeds N ms.

Limit signifies the upper and lower boundaries between conformance and non-conformance levels, if crossed, results in serious action. For example, traffic that has crossed limit is brought back to conformance by delaying or dropping packets.

Performance Characteristics

As described above, services may comprise one or more performance characteristics.

Capacity

It is the ability of network service to transfer information in the form of data, voice, video or a combination of these. Capacity can be defined for bandwidth, throughput or goodput. Example: SONET OC-3c link has 155.52 Mbps bandwidth.

Delay

It is time taken to transfer information across the system. The information unit can be a bit, byte, cell, frame or packet. Delay can be measured in one direction (end-to-end) or both directions (round-trip). Delay can be defined for processing, propagation, queuing, transmission, etc. Latency is the response time of an application or network device (e.g.: switch or router).

Reliability

It represents the frequency of failures in the network, resulting in unscheduled outage of services.

Maintainability

It is the time taken for a network to be up and fully functional after experiencing a failure.

Availability

It is a measure of the overall uptime of the system.

1.16. Cisco Service-Oriented Network Architecture

Now-a-days a business analyst focuses on application-level business solutions. As a result, an extremely vast variety of business solutions at the application level are present in the market. Such applications need to be integrated which demands more intelligent network architecture. The focus in designing network infrastructure needs to shift from traffic transport-oriented approach towards the application-oriented or service-oriented approach. This section introduces Cisco SONA architectural framework which helps the customer build an

Scanned by CamScanner

intelligent application-oriented network infrastructure. Before we move ahead, let us discuss which factors prove to be the business drivers for new network architecture.

Evolution of Network Architecture

Customers demand fast, efficient, flexible, secure and cheaper services and products. The market and customer demands drive the enterprises to explore the latest IT solutions to be ahead in the intense competitive business environment where the window for time-to-market is reducing each day. Such demands result in a need of new network architecture that meets new business requirements, applications growth and evolution of IT. The evolution of the network is depicted in Figure 31

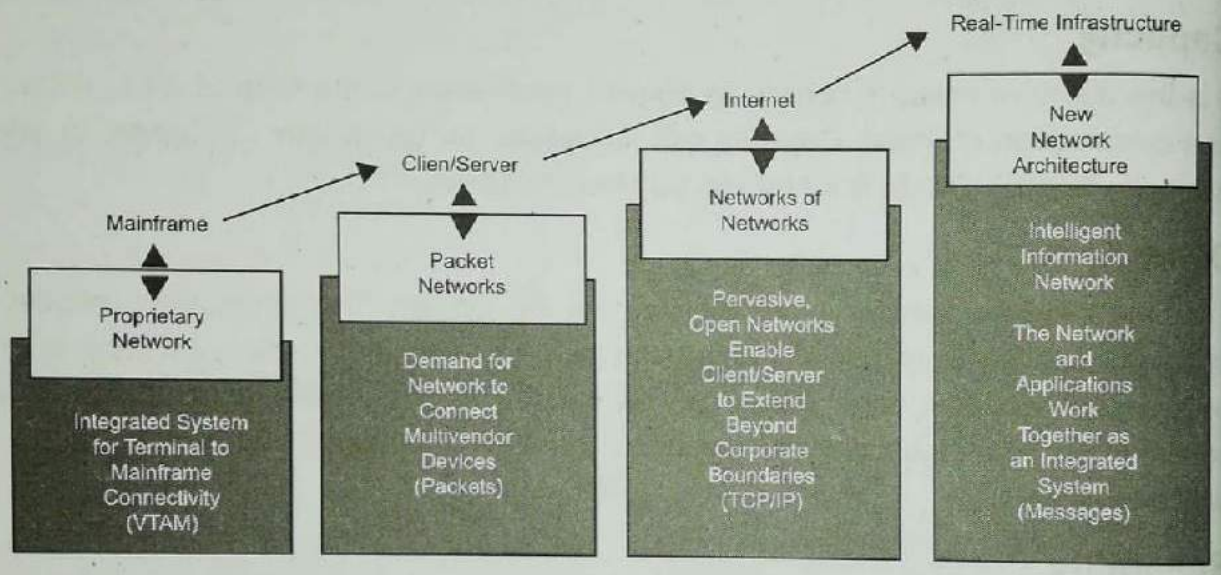


Figure 31: Network Evolution

Today's network infrastructure connects organisational resources internally i.e. within the organisation as well as externally i.e. to the Internet. Initially, IT was a proprietary network that was built on Mainframe. In this, the system was integrated from terminal to mainframe connectivity. As many vendors started manufacturing different network devices, need to be aroused to connect various devices from multiple vendors in the network. This resulted in Client/Server architecture. As IT evolved, in order to expand the boundaries of the corporate network, there was a need to connect the Client/Server architecture-based network to different networks. This gave rise to the network of networks, that is, the Internet which is based on the TCP/IP model.

Today, the role of the network is not limited to providing connectivity, rather it has expanded to enhance business performance and process. Network intelligence can significantly improve the communication and collaboration process which results in business success. Need is for a real-time infrastructure which integrates intelligent network and application. Thus, starting from the mainframe model, IT infrastructure has evolved to the Client/server model and later,

Scanned by CamScanner

Network and applications. Cisco vision supports the real-time, intelligent and integrated infrastructure.

Intelligent Network

Since the term 'Intelligent Network' has been used in the above section, let us understand what makes a network intelligent or how to make a network intelligent. To make a network intelligent, the network needs to be aligned to business requirements and business priorities. For this, closely integrate the network resources with the unlinked information assets. Currently, the intelligence built on a network component is limited. It is time to extend this intelligence across the network infrastructure to multiple products. Once the intelligence is extended, it can be used by the network to actively participate in the delivery of applications and services by managing, monitoring and optimising. Thus, adding intelligence to the network promotes agility, unified control and transparency in the business.

Intelligence in the network can be divided into three phases as per Cisco vision. These three phases are:

1. Integrated Transport
2. Integrated Services
3. Integrated Applications

Figure 32 shows the three phases of network intelligence:

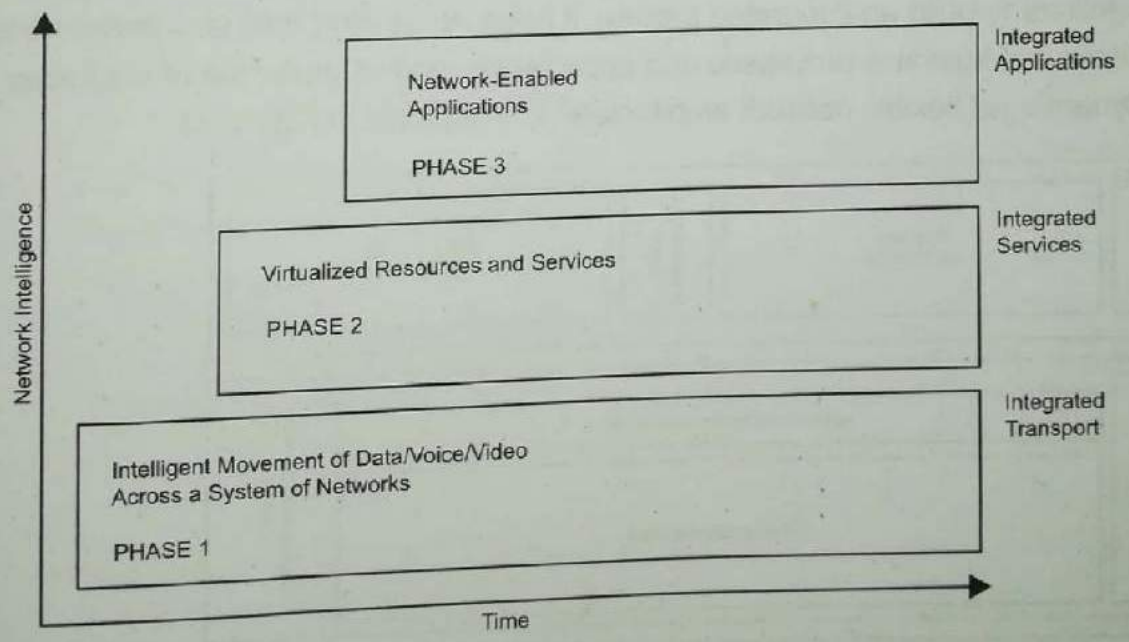


Figure 32: Network Intelligence

Let us understand each phase along with their advantages:

Scanned by CamScanner

Phase 1 – Integrated Transport

In order to simplify network management and improve efficiency, everything including data, voice and video should be transported in a unified modular network. This leads to network convergence where various Cisco Unified Communication products such as video conferencing, voice mail, video telephony etc. can be efficiently utilised.

Phase 2 – Integrated Services

Network convergence paves the way ahead for pooling and sharing as well as virtualising IT resources. This helps tackle the changing needs of the organisation more efficiently. In the case of failure, the intelligent network shares the resources so that the customer gets uninterrupted service. Thus, business continuity is enhanced by integrating services.

Phase 3 – Integrated Applications

The performance of the applications can be optimised by integrating application intelligence in the network. An application-aware network can integrate intelligent application message handling, optimisation and security into the existing network. It simplifies the application infrastructure on one hand and enables efficient delivery of networked applications on the other hand.

Cisco SONA Framework

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

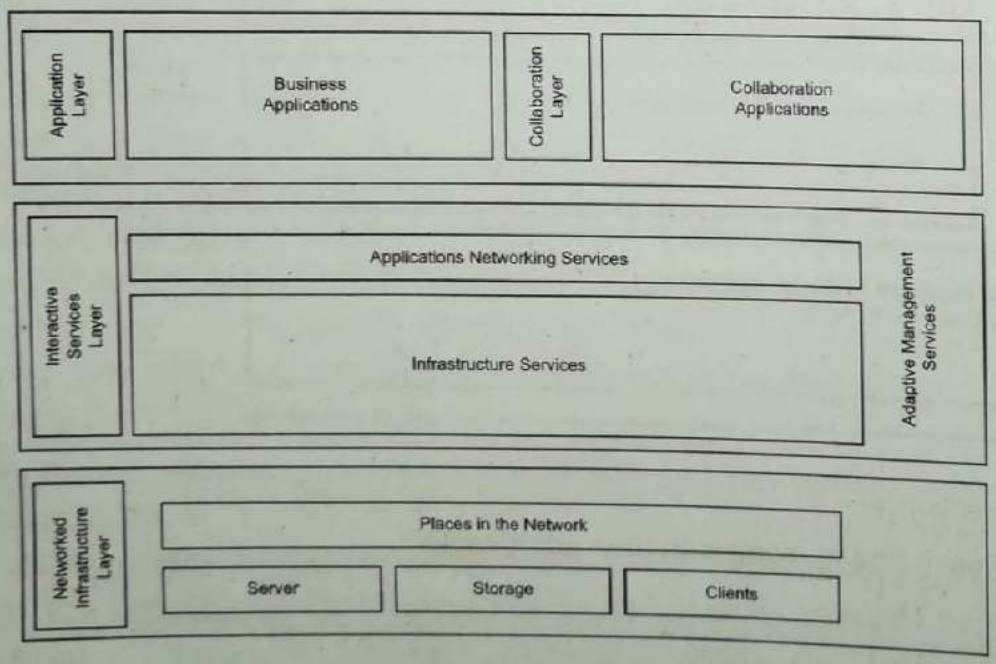


Figure 33: Cisco SONA Framework

Scanned by CamScanner

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

1. **Networked Infrastructure Layer**

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

2. **Interactive Services Layer**

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

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

Scanned by CamScanner

The services provided by Cisco SONA are shown in Figure 34

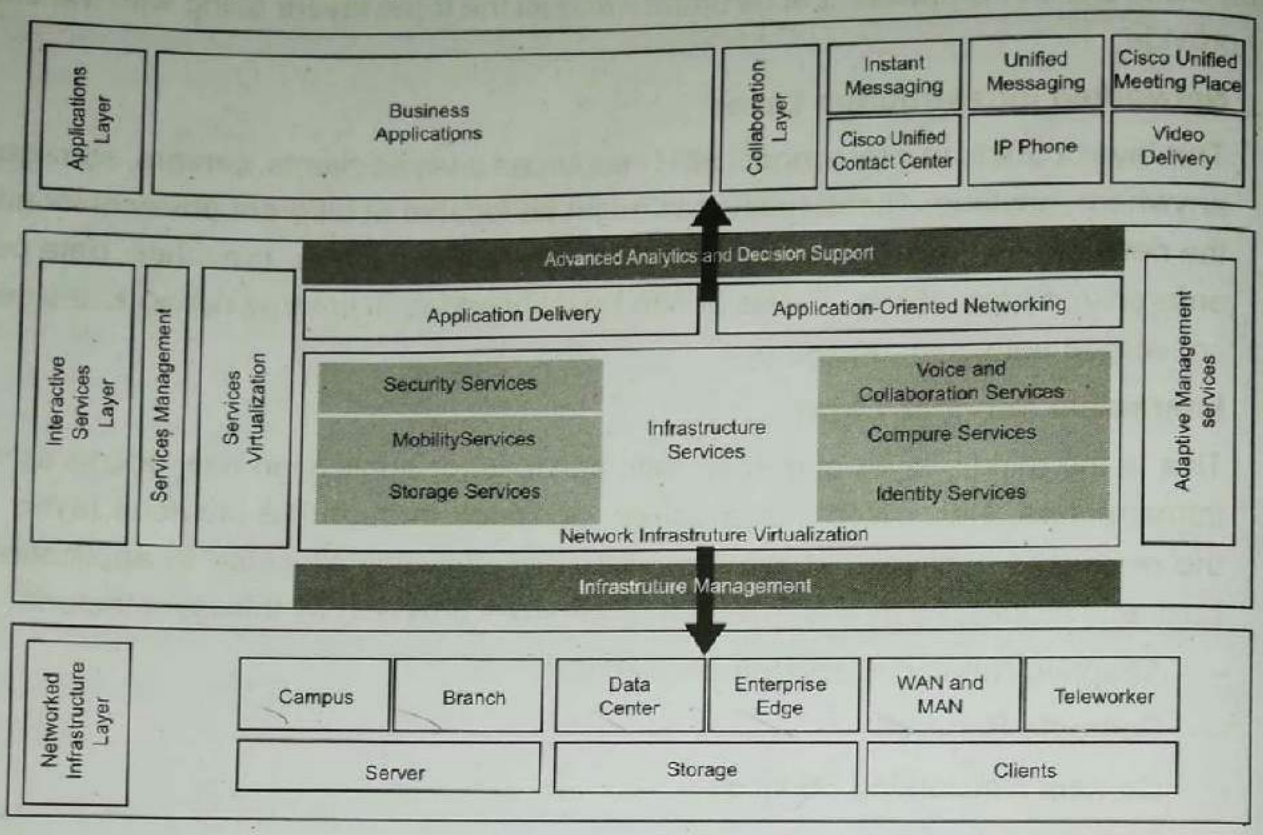


Figure 34: Cisco SONA Offerings

3. **Application Layer**

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

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

The Cisco SONA Framework has several advantages as listed below:

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

Scanned by CamScanner

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

1.17. Network Design Methodology

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

PPDIOO Methodology

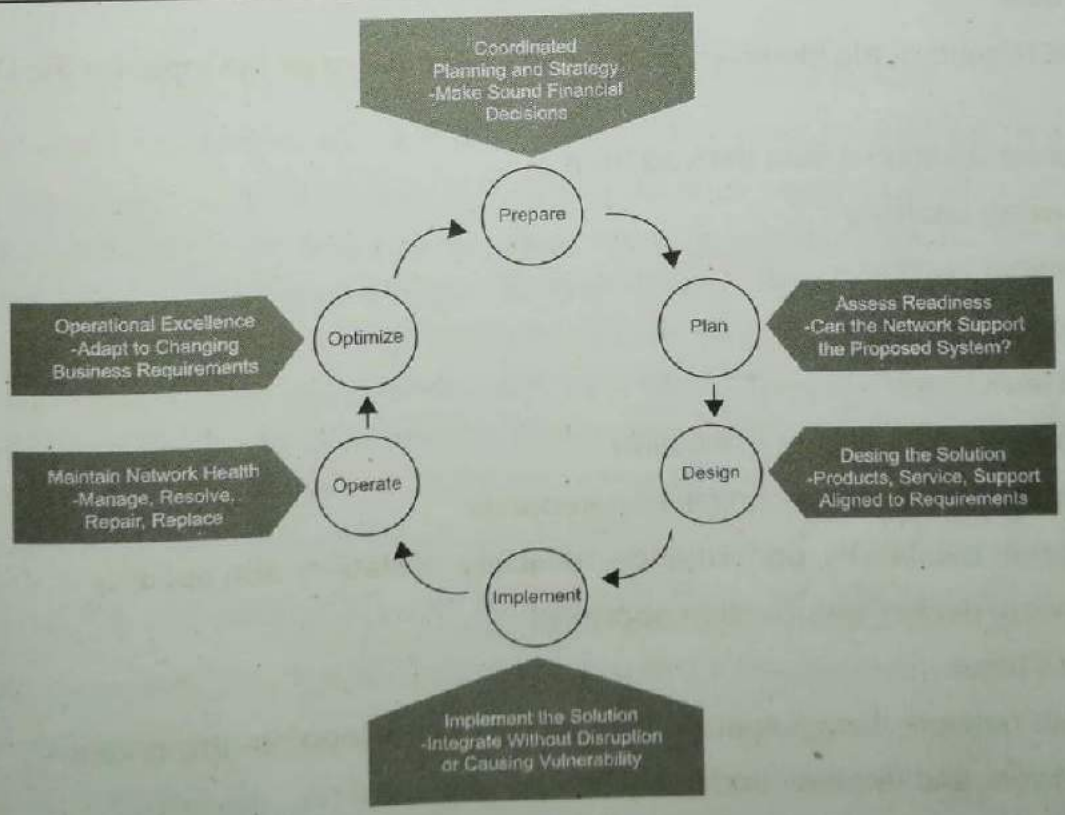


Figure 35: PPDIOO Methodology

Scanned by CamScanner

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

1. **Prepare Phase**
   - Establish business requirements
   - Develop a network strategy
   - Propose a high-level conceptual architecture
   - Identify technologies that support proposed conceptual architecture
   - Assess business case for proposed conceptual architecture
   - Establish financial justification for the network strategy
2. **Plan Phase**
   - Identify network requirements
   - Perform gap analysis to determine whether the existing network infrastructure ha 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 Desig phase
   - Incorporate additional data derived from
     - Network analysis
     - Network audit
     - Network managers
     - Network users
   - Prepare network design specification
     - Meet business and technical requirements
     - Support availability, performance, reliability, scalability and security
   - Get network design specification approved
4. **Implement Phase**
   - Approved network design specification serves as the input for this phase.
   - Built network and required additional components
   - Integrate network devices

Scanned by CamScanner

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

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

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

Benefits of PPDIOO on Network Design Methodology

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

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

Scanned by CamScanner

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

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

Scanned by CamScanner

Design Methodology

Design methodology refers to a systematic way of designing the network even in tight time constraints. First, let us understand the need for a design methodology.

- Without having a procedure to design network, some of the steps in the network design process could be missed out.
- Network designers may not be able to set appropriate deadlines, ultimately leading to customer dissatisfaction.
- If no design methodology is followed, there is no way that managers or customers can validate whether the network designers have covered all the business and technical requirements.

Thus, 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 phase, customer requirements are identified.
   - This step is part of Prepare phase of PPDIOO.
   - These requirements are used to prepare high-level conceptual architecture.
2. **Characterise the existing network and sites**
   - This step is a part of PPDIOO Plan phase.
   - Integrity and quality of the existing network are thoroughly assessed during the network audit.
   - Traffic, congestion and other network performance parameters of existing network are analysed during network analysis.
   - Capability of the existing network infrastructures and operational environments are analysed to determine whether it can support the proposed system.
3. **Design the network topology and solutions**
   - Output of the above two steps serves as the input for this step.
   - Network topology, infrastructure, infrastructure services and applications are finalised in this step.
   - A prototype network is created to:
     - verify the design appropriateness
     - identify and correct problems, if any.
   - Detailed design document is prepared.

Scanned by CamScanner

Once the design document is ready, the next step is to implement the design. The design implementation process consists of three steps as listed below:

1. **Plan the implementation**
   - Part of PPDIOO Design phase
   - Prepare implementation procedures
   - Perform cost assessment

- **Implement and verify the design**
  - Similar to PPDIOO Implement phase
  - Actual implementation of proposed network architecture
  - Verification of proposed conceptual design
- **Monitor and optionally redesign**
  - Part of PPDIOO Operate phase and Optimise phase
  - Constantly monitor built network for errors or faults
  - Frequent troubleshooting calls for redesigning the network
  - Unmanageable faults also call for redesigning of the network

We shall cover all the steps listed above in detail in the upcoming sections of this chapter.

1.18. Identifying Customer Requirements

Customer requirements are identified in the initial phase of the network design. It serves as the base for the network design. For this, the scope of the network design project is assessed. Applications in the existing network along with the new applications planned are determined. Next step is to identify what are the organisational goals to be achieved from this network design. Once organisational goals are identified, determine the organisational constraints under which the goals are to be achieved. On similar lines, technical goals and technical constraints are identified. Determine missing information, if any, and reassess the scope of the network design project.

Assessing the Scope of a Network Design Project

One way of assessing the scope of the network is from assessing what all areas are getting impacted by the network design and how large is the impact. The first step is determining whether the scope of the network design is for the existing network or a new network is to be designed from scratch. In any case, identify whether the design is limited to an individual network segment or a subnetwork or spans the entire network. The network design may implement a single functionality or might impact the entire network's functionality. Even this needs to be determined.

Scanned by CamScanner

Another perspective is to identify which all OSI reference model layers are getting impacted due to this network design. This includes network topology, network protocols, physical media, network applications and services impacted. Table 9 gives a glimpse of features getting impacted at each layer:

Table 9 Assessing Scope of Network Design

OSI Layer	Design
Application	Application data transport
Network	Routing and addressing design
Physical and Data link	Connection types and technologies

An example for this can be as shown in Table 10:

Table 10 Scope Assessment for a Network Design Project

Design Scope	Observation
Entire Network	• Upgrade all LANs to Fast Ethernet technology
Network layer	• Addressing plan for private IP address • Segment LANs • Redesign routing plan
Data link layer	• Redundant links and equipment • Wireless radio frequency site survey.

Identifying Required Information

This is a two-step process as listed below:

1. **Extracting Initial Requirements**

   Request for Proposal (RFP) or Request for Information (RFI) are the documents issued by the customer that enlists all customer requirements. These documents serve as the primary source of information regarding customer requirements. RFP is a formal document provided to the vendor. RFI is a comparatively less formal document where the organisation has requested the vendor to provide the required information. Based on these documents, identified design requirements are listed down. The customer is also queried orally or verbally to get additional initial requirements, if any. These requirements are reordered and/or reframed. This process is known as pre-documenting. As a result, a design draft containing design requirements in detail is produced. This design draft is sent to the customer for review. The customer verifies the network design requirements. Changes to add, modify or delete design requirements are suggested. Based on review comments received, appropriate changes are made to draft an error-free design requirement. Updated draft is again sent for review and

Scanned by CamScanner

modifications made until the draft is approved by the customer. This process is depicted in Figure 36:

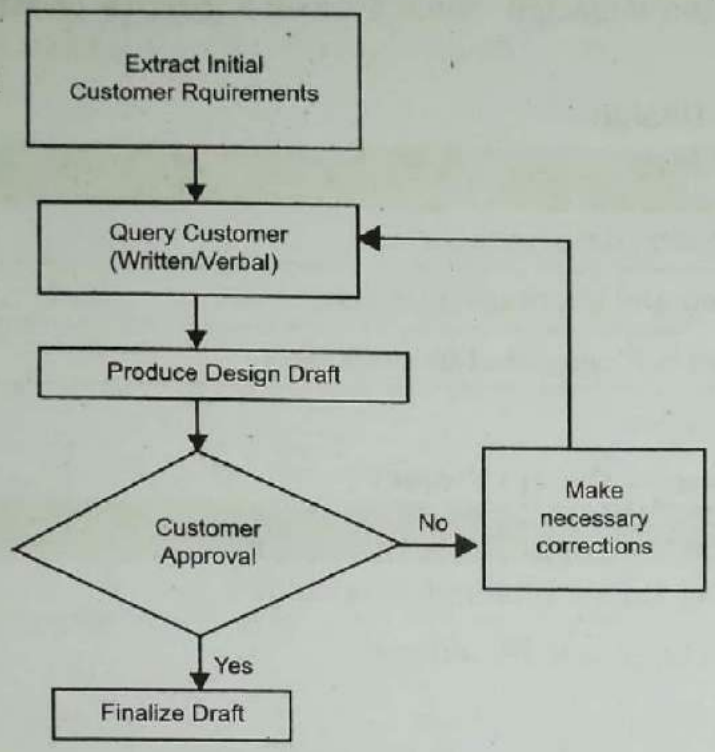


Figure 36: Identify Customer Requirements

2. **Gathering Network Requirements**

Various steps for gathering additional design requirements are given in Figure 37:

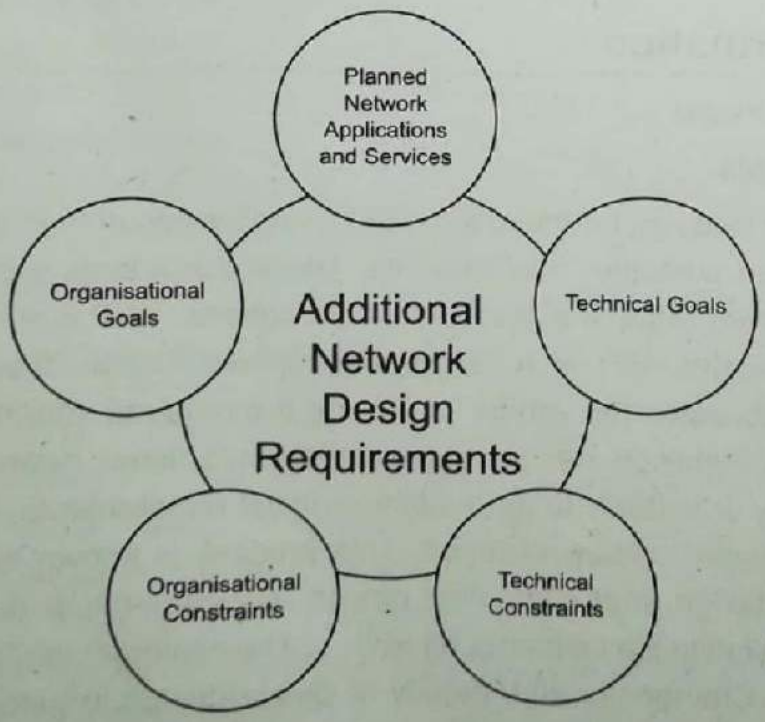


Figure 37: Gathering Network Requirements

Scanned by CamScanner

Additional network requirements are gathered from the staff, discussed and included in design requirements. Steps for gathering additional design requirements are as follows:

1. Identify planned network applications and services
2. Define organisational goals
3. Identify organisational constraints
4. Define technical goals
5. Identify technical constraints

In each step, notes are taken and documented. These notes are findings shared with the customer and discussed. In case any queries arise, any, few or all of these steps are repeated. Thus, all the above steps result in gathering data which is judiciously analysed and documented. These five steps are described in the upcoming sections:

Planned Applications and Network Services

In this step, the designer identifies and lists down all the network applications and network services that will be utilised. Separate tables are prepared for network applications and network services. These tables help organise and analyse the data.

For planned applications, the information in the table includes:

1. **Application type**

   Type of the planned application

   Examples:

   - E-mail
   - Video-on-demand
   - Voice networking

2. **Applications**

   Specific application in that domain

   Examples:

   - Microsoft Office Outlook
   - Windows 10 Mail
   - Apple Mail

3. **Importance level**

   Significance of application to the organisation

   Examples:

   - Critical

Scanned by CamScanner

- Important
- Not important

4. **Comments**

   Notes providing additional information about data gathered

   Examples:

   - Oracle to store all organisational data

Table 11 depicts an example of planned applications for an organisation:

Table 11 Planned Network Applications

Application Type	Application	Importance Level	Comments
Database	Oracle	Critical	Entire data storage on Oracle
Email	Microsoft Office Outlook	Important	
Web Browser	Microsoft Internet Explorer, Google Chrome	Important	

Similar to the planned applications, the table is prepared for network services. This table simply includes the service and information regarding that service. Table 12 shows an example of planned network services.

Table 12 Planned Network Services

Service	Comments
High Availability	• Eliminate single point of failure • Add redundant links
IP Multicast	• Required for e-learning • Required for video conferencing
QoS	• High priority for voice traffic • Low priority for HTTP traffic
Security	• Authentication, authorisation and accounting systems • Firewall • Intrusion detection and prevention system • Virus scanning application

Scanned by CamScanner

Organisational Goals

Organisational goals are of high importance when designing a network because the success of the designed network is ultimately measured by the achievement of organisational goals. For this purpose, both short-term and long-term goals should be traced. An initial study is required regarding current products, services, suppliers, etc. of the organisation. This step helps in identifying customer's priorities. The designer can determine organisational goals by gathering information, such as:

- Accomplishment expected from this project
- Critical applications for organisation
- Currently faced business challenges
- Metrics for measuring success of this project
- Need for change
- Objective of project
- Other business growth affecting the organisation
- Skill set of current technical staff

Table13 illustrates an example of organisational goals for an organisation.

Table 13 Organisational Goals

Organisational Goal	Current Situation	Comments
Add new customer services	Telephone and fax orders	Secure web-based ordering
Increase competitiveness	Company B	Better products
	Company C	Reduced costs
Improve customer support	Manual order tracking	Web-based order tracking
Reduce cost	Multiple data entry	Single data entry point
		Simple data exchange

Organisational Constraints

Organisational constraints act as a barrier to achieve organisational goals. Therefore, it is very important to gather and analyse organisational constraints. The designer can determine organisational constraints by gathering information, such as:

- Budget approved projects
- Budget for technical growth of staff
- Current barriers in organisation
- Current processes working properly

Scanned by CamScanner

- Current processes not working properly
- Financial constraint
- Labour-intensive processes
- Plan to hire new staff
- Policies affecting current project
- Time limitation

Table 14 illustrates an example of organisational constraints for an organisation.

Table 14 Organisational Constraints

Organisational constraint	Current situation	Comments
Budget	INR 7,00,000	INR 1,00,000 scope of extension
Personnel	Two CCNA certified network engineer Two engineers for OS and application maintenance	Plan to hire three engineers for network maintenance
Policies	Single vendor	Currently Cisco
Schedule	New applications to be introduced in the month of December	IP telephony and video conferencing

Technical Goals

The designer must gather information to determine technical goals. Below listed information can help in determining technical goals of the organisation.

- Current network infrastructure issues
- Current network management issues
- Current network performance issues
- Expected growth in number of users from this project
- Mission-critical network segments
- Skills to be acquired by technical staff
- Technology priorities
- Technology budgeting process

Scanned by CamScanner

Table 15 illustrates an example of technical goals for an organisation.

Table 15 Technical Goals

Technical Goals	Importance	Comment
Adaptability	10	Training process
Availability	25	99.99% availability required
Manageability	5	
Performance	20	Important for Head office
Scalability	25	
Security	15	Mission-critical data must be secured

Technical Constraints

Similar to organisational constraints, technical constraints limit the realisation of technical goals. Therefore, it is equally important to gather and analyse technical constraints. The designer can determine technical constraints by gathering information such as:

- Current technical problems
- Current solution for technical problems
- Metrics for determining technical priorities
- Need for special network features
- Plan for technical development of staff

Table 16 illustrates an example of technical constraints for an organisation:

Table 16 Technical Constraints

Technical Constraints	Current Situation	Comments
Existing equipment	Coaxial Cable	• Replace cables with twisted pair to the desktop • Replaces cables with fibre optics for distribution and core
Bandwidth availability	64-kbps WAN link	• Upgrade bandwidth • Change Service provider
Application compatibility	IP version 6-based applications	• IPv6 compatible network equipment

Scanned by CamScanner

1.19. Characterising the Existing Network and Sites

This is the second step of network design methodology. Network design is highly influenced by software, hardware and capacity of the existing network. In this step, network characteristics are audited and analysed. For this purpose, the customer input is taken as well as network tools are used for auditing and analysing network traffic. Once the data is gathered, a check based on network health checklist is done. Accordingly, a report summarising the collected information is prepared. Thus, a thorough analysis of the existing network is utilised to create a network design draft. This entire process can be systematically represented as in Figure 38

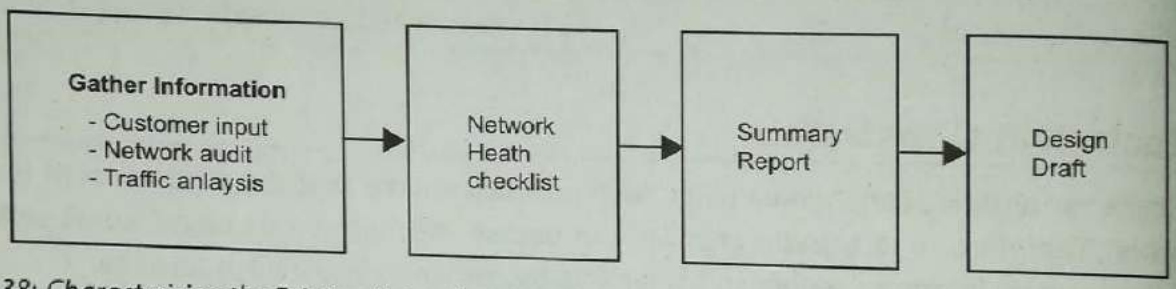


Figure 38: Characterising the Existing Network and Sites

Subsequent sections describe each of these steps in detail.

Customer Input

This is the initial step where existing network information is collected through customers. Existing network documentation is helpful in getting a better insight into existing network characteristics. Moreover, verbal input is also taken from customers based on their experience. Even though this is the initial and mandatory step but not self-sufficient.

Based on network design project scope, designers can request for the below listed documentation from customers:

- Existing network infrastructure: Physical features
  - Applications supported by servers
  - Availability of additional receptacles
  - Availability of power sources
  - Cabling information
  - Locations of network devices
  - Locations of power receptacles
  - Locations of servers
  - Locations of telephone service demarcation points
  - Locations of WAN connection feeds

Scanned by CamScanner

- Locations of wiring closet
- Network interface connection details
- Types of network devices
- Types of servers
- WAN speeds

- Existing network infrastructure: Logical features
  - Addressing schemes
  - Infrastructure services
  - Routing protocols
- Expected network functionality
- Site contact information

Based on collected information from the above documents and customer inputs, below information regarding the existing network and planned network can be obtained:

- Network topology
  - Connections bandwidth
  - External connections
  - Frame types
  - IP addressing
  - Network devices
  - Physical and logical links
  - Routing protocols
- Network services
  - High availability
  - QoS
  - Security
  - Storage
  - Voice
  - Wireless
- Network applications
  - Unified messaging and video delivery

All the above-listed information can be utilised to modularise the network. Hence, the design document should contain all this information.

Scanned by CamScanner

Sample Site Contact Information

Some network design projects need remote deployment. In such cases, coordination is required between equipment delivery and installation. For this purpose, information regarding the site is collected by the designer either from the customer or by conducting a physical site audit or both.

Below listed is the information that a designer can collect regarding the site contact:

- Building and room access procedures
- Equipment cabinets and racks location
- Security and safety procedures
- Shipping address
- Site address
- Site contact person details
- Site maintenance
- Site operation hours
- Site ownership
- Site location/name
- Union/labour procedures

Sample High-Level Network Diagram

Based on the high-level network diagram provided by the customer, information regarding various network aspects can be queried, such as:

- IP addressing mechanism
- Level of availability in the existing network
- Level of availability in the planned network
- Level of redundancy in the existing network
- Level of redundancy in the planned network
- Layer 2 and Layer 3 topologies planned
- Link speed
- Link types
- Network infrastructure services existing
- Network infrastructure services planned
- Network management tools
- Remote data centre connectivity
- Remote sites connectivity

Scanned by CamScanner

- Routing protocols
- Security design details
- Existing Wireless devices
- Planned Wireless deployments

Auditing or Assessing the Existing Network

This is the second step in gathering information regarding the existing network. There are three sources of information in this step i.e. existing documentation, existing tools and new tools. Existing documentation is the information provided by the customer. Network management tools used by the organisation serve as another source of input. If information from these two sources is not sufficient, designers can introduce new tools on the temporary or permanent basis to collect required network information. Network audit includes details regarding network devices such as configuration, CPU utilisation, memory utilisation, hardware specification, software specification, types, unused modules, unused ports, unused slots, etc. For large networks, automated auditing is preferred over time-consuming and less reliable manual auditing. Central location in the existing network is preferred to perform auditing as it has access to all network devices.

During the network audit, sample information collected can be such as:

- Average CPU utilisation
- Average link utilisations
- Configuration
- CPU type
- FLASH size
- Interface types
- IOS version
- Memory size and utilisation
- Router type
- Routing tables
- Speeds
- Unused interfaces
- Unused modules
- Unused slots

Scanned by CamScanner

Various third-party tools are available for network assessment, few are depicted in Table 17:

Table 17 Network Assessment Tools

Company	Tool
Castle Rock Computing	SNMPc
Ipswitch	WhatsUp Professional
Open-source	Cacti
Netcordia	NetMRI
NetQoS	NetVoyant

Analysing Network Traffic and Applications

This is the third step in gathering information to characterise the existing network. It is used to gather information about traffic patterns in the network for different applications and protocols. Information collected regarding each network application and protocol must include:

- Importance to customer
- QoS requirements
- Scope
- Security requirements

To identify various applications and protocols used in a network, an interactive approach is used which has the following steps:

1. List applications using input from the customer
2. Verify the list of applications using traffic analysers
3. List discrepancies and discuss with the customer
4. Generate the final list of applications along with requirements

Table 18 depicts an example of the information collected for an application:

Table 18 Network Application Information

Feature	Description
Name	Application No. 25
Description	Marketing software
Protocol	Transmission control protocol TCP port 5151
Clients	60
Servers	2
Scope	Branch
Importance	High
Average	50 kbps with 10-second bursts to 1 megabit per second (Mbps)

Scanned by CamScanner

Cisco products as well as third-party tools are available to analyse network traffic.

Examples of Cisco tools:

- Network-Based Application Recognition (NBAR)
- NetFlow

Examples of third-party tools are given in Table 19

Table 19 Network Analyser Tools

Company	Tool
Open-source	Cacti
Open-source	Wireshark
Network General	Sniffer
SolarWinds	Orion
WildPackets	AiroPeek
	EtherPeek

Network Health Checklist

A network health checklist is a list of criteria that must be satisfied by a healthy existing network. For each criterion, an approximate threshold is set up. This approximation is based on the criteria for accepting network performance. Existing applications, devices, topology and traffic also contribute to threshold setup.

Table 20 is a sample for network health checklist.

Table 20 Network Health Checklist

Checkbox	Criteria	Threshold
☐	Broadcast or multicast by a segment	20%
☐	Collision on an Ethernet segment	0.1%
☐	Cyclic redundancy check error per million bytes of data	1
☐	Ethernet segment network utilisation	40%
☐	Number of buffer misses in an hour	25
☐	Number of ignored packets in an hour	10
☐	Number of input queue drops in an hour	50
☐	Number of output queue drops in an hour	100
☐	Response time (in milliseconds)	100
☐	WAN link network utilisation	70%

Scanned by CamScanner

Summary Report

After taking the input from the customer, auditing the existing network and analysing existing network traffic; the next step is to create a summary on network's health. Rather it is to highlight the problems identified in the existing network and solutions for the same. Thus, a summary report must include:

- Missing network features
- Limitations and problems of existing network
- Recommended action

This helps in identifying hardware and/or software upgrades required in the existing network infrastructure to support the new design. The information that a sample summary report includes:

- Number of routers used in network
  - Count of routers along with software version
  - **Example:** 25 routers use Cisco IOS software version 12.1
- Requirement
  - **Example:** QoS congestion management required in WAN
- Identified problem for the respective requirement
  - **Example:** 20 out of 25 routers do not have enough memory to upgrade to the latest software
- Recommended action
  - **Example:** 20 memory upgrades to 64 MB
- Alternatives
  - **Examples:** Replace hardware as well as software

Creating a Draft Design Document

This is the last step in characterising the existing network. A design draft must start with a section on design requirements followed by another section on the existing network infrastructure. Details related to network topology, network audit, network applications, network health analysis and recommended changes to the existing network must be specified in this section. The appendix may include the list of network devices in the existing network infrastructure and their configuration.

A list of details that must be included in a design draft is given here:

- Layer 3 (Logical) topology map or maps
- Layer 2 (Physical) topology map or maps
- Application and overlay services

Scanned by CamScanner

- Issues affecting new design
- Network audit results
  - Suboptimal traffic path
  - Traffic congestion points
  - Traffic types
- Network devices
  - Configuration
  - Platform
  - Software
- Network services
  - Border Gateway Protocol (BGP)
  - Internet Protocol Security (IPSec)
  - Open Shortest Path First (OSPF)

1.20. Using the Top-Down Approach to Network Design

After identifying the customer requirements and characterising the existing network, the next step is to design the network. Designing the network is a complex process especially when the network to be designed is large or even medium. Two approaches to design the network are:

1. Bottom-Up approach
2. Top-Down Approach

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, datalink 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 redesign.

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 of the OSI model. Initially, requirements of upper layers (application, presentation and session layers) are worked upon and then lower layers (transport, network, data link and physical layers) are designed to support functionalities of the upper layer. That is, customer

Scanned by CamScanner

requirements are thoroughly analysed to determine the services and applications expected from the network to be designed. To fulfil the network services required by application, the decision is made regarding the network infrastructure which includes type, speed, 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 need to be considered while designing the network. Thus, in the top-down approach network design, applications and services required to drive the design of physical infrastructure.

Comparison between Top-Down Approach and Bottom-Up Approach is given in Table 21

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

Decision Tables in Network Design

A network is designed to provide the optimal solution for the existing network problems. One network problem might have more than one solution. How to determine which solution is most appropriate from different perspectives? The answer is Decision Table. A decision table is a systematic way of listing and comparing all the solutions available on different metrics. It gives a clear picture of several aspects that can be used to justify the selection of the most appropriate solution. Selection of the most appropriate solution is done on the basis of degree of compliance with technical requirements.

Network design decision table should be created by the following guidelines.

1. Determine the network design factors for which the decision is to be made. For example, routers, routing protocol, topology, media, etc.
2. All possible options should be collected for each decision. None to be missed. This requires a thorough knowledge of network infrastructure including devices, components, protocols and their advantages and limitations. Also, a sound characterisation of the existing network gives a better insight for available options.

Scanned by CamScanner

3. List down all requirements as well as collected solutions. Metrics based on which solutions will be evaluated must also be included in a table.
4. Make a comparison of requirement with available solutions on various metrics.
5. The solution that matches the maximum requirements is the most appropriate solution.

In the above procedure, all requirements are treated equally. Nevertheless, in real-life scenarios, some requirements have more significance than others. In such cases, if all requirements are treated equally, the selected option might not be the most appropriate one. Therefore, for such scenarios, a weight factor is assigned to each requirement. The weight factor indicates the importance of the respective requirement. It eases out the decision-making process.

Decision Table Example

Let us consider a network design scenario for an organisation where the routing protocol is to be selected.

Customer requirements/considerations for selecting the routing protocol are:

1. Support a large network
2. Support an enterprise environment
3. Support Variable Length Subnet Masking (VLSM)
4. Existing staff should have good knowledge so that no need to employ new staff for network maintenance.

Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS) and Border Gateway Protocol (BGP) are the four routing protocols are considered for evaluation. Four metrics viz. network size, enterprise favourable, VLSM support and skilled staff availability, are used to evaluate each routing protocol. A decision table is given in Table 22:

Table 22 Decision Table

Metrics/ Solutions	EIGRP	OSPF	IS-IS	BGP	Network Requirements
Network Size	Large	Large	Very Large	Very Large	Large
Enterprise favourable	Yes	Yes	No	No	Yes
VLSM support	Yes	Yes	Yes	Yes	Yes
Skilled Staff Availability	High	Medium	Low	Low	High

Scanned by CamScanner

As shown in Table 22, all requirements have equal weightage. EIGRP satisfies all the network requirements. It supports a large network size and is favourable for the enterprise network. It also supports VLSM. Moreover, many staff in the organisation already have good knowledge of EIGRP. Therefore, for the given scenario, EIGRP is selected.

Structured Design

The top-down approach is a preferred approach for network design. Business goals, technical requirements, applications and services required, future developments, etc. are all considered while designing the network using the top-down approach. Network infrastructure such as components, protocols or technologies, etc. adapt to the network applications and services. As mentioned in the previous section, network design is a complex process. Structured design breaks this complex process into simpler design tasks.

Below are the steps for structured design:

1. Based on customer requirements, determine what are the applications required for network design.
2. Based on application requirements identified, determine network services required by applications and network infrastructure required to support such applications and services.
3. To build a hierarchy for efficiently utilising network infrastructure, categorise network functionality.
4. For each functionality, design the network infrastructure. While designing the solution, do not ignore other functionalities rather have a relative design. For example, network infrastructure determines the capability of the network to provide infrastructure services. Hence, network infrastructure and infrastructure services correspond to the same functional model.
5. For each identified network infrastructure requirement, decompose it into logical structures. Logical structures include routing protocols, security, addressing, etc. Each one should be designed separately but keeping other structures under consideration.

All the above discussion is related to logical structuring of the network. Now let us shift our focus to physical structuring of the network. A network can be physically designed in a single, large, flat structure but such a network is inefficient, fault detection is troublesome and resources are not optimally utilised. Another option is to design a physical structure of the network in a hierarchical manner. The network achieves better performance when designed in a hierarchical fashion: core, distribution and access layers. In such an approach, it is simpler and easier to clearly define the functionalities and identify technologies required for the same. This hierarchical network structure is covered in Chapter 2 in more depth.

Scanned by CamScanner

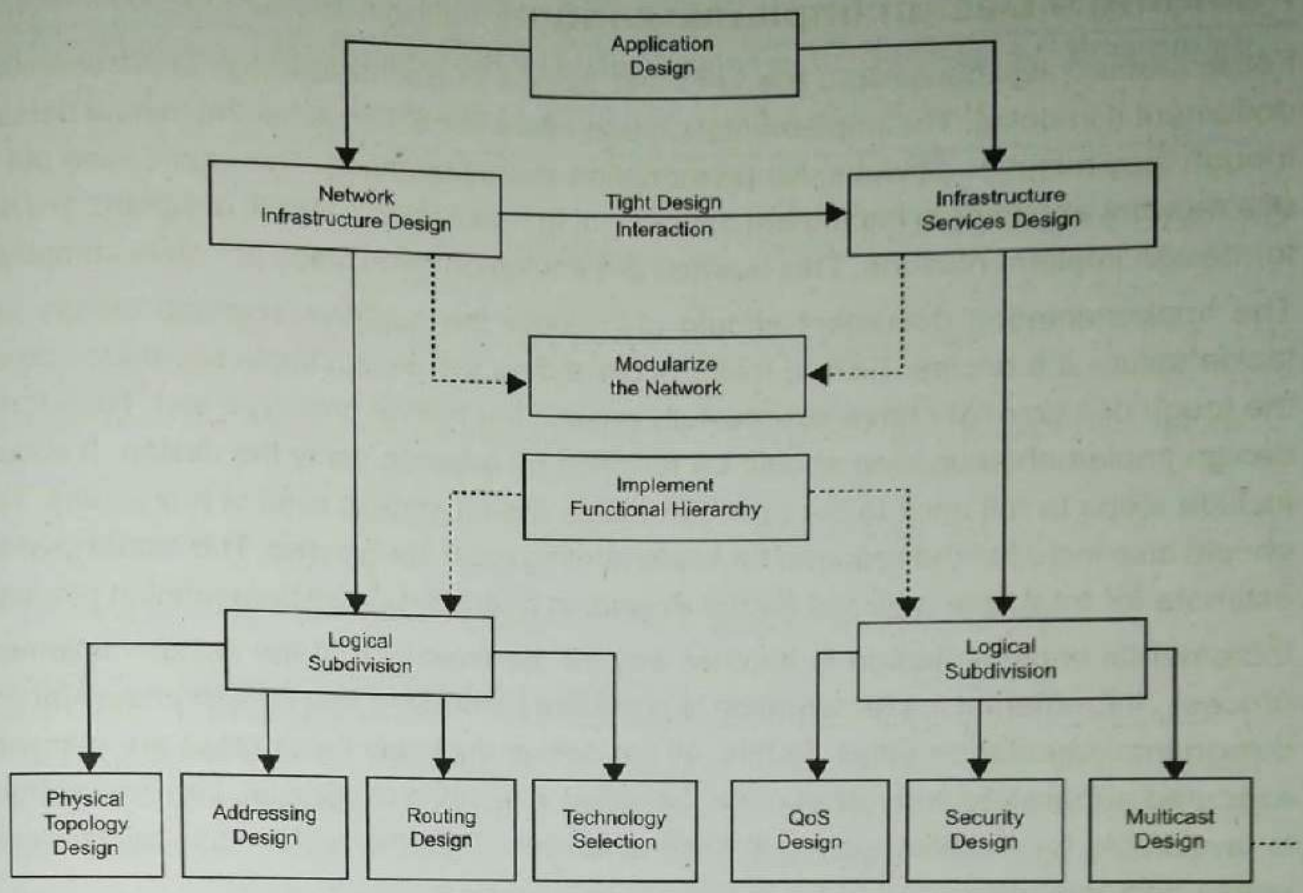


Figure 39: Example of Structured Design

The above figure is an example of structured design for the top-down approach. As reflected from the figure, network designing is done in a modular fashion starting from top and moving towards the bottom. Network design starts with Application design. Based on application requirements, Network infrastructure design and Infrastructure services design are crafted. Both are tightly integrated with each other and share logical, physical and functional modules. Addressing design, physical topology design, routing design and technology selection are logical subdivisions of network infrastructure design. Multicast design, QoS design and Security design are logical subdivisions of infrastructure services design.

1.21. Design Implementation Process

After identifying customer requirements, characterising the existing network and sites and designing the network topology, the design is complete. Next step is the implementation of design. The three steps of the design implementation process are:

1. Planning a design implementation
2. Implementing and verifying the design
3. Monitoring and redesigning the network

Scanned by CamScanner

Planning a Design Implementation

For implementing the design, the very first step is to plan the design implementation and document it in detail. The implementation document should cover all the minute details even though they might be obvious. No presumption should be made. This would ease out the job of a network engineer to implement the design. In rare cases, network designers are required for design implementations. This is when the implementation steps are quite complex.

The implementation document should also cover the negative scenario means steps to tackle failure if it occurs. Failure might occur during the design implementation phase even the tough design might have successfully passed the pilot or prototype test. Therefore, each design implementation step should be followed by a test to verify the design. It should also include steps to roll back to the previous stable design state in case of any issues. The plan should also include time required for implementing each design step. This would give a better estimate for total time required for the execution of the design implementation process.

Incremental implementation is another way for the execution of the design implementation process. Incremental implementation is preferred for designs that consist of several complex design implementation steps. In this, all the design implementation steps are planned to be executed separately and not at once. Separate execution of complex implementation steps is favourable for troubleshooting in case of failures. Also, the system can quickly revert to a stable design state.

Network design implementation is a several-phase process. Each phase consists of several design implementation steps. To ease the implementation process, every implementation step should be described in detail. It should give reference to the respective design document. All the guidelines for implementation should be detailed. To handle failure, rollback guidelines should also be detailed. As mentioned above, it should also include the time estimate for the execution of respective network design implementation step.

In order to verify that the network is behaving as expected, the implementation document should also include a list of checks to be performed after completion of design implementation.

Table 23 depicts a sample summary of network design implementation plan.

Table 23 Design Implementation Plan Summary

Phase	Date	Description	Implementation Details	Complete
Phase 4	15/06/2019	Install campus hardware	Section 5.2.4	√
Step 1		Connect switches	Section 5.2.4.1	√
Step 2		Install routers	Section 5.2.4.2	√
Step 3		Complete cabling	Section 5.2.4.3	√

Scanned by CamScanner

Phase	Date	Description	Implementation Details	Complete
Step 4		Verify data link layer	Section 5.2.4.4	√
Phase 5	15/07/2019	Configure campus hardware	Section 5.2.5	
Step 1		Configure VLANs	Section 5.2.5.1	
Step 2		Configure IP addressing	Section 5.2.5.2	
Step 3		Configure Routing	Section 5.2.5.3	
Step 4		Verify connectivity	Section 5.2.5.4	

There should be a detailed description of each implementation step in Table 23.

Implementing and Verifying the Design

Network design gets completed once a pilot or prototype network has been successfully implemented. This is done for proof of concept. Yet real test of network design is the actual, live implementation process. Design weakness might get highlighted during the implementation phase. Therefore, to verify the design during the implementation phase and to take remedial actions for failures, a designer should be present to assist throughout the implementation phase. After implementation, verify whether the network is behaving as required based on the checklist documented while planning the implementation phase.

Monitoring and Redesigning the Network

Once network design is implemented successfully, the network is operational and under constant surveillance for any problems or errors. Frequent troubleshooting or too many errors is a matter of serious concern. If unmanageable, go for network redesign. Proper completion of each and every step of network design methodology helps to avoid such scenarios. Thus, healthy operation of the network, after design implementation, is the real check of design appropriateness.

Example:

Problem after implementation:

- Frequent network congestion

Redesign Solution:

- Add filters
- Increase bandwidth

Scanned by CamScanner

- Move highly loaded servers
- Increase device capacity

1.22. Summary

This chapter starts with basic networking fundamentals that include transmission media, transmission topologies, internetworking devices and VLAN basics. Cisco SONA architecture framework describes the network design from the service/application perspective. The network design methodology is described in three simple steps based on the PPDIOO network lifecycle. The chapter concludes with the design implementation process.

QUESTIONS

1. Explain Cisco SONA framework in detail.
2. Describe various phases in PPDIOO network lifecycle.
3. List and explain network design methodology steps.
4. Explain steps to implement a design.
5. What is meant by organisational goals and constraints? How do they restrict network design?
6. Explain top-down network design in detail.

Scanned by CamScanner

Structuring and Modularising The Network

2

OBJECTIVES

After reading this chapter, the student will be able to:

- To understand network hierarchy
- To apply modular hierarchical approach for network design
- To understand modular network services
- To apply network management protocols and features

Scanned by CamScanner

As seen in previous chapters, the process of enterprise wide network design is equivalent to the process of developing software for an enterprise. This is due to the fact that an enterprise network acts as a complete system to support the business processes of an enterprise the way software developed for an enterprise acts as a complete system. We are also aware that various software development methodologies promote the idea of modular design for software and hence, on similar lines, we need to use a modular approach to design the network for an enterprise. We have already discussed the importance of network hierarchy and diversity in Chapter one. This chapter explains the hierarchical network model and also discusses specific Cisco standards.

2.1. Network Hierarchy

Network hierarchy can be represented in the form of a hierarchical network model. Different design layers of the hierarchical model are explained in the subsequent sections.

Hierarchical Network Model

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

Hierarchical Network Design Layers

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

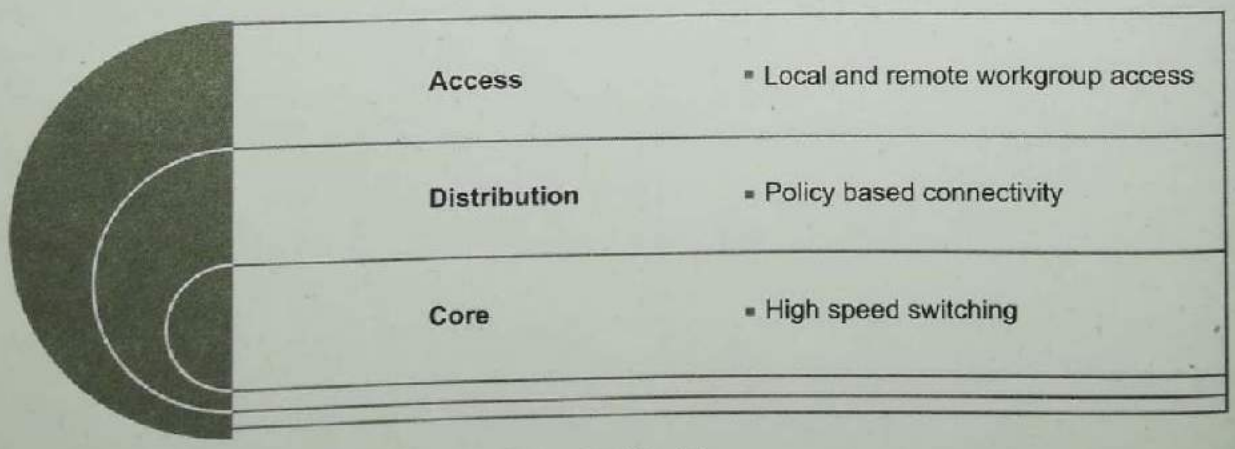


Figure 1: Three layers of Hierarchical Network Design Model

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

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

Scanned by CamScanner

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

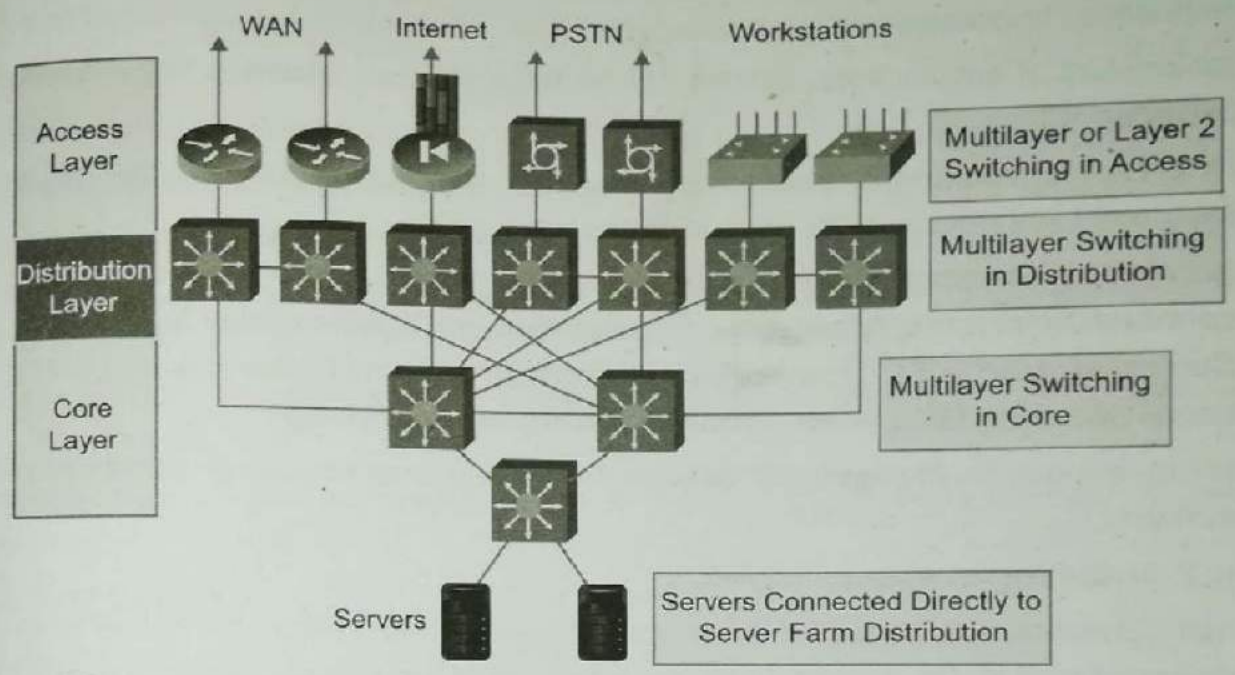


Figure 2: Sample Network Using Hierarchical Network Design

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

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

Access Layer Functionality

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

Scanned by CamScanner

Role of Access Layer

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

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

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

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

Layer 2 Switching in Access Layer

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

For large networks:

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

Scanned by CamScanner

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

Multilayer Switching in Access Layer

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

Access Layer Example

Figure 3 displays an example of the access layer:

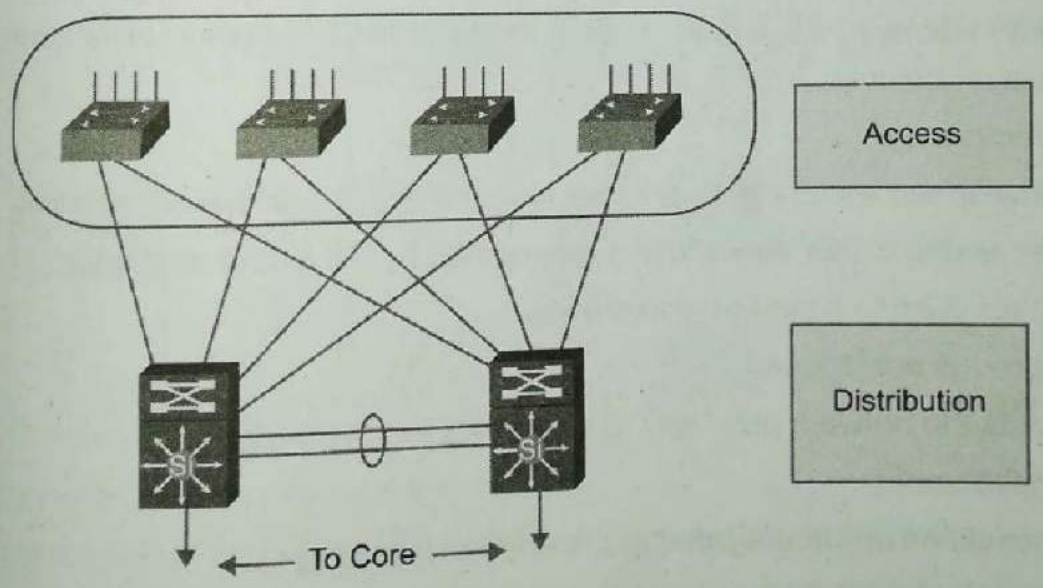


Figure 3: Access Layer Example

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

Scanned by CamScanner

Distribution Layer Functionality

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

Role of Distribution Layer

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

Various examples of implementing policies are given as follows:

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

Characteristics of distribution layer are stated as follows:

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

Scanned by CamScanner

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

Distribution Layer Example

Figure 4 displays an example of distribution layer connectivity:

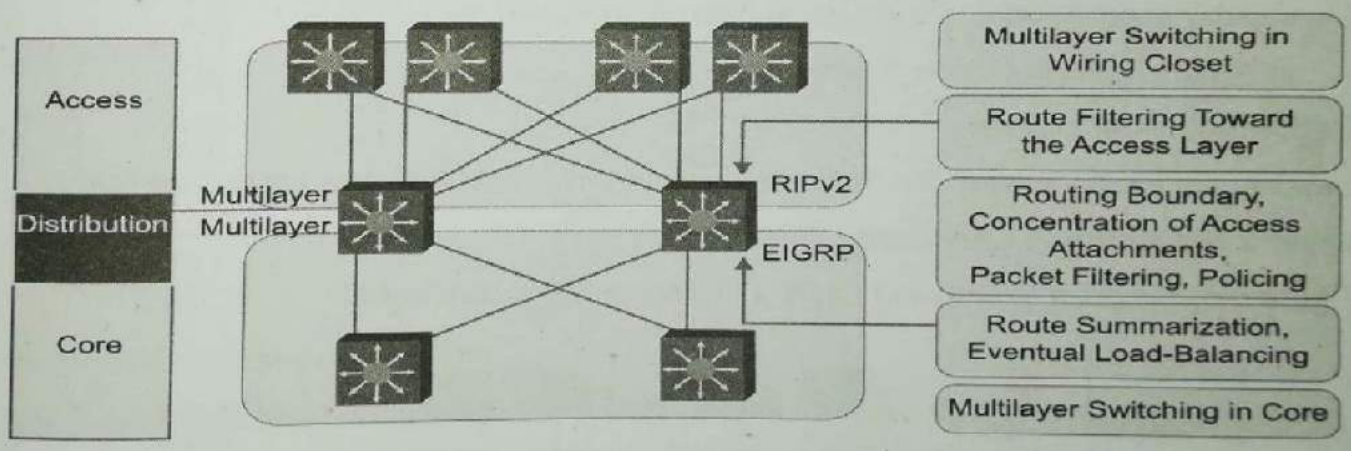


Figure 4: Distribution Layer Connectivity

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

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

Scanned by CamScanner

- Distribution layer exchanges routes between RIPv2 and EIGRP.

Core Layer Functionality

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

Role of Core Layer

Characteristics of core layer are stated as follows:

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

Switching in Core Layer

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

Layer 2 Switching in LAN Core

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

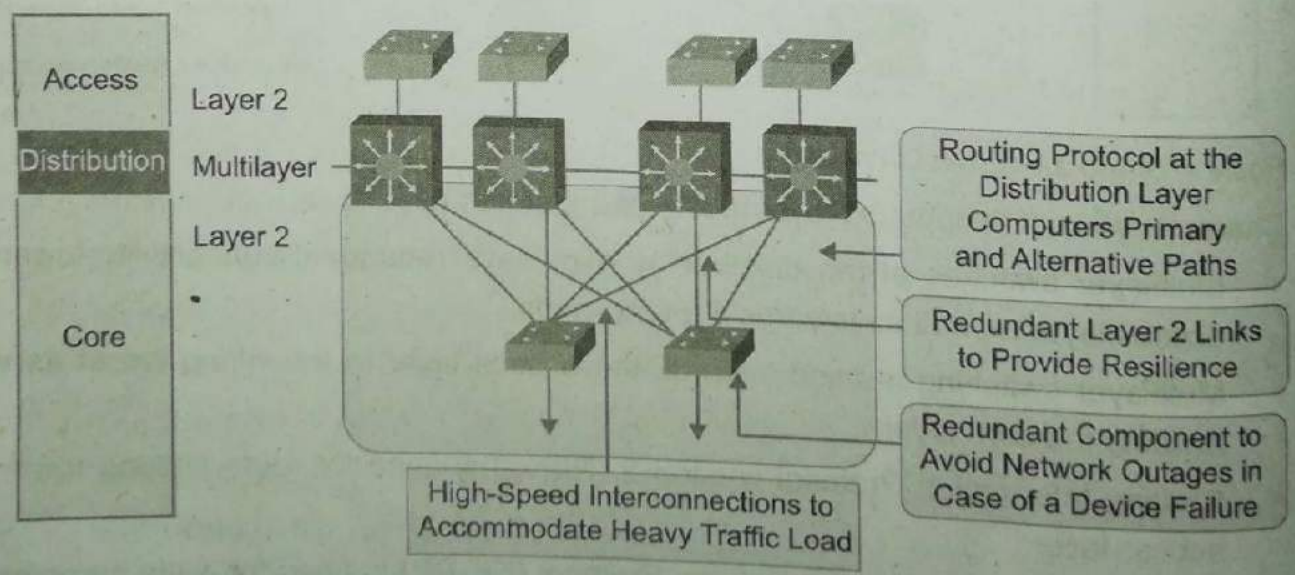


Figure 5: Layer 2 Switching in Core Layer

Scanned by CamScanner

Figure 5 illustrates an example of Layer 2 switching in the core layer. As depicted from the figure, the access layer uses Layer 2 switching, the distribution layer has multilayer switching and the core layer has Layer 2 switching. Layer 2 switches at the access layer route the packet to the distribution layer. There are many redundant paths between the distribution layer and the core layer to provide resilience. These high-speed interconnections accommodate heavy traffic load. The multilayer switch at the distribution layer computes all possible paths to the core layer and forwards the packet to the core layer from an optimum path. At the core layer, many redundant network components exist. These devices help in avoiding network outages in case of device failure. Layer 2 switching is performed by the core layer across LAN. At the distribution layer of the receiving end, the packet is multilayer switched to the access layer. The access layer switch performs Layer 2 switching to send a packet to the destination host.

Layer 3 Switching in LAN Core

Figure 6 displays an example of Layer 3 switching in the core layer:

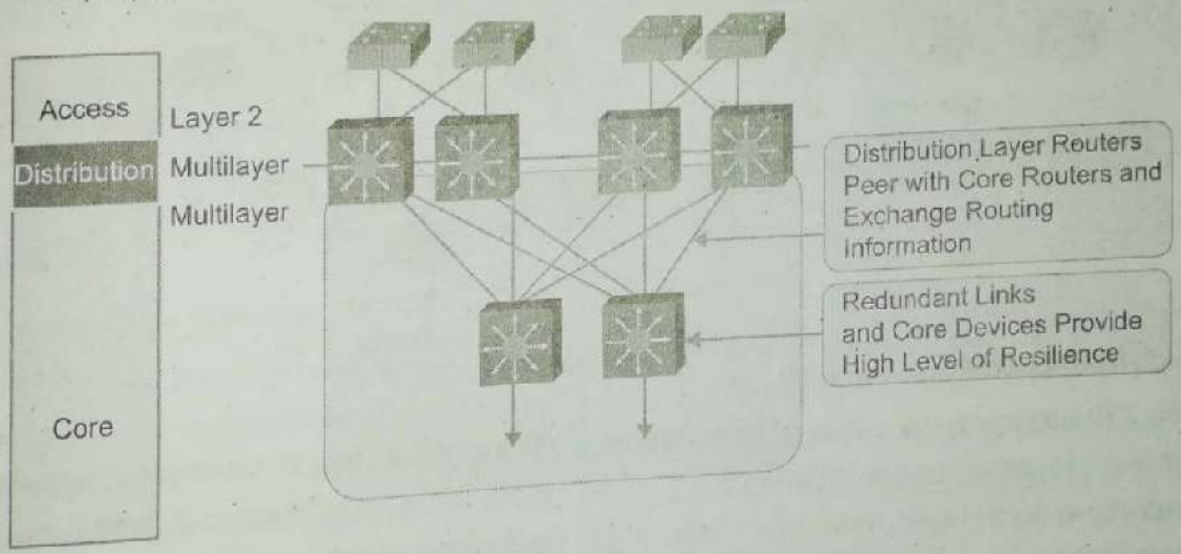


Figure 6: Layer 3 Switching in Core Layer

Figure 6 illustrates an example of Layer 3 switching in the core layer. As depicted from the figure, the access layer uses Layer 2 switching whereas the distribution layer and the core layer both have multilayer switching. Layer 2 switches at the access layer route the packet to the distribution layer. Multilayer switches at the distribution layer peer with core routers and exchange information. There are redundant links between the distribution and core layers providing high resilience. Multilayer switching is performed by multilayer switches at the distribution layer towards the core layer. Multilayer switching is also performed by Layer 3 switches at the core layer across the LAN core. Again, multilayer switching is performed by multilayer switches at the receiving distribution towards the access layer. Finally, the access layer switch performs Layer 2 switching to the destination host.

Scanned by CamScanner

Hierarchical Routing in WAN

Figure 7 displays an example of hierarchical routing in WAN:

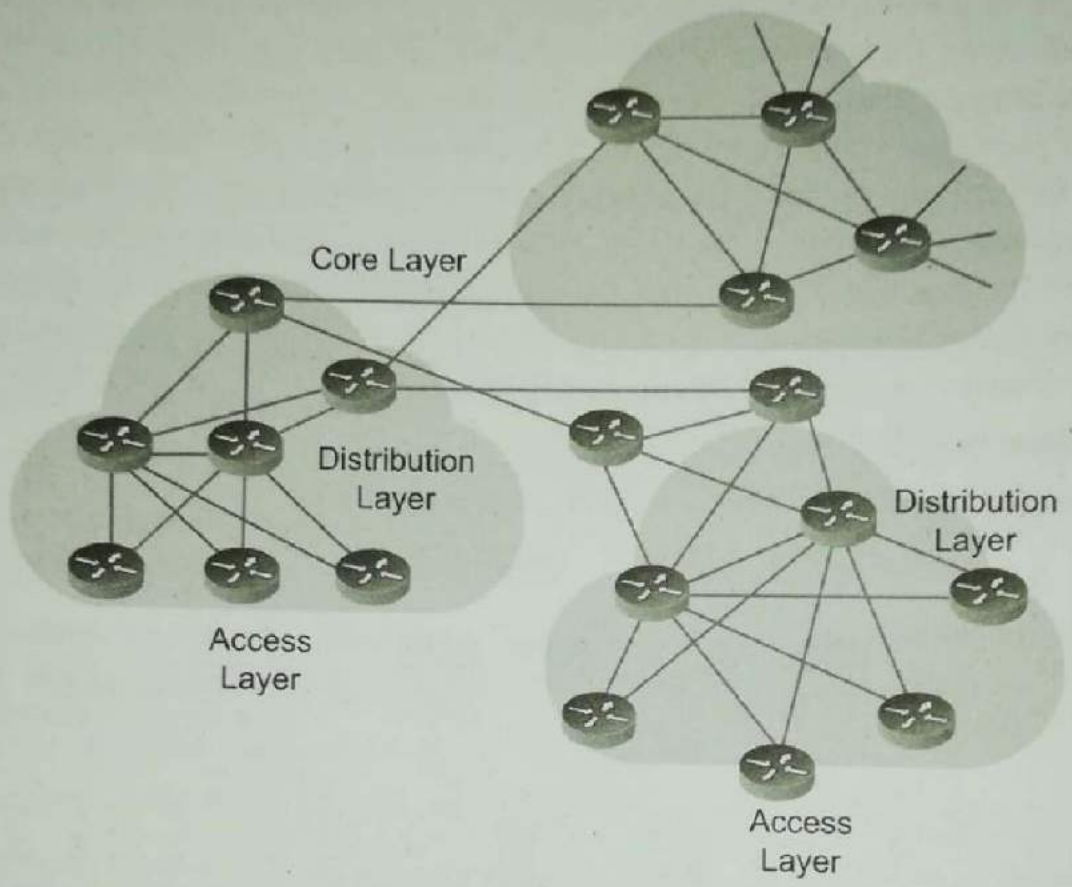


Figure 7: Hierarchical Routing in WAN

Figure 7 illustrates an example of hierarchical routing in WAN. In this example—access layer, distribution layer and core layer—all the three layers have multilayer switches, i.e. routers. Therefore, at each layer, multilayer switching is performed while forwarding the packet to the subsequent layer.

2.2. Using A Modular Approach To Network Design

Initially, the network was created so that resources, such as printers, could be shared across an organisation. As the organisations expanded, a need for connection developed among organisations. This added complexity to network growth. The hierarchical model, as discussed in the previous section, suggests access layer, distribution layer and core layer for network designing. However, this model may not be efficient for designing a large network as it does not scale well for a large network. A better approach is to break a large complex network into smaller functional modules. Each functional module can then be designed hierarchically. Cisco Enterprise Architecture supports such network design. The Cisco Service-Oriented Network Architecture (SONA) framework is detailed in this section along with the functional areas of Cisco Enterprise Architecture.

Scanned by CamScanner

Cisco SONA Framework

Figure 8 displays the Cisco SONA framework:

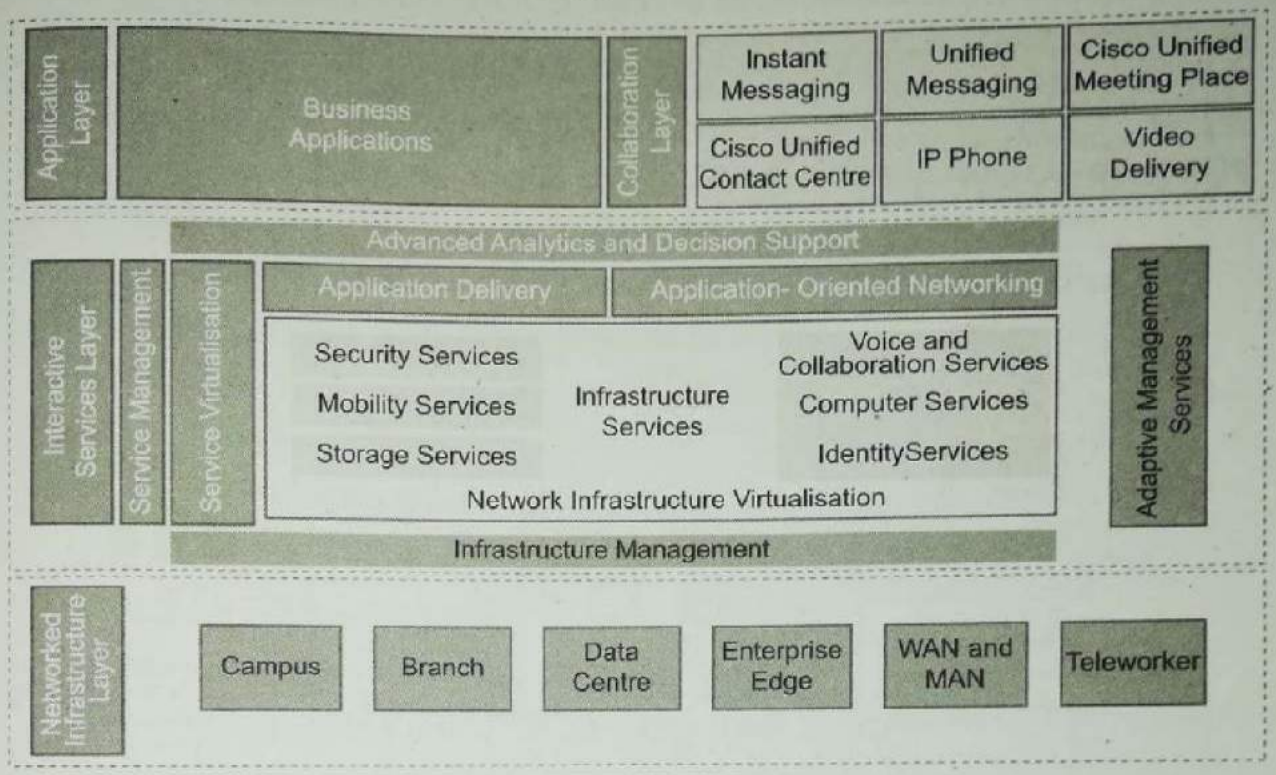


Figure 8: Cisco SONA Framework

Figure 8 depicts the framework for Cisco SONA. As illustrated in the figure, the network infrastructure layer integrates branch, campus, data centre, enterprise edge, teleworker and WAN. Each of these modules has a separate network infrastructure and network services. All these modules represent separate functional areas in Cisco Enterprise Architecture.

Functional Areas of Cisco Enterprise Architecture

Cisco Enterprise Architecture has six functional areas. Functional areas of Cisco Enterprise Architecture are also referred as functional modules. Each functional module maintains the core-distribution-access layers hierarchical concept.

The six functional areas of Cisco Enterprise Architecture are listed as follows:

- Enterprise Campus
- Enterprise Edge
- Enterprise Data Centre
- Enterprise Branch
- Enterprise Teleworker
- Service Provider

Scanned by CamScanner

Please note that the Service Provider functional area is not implemented by an enterprise network. Also, WAN and MAN are parts of the Enterprise Edge functional area.

Figure 9 illustrates the functional areas of Cisco Enterprise Architecture:

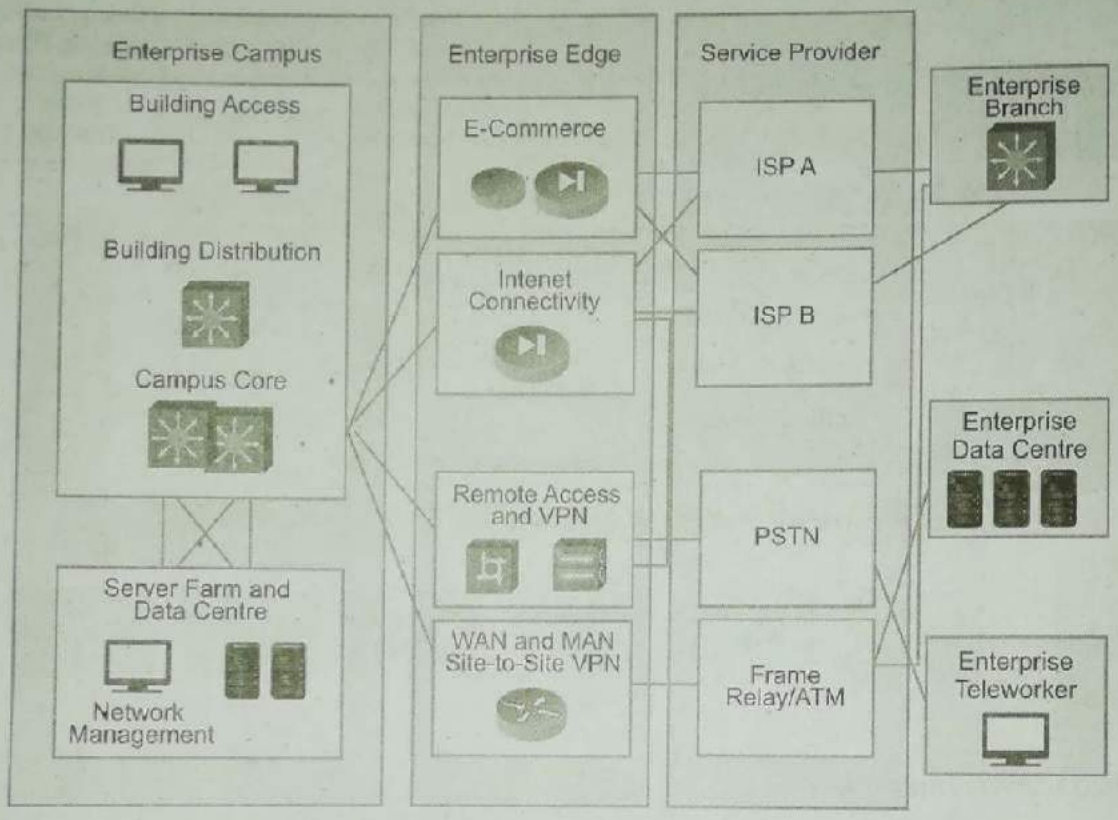


Figure 9: Cisco Enterprise Architecture

Let us discuss each of these in detail.

1. **Cisco Enterprise Campus Architecture**
   - It consists of access layer and distribution layer in building.
   - It consists of core layer at the campus level.
   - Server farm and data centre are connected to the core layer.
   - The core layer has intelligent switching and routing functionality.
   - The core layer is tightly coupled with productivity-enhancing technologies.
   - High availability is achieved through:
     - Automatic network paths reconfiguration to handle failures.
     - Redundant hardware and software.
     - Resilient multilayer architecture.
   - Optimised bandwidth consumption is achieved through IP multicast.
   - Real time traffic is not delayed or dropped.
   - Impact of network attacks is mitigated through integrated security.

Scanned by CamScanner

2. **Cisco Enterprise Edge Architecture**
   - It consists of e-commerce and Internet connectivity.
   - It supports remote access and VPN.
   - WAN and MAN are part of this functional area.
   - Site to site VPN is also part of this functional area.
   - It offers secure delivery of high-quality data, voice, and video to other enterprise networks.
   - It offers convergence of data, voice, and video services.
   - It supports a large geographic enterprise area.
   - It handles service level, security, and QoS issues.
   - It reduces cost.
3. **Cisco Enterprise Data Centre Architecture**
   - It is located at a campus or at a remote area.
   - It enables enterprise scaling.
   - Performance is enhanced by load balancing.
   - It provides a backup of data by synchronously or asynchronously replicating data and application.
   - It simplifies management by reducing overhead.
   - It supports business continuance, consolidation and security.
   - It supports on-demand computing, virtualisation and service-oriented architecture.
   - It secures access to applications and resources.
4. **Cisco Enterprise Branch Architecture**
   - It extends services and applications at the head-office to all the branches and end-users at remote locations.
   - Integrated Service Router (ISR) supports the integration of various services such as caching, converged voice and data services, network analysis, security and switching at the branch level.
   - It provides secure access anywhere, anytime to voice, video and mission-critical data.
   - It reduces traffic and saves bandwidth.
   - It supports advanced routing, application content caching, VPNs, and redundant WAN links at all branches.
5. **Cisco Enterprise Teleworker Architecture**
   - It extends campus security policies to the teleworker.

Scanned by CamScanner

- It minimizes IT support costs.
- It provides business resiliency solution for the enterprise.
- It provides secure access to authorised applications and services.
- It securely delivers data and voice services to Small Office, Home Office (SOHO).
- Security challenges are mitigated through robust integrated security.
- It supports flexible work environment for staff.

Guidelines for Creating an Enterprise Network

Figure 10 displays a network divided into functional areas:

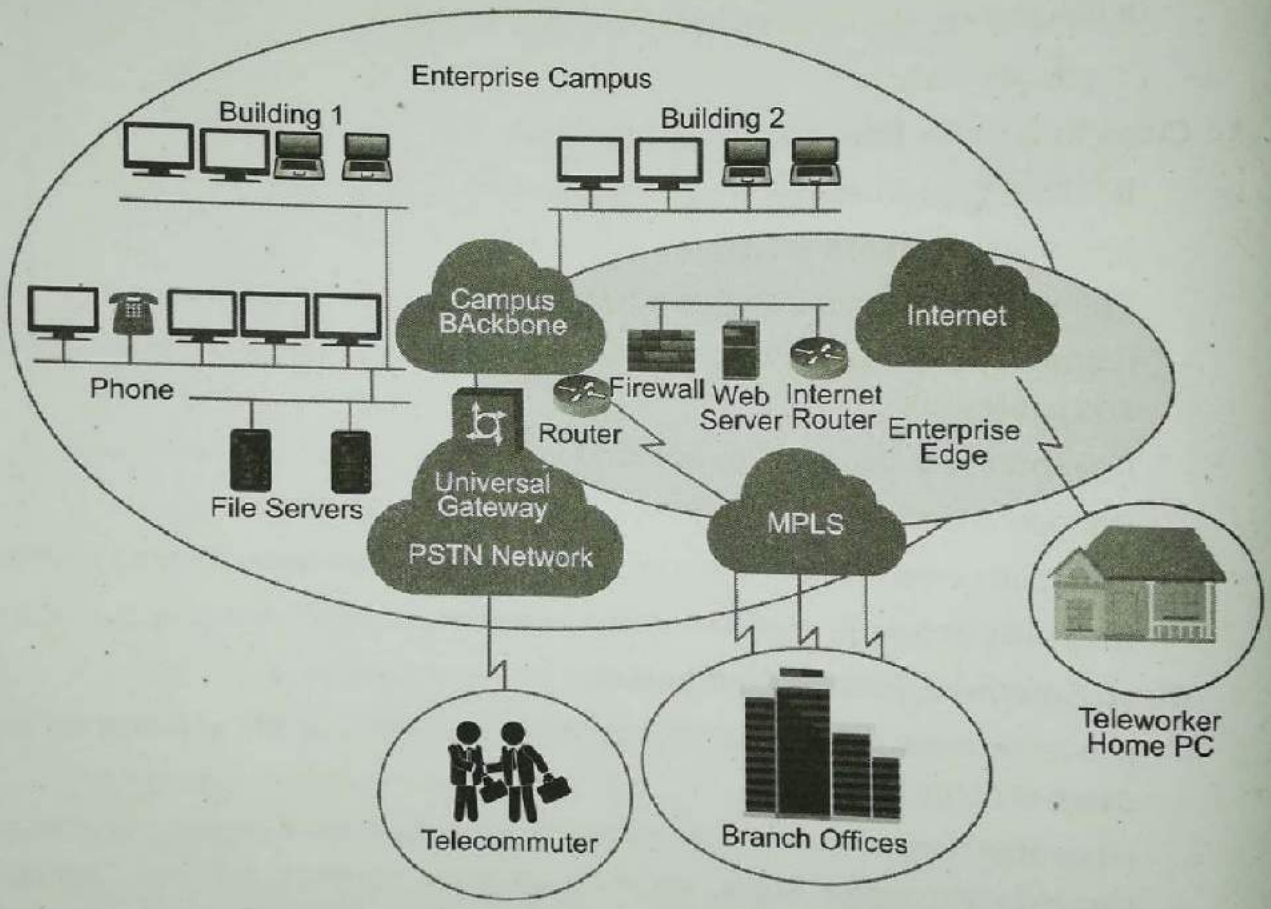


Figure 10: Network Divided into Functional Areas

While designing a network for an enterprise, clear boundaries of each functional area needs to be defined. All network devices and links at the campus are part of Enterprise Campus, whereas communication to the outside world, including the Internet and remote location, is covered by Enterprise Edge. Branches, teleworker and data centre are all part of remote modules. Figure 10 illustrates such a division of an enterprise network. The following sections describe each of these functional areas in more detail.

Scanned by CamScanner

Enterprise Campus Modules

Figure 11 displays the Enterprise Campus functional area:

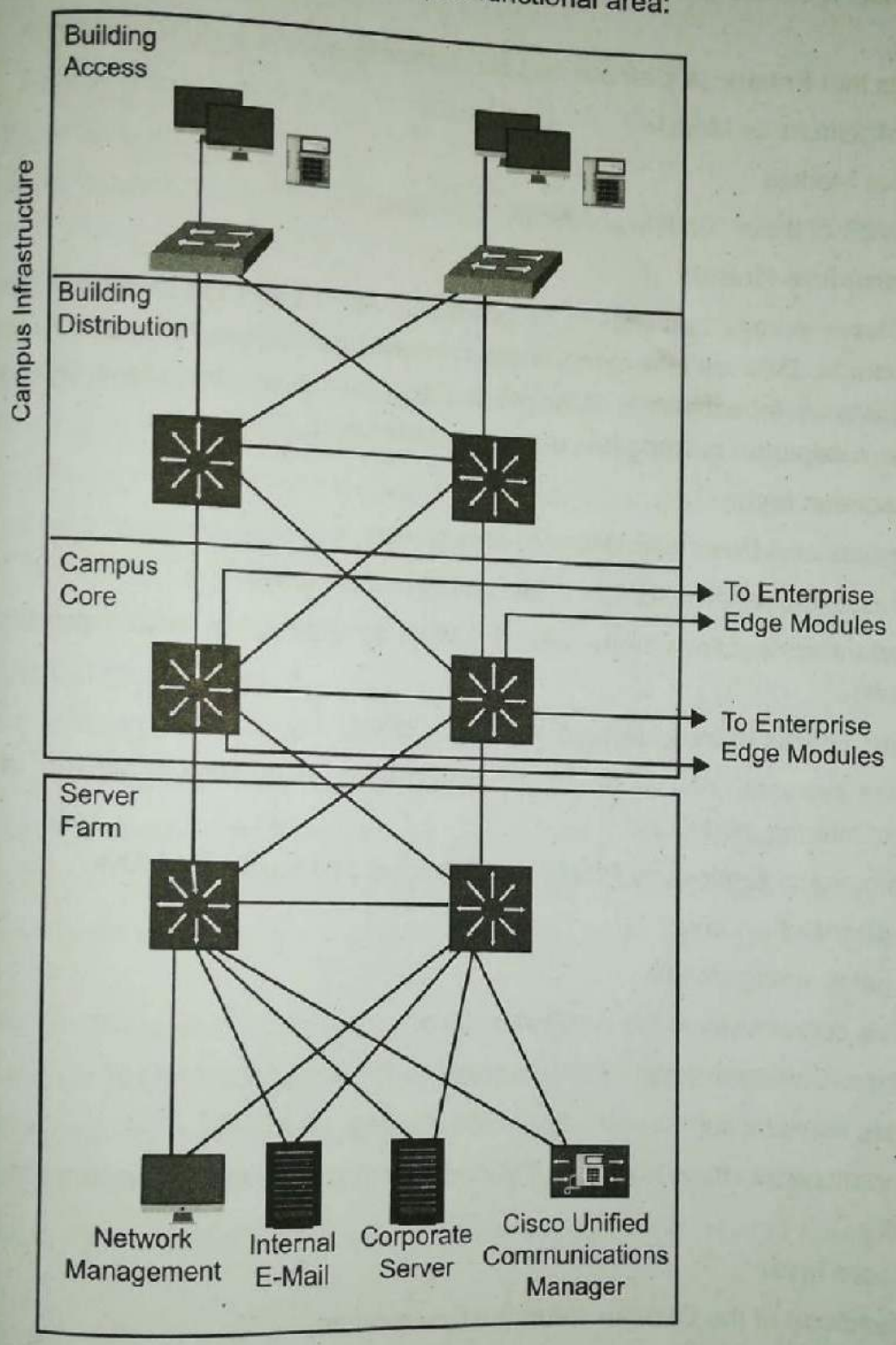


Figure 11: Enterprise Campus Functional Area

Scanned by CamScanner

Enterprise Campus generally refers to a very large area such as a head office or headquarter. Data and information across branches, SOHOs and mobile users are offered through the central campus.

Figure 11 depicts that Enterprise Campus can be divided into:

1. Campus Infrastructure Module
2. Server Farm Module

Let us discuss each of these modules in detail.

Campus Infrastructure Module

A campus may have several buildings in its premises. All of them fall under the Campus Infrastructure module. Devices in a campus are connected to Server Farm and Enterprise Edge through Campus Infrastructure. A single building may have an access layer and a distribution layer. A separate building has a campus core layer.

1. **Building access layer**
   - Aggregates end-users from different workgroups
   - Contains end-user devices connected to Layer 2 switches
   - Redundant connections from access switch to distribution switch provide high availability
   - Provides uplinks to the building distribution Layer
   - Provides services such as broadcast suppression, IP multicast, network access, protocol filtering, and QoS.
   - Supports voice services by Power over Ethernet and auxiliary VLANs
2. **Building distribution layer**
   - Aggregates wiring closets
   - Provides connectivity to the distribution layer
   - Data from multilayer switches is forwarded to the campus core layer
   - Provides services such as access control, routing, and QoS
   - Redundant connections to access layer and core layer for load balancing and failure recovery
3. **Campus core layer**
   - The backbone of the Campus Infrastructure module
   - Connects several buildings in a campus

Scanned by CamScanner

- Connects the Server Farm module and the Enterprise Edge module to the building distribution layer
- Multilayer switches support high throughput
- Provides services such as routing, QoS, and Security
- Routes and switches traffic among modules

Server Farm Module

- Consists of application servers, database servers, DNS servers, email servers, web servers, etc.
- Has high capacity
- Provides internal server resources
- Provides services such as configuration management, system logging, network monitoring, and troubleshooting
- Redundant connections from servers to switches for load sharing
- Redundant connections between Server Farm module switches and campus core layer switches for high availability and failure recovery
- Supports end to end network management services

Enterprise Campus Guidelines

Guidelines to design Enterprise Campus are given as follows:

- For access and distribution layers, identify the building in the campus
- Based on end-users, select count and location of access switches
- Based on access switches, determine the number of distribution switches
- Add redundant connections between access layer switches and distribution layer switches
- Determine the location for the Server Farm module
- Add redundant connections between distribution layer switches and servers
- Determine a location for the core Layer
- Add redundant connections for connectivity among different modules
- Connect the core layer with all the other modules of the enterprise network

Scanned by CamScanner

Enterprise Edge Modules

Figure 12 displays the Enterprise Edge functional area:

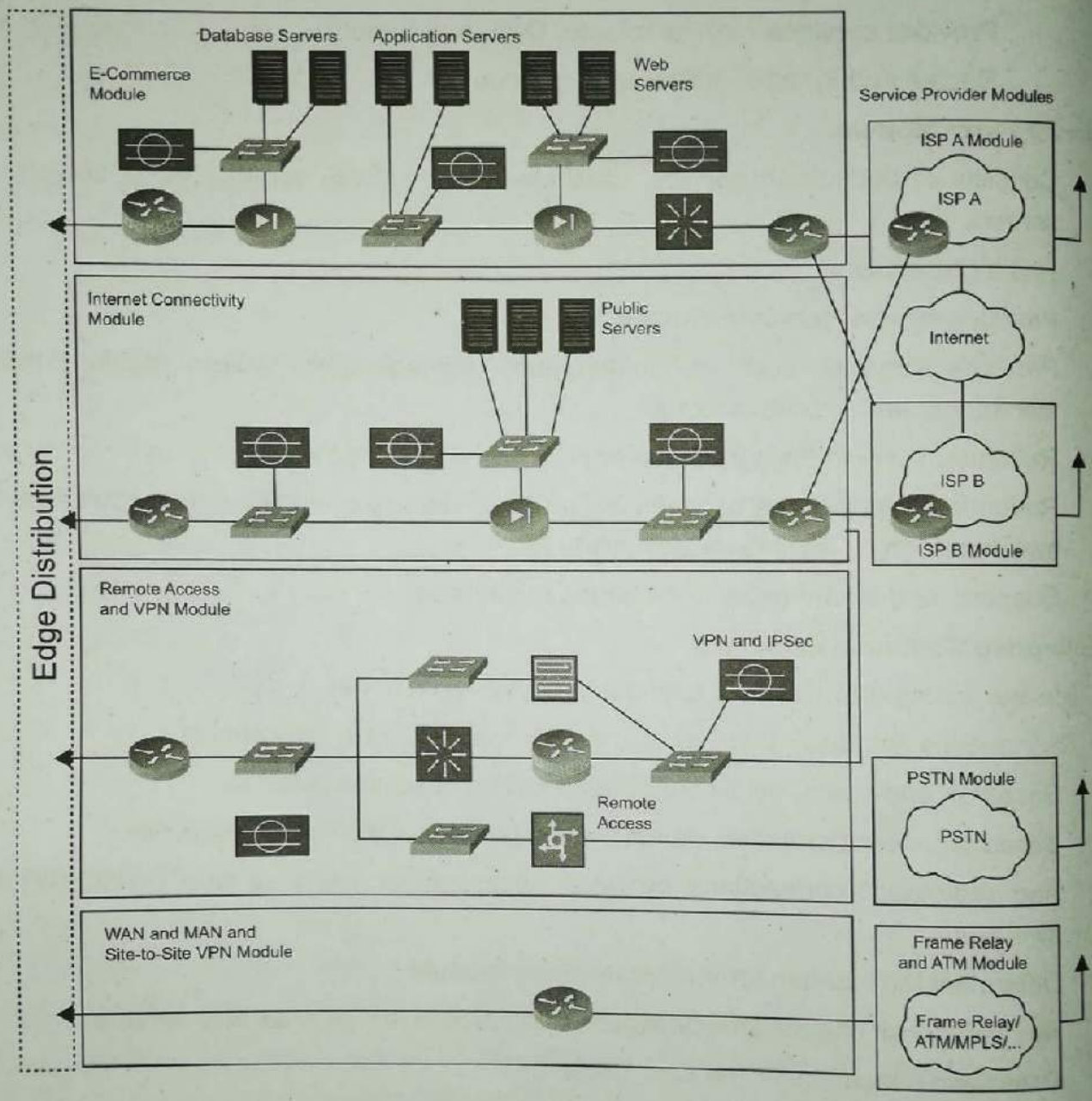


Figure 12: Enterprise Edge Functional Area

The Enterprise Edge module connects an enterprise network to the outside world. Services from public networks and the Internet are provided to Enterprise Campus through the Enterprise Edge module. Components of the Enterprise Edge module are listed as follows:

1. E-Commerce module
2. Internet Connectivity module
3. Remote Access and VPN module
4. WAN and MAN and Site-to-Site VPN module

Scanned by CamScanner

Let us discuss each one of them in detail.

E-Commerce Module

- Includes network devices and management services to support e-commerce applications
- Provides high availability, scalability, and security
- Supports intelligent services

Network devices for an Enterprise Edge E-commerce module include:

- Application servers
- Database servers
- Firewalls
- Host-based intrusion protection system
- Network intrusion detection and protection system appliances
- Web server

Application servers provide services to host web applications. They support load balancing, clustering, and failure recovery services. They may support Java application, PHP application, mobile application, .net framework, or other types of applications. Application servers are specific to the type of application they support. Example: Apache Tomcat is the application server for Java applications; Zend server is for PHP applications, etc.

Database servers provide database services to e-commerce applications. They support data storage, data retrieval, data analysis, data archiving, etc. Example: Apache.

Firewalls provide network security while communicating with the outside world as well as for communication within the enterprise network. A firewall separates the private network of an enterprise from the public network (Internet). Example: PeerBlock, Check Point.

Critical data contained on computers is protected from malware or virus or any other malicious attack by an additional level of security provided by a host-based intrusion protection system. It identifies intrusion by analysing application logs, system calls, or any file system modification in access control list, binaries, capability databases, or password files, etc. Example: OSSEC.

Network traffic from multiple hosts and network devices is monitored by network intrusion detection and protection system appliances. Such appliances are generally placed at network borders such as DMZ. Example: Snort.

Web servers provide hardware and software support required to run e-commerce applications. They serve client requests as well as store, process and deliver requested pages from e-commerce applications. Example: Apache Server, Microsoft IIS.

Internet Connectivity Module

- Provides access to enterprise's public servers
- Provides connectivity to Internet services

Scanned by CamScanner

- Provides VPN connectivity to remote users and remote sites
- Supports DNS, FTP, HTTP and SMTP

Network components for the Internet Connectivity module include:

- SMTP mail servers
- DNS servers
- Public servers
- Firewalls
- Edge routers

SMTP mail servers are the mail servers that relay emails across IP networks. They, thus, provide connectivity between intranet mail servers and the Internet. These servers are specifically used to send emails over SMTP. Example: Gmail SMTP server.

DNS servers provide domain name resolution services to an enterprise. They resolve internal and external queries for a URL of an enterprise in a secure and scalable way.

Public servers provide access to public information about enterprises. Commonly used public servers are FTP servers and HTTP servers.

Firewalls provide network level security by filtering traffic.

Edge routers provide basic filtering and multilayer connectivity to the Internet.

Remote Access and VPN Module

- Authenticates dial-in connections from PSTN
- Grants dial-in access to a network
- Initiates VPN connection to remote sites
- Terminates dial-in connections from PSTN
- Terminates traffic for VPN and remote access

Network components for Remote Access and VPN module include:

- Dial-in access concentrators
- Firewalls
- Network intrusion detection system (NIDS) appliances

Dial-in access concentrators terminate requests for dial-in connection coming from PSTN and provide authentication services for every dial-in request.

Firewalls provide security to network resources by filtering traffic. Remote sites are authenticated by firewalls and secure connectivity is provided by using IPSec tunnels.

NIDS appliances monitor network segments at the top OSI layers.

Scanned by CamScanner

WAN and MAN and Site-to-Site VPN Module

- Can use traditional media; example: leased line.
- Can use Circuit Switched Data link technologies; example: Frame Relay, ATM.
- Can use WAN technologies; example: DSL, MPLS, Metro Ethernet, SONET, SDH, Wireless.
- Provides services such as access control, routing, and QoS.
- Routes traffic from a remote site to the central site and vice versa.

Enterprise Edge Guidelines

Guidelines to design Enterprise Edge are given as follows:

- Determine business application and/or database servers that must be available over the Internet
- Create an E-Commerce module for identified applications
- Deploy security policy to restrict user-access to predefined services
- Application servers, database servers and web servers are part of the E-Commerce module
- Create Internet Connectivity module to extend the enterprise network to the Internet
- Deploy security policy to restrict authorised access from the Internet to the enterprise network
- Public web servers are part of the Internet Connectivity module
- Determine whether the enterprise requires a VPN connection
- Determine whether the enterprise requires a dial-in connection
- Create Remote Access and VPN module
- Deploy security policy to authorise and authenticate users
- Identify permanent connectivity options for enterprise remote locations
- Create WAN, MAN and site-to-site VPN module
- Locate all WAN devices supporting WAN technologies in this module

Scanned by CamScanner

Service Provider Modules

Figure 13 displays the Service Provider functional area:

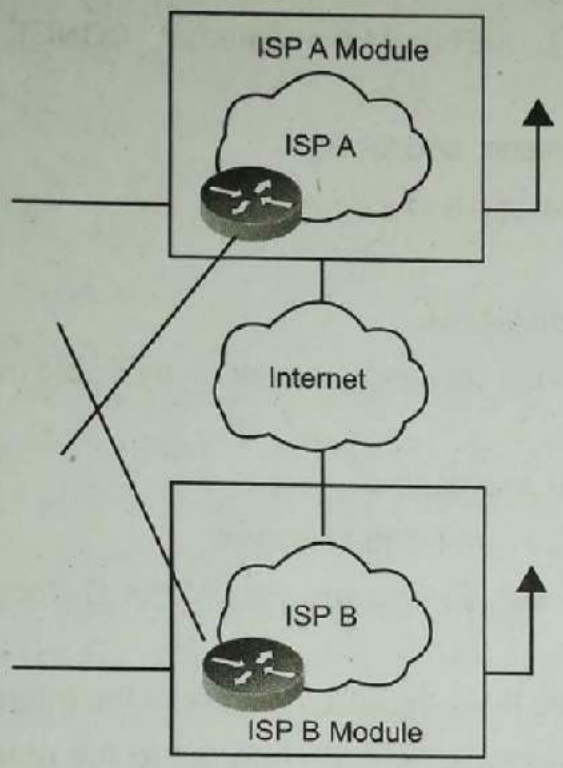


Figure 13: Service Provider Functional Area

The functional areas of Service Providers are implemented by Service Providers and not by an enterprise. They enable communication with Internet Service Providers and other networks. Modules within the Service Provider functional area include:

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

Since PSTN and Frame Relay/ATM are obsolete technologies for an Internet connection, we will discuss only about the Internet Service Provider module.

Internet Service Provider Module

- Enables Enterprise Edge services provided by Enterprise Edge modules
- Provides IP connectivity to the enterprise
- Provides access to the Internet through the ISP network
- Connection to more than one ISP for redundancy and failure recovery

Scanned by CamScanner

Remote Enterprise Modules

Remote enterprises consist of the following modules:

1. Enterprise Branch module
2. Enterprise Data Centre module
3. Enterprise Teleworker module

Let us discuss each of these modules in detail.

Enterprise Branch Module

- Extends an enterprise to a remote location
- Provides resilient network architecture
- Provides mobility and security
- Provides access to enterprise information at a central site
- Uses a simplified version of the Campus Infrastructure module
- Uses different technologies for remote access such as the Internet, VPN, videoconferencing, etc.

Enterprise Data Centre Module

- Enhances the capability to adapt to changing business requirements
- Enhances the capability to adapt to increasing network, security, or other regulatory requirements
- Enhances services provided by network applications, servers, and storage solutions
- Requires highly available WAN connectivity to support business continuance
- Supports different technologies such as Gigabit Ethernet, 10 Gigabit Ethernet, or InfiniBand connections for the Data Centre network infrastructure layer
- Supports different services for application optimisation, storage fabric, security, etc. for the Data Centre interactive services layer
- Supports different tools for network management for the Data Centre management layer
- Uses a simplified version of Server Farm module

Enterprise Teleworker Module

- Teleworker means people working from home, hotels, or any random place
- It also includes people working on mobile while travelling or otherwise
- It provides secure access to enterprise network applications and resources

Scanned by CamScanner

2.3. Services within Modular Networks

This section explains various network services which are the basic requirements for business applications.

Interactive Services

In a network, forwarding is a very basic service. This service was offered in packet-based communication. The forwarding service in an IP network was designed to work with intelligent end nodes and cater to non-intelligent core layers. At present, the network has various intelligent mechanisms to offer forwarding services and is not simply limited to forwarding the datagram. For example, delivery, performance and security can be improved based on traffic information.

Figure 14 displays the Cisco SONA Framework:

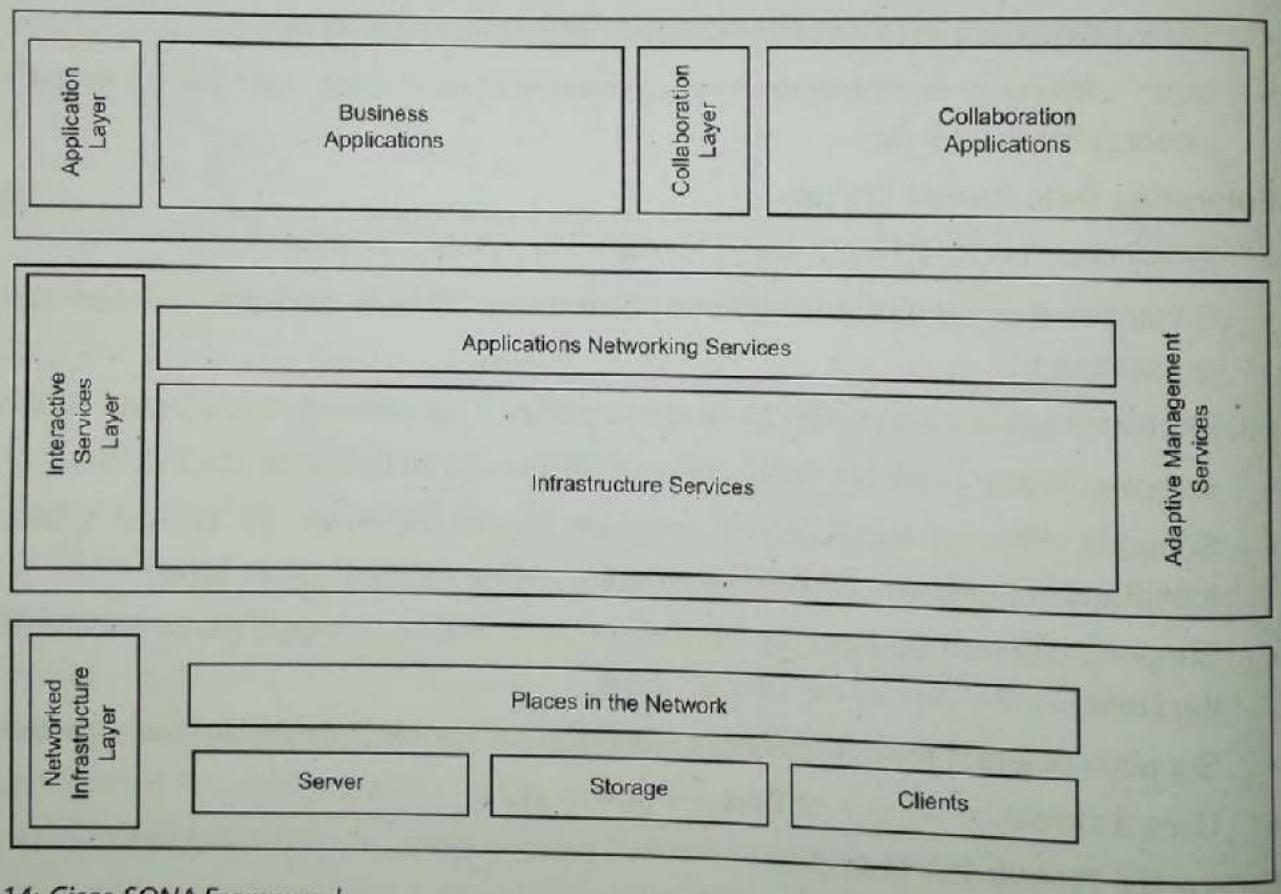


Figure 14: Cisco SONA Framework

Figure 14 depicts the Cisco SONA Framework which consists of interactive services layer. As seen from the figure, the infrastructure services layer contains application networking services and infrastructure services. Infrastructure services provided to applications include:

- Computer services: Virtually connect the computing resources as per the application requirement

Scanned by CamScanner

- Identity services: Helps in authenticating the user and in providing access to network resources as per policy
- Mobility services: Enables one to connect to an enterprise network from anywhere to access resources
- Security services: Includes securing devices, links, transmission, storage, and retrieval of data
- Storage services: Enables storage of data at distributed locations as well as supports virtual storage
- Voice services: Provides secure and reliable media to transport voice

Apart from the aforementioned services, the following services are also an implicit part of infrastructure services.

- Network management includes:
  - LAN Management: Management of multilayer switches
  - WAN Management: Access control, monitoring, and traffic management
  - Managing Service Level Agreements (SLAs)
  - VPN Security Management
- High availability includes:
  - End to end service delivery
  - Fault tolerance: Identify and overcome failures
  - Resilient network: Redundant network devices and connections
- QoS includes:
  - Meeting requirements for data, voice, and video applications
  - Managing bandwidth availability, delay, jitter and packet loss
  - Providing value-added functionality
  - Classifying traffic based on application
- IP Multicasting includes:
  - Distributing distance learning, corporate communication, videoconferencing, etc.
  - Providing bandwidth conserving technology
  - Reducing network traffic

Based on the application requirement, these services might be deployed in some or all the modules of an enterprise network. The subsequent sections describe these infrastructure and application networking services.

Scanned by CamScanner

Security Services in Modular Network Design

Security is protecting the network resources from unauthorised access and threats. Threats may be internal (at Enterprise Campus) or external (at Enterprise Edge). Network resources should be protected from both types of threats to maintain the integrity of the network. For this, there is a need to have a complete understanding of threats that can be encountered. This helps in proper configuration of network security policies and devices. Different measures for handling threats, in case they occur, can be appropriately devised.

Enterprise Campus and Enterprise Edge, both should be secured from internal and external threats. However, security should be implemented in a layered approach so that a security breach at one module does not propagate to another module or the entire network. This layered security technique is better known as defence-in-depth security.

Internal Security

Security at each level is needed in a network. Each and every network device and component should be secured. For this purpose, apart from physical security, Enterprise Edge as well as Enterprise Campus should be protected.

Figure 15 illustrates the internal security for enterprise architecture:

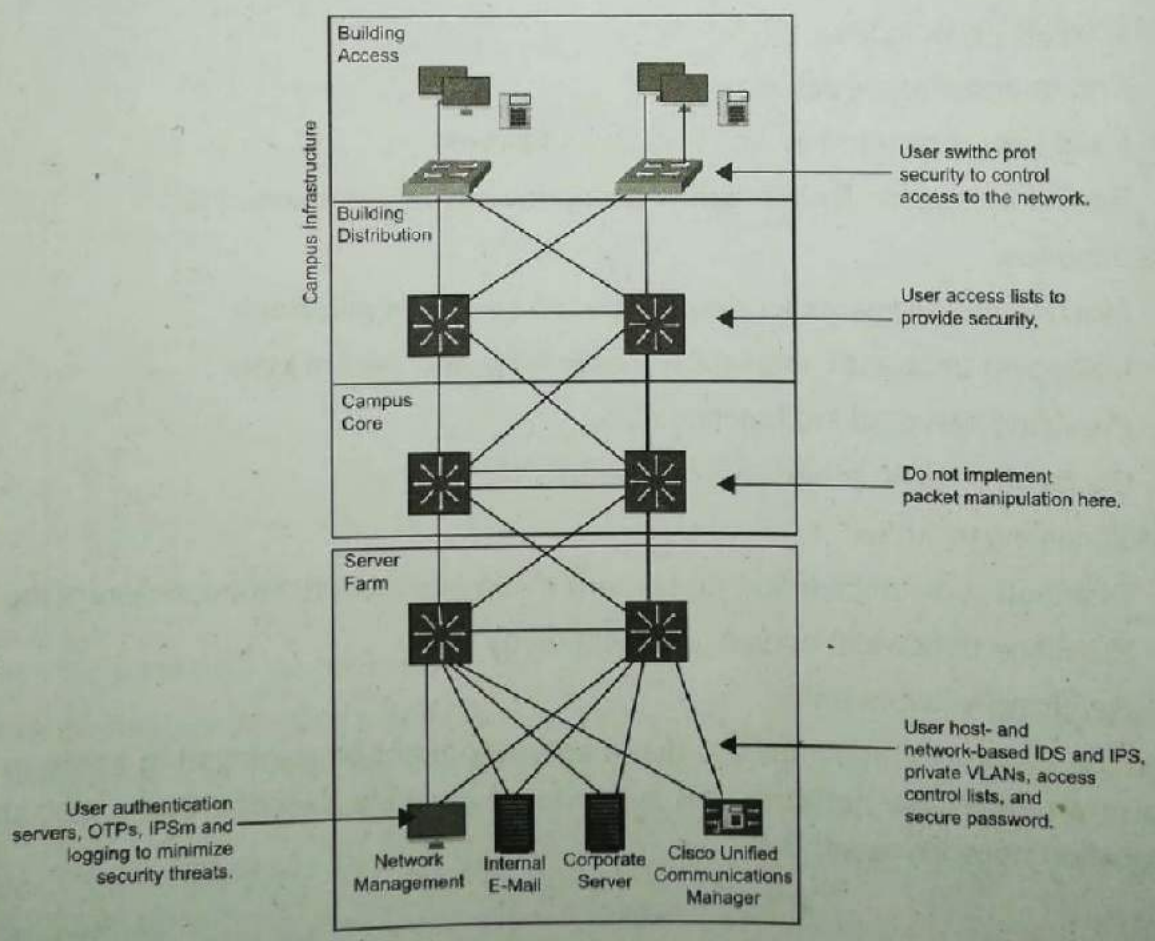


Figure 15: Internal Security for Enterprise Architecture

Scanned by CamScanner

Figure 15 gives a glimpse of Cisco Enterprise Architecture with internal security features deployed at different layers. Let us understand how each module of Cisco Enterprise Architecture can be secured.

- **Security at Building Access Layer**
  - Access to the network is restricted by controlling access at the port of the access switch.
  - **Example:** Port authentication and traffic filtering based on MAC address
- **Security at Building Distribution Layer**
  - Flow of unnecessary traffic from the campus core to the building access layer is restricted by security at the building distribution layer.
  - Traffic is filtered based on the network layer information.
  - Access list is used at multilayer switches to provide security.
- **Security at Campus Core Layer**
  - The campus core layer is specifically designed to switch packets at a very high-speed.
  - Implementing security at the campus core layer will decrease the speed of packet switching.
  - Hence, security is not implemented at the campus core layer.
- **Security at Server Farm Module**
  - Servers are favourite targets for internal attacks.
  - Security through passwords is not sufficient for the security of data and applications at servers.
  - For security at the Server Farm module, a host-based intrusion detection and prevention system and a network-based intrusion detection and prevention system are deployed to prevent, identify and restrict attacks.
  - Private VLANs can make the network more secure by segmenting it virtually based on the application, the department, the project or the task performed.
  - Access control list is implemented to provide secured access to limited resources only to the authorised users.
  - A network management system is deployed to secure all network devices, components and hosts.
  - One-time password is used to provide a high-level of security while authentication, authorisation and accounting are performed for server security.

Scanned by CamScanner

External Threats

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

Figure 16 displays external threats:

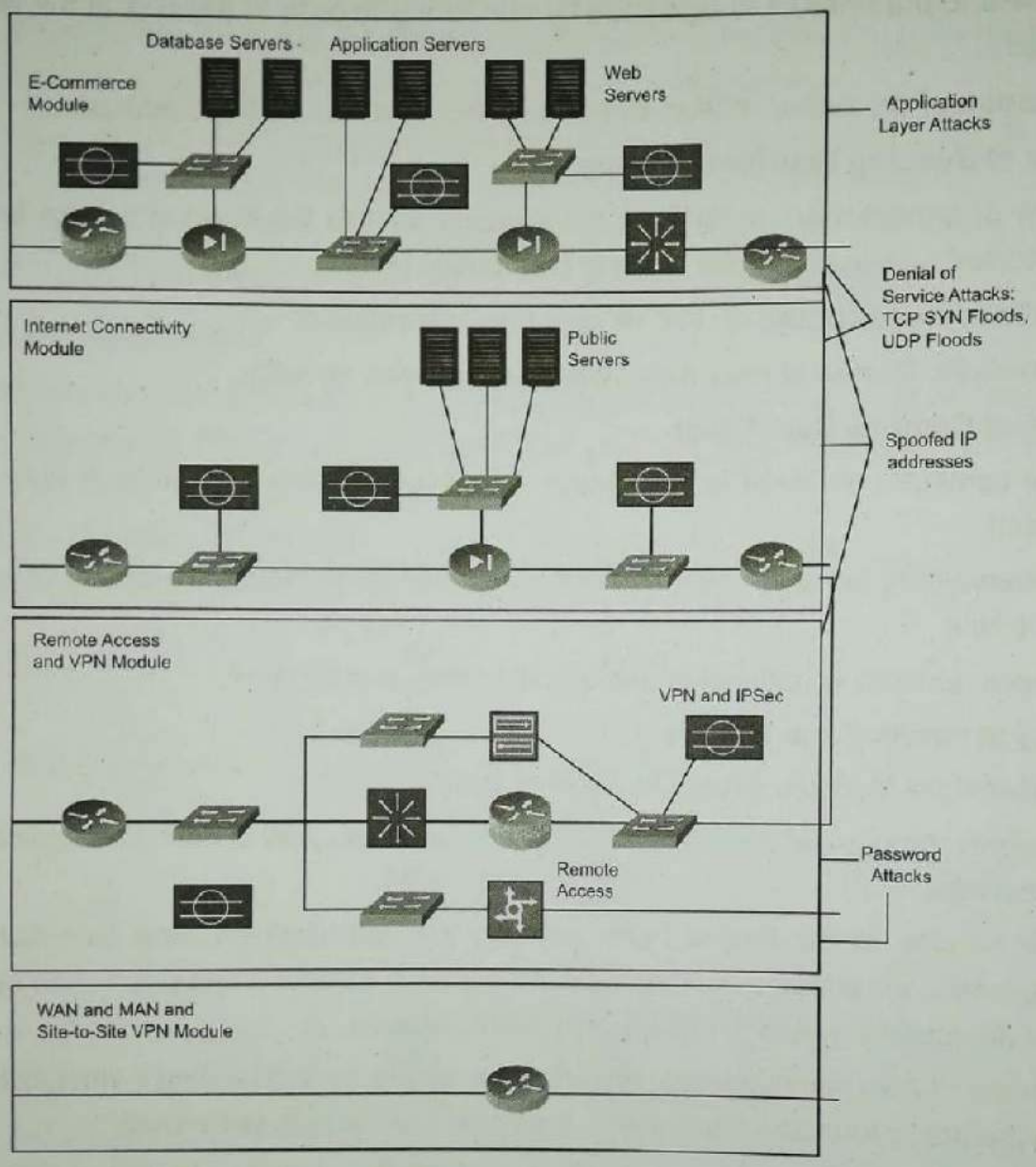


Figure 16: External Threats

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

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

Scanned by CamScanner

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

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

Scanned by CamScanner

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

High-Availability Services in a Modular Network Design

High availability is another network infrastructure service. This service is very important for mission-critical applications which require 24*7 network connectivity. Thus, along with security to preserve the integrity and resilience of such networks, high availability is a much-required network infrastructure service.

Designing High Availability into a Network

Any network resource or connection, whose failure results in disabling critical applications, is termed as a single point of failure. In any enterprise network architecture, single points of failure are eliminated. This is achieved by redundancy. Network connections or devices are duplicated to remove single points of failure. Such network topologies, when implemented, prove to be complex, expensive and difficult to maintain. Addressing and routing mechanisms in redundant network topologies are more complex. Therefore, while designing redundant network solutions, constraints to achieve availability requirements are evaluated along with business and technical goals to be achieved.

To design a redundant network, the first step is to determine applications, connections, devices, etc., that can serve as a single point of failure. Next is to evaluate the loss that might be incurred if redundancy is not opted for with respect to cost for redundancy implementation. Similarly, the complexity of the network should be evaluated while opting for redundancy.

Similarly, identify critical network connections and add redundant connections. However, simply adding redundant connections will not suffice if the connections terminate at the same network device. This is because the device might be a single point of failure. In such cases, redundant connections should terminate at different network devices.

Port redundancy, card redundancy, device redundancy, connection redundancy, route redundancy, link redundancy and power redundancy are different types of redundancies that can be implemented in enterprise modules.

Scanned by CamScanner

High Availability in the Server Farm

Server Farms can be connected in various ways to the Campus Infrastructure. Whichever technique may be used for connection, it should ensure availability through redundancy. Let us discuss the connectivity methods for Server Farms and for making them highly available.

- **Single Attachment**

  A server must know the address of the router in order to send traffic outside the network. In case of failure, an alternative router needs to be discovered. In case of single attachment method, various mechanisms that can be used to dynamically discover an alternative router include Address Resolution Protocol, Gateway Load Balancing Protocol, Hot Standby Router Protocol, Router Discovery Protocol, and Virtual Router Redundancy Protocol.

- **Redundant Transceiver**

  Figure 17 shows a redundant transceiver:

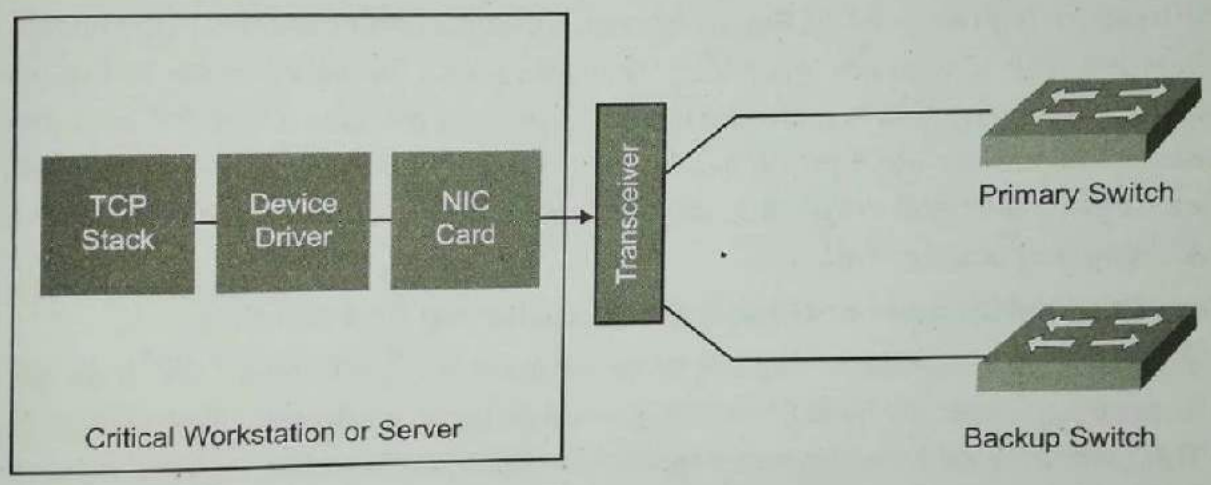


Figure 17: Redundant Transceiver

Redundant transceiver method is preferred for environments not supporting redundancy. As shown in Figure 17, a critical server is connected to switches via a redundant transceiver. The transceiver is connected to two access switches, i.e. primary switch and backup switch, via two uplink ports. If a carrier loss, i.e. physical failure, is detected on the primary port, the backup port is activated by the transceiver. Failures inside a switch or beyond a switch cannot be detected by a transceiver.

Scanned by CamScanner

- **Redundant Network Interface Cards**

  Figure 18 displays redundant NICs:

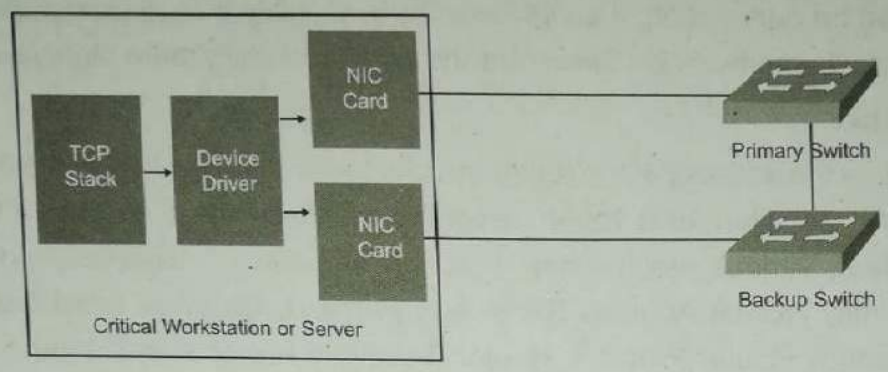


Figure 18: Redundant NICs

Dual Network Interface Cards (NICs) are supported by UNIX servers. One NIC is primary and the other one is for backup. When the primary NIC fails, the other NIC can be used for high availability. Figure 18 shows that the redundant NIC in the critical server provides high availability. An NIC is presented as a single interface to the operating system. A backup NIC is activated when the primary link dies. Common or distinct MAC addresses can be used by the two NICs. In case of distinct MAC addresses, when the primary link dies and the backup card activates, ARP messages are sent for IP-to-MAC address mapping on switches.

- **Fast EthernetChannel or Gigabit EthernetChannel Port Bundles**

  Multiple Fast Ethernet or Gigabit Ethernet ports can be bundled into a single logical transmission path by Fast EthernetChannel or Gigabit EthernetChannel Port bundles. This path may be between two switches, a switch and a router, or a switch and a host. Such EthernetChannel seems to be like a logical link. Frames can be distributed by switches based on the MAC address or IP address.

Designing Route Redundancy

Redundant routes play a significant role in enterprises demanding high availability. They are used to accommodate link failures and internetworking device failures. They also support load balancing when traffic is high. To make a connection redundant, either duplicate links can be added between switches and routers or backup LAN and WAN links can serve the purpose. Similarly, to make a network redundant, use a full mesh or partial mesh network. The preferred approach is to use a partial mesh. In a partial mesh, only critical devices have redundant connections. This approach is, thus, less expensive and more scalable. A full mesh network is preferred for a smaller network with a reasonably limited number of devices. This is because in a full mesh network, each and every device is connected to any other device in the network. For n internetworking devices, n(n-1)/2 connections are required in a full mesh network.

Scanned by CamScanner

Figure 19 illustrates route redundancy:

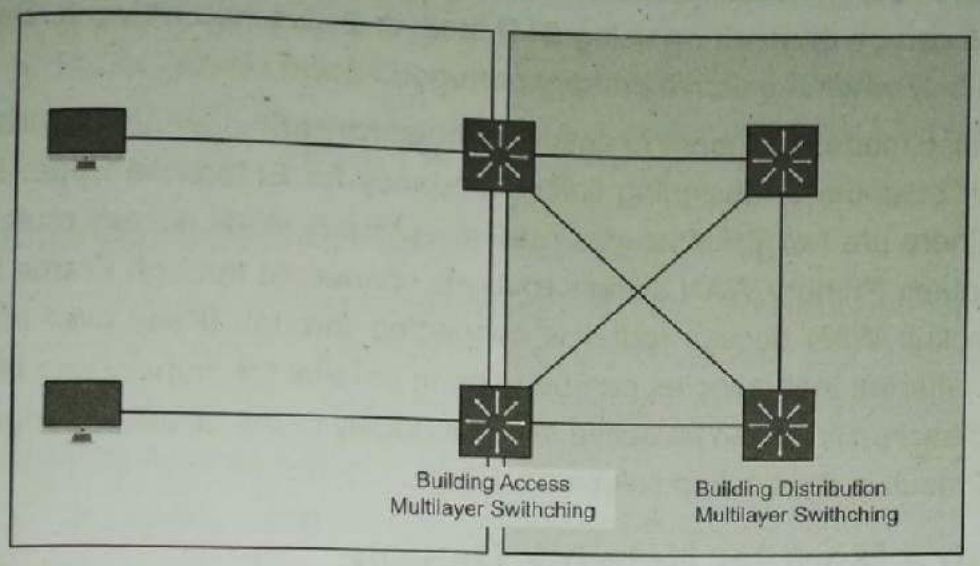


Figure 19: Route Redundancy

As shown in Figure 19, each host is connected to a Building Access Multilayer switch. The two Building Access Multilayer switches are fully meshed with two Building Distribution Multilayer switches. The campus can now accommodate the failure of a distribution multilayer switch as the access layer can now connect to the distribution layer. Primary and backup paths are selected between these two layers based on the routing protocol in use. Information about the best path is stored in the forwarding table. In case the two paths have equal cost, then both can be used for load sharing.

Designing Link Redundancy

Figure 20 displays link redundancy:

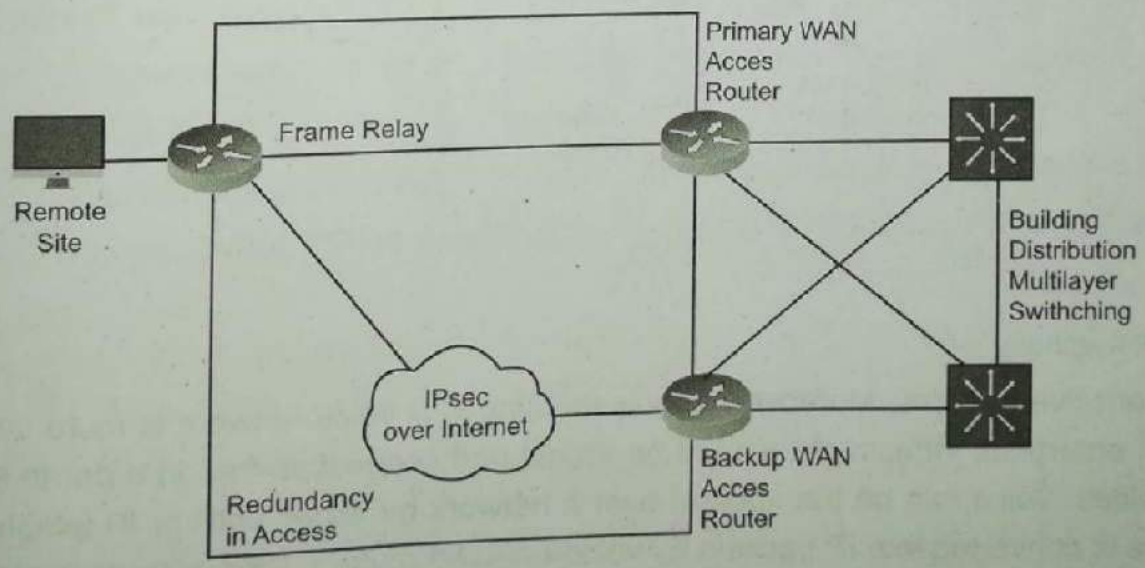


Figure 20: Link Redundancy

Enterprise Edge that supports mission-critical applications must have redundant links for uninterrupted communication. Such redundant links should not result in a broadcast storm,

Scanned by CamScanner

i.e. looping of broadcast in the network. At a time there should be only one active path in a broadcast domain. This can be ensured by using STP in layer 2 switched network. Backup media becomes active only when the active primary path goes down.

WAN connections are also made redundant to ensure connectivity and offer high availability. Figure 20 illustrates an example of designing link redundancy for Enterprise Edge. In the building access layer, there are two WAN access routers—primary WAN access router and backup WAN access router. Primary WAN access router is connected through Frame Relay circuit whereas the backup WAN access router is connected through IPsec over Internet technology. Thus, two different technologies can be used in parallel for primary and backup links. Both primary and backup links can be active simultaneously or the failure of congestion of the primary link can result in the backup link being active.

Voice Services in a Modular Network Design

Figure 21 illustrates IP telephony:

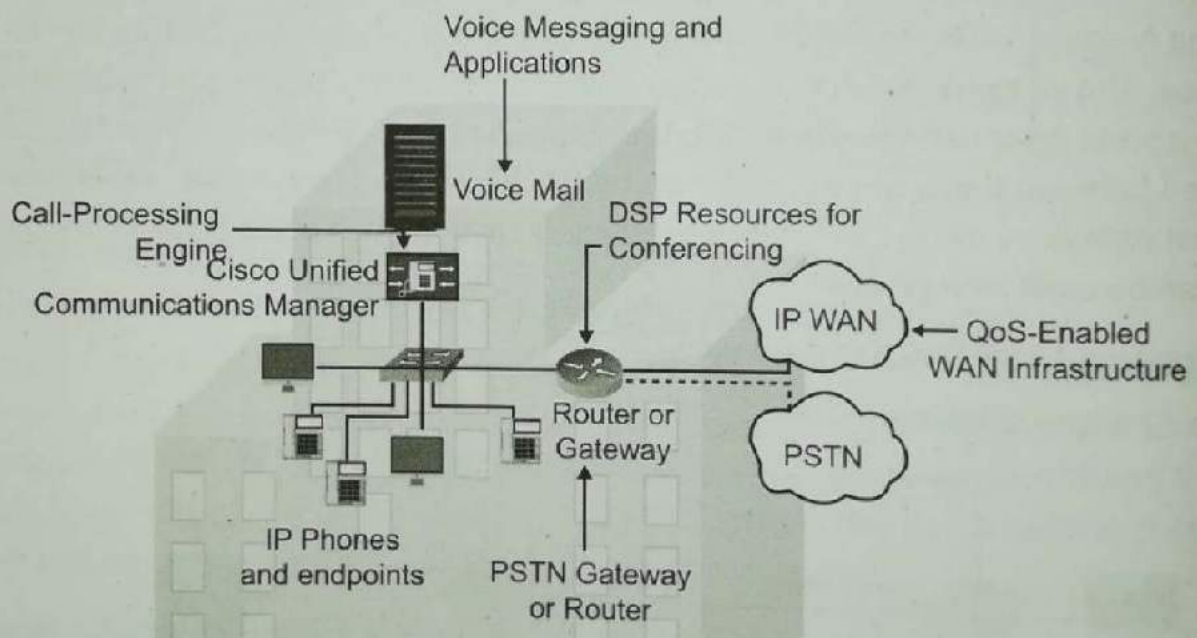


Figure 21: IP Telephony

Voice is sensitive to delay. Moreover, troubleshooting in a voice network is more complex. Therefore, enterprise infrastructure must be robust and congestion-free in order to support voice services. Voice can be transported over a network by either VoIP or IP telephony. In VoIP, voice is converted into IP packets by voice-enabled routers. PBX of traditional phones is connected to such routers which serve as entry points for VoIP. In IP telephony (Figure 21), voice to IP conversion and vice versa is performed by IP phones and not voice-enabled routers, as in VoIP. They perform coding and compression for voice to IP conversion. Voice

Scanned by CamScanner

enabled routers are required in IP telephony to connect a PSTN. Such routers are also referred as voice-enabled switches or voice gateways. These routers offer services such as coding and compression for voice-to-IP conversion, backup call processing, IP packet routing, PSTN access, etc. IP phone initialisation, call setup, call routing, call control, call signalling and configuration management is performed in IP telephony by a server or call-processing manager.

Modular Approach in Voice Network Design

As mentioned in the previous section, voice is delay sensitive. Enterprise infrastructure should accommodate changes required to support voice services. The following are enterprise architecture components along with changes to offer voice services.

- **Building Access Layer**
  - IP phones are located in the building access layer.
  - IP phones are connected to access switches and get power from access switches.
  - QoS packet classification and marking are done by access switches.
- **Building Distribution Layer**
  - For scenarios where access switches are unable to perform QoS packet classification and marking, these tasks are done by the distribution layer switches.
  - If the building access layer is not within a trusted boundary, then also the distribution layer performs QoS packet reclassification.
- **Campus Core Layer**
  - The campus core layer simply does high-speed packet forwarding; no specific changes for voice services are required in this layer.
- **Server Farm Module**
  - Call processing manager is located in this module.
- **Enterprise Edge**
  - IP telephony is extended from Enterprise Campus to remote locations.
  - Internet, WAN, PSTN may be different media used for network communication

Scanned by CamScanner

Figure 22 displays enterprise architecture along with a voice network:

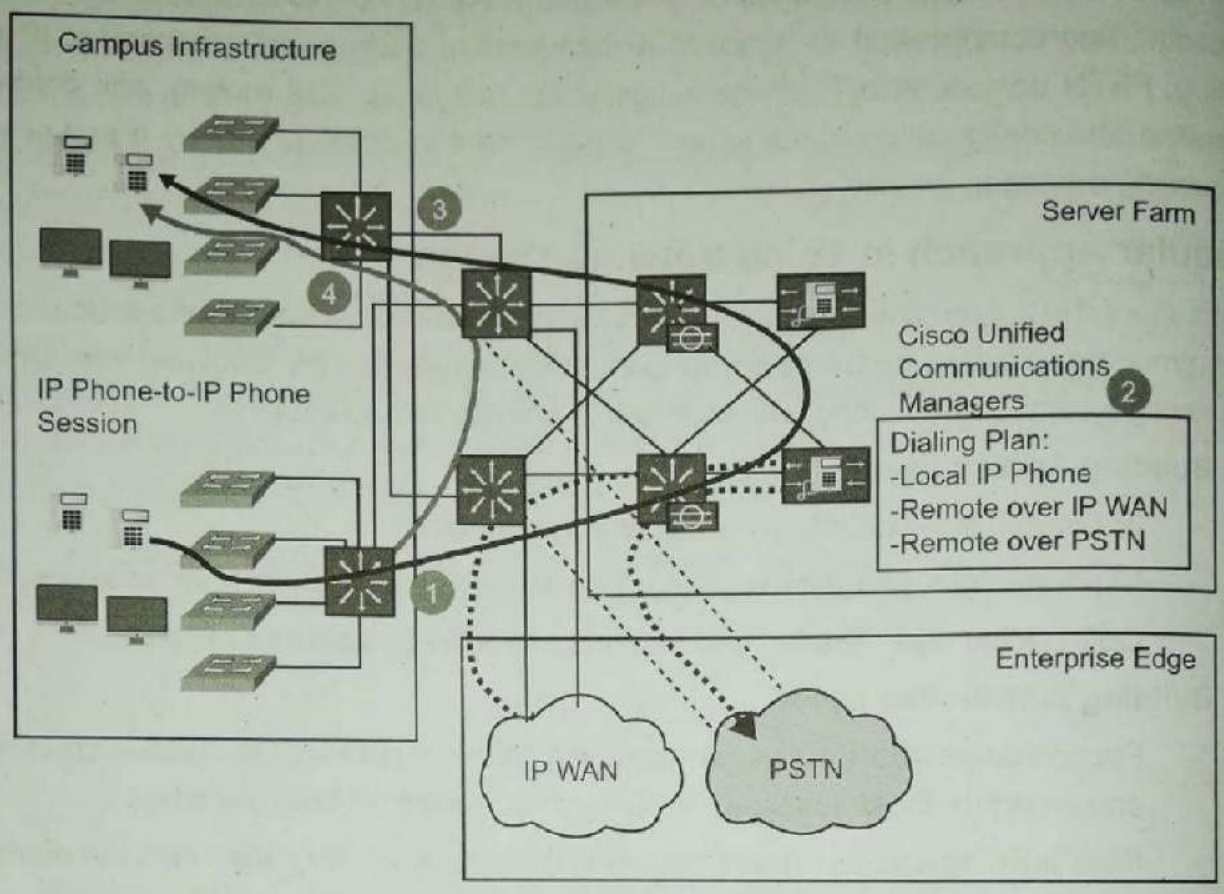


Figure 22: Voice Network

As depicted in Figure 22, IP phones are placed in Campus Infrastructure whereas the call processing manager is in the Server Farm module. A call is initiated on an IP phone at Campus Infrastructure. The call processing manager sets up the call. Based on the destination IP phone, the end to end session between the two IP phones is established. The call may be destined for a remote location or PSTN public phone number. In any case, the call travels through the Enterprise Edge module. It may be routed through the Remote Access and VPN module or WAN and MAN and Site-to-Site VPN module of Enterprise Edge.

Evaluating the Existing Data Infrastructure for Voice Design

If voice services are to be supported by an enterprise network, then the existing enterprise infrastructure must be evaluated and documented. Upgrade requirements for voice network can be determined through such evaluation. Parameters for enterprise network evaluation include:

- Performance
  - Analyse the existing enterprise network design
  - Analyse the existing devices and connections
  - Identify devices and connections with high traffic

Scanned by CamScanner

- Identify devices with high CPU usage and high memory usage resulting in buffer misses and queuing drops

- Availability
  - Analyse all the existing redundant devices and connections
  - Determine whether the current network meets IP telephony availability requirements
  - If not, design a new network to meet IP telephony availability requirements
- Capacity
  - Analyse the overall network capacity
  - Analyse the impact of adding IP telephony service in the network with respect to capacity requirements and adverse effects on existing applications
- Features
  - Analyse the existing router and switches to ensure that they support IP telephony features.
  - Power
  - Analyse power requirement for adding IP telephony service
  - Analyse the use of PoE for powering IP telephony devices

Wireless Services in a Modular Network

In a wireless network, a cable or wire for physical media transmission is replaced by radio frequency transmissions through air. Therefore, the user of a wireless LAN (WLAN) does not have physical connectivity to the network. Rather, the wireless LAN provides network services to mobile users over the wireless network. This wireless network may be extended to a building, an application within line-of-sight or both. However, due to interference from other wireless sources, such as hidden node problem, multipath distortion, etc., the wireless network may not be available in the entire destined region. To avoid such issues, a better option is to go for a site survey. Areas having high interference can be identified. Regions with multipath distortions can be discovered during a site survey. And solutions to eliminate identified issues can be worked upon.

Scanned by CamScanner

Centralised WLAN Components

Figure 23 displays WLAN components:

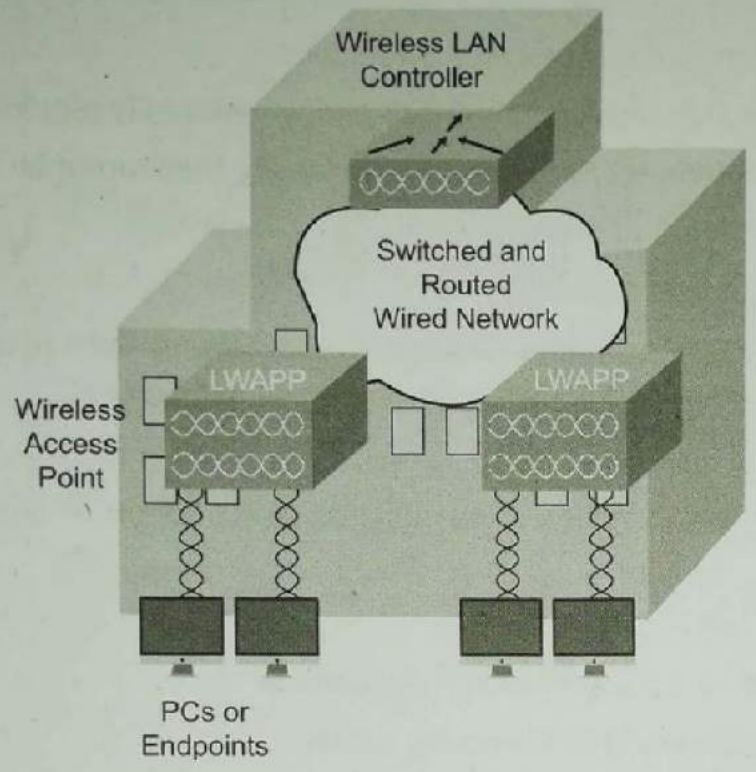


Figure 23: WLAN Components

Figure 23 depicts four major WLAN components viz. PCs or endpoints, Wireless Access Point, Wireless LAN Controller (WLC), and Switched and Routed Wired Network. Wireless NIC is used by PCs or endpoints in the access layer to connect to the Wireless Access Point using radio waves. The Wireless Access Point is in the access layer of an enterprise network, whereas WLC is in the core layer. Wireless Access Points connect to the existing switched and routed wired network. Control, configuration, management and support of wireless services is done by WLC.

Application Networking Services in a Modular Network Design

Along with the network, applications designed to offer end-user services have also evolved over time. Today, applications are not restricted to static web pages or emails. All types of data including voice, video, broadcasts, online training, and conferencing are part of network applications. Since different types of data are carried over a network, the network should be aware about the content that is being carried to make optimal use of the available network resources. Merely increasing the bandwidth will not suffice to meet the increasing demand for applications from the network infrastructure. Networks need to be smarter and intelligent to handle traffic and delivery based on the content carried, and provide service accordingly. Application Networking Services (ANS) is the solution for issues related to network infrastructure services for applications.

Scanned by CamScanner

ANS Examples

The following are a few examples describing application deployment issues and respective ANS solutions.

Example 1

- **Application Problem**: Employees working from remote locations experience slow access to centrally managed applications working on consolidated data centres.
- **ANS Solution**: Specialised WAN-application services at a remote location. These services compress, cache and optimise content to provide faster access to end-users.

Example 2

- **Application Problem**: Poor responsiveness during the checkout process, in a web-based ordering system, leads to the abandonment of a large number of orders.
- **ANS Solution**: Content-based web-stream optimisation to improve responsiveness.

Example 3

- **Application Problem**: A new requirement to provide access to back office applications.
- **ANS Solution**: Secure services at a remote location providing access to back office applications to authenticated end-users and providing an encrypted, secure and prioritised response.

Example 4

- **Application Problem**: A new business requirement to track and log large orders by a purchasing application.
- **ANS Solution**: An application messaging service to implement business policy rules for compliance purposes. Checks purchase orders having a value greater than the threshold and logs them into the database.

2.4. Network Management Protocols and Features

Once a network is designed, the next step is to make sure that it is working as expected. To ensure that the network works smoothly, provides seamless services and meets customer requirements, it is obligatory to configure, monitor, test and troubleshoot network components. This entire process is better termed as Network Management. It helps in achieving QoS committed to customers.

Network management possesses the following basic questions:

1. What to manage?

   Network devices, connection and services are the entities that can be managed. In enterprise architecture, PCs and devices are at the bottom of the architecture. These are connected to the access layer which has layer 2 switches. On the top of the access layer is the distribution layer, which has layer 3 switches or multilayer switches, routers,

Scanned by CamScanner

firewalls and gateways. All the aforementioned network components from the bottom till the distribution layer are manageable.

2. What to measure?

   Based on the network component being managed, various metrics can be identified for network management. For example, the performance of routers and switches can be measured based on metrics: bits per second (b/s) and packets per second (p/s). Apart from metrics bits per second (b/s) and packets per second (p/s), connections per second (c/s) and maximum current connections (mcc) can be used to accurately measure the performance of a firewall, load balancer or intrusion detection system. For a network connection, i.e. network link, bandwidth is the metric for evaluation. It can be measured in bits per second (b/s), packets per second (p/s) or frames per second (f/s). Thus, throughput, delay, jitter, speed, packet loss, etc., are various metrics for performance evaluation. Similarly, metrics are identified for configuration, accounting, security and fault management.

3. How to manage?

   Once the managed devices and related metrics for management are identified, the next step is to monitor the managed device. Monitoring the device means keeping a check on the device that it is working fine as per the standards or business policies defined, i.e. keeping a check on availability and performance status. This helps in early fault detection and mitigation. The question is what should be the monitoring interval, i.e. how frequently should the device be polled to monitor the performance of the device? Failure of a router or a server will result in making a huge impact on the business. Such devices are critical to business needs and hence, should be frequently polled in a small monitoring interval. On the other hand, a desktop or printer is not a critical device. Therefore, such devices can be polled in a comparatively large interval.

   Network monitoring, thus, reports every single network incident such as DoS attack, device failure, unhealthy bandwidth level, etc. Once a network incident has been reported, network controlling comes into the picture to take countermeasures. Network controlling is the preventive/corrective measure taken to resolve a network incident. It ensures that the performance of a network resumes to acceptable levels.

Performance management is one of the basic functions of a Network Management System. Major functions of a network management system are stated as follows:

1. Configuration management involves managing the status of each network device and its relation with other devices in the network.
2. Fault management includes preventing faults from occurring as well as handling faults once they have occurred.
3. Performance management includes monitoring and controlling of the network so that

Scanned by CamScanner

the service provided to the customer never degrades to an unacceptable level.

4. Security management includes authorising and authenticating access to a network as per the enterprise defined policy.
5. Accounting management involves providing controlled access to network resources.

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

Network Management Architecture

Figure 24 shows a simplified network management architecture:

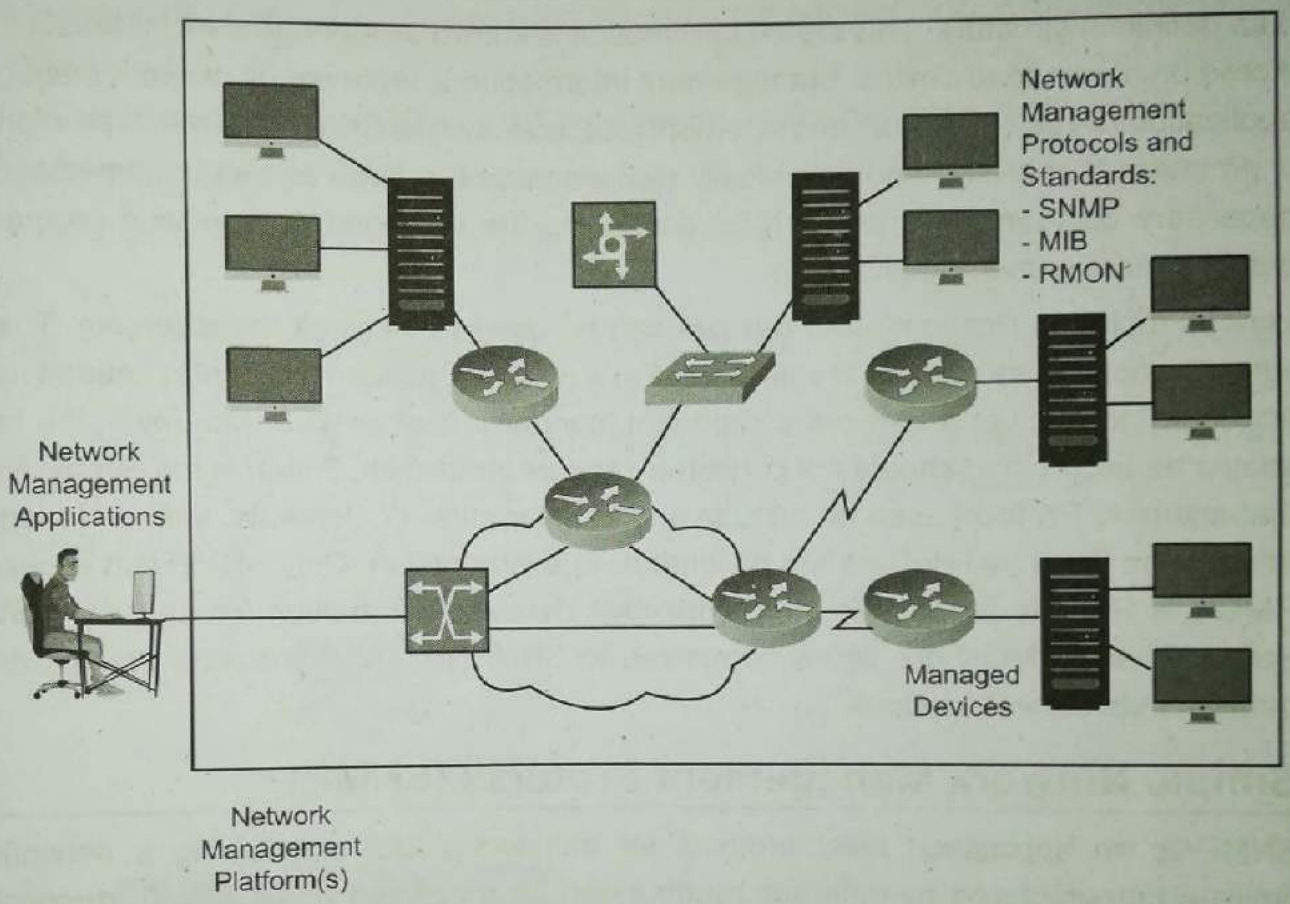


Figure 24: Network Management Architecture

Components of a network management architecture are listed as follows:

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

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

  Example: router, firewall, servers.

Scanned by CamScanner

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

  Example: SNMP agents, RMON agents.

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

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

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

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

Simple Network Management Protocol (SNMP)

SNMP is an application level protocol for monitoring and maintaining a network. The devices manufactured by different vendors can be monitored using SNMP irrespective of the underlying networking technology. Heterogeneous networking environments constituting different LANs and WANs can be managed using SNMP.

SNMP Components

SNMP consists of various components which are described as follows:

- **Manager**

  Manager is a network management application in a network management system. It is a host that executes the SNMP client program. It periodically polls the management agent to get the data stored on the managed device. Received data is reflected in the graphical format on the network management system.

- **Protocol**

Scanned by CamScanner

SNMP is the protocol to exchange network management information between a network management system and managed devices. User Datagram Protocol is used by SNMP to exchange information.

- **Managed Device**

  Managed devices are the devices managed by a manager. This is because the manager can change the values of variables to control the behaviour of managed devices.

- **Management Agent**

  Management agent of SNMP resides on a managed device and performs various operations such as:

  – Collect and store network related information on the managed device
  – Give response to SNMP manager request
  – In case of any incident, inform the SNMP manager by generating traps

- **MIB**

  Data collected by the management agent is stored on the managed device in MIB. Information is stored in the form of objects and MIB is a database of such objects that contain information about the managed device. MIB can be accessed only if one has a Community String, i.e. a password for MIB. Someone who has authorised access can read or write variables on MIB.

Figure 25 displays SNMP components:

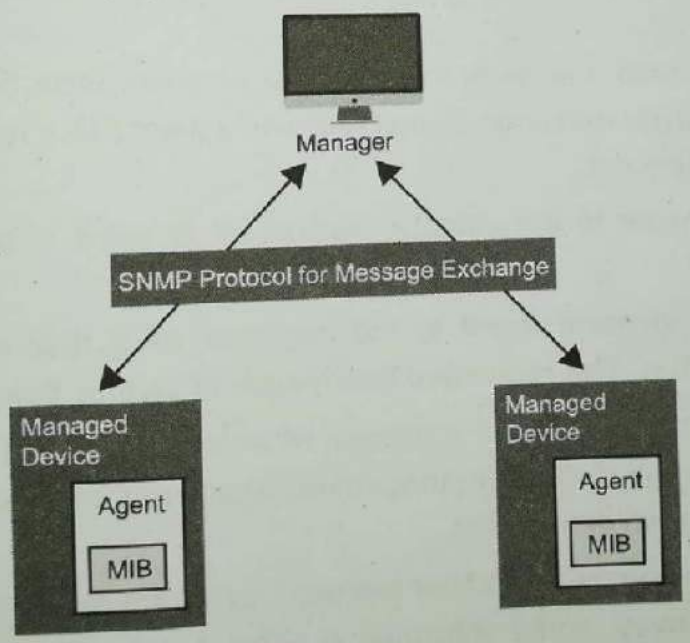


Figure 25: SNMP Components

As illustrated in Figure 25, SNMP consists of Managers, Managed Devices, Management Agents, MIBs and SNMP protocol for message exchange. The management agent is residing on the managed device. It stores data collected from the managed device in MIB. The manager frequently polls the management agent using the SNMP protocol. The management

Scanned by CamScanner

agent sends the collected data stored in MIB using the SNMP protocol to the manager. The manager displays the data received from the management agent in a GUI to the network management system. After analysis, the manager may send a request to the management agent to change variables in MIB. On the other hand, if any event occurs, the management agent does not wait to get polled by the manager. Rather, the management agent generates trap to inform the manager regarding the event.

SNMP Packet Data Units (PDUs)

For the transfer of data between the manager and the management agent or another manager, the following PDUs are defined by the SNMP protocol:

- **GetRequest**: It is sent by the manager to the management agent to get the value of an object stored in MIB.
- **GetNextRequest**: If all values from a table are to be retrieved, one way is that the manager sends GetRequest by specifying ObjectID for each object. This is a crude method. Moreover, the manager might not know how many objects/entries are there in the table or have ObjectIDs of all objects. A solution to this is GetNextRequest PDU which retrieves the value of an object that is next to the objectID specified in the PDU. The manager can specify an ObjectID for the table and use GetNextRequest. It gives ObjectID of the first entry in the table and corresponding values. The manager can now specify the ObjectID of the first entry in GetNextRequest and retrieve the value of the second entry in the table, so forth and so on. In this way, all the values can be retrieved from a table.
- **GetBulkRequest:** It is used to retrieve a large amount of data at once. Data from an entire table can be retrieved by a single message using GetBulkRequest PDU. It avoids repetitive GetRequest or GetNextRequest.
- **SetRequest:** It is sent by the manager to the management agent to set a value of a variable in MIB.
- **Response:** It is sent by the management agent to the manager as a response to GetRequest or GetNextRequest PDUs. The requested information is sent by this PDU.
- **Trap:** It is sent by the management agent to the manager when an unsolicited event occurs. Examples of unsolicited events include management agent reboot, managed device failure, state change in managed device, etc.
- **InformRequest:** It is sent by one manager to another manager to inform regarding the occurrence of some event or convey some information. The receiving manager acknowledges the InformRequest by sending a Response PDU. Example: InformRequest can be used to inform regarding traps to other managers.

Scanned by CamScanner

SNMP has messages for three security levels too. These are stated as follows:

- **NoAuthNoPriv:** This PDU is for the lowest level of security. It supports message exchanges without authentication and privacy.
- **AuthNoPriv:** It supports authentication but not privacy. Hash-based Message Authentication Code (HMAC) - Message Digest 5 or HMAC-Secure Hash Algorithms are used for authentication.
- **AuthPriv:** It supports both authentication and privacy. For authentication, HMAC-Message Digest 5 or HMAC-Secure Hash Algorithms are used. For privacy, 56-bit Cipher-Block Chaining-Data Encryption is used.

MIB

MIB is a collection of objects containing information related to the managed device. This information is stored by the management agent and later sent to the manager on request. A Unique Identifier, i.e. ObjectID, is assigned to each MIB object. An ObjectID is used to identify the object and retrieve information by the manager.

Figure 26 displays the Internet MIB Hierarchy:

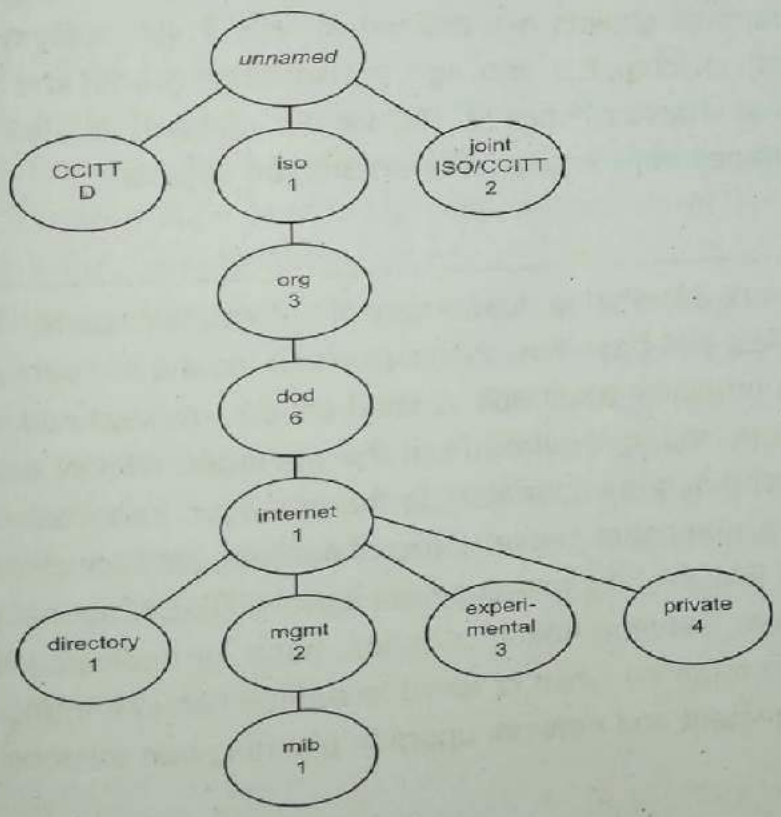


Figure 26: Internet MIB Hierarchy

As represented in Figure 26, in the Internet, MIB is represented in a tree hierarchy. At the top of the diagram is the unnamed root. It is further divided into three categories and so on. The identity of an object can be represented by a sequence of integers separated by dots

Scanned by CamScanner

or a sequence of names separated by dots. Example: MIB in integer-dot notation can be represented as '1.3.6.1.2.1' and in name-dot notation as 'iso.org.dod.internet.mgmt.mib'. Figure 27 displays MIB-2:

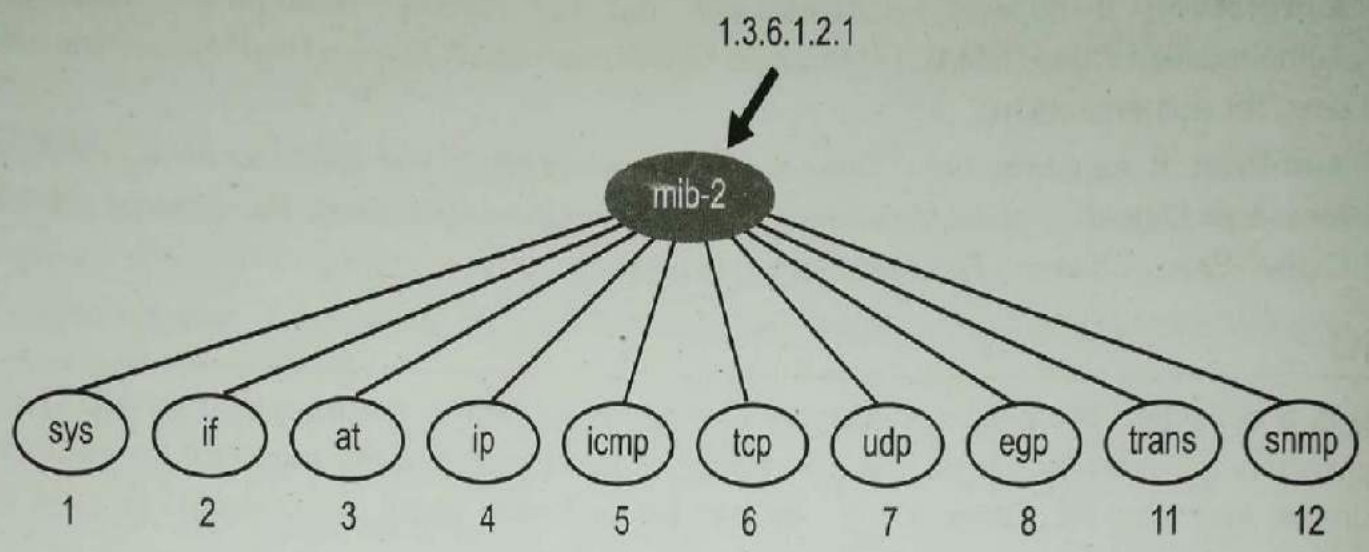


Figure 27: MIB-2

MIB has a tree-like hierarchical structure, as shown in Figure 27. Similar objects are grouped under the same branch. Ten groups of objects are defined in MIB 2 viz. system (sys), interface (if), address translation (at), ip, icmp, tcp, udp, egp, transmission (trans) and SNMP. These ten categories are referred as standard objects. The vendor can add its own object categories referred as custom managed objects or privately managed objects.

RMON

RMON stands for Remote Network Monitoring management information base. MIB-2, discussed in the previous section, is a poll-based mechanism, which means the data is sent only when requested. RMON is a proactive approach to send network-related information automatically to the manager. No polling is required from the manager. RMON monitors network traffic on LAN segments and sends information to the manager. Information such as broadcasts, busiest hosts, errors, number of packets, size of packets, network utilisations and many more can be tracked by RMON. Like management agents, RMON agents reside in managed devices such as routers, servers, hosts, switches, hubs, or dedicated RMON probes. Thresholds can be set and reported when crossed to reduce network traffic. Fault management, performance management and network upgrade planning can be done using RMON.

Scanned by CamScanner

Figure 28 displays RMON:

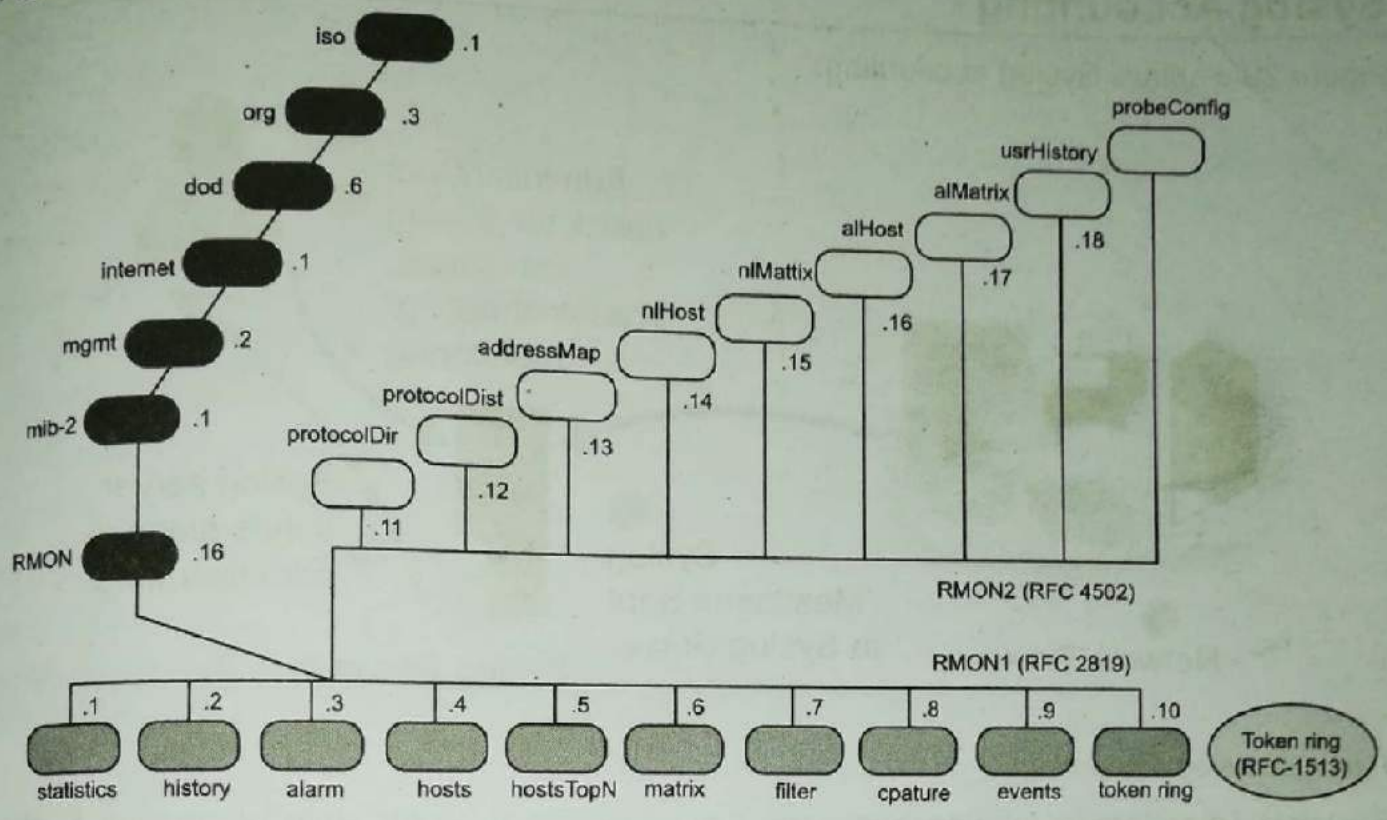


Figure 28: RMON

RMON1 tracks network information from LAN segments at the data link layer. They get the information at the frame level. Ten groups of information can be fetched by the RMON agents. These groups include statistics, history, alarm, host, host top, matrix, filters, packet capture, events, and token ring.

Monitoring of RMON1 is restricted to issues at the data link layer and the physical layer. However, network problems can occur at the upper layers of the OSI model, i.e. from the network layer till the application layer. RMON2 can monitor the upper layers by adding nine more groups. RMON2 provides end-to-end visibility such that the traffic generated by a specific application can also be tracked. Nine groups of RMON2 include protocol directory, protocol distribution, address mapping, network layer host, network layer matrix, application layer host, application layer matrix, user history collection, and probe configuration.

Scanned by CamScanner

Syslog Accounting

Figure 29 displays Syslog accounting:

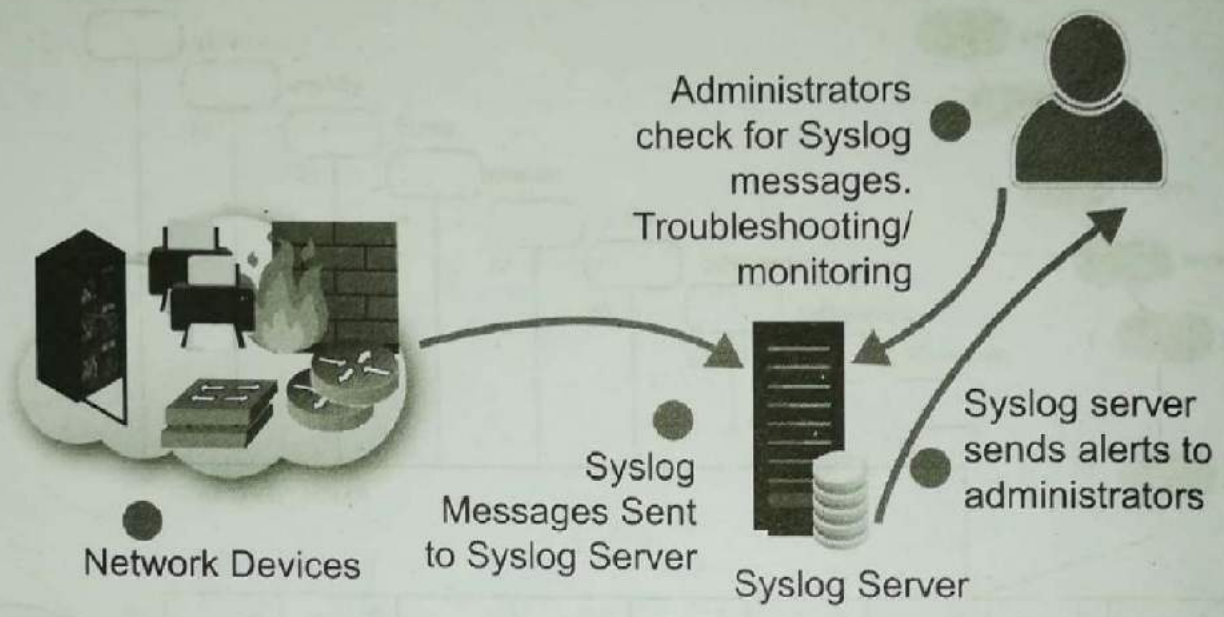


Figure 29: Syslog Accounting

Syslog is a standard for logging messages. It gives details of system state information. Syslog accounting reports system activities to the network management system. Applications, firewalls, printers, routers, web servers, etc., all have the ability to generate Syslog messages. Example: a web server generates Syslog messages to report events related to access denial. Syslog messages are sent to the Syslog server. The Syslog server captures messages from multiple sources. It has a Syslog Listener to listen to incoming messages. The messages received are stored on a Syslog server database. Since a large amount of data is stored on the Syslog server database, filters are applied to identify critical messages and generate alarm, alert or notification to inform the network administrator. Based on the criticality of a message, the network administrator can take quick action. Thus, Syslog helps in security audit, high availability, increased productivity, reduced downtime, performance management and failure management. Many tools are available in the market for Syslog accounting. Nagios is one of them.

Syslog Messages

Structure of Syslog messages is as follows:

Sequence no. : timestamp : % facility - severity - mnemonic : description

Example:

12345 : 05:29:34 : % SYS - 5 - MOD_OK : Module 2 is online

Scanned by CamScanner

Above parameters are as follows:

- **Sequence number**: The service sequence number command needs to be configured to reflect a sequence number in Syslog messages.
- **Timestamp**: The service timestamps log [datetime | log] command needs to be configured to reflect the data and time of occurrence of an event. The time stamp can be in one of the three formats—mm/dd hh:mm:ss, hh:mm:ss, d h.
- **Facility**: It indicates to a software program, an application, a protocol, a device, etc., that is the originator of this message. It indicates that the message belongs to this facility. Example: Facility '0' means 'kernel' is the source of a message.
- **Severity**: It indicates the severity level of a message. Severity is represented by a single-digit code where the lower the value, the higher the severity.

Table 1 shows the severity levels.

Table 1 Severity Levels

Severity Level	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

- **Mnemonic**: It is a code to represent a message.
- **Description**: It is a text specifying details about a message. In case of events, it can contain details such as network address, port number, etc.

Facility and severity are the parameters used to filter critical messages and take quick action or aggregate data for analysis. To avoid having a large amount of data at Syslog Server, precautions should be taken that only those messages are collected which are useful for analysis and network monitoring.

Scanned by CamScanner

2.5. Summary

In this chapter, network hierarchy is explained with the help of hierarchical network model. Enterprise network is integrated with Cisco SONA framework. The Cisco SONA framework-based Cisco Enterprise Architecture has six functional areas viz. Enterprise Campus, Enterprise Edge, Service Provider, Enterprise Branch, Enterprise Data Centre and Enterprise Teleworker. Infrastructure services, security services, voice services, wireless services, high availability services, and application networking services are modular network services. For network management, protocols such as SNMP, MIB, RMON, and Syslog Accounting are widely used.

QUESTIONS

1. Describe each layer of the hierarchical network model in detail.
2. How many functional areas are there in Cisco Enterprise Architecture? Explain each one in detail.
3. What is route redundancy? Why is it preferred while designing a network?
4. What are the different services in modular network design? Explain in detail.
5. Write short notes on: SNMP, RMON, Syslog Accounting, MIB.

Scanned by CamScanner

Designing Basic Campus and Data Centre Networks

3

OBJECTIVES

After reading this chapter, the student will be able to:

- To understand the considerations for Campus Design
- To explore Enterprise Campus Design at different scales
- To comprehend considerations for Data Center Design

Scanned by CamScanner

A campus is a large area consisting of various buildings and other structures of an institution. A network in a campus is the interconnection of many local area networks through switches and routers. A campus area network (CAN), thus, interconnects multiple buildings in a campus to form a single network. A CAN is smaller than a metropolitan area network and a wide area network, usually around 1 km to 5 km in range. An educational campus and an enterprise campus are examples of different types of campuses. An educational campus network may interconnect laboratories, training centres, conference rooms, administration building, library, etc. Example: Massachusetts Institute of Technology's (MIT) Project Athena. An enterprise campus network interconnects various buildings through a high-speed Ethernet such as 10 Gigabit Ethernet. A well-designed campus area network helps to achieve high performance, availability and reliability. Therefore, this chapter starts with a detailed analysis of various characteristics to be considered while designing an enterprise campus. Next section describes design considerations from each layer's perspective, i.e. access layer, distribution layer and core layer. It also briefs about design considerations to place a server in the network. The last section of the chapter introduces the concept of data centres and their need. Design considerations for different layers of the enterprise data centre conclude this chapter.

3.1. Campus Design Considerations

Applications, environment and infrastructure are the factors that highly influence a campus network design. This section discusses each of these factors in detail.

Application Considerations

An organisation is identified by the services it provides through various network applications. Web applications, data processing applications, system applications are various examples of networking applications. Applications in the network, thus, have varied requirements in terms of speed, bandwidth, memory, data storage, etc. based on their purpose. All of these, along with availability, throughput, reliability and security requirements, highly influence the enterprise network design such as network traffic pattern, network bandwidth requirement, and transmission media selection. Also, the enterprise network design is influenced by the type of communication among applications.

Scanned by CamScanner

Peer to Peer Network Applications

Figure 1 shows peer to peer network applications:

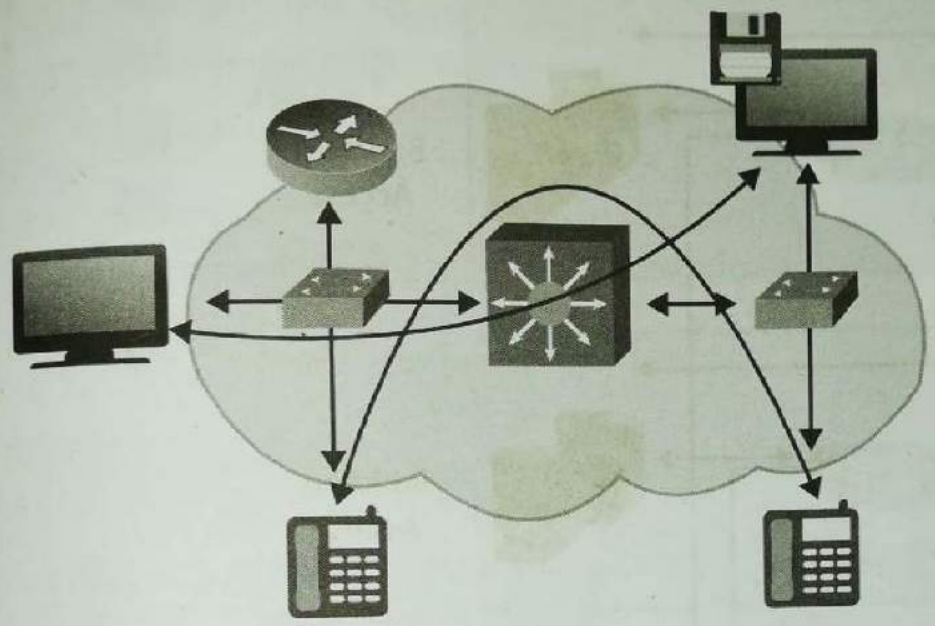


Figure 1: Peer to Peer Network Applications

Communication between two members in an organisation is termed as peer to peer communication. In an enterprise campus network, it is during the communication among two individuals through a network edge device where traffic passes over the enterprise's network. Two peers may communicate in various ways. One of the most common modes of peer to peer communication is instant messaging. Here, there is direct communication between two peers wherein messages are exchanged. Another common mode of peer to peer communication is IP phone calls. This mode supports voice communication over the network. In order to maintain Quality of Service for IP phone calls, stringent network requirements are to be satisfied. Peers may also opt for the video conference mode of communication. In this mode, bandwidth consumption is more as compared to IP phone calls. In an enterprise, peers may heavily share files among themselves or may be required to access data available on different workstations. Thus, the type of communication among peers defines network application requirements and helps network designers to design efficient networks.

Apart from the type of communication, the number of clients in the workstation also defines the network design. When the number of clients in a workstation is four or less, shared media is preferable. For a greater number of clients, LAN switching at Layer 2 is used to meet the demand for high performance and increased bandwidth.

Scanned by CamScanner

Client to Local Server Network Applications

Figure 2 displays client to local server network applications:

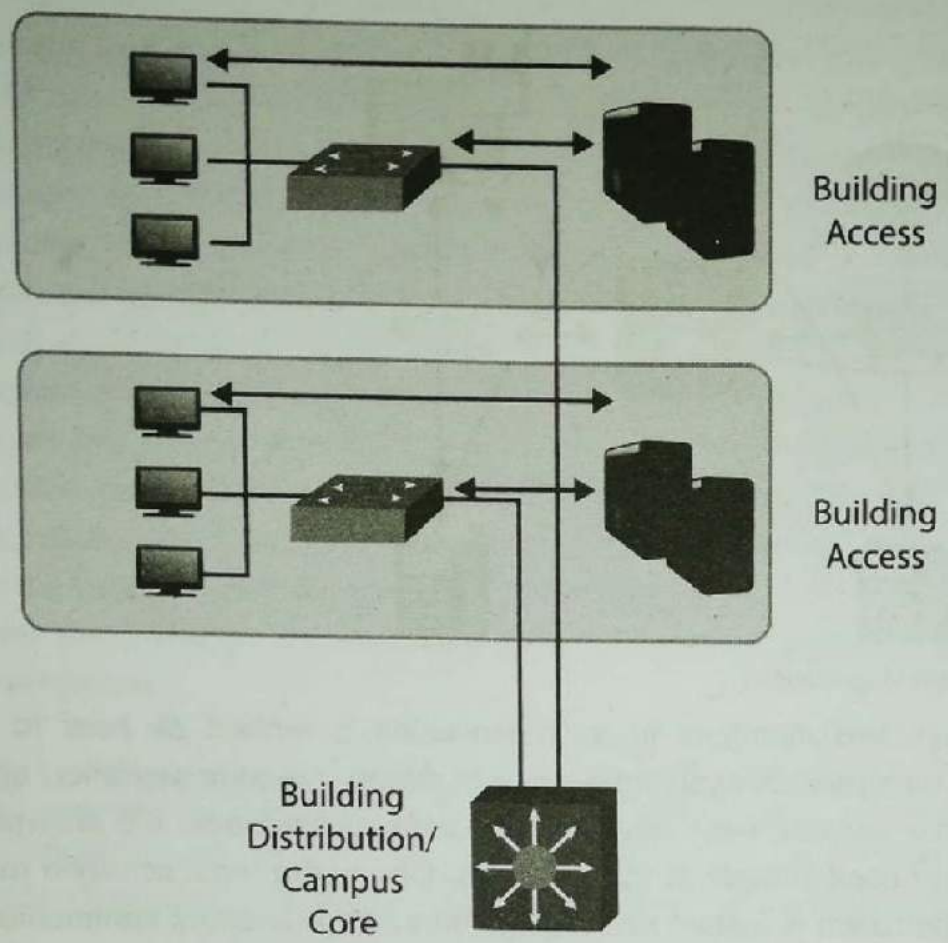


Figure 2: Client to Local Server Network Applications

Traditionally, LAN segments worked on 80:20 principle where 80% of the traffic was local, i.e. within LAN, whereas 20% of the traffic was for the outside network. In such a network, both the client and the server were connected in a single LAN. Over time, the traffic in the enterprise network increased tremendously. As a result, the enterprise network was split into several VLANs, as shown in Figure 2. Each VLAN represents a local network for a department in the enterprise. Each VLAN has a local server for applications which is managed by the respective department administrators. The majority of communication takes place within a department; hence, the major part of the traffic is observed within VLAN. For inter-department communication, data travels to a different VLAN. For Internet communication, data travels outside the local network over the campus backbone. Therefore, the bandwidth requirement for the local network is higher as compared to communication outside the local network or among local networks. Layer 2 switching is preferred for connectivity to provide more bandwidth.

Scanned by CamScanner

Client to Server Farm Network Applications

Figure 3 displays client to server farm network applications:

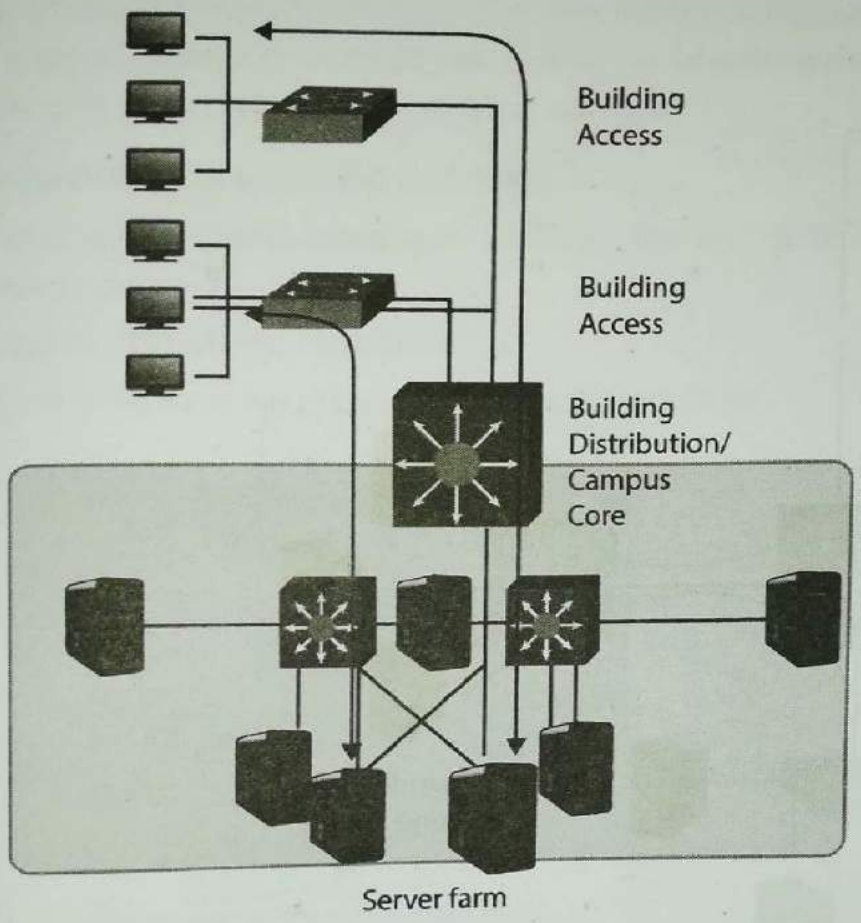


Figure 3: Client to Server Farm Network Applications

Some applications access database servers, file servers, mail servers, etc., that are critical for the enterprise. Such applications are heavily utilised by users. Due to the heavy usage, such applications and respective servers must be instantly, easily and securely accessible to the users across the enterprise. Therefore, Server Farm is designed which contains these servers at a centralised location. This eases administrative tasks as well as reduces administration cost. In this scenario, the business work on 20:80 rule, i.e. 20% of the traffic is within LAN whereas the majority of the traffic (80%) is outside LAN to centralised servers, Internet, etc. Server Farm needs to have a network having high availability, high throughput and security. Therefore, high capacity-links are used to connect applications to the servers in the Server Farm. Various buildings in the enterprise are connected to Server Farm using the fastest LAN technologies such as Gigabit Ethernet.

Scanned by CamScanner

Client to Enterprise Edge Network Applications

Figure 4 displays client to enterprise edge network applications:

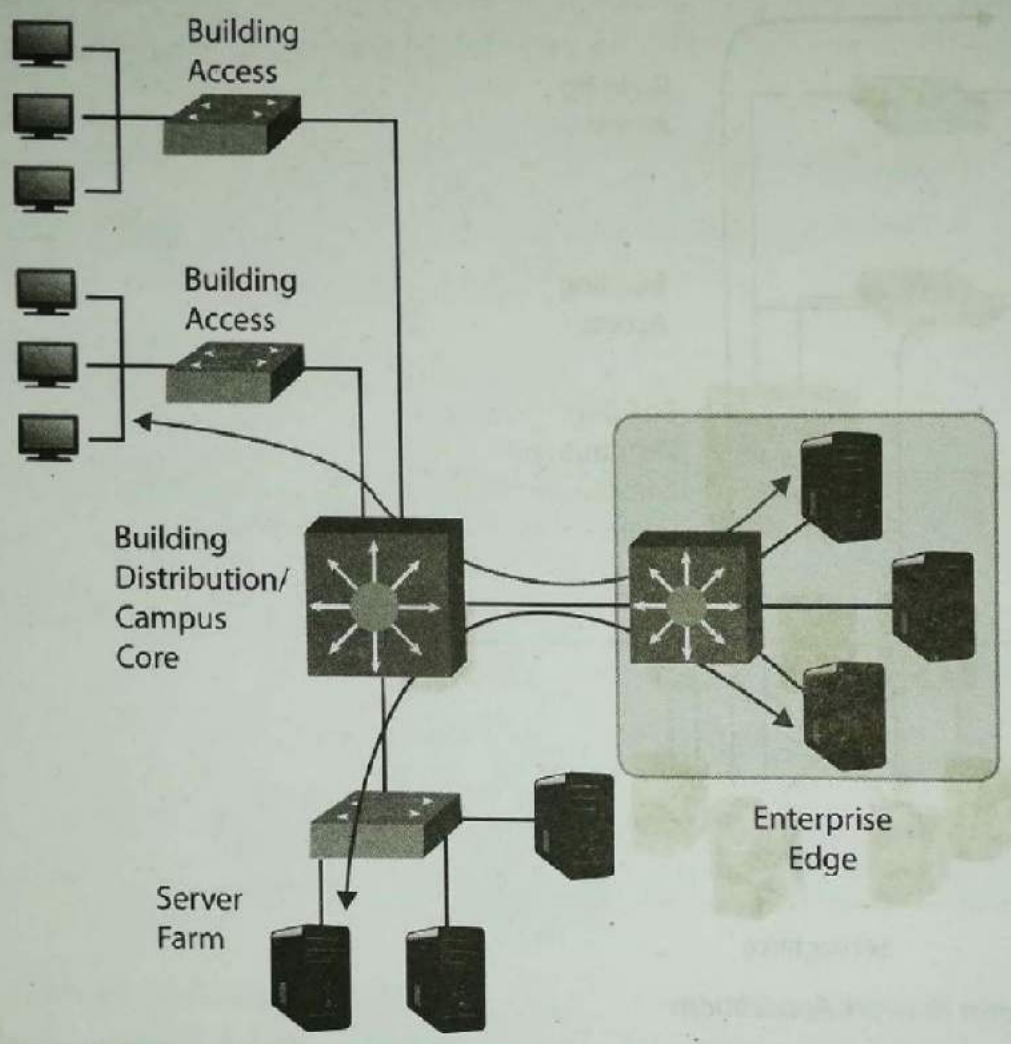


Figure 4: Client to Enterprise Edge Network Applications

DNS servers, external mail servers, e-commerce servers and web servers are all public servers in an enterprise. These servers are frequently used by Enterprise Edge network applications such as web applications, e-commerce applications, etc., to interact with the outside world. These servers support two-way communication and data exchange between the enterprise and the outside world. Therefore, Enterprise Edge applications require a highly redundant, resilient and secure network.

Environmental Considerations

A campus may include one building or many buildings. The count of buildings as well as the 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.

Scanned by CamScanner

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

Nodes in a campus, along with their location and distance, make a significant impact in network design.

Network Structure: Intrabuilding

Figure 5 displays the intrabuilding network structure:

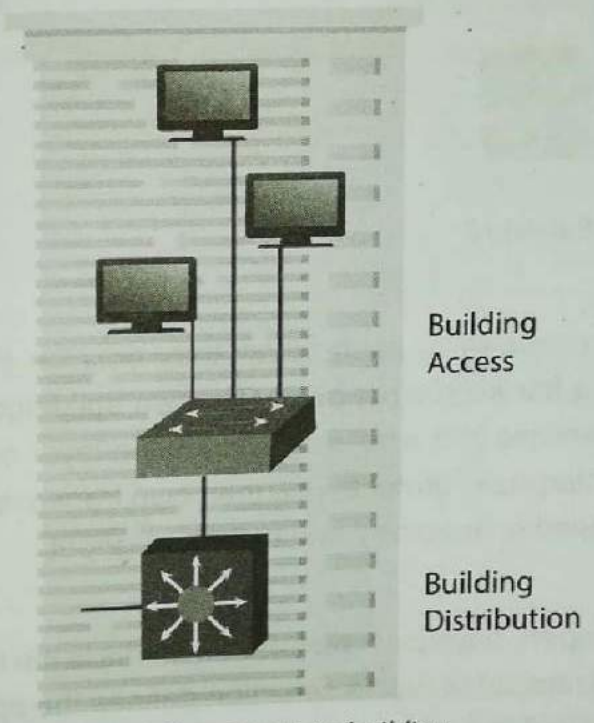


Figure 5: Network Structure: Intrabuilding

If all nodes are located in 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.

Scanned by CamScanner

Network Structure: Interbuilding

Figure 6 displays the interbuilding network structure:

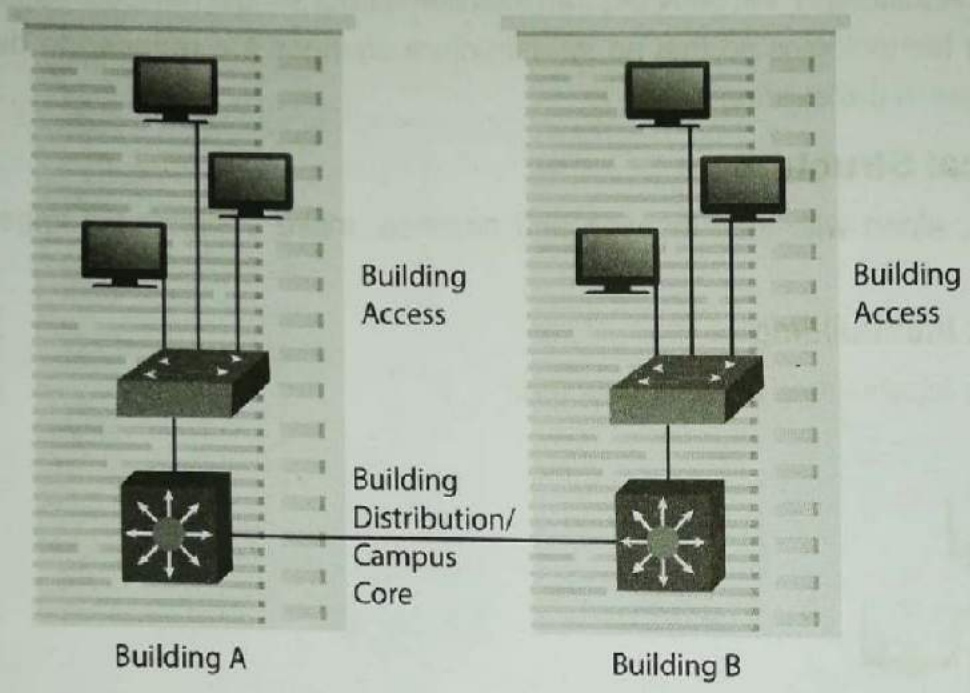


Figure 6: Network Structure: Interbuilding

Two buildings in a campus might be in close proximity to each other; they may be a few hundred metres apart or comparatively far, i.e. a few kilometres away. The two buildings are connected in a network through their central switches in the building distribution layer or the campus core layer. To connect two buildings, enterprises prefer to use their own transmission media, such as optical fibre, to support high-speed connectivity and high throughput.

Network Structure: Remote Location

When buildings are more than a few kilometres apart, physical transmission media is the most determining factor in the network design. This is because media selection defines the speed and cost of network infrastructure. To make optimal use of bandwidth, critical applications in the network are identified and intelligent network services are used to maintain QoS for such applications. For connectivity in remote locations, it might not be feasible for an enterprise to own the transmission media such as optical fibre or copper link. In such cases, traditional WAN or Metro Ethernet, connectivity options available via public service providers, is used to connect Enterprise Campus to Enterprise Edge. Further details regarding remote location connectivity can be explored in Chapter 4 (Designing Remote Connectivity).

Network Transmission Media

A campus is connected via transmission media. Various types of connection options such as copper wires, optical fibres, and IEEE 802.11 LAN technologies are available in the market. Characteristics of transmission media have been covered in detail in Chapter 1, Applying a Methodology to Network Design, Section: Transmission Media. A network designer needs

Scanned by CamScanner

to consider physical media characteristics such as signal attenuation and electromagnetic interference along with cost and budget while selecting the transmission media. This is because cabling infrastructure is a one-time investment that lasts for around ten years or so. Therefore, the transmission media must be selected judiciously. Moreover, based on the distance among the devices to be connected and bandwidth requirement, the choice of transmission media would differ. A copper twisted pair is preferred for wiring closet where the devices are in a range of 100 metres. Multimode – Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet can be used to connect devices inside buildings over a distance of 2 km, 550 m, and 300 m respectively. Single mode - Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet can be used to connect buildings in a campus over a distance of 10 km, 5 km, and 80 km respectively.

Figure 7 displays network transmission media.

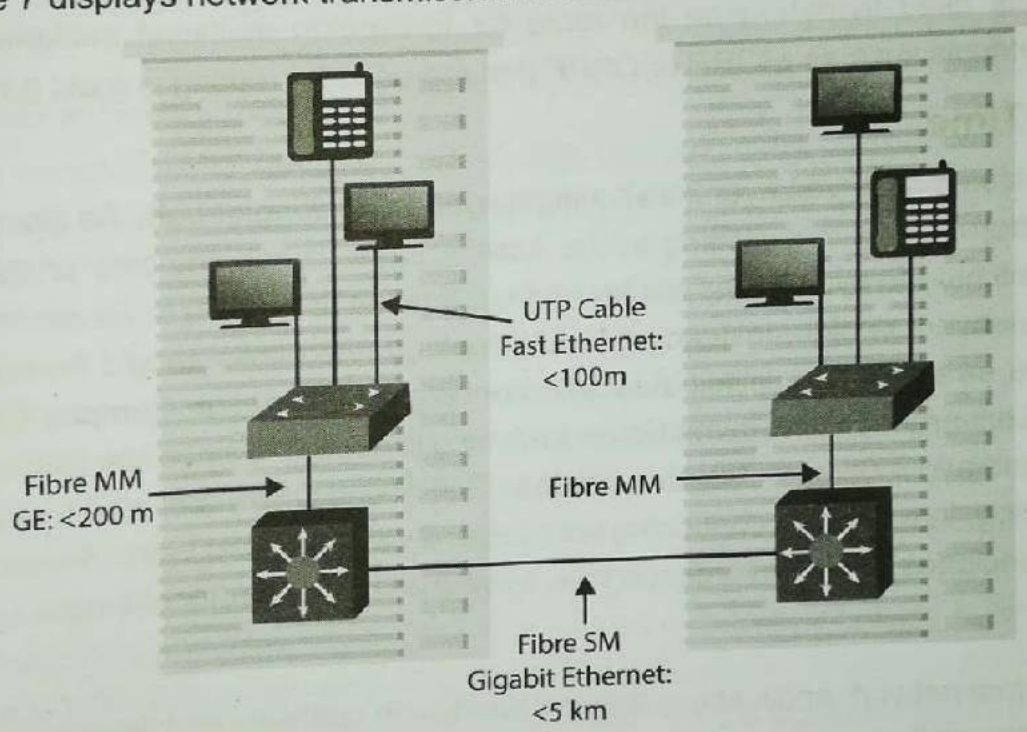


Figure 7: Network Transmission Media

As shown in Figure 7, Untwisted Pair (UTP) wiring or Fast Ethernet can be used to connect end users' workstations, printers, IP phones and other network devices which are within 100 m distance. For connections within a building, Multimode Fibre Gigabit Ethernet is preferable to connect devices at a distance not more than 200 m. Single Mode Fibre Gigabit Ethernet is used to connect devices that are at larger distances, i.e. around 5 km.

Infrastructure Considerations

Switched technology is preferred over shared media to connect devices in a network. Switched technology has various advantages listed as follows:

- Bandwidth can be dedicated for each device on the network.

Scanned by CamScanner

- It supports network infrastructure services. For example, Security and QoS.

Data link layer switches and multilayer switches can be used in a network based on business requirements and network topology. Many factors determine which switch is to be used when. Let us discuss each of these factors in detail.

IP Multicast

IP multicast is the technology which is used when the same data is to be sent to various destinations. In this technology, data is not replicated unless it is to be sent to multiple interfaces to reach its destination. Class D IP addresses (224.0.0.0 – 239.255.255.255) are used to identify multicast groups. Internet Group Management Protocol (IGMP) is used to form multicast groups in a network and forward destined packets. Hosts register on a router to join or leave multicast groups using this protocol. Protocol Independent Multicast Routing Protocol (PIMRP) is used to determine the route for forwarding multicast packets. It is independent of protocols such as EIGRP or OSPF that are used for routing unicast packets.

Convergence Time

A network in a campus may have Layer 2 switching, Layer 3 switching or both. As discussed in Chapter 2, Section: 'Layer 2 Switching in the Access Layer', spanning tree protocol is used in Layer 2 switching to avoid loops during routing. It takes around 30 to 50 seconds to converge. During network design, instead of VLAN trunks, routed links should be used to connect to the core switches. This eliminates STP convergence issues in Campus Core in Layer 2 topology. Convergence time in multilayer switching is negligible since link failures are immediately detected and routing routes are updated. EIGRP and OSPF are used for routing in multilayer switching. In a network containing both Layer 2 switching and Layer 3 switching, convergence time includes STP convergence time as well as routing protocol timers.

QoS

A campus may contain network applications that are bandwidth intensive and delay sensitive. Such applications demand a secure network with predictable delays and guaranteed services. To provide such services, network resources must be managed efficiently to deliver agreed QoS. A simple solution that can be thought of is having a high-capacity switch in the network, but unfortunately, this does not ensure QoS. In an access layer switch, when all the ports of a switch are fully used, the uplink port is congested. To avoid such congestion due to switch oversubscription, QoS mechanisms are required from Access to Distribution as well as from Distribution to Core layer. Bandwidth, delay, jitter, and packet loss are prominent factors to be considered while ensuring QoS.

Figure 8 shows network QoS:

Scanned by CamScanner

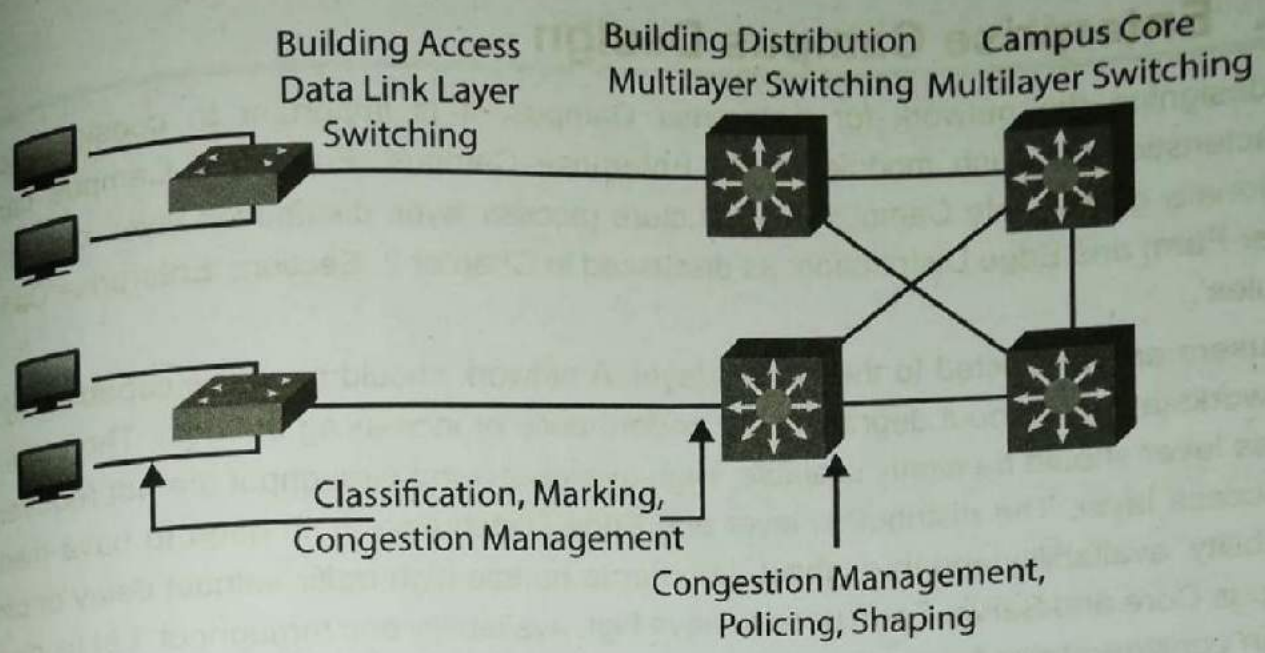


Figure 8: Network QoS

Marking, classification, queuing, scheduling, shaping and policing are various QoS mechanisms that can be implemented on LAN switches. In marking, the priority level or class of service is set for each packet or frame. In classification, the network traffic is classified based on the priority level or class of service assigned to the packet or frame. The MAC address or input port of a switch can be used for classification and marking at Layer 2 switches. This way traffic from a specific host can be prioritised. At Layer 3, traffic can be classified based on application by using IP addresses, port numbers or QoS bits in the IP packet. Queuing is the QoS mechanism used to ensure that during congestion the data stream from critical applications reaches the destination with the least delay and jitter. For this, the traffic is separated into different queues or buffers based on the priority or class of service marked in the packet or frame. But, which queue should be serviced, when, or in which sequence? This is determined by scheduling. If some traffic violates the threshold, shaping buffers the frame for a small amount of time to ensure that the traffic is confined within a predetermined rate. In some cases, the priority of the packet is lowered or even dropped. This is referred as policing. Queuing, shaping, and policing is implemented at distribution layer switches and Campus Core switches. All these techniques are used to implement QoS in the network, making the bandwidth usage effective and network performance predictable.

Scanned by CamScanner

3.2. Enterprise Campus Design

For designing the network for Enterprise Campus, it is important to consider design characteristics for each module of the Enterprise Campus. Enterprise Campus can be functionally divided into Campus Infrastructure (access layer, distribution layer, core layer), Server Farm and Edge Distribution, as discussed in Chapter 2, Section: 'Enterprise Campus Modules'.

End users are connected to the access layer. A network should have the capability to add new workstations without degrading the performance or increasing the cost. Therefore, the access layer should be highly scalable. High availability and throughput are not required for the access layer. The distribution layer and Edge Distribution, both need to have medium scalability, availability and throughput. In order to handle high traffic without delay or drops, Campus Core and Server Farm need to have high availability and throughput. Let us discuss design considerations for each module in detail.

Building Access Layer Design Considerations

The first step in designing a network for building access layer is to identify the requirements of the building access layer. The factors that prominently determine the access layer requirements include:

- Current cabling and cabling options for uplink connectivity at the wiring closet
- Link capacity to building distribution layer switches
- Multicast traffic management
- Number of end users in present and future
- Number of ports available for end user connectivity
- Number of VLANs per access switch
- Number of VLANs spread across multiple switches
- Performance requirement by the data link layer
- QoS
- Redundancy level
- Security

Analysing each of the aforementioned factors helps in selecting appropriate network devices for the building access layer.

Scanned by CamScanner

The best practice recommendations for designing the building access layer are listed as follows:

VLANs and STP Management

- VLAN should be limited to a single wiring closet
- For a highly reliable, available and predictable network, avoid using any type of STP
- If unavoidable, use Layer 3 routing to isolate different STP domains

Trunks Management

- To support Dynamic Trunking Protocol (DTP) encapsulation, set DTP to 'desirable' and 'desirable with negotiate option' on one side each.
- To avoid broadcast propagation, manually prune the VLANs that are not used from trunked interfaces.
- To decrease the potential for operational error, use the VTP transparent mode.
- To prevent VLAN hopping, identify the ports on which hosts will be attached and disable trunking on such ports.

Building Distribution Layer Design Considerations

Building distribution layer is the intermediate layer between the building access layer and the campus core layer. It aggregates data from the access layer and provides it to the high-speed campus core layer. To facilitate this functionality, multilayer switching is implemented at the building distribution layer. It also needs to incorporate network infrastructure services such as enterprise policy enforcement, security, high availability, traffic filtering, and QoS. The factors to be considered while designing the building distribution layer are listed as follows:

- Current cabling at a wiring closet and cabling options for uplink connectivity
- Number of building distribution switches
- Number of devices for each building distribution switch
- Redundancy type and level
- Number of redundant building distribution switches
- Number of redundant links
- Number of uplinks
- Speed of uplinks

Analysing each of the aforementioned factors helps in selecting appropriate network devices and transmission media for the building distribution layer.

Scanned by CamScanner

The best practice recommendations for designing the building distribution layer are listed as follows:

First-Hop Redundancy Protocols

- Layer 2 or Layer 3 is used between the building distribution layer and the building access layer.
- If Layer 2 is used, the convergence time on node failure or link failure depends on default gateway redundancy and failover time.
- Default gateway redundancy is provided by building distribution switches by using first-hop redundancy protocols.
- Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) are all examples of first-hop redundancy protocols.
- If Layer 3 is used, there is no need to use a first-hop redundancy protocol since the default gateway is in a multilayer switch at the building access layer.

Layer 3 Routing Protocols Between Building Distribution and Campus Core

- For fast convergence on the failure of links, deployment of routing protocols between building distribution and campus core switches is advisable.
- This helps in rerouting network traffic to alternate equal-cost path.
- Deterministic convergence can be achieved by building triangles instead of rectangles for alternate equal-cost paths.

Figure 9 illustrates network redundancy:

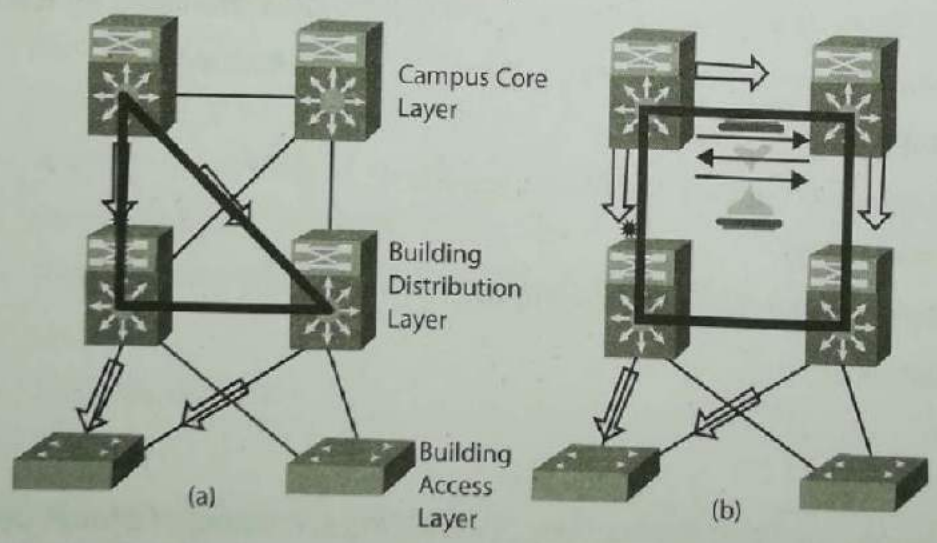


Figure 9: Network Redundancy

Figure 9 (a) depicts a network with triangle redundancy, whereas Figure 9 (b) depicts a network with rectangle redundancy. Since alternate paths in Figure 9 (a) are of equal-cost, entries for these paths are stored in a routing table. On failure of any link, no recalculation

Scanned by CamScanner

for routing is required. Instantly, an alternate path from the routing table is used. In Figure 9 (b), the failure of a link requires recalculation of an alternate route and hence, takes time to converge.

Campus Core Design Considerations

For a small or medium sized campus, the campus core layer can be merged in the building distribution layer. The campus core layer is required only for a large campus. The campus core layer gets traffic from the building distribution layer. This layer also integrates with Server Farm and Enterprise Edge. For this purpose, multilayer switching is used at the campus core layer. The factors to be considered while designing the campus core layer are listed as follows:

- Enterprise Edge and WAN connectivity
- LAN, WAN, MAN convergence
- High availability, redundancy and scalability requirements
- Performance requirements
- Number of high-capacity ports
- Number of intelligent multilayer switches

Analysing each of the aforementioned factors helps in selecting appropriate network connectivity options for the campus core layer.

Large Campus Design

Figure 10 displays the campus core design for a large campus:

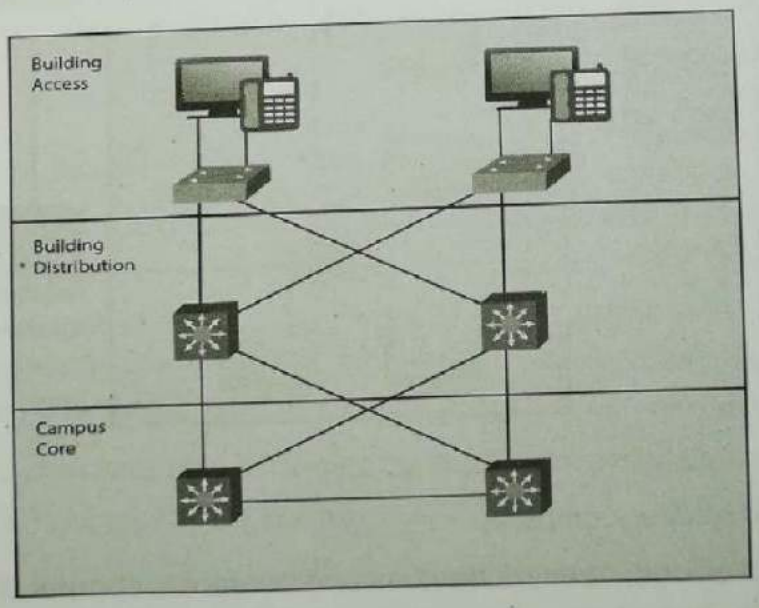


Figure 10: Campus Core Design for a Large Campus

In a large campus, the campus core layer should have more than one multilayer switch to make the network highly available, scalable and redundant. In Figure 10, dual multilayer switches

Scanned by CamScanner

are used to connect the campus core layer to the building distribution layer. As depicted in the figure, a triangle configuration is used to redundantly connect the building distribution switches to the campus core switches. The advantages of using such configurations are listed as follows:

- The network can be scaled to a large size
- Supports load sharing
- No STP is required
- Provides multicast and broadcast control
- Supports network infrastructure services
- Fast recovery from link failure
- High throughput

Thus, dual multilayer switches should be used while designing the campus core layer for a large campus.

Small and Medium Campus Design

Figure 11 shows the campus core design for small and medium campuses:

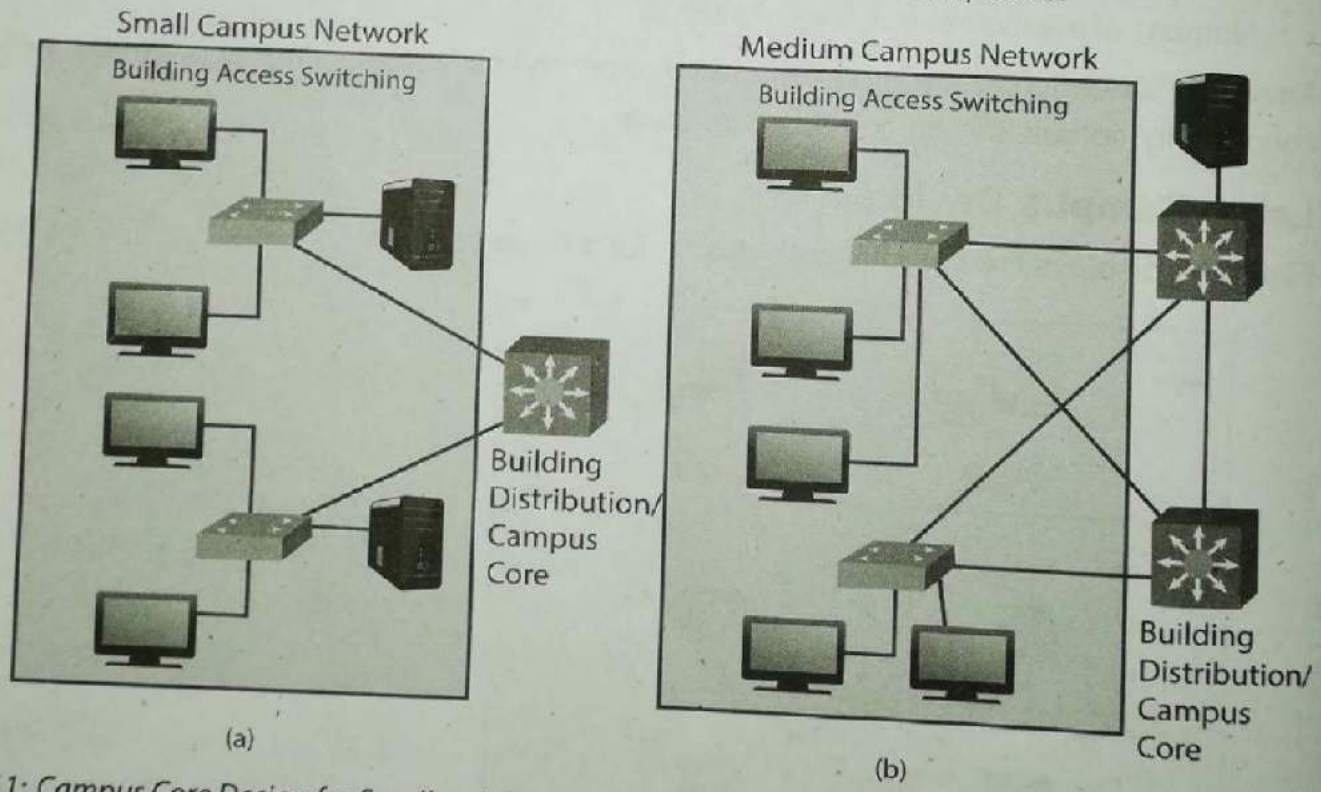


Figure 11: Campus Core Design for Small and Medium Campuses

In a small campus, the number of workstations, network devices and servers is comparatively less. They might be connected to the same wiring closet. Scaling or high-end switching performance is not required in a small campus. Therefore, for a small campus, the campus core layer can be combined with the building distribution layer, as shown in Figure 11 (a).

Scanned by CamScanner

For a medium campus, end users are comparatively more than a small campus. In such a campus, servers are connected to multilayer building distribution switches, as shown in Figure 11 (b). Also, redundant multilayer switches at the building distribution layer are used to connect to building access layer switches for high performance and availability. Even in a medium campus, the campus core layer is combined with the building distribution layer.

Edge Distribution Design

Figure 12 shows the edge distribution design at Campus Core:

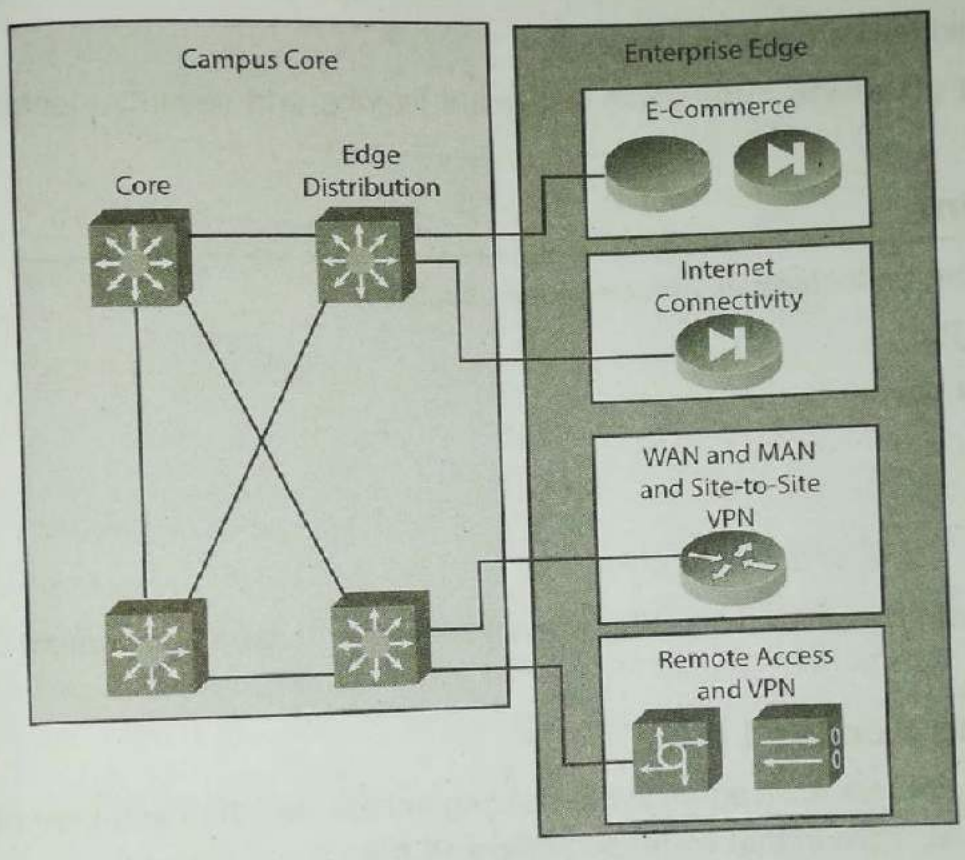


Figure 12: Edge Distribution Design at Campus Core

Edge Distribution is the module which is optionally used to connect Enterprise Edge to the Campus Core. Enterprise Edge may contain e-commerce servers, web servers, WAN and MAN and site to site VPN, Remote Access and VPN, etc. All these devices located in the Enterprise Edge module need to be isolated; controlled access to such devices must be provided. In short, security is one of the major requirements while designing the Enterprise Distribution module. This can be achieved by using dual multilayer switches at Enterprise Distribution, as shown in Figure 12.

Scanned by CamScanner

The functionality of enterprise distribution multilayer switches are listed as follows:

- Aggregate Enterprise Edge connectivity
- Filter and route traffic to the campus core layer
- Security to devices located in the Enterprise Edge module
- Restrict unauthorised access
- Avoid DoS attack
- Avoid packet sniffing
- Filter traffic to avoid network reconnaissance

Thus, while designing enterprise distribution, additional filtering and security mechanisms should be considered.

Server Placement

Servers in a network can be located at various places such as:

- Building access layer
- Building distribution layer
- Campus core layer
- Server Farm
- Data centre

Let us discuss how design considerations differ when the location of server placement varies in the network.

Servers in Building Access Layer

- In a small campus, servers are connected to building access switches and they mostly get traffic local to a workgroup that corresponds to a VLAN.

Servers in Building Distribution Layer

- In a medium campus, servers are connected to building distribution switches as they communicate with clients at different VLANs.

Scanned by CamScanner

Servers in Campus Core Layer

Figure 13 displays servers in the campus core layer:

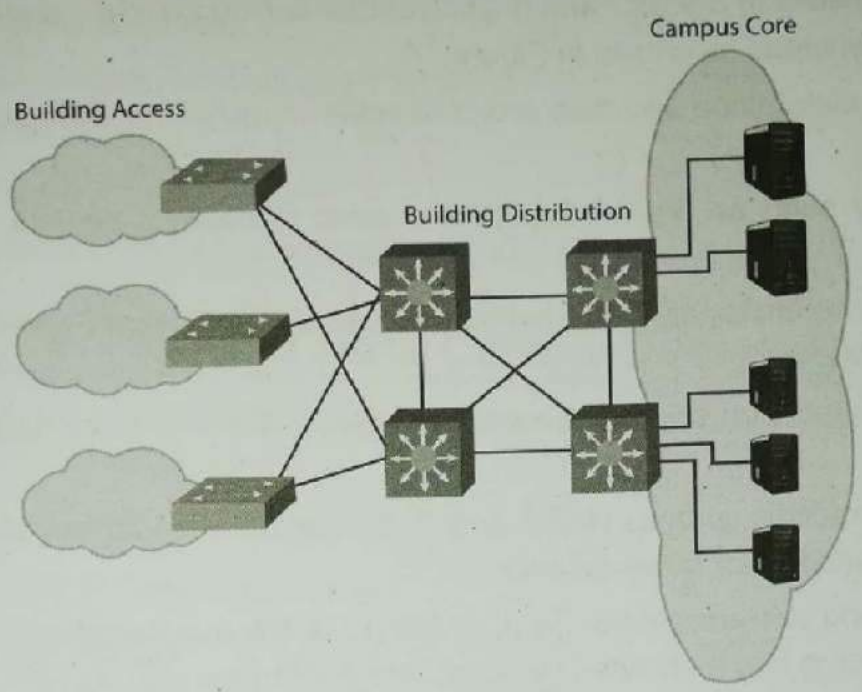


Figure 13: Servers in Campus Core Layer

- Servers can also be connected to campus core switches if the campus core layer has not been combined with the building distribution layer for a medium campus.
- Due to limited ports in campus core switches, the access control list and QoS configurations are done in the building distribution layer.

Servers in Server Farm

Figure 14 displays servers in Server Farm:

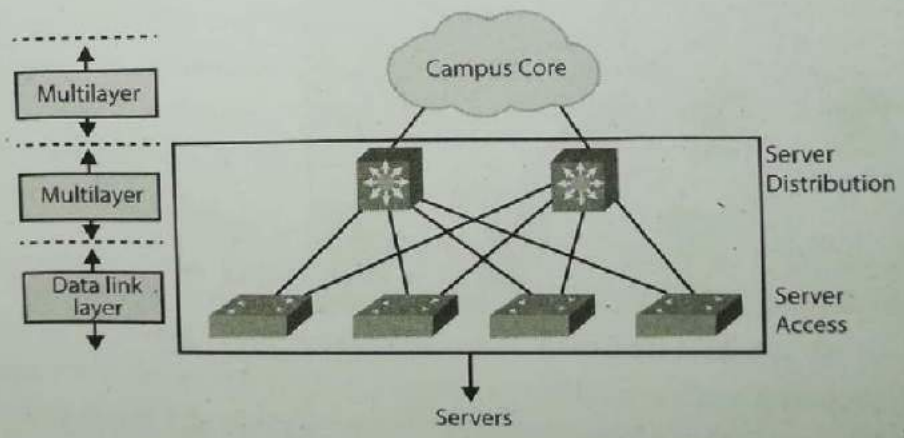


Figure 14: Servers in Server Farm

Scanned by CamScanner

In a large campus, servers are located in Server Farm which is connected to the campus core layer.

- Server Farm module consists of Server Farm multilayer distribution switches and Server Farm Layer 2 access switches, as shown in Figure 14.
- Server Farm multilayer distribution switches are connected to multilayer Campus Core switches.
- High-speed connectivity such as Gigabit Ethernet is used to connect servers to the Server Farm.
- Access to the servers is controlled by implementing Access Control List at Server Farm multilayer distribution switches.
- Redundant multilayer distribution switches are used at Server Farm to have negligible convergence time.
- First-hop redundancy protocols such as HSRP and GLBP can be used at Server Farm multilayer distribution switches for faster failover.
- For communication among servers, Server Farm multilayer distribution switches handle the traffic without forwarding it to multilayer Campus Core switches.

Server Farm Design Guidelines

Figure 15 displays the Server Farm design:

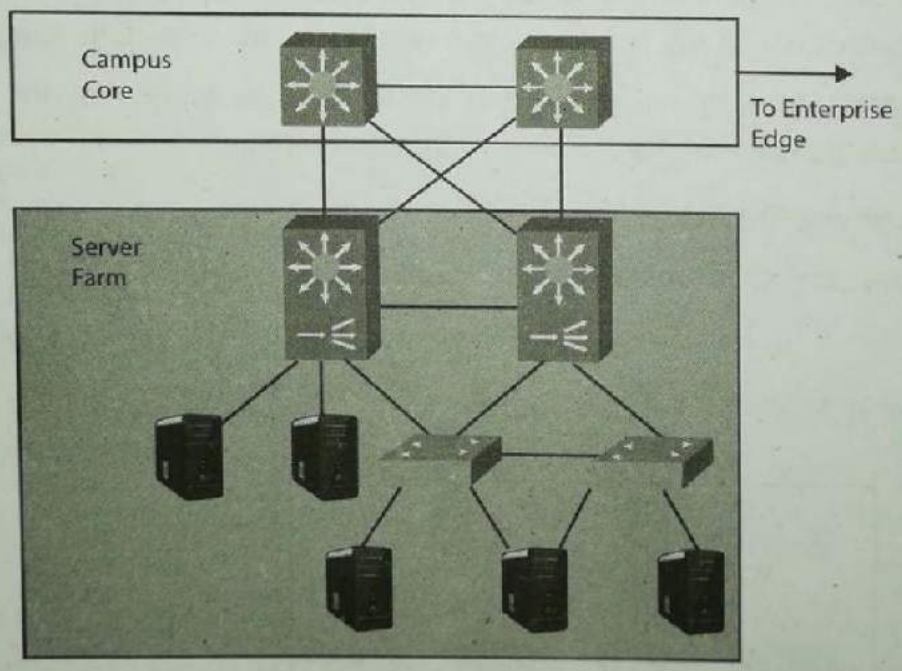


Figure 15: Server Farm Design

Scanned by CamScanner

Guidelines to be considered while designing the Server Farm module are listed as follows:

- QoS mechanisms to be implemented at server links to avoid frame drops for business-critical applications
- Bandwidth requirements
- Performance requirements
- Server's capabilities
- Uplink ports at Server Farm switches are not oversubscribed

3.3. Enterprise Data Centre Design Considerations

Before discussing design considerations for an Enterprise Data Centre, let us have an overview of a data centre.

Data Centre

Figure 16 shows a data centre:

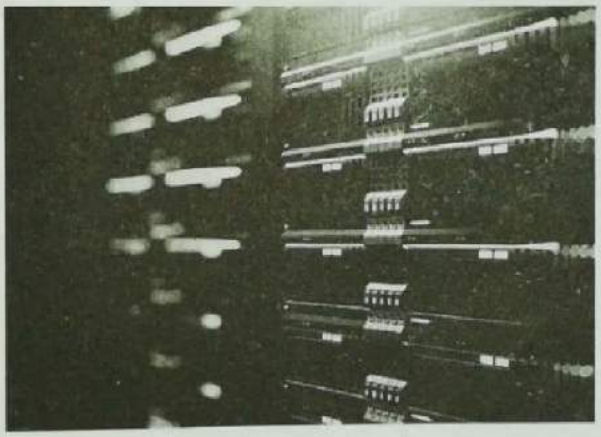


Figure 16: Data Centre

A data centre is a centralised repository of a large group of networked servers used for storage, processing, management and dissemination of business data. An Enterprise Data Centre is a custom shelf of enterprise applications. It facilitates load sharing, high availability, redundancy and reliability for business-critical applications. It has proper heating, ventilation and air conditioning (HVAC), power supply, security system, and surveillance system. A modular data centre design allows flexibility and scalability with reduced maintenance.

The Enterprise Data Centre

An Enterprise Data Centre enables end users and clients to access data and network resources for a large enterprise. Initially, applications were developed as per business needs and implemented. Each application deployed worked in isolation with the other. A data centre thus became a collection of computing platforms, operating system and storage system. This led to the underutilisation of data centre infrastructure. It resulted in expensive backup,

Scanned by CamScanner

management and security of deployed applications. Thus, the server-centric data centre model evolved to service-centric data centre model.

Figure 17 shows the evolution of the data centre:

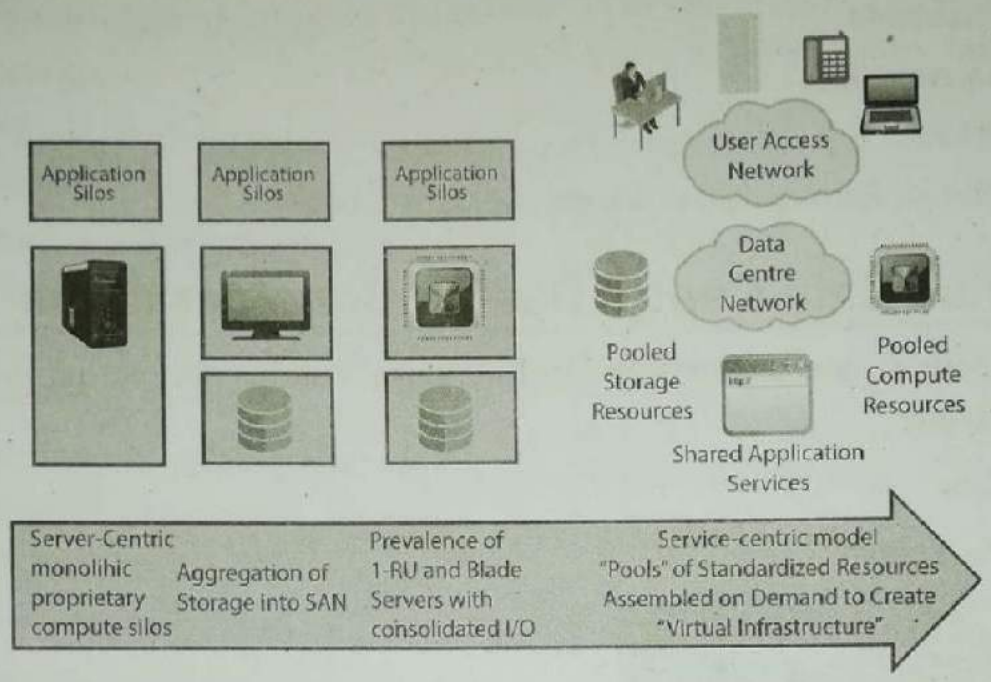


Figure 17: Data Centre Evolution

The evolution of the data centre started with the server-centric approach. The virtual machine software allowed multiple applications to run on a single server. The next step was to separate the pool of storage devices connected via the network to the server.

Figure 18 displays a storage area network:

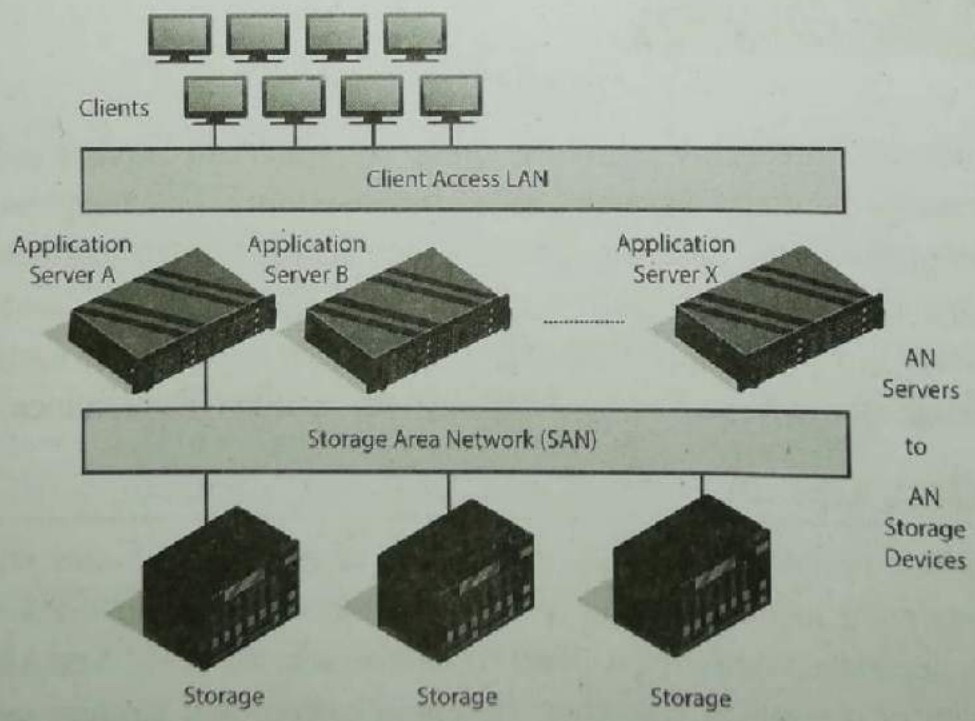


Figure 18: Storage Area Network

Scanned by CamScanner

Storage Area Network (SAN) is an example of this stage of data centre design. It is a high-speed network of storage devices that are connected to servers. It provides block-level storage, hence, is specifically designed to store structured data such as databases and spreadsheets. All the applications on the networked server can access the storage device. Thus, SAN contributed to the virtualisation of the data centre.

Figure 19 displays a Network Attached Storage (NAS):

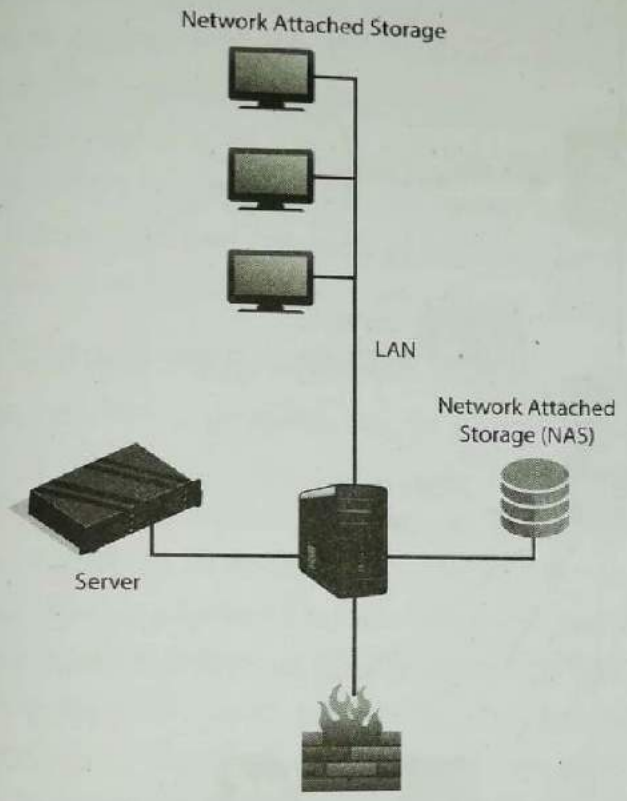


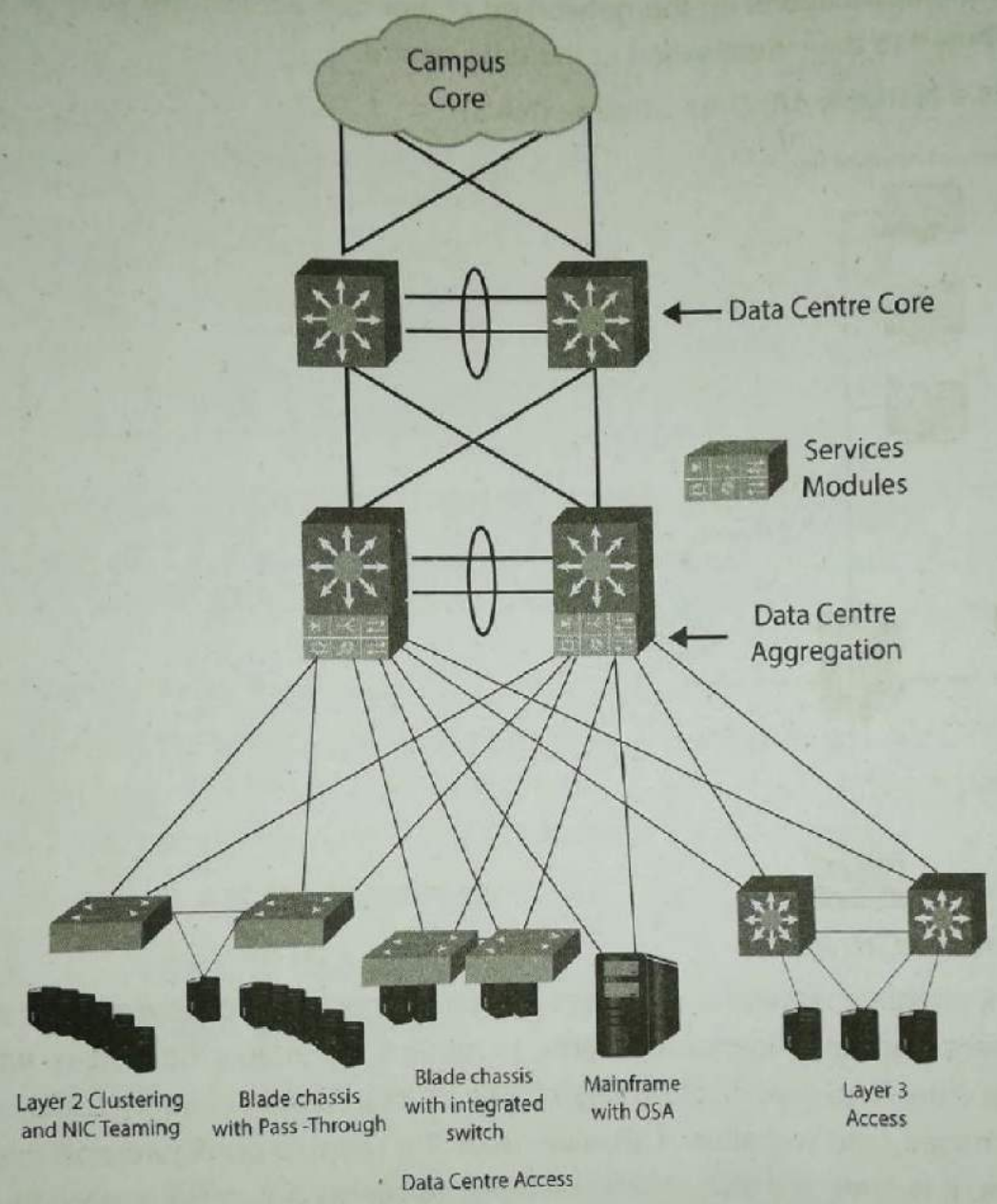
Figure 19: Network Attached Storage

Similarly, a network attached storage is a storage device connected to a network that allows authorised end users and heterogeneous clients to store and retrieve data. It is easy to archive and backup data. NAS is particularly used for unstructured data such as audio, video, text files, emails, images, and websites. This eliminates the need to configure and manage different file servers. It is preferred for scenarios where the clients are located remotely or in different time zones. It, thus, facilitates storage space virtualisation for a data centre. Later, pools of one-way, two-way and four-way servers were created on-demand. The next stage facilitated high-speed I/O operations. Rack units and blade servers were used in this stage. I/O resources could be consolidated and provisioned on-demand to connect to different servers and storage. The current stage is a pool of I/O, storage and computing resources that can be utilised for any application over the data centre network. All applications and services can, thus, be integrated on the network. Hence, the name, service-centric data centre model. Now, let us discuss the Enterprise Data Centre Infrastructure in detail.

Scanned by CamScanner

Enterprise Data Centre Infrastructure

Figure 20 shows the data centre infrastructure design:



OSA = Open Systems Adapter

Figure 20: Data Centre Infrastructure Design

As shown in Figure 20, data centre infrastructure design consists of three layers, i.e. core layer, aggregation layer and access layer. The aggregation layer in the data centre corresponds with the distribution layer in enterprise design. Let us discuss each of these three layers in detail.

Scanned by CamScanner

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.

Scanned by CamScanner

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.

3.4. Summary

In this chapter, various factors to design an enterprise campus are explained. Network application characteristics, environmental characteristics and infrastructure device characteristics highly influence Enterprise Campus network design. While designing an Enterprise Campus, the design of each module in the six functional areas should be considered. Design considerations vary for an Enterprise Data Centre design and are discussed for each layer.

QUESTIONS

1. What are the various factors to design an Enterprise Campus? Explain each one in detail.
2. Describe the design considerations for all six functional areas of an Enterprise Campus.
3. How does the Enterprise Data Centre design vary for Enterprise Campus design? Justify.

Scanned by CamScanner

DESIGNING REMOTE CONNECTIVITY

4

OBJECTIVES

After reading this chapter, the student will be able to:

- To learn WAN interconnections and WAN transport technologies
- To explore remote connectivity network design
- To comprehend application and technical requirements for WAN design
- To understand Enterprise Edge WAN and MAN architecture
- To analyse hardware and software selection for Enterprise Edge components
- To understand Enterprise Branch and Teleworker Design

Scanned by CamScanner

4.1. Enterprise Edge Wan Technologies

This section starts by introducing WANs. Then, different types of WAN interconnections along with traditional WAN technologies are discussed in this section. Various technologies are available for WAN transportation. These are discussed further in this section.

Introduction to WANs

WAN is a network which occupies a large geographical area for commuting data over a network. It involves the interconnection of different LANs so that users at different locations can communicate with each other. It is used to transmit data by using facilities provided by the service provider.

A WAN provides different services for which the network provider charges a tariff. It is designed using leased lines, circuit switching, packet switching, etc. Frame Relay and asynchronous transfer mode are some examples of packet switching. The main purpose of a WAN is to connect to various applications or the outside world. It should be designed in such a way that these applications can always be made available to the enterprise modules in a cost-effective manner.

WAN Interconnections

Figure 1 displays WAN interconnections:

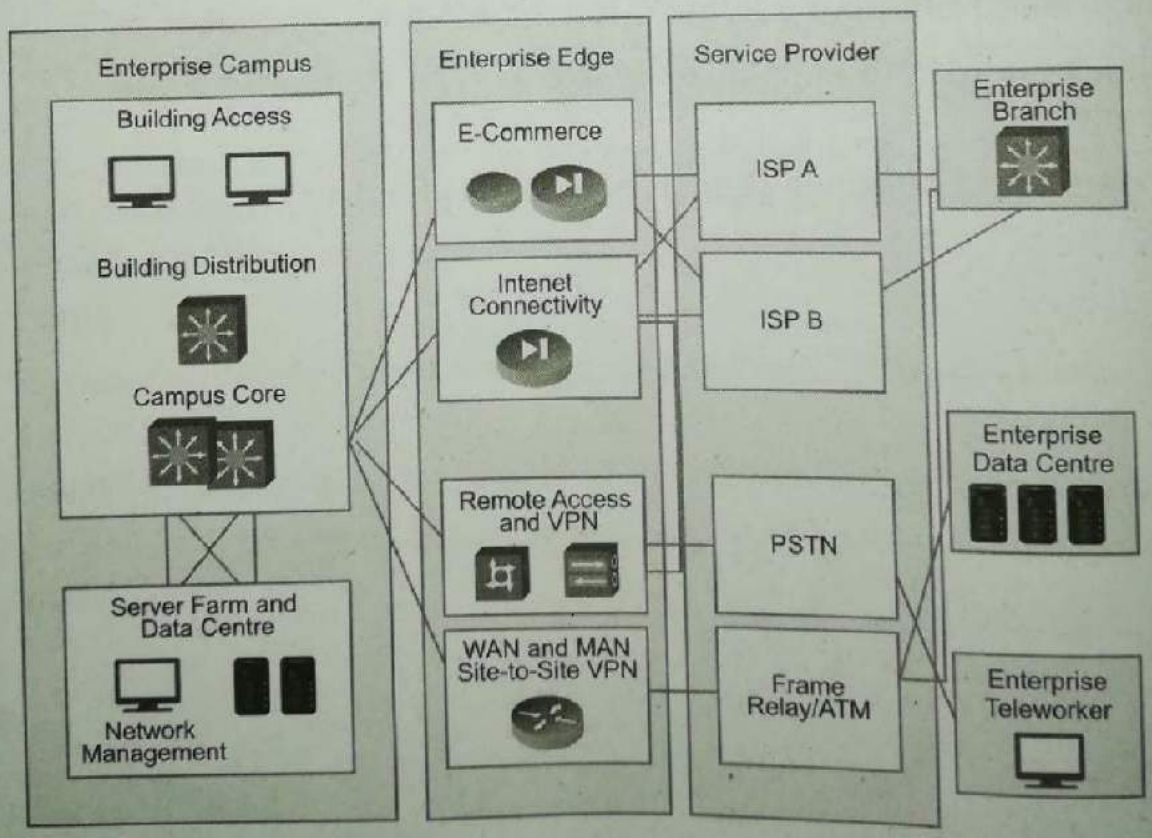


Figure 1: WAN Interconnections

Scanned by CamScanner

A WAN provides different interconnections. It establishes connections with the outside world from enterprise module to provide the following connections:

1. Connection with the Internet service provider (ISP) from the enterprise module.
2. Connection between various enterprise sites over the ISP network.
3. Connection between enterprise sites over a public-switched telephone network.

WAN connections are of two types viz. point to point between two locations or connections to a multipoint.

Traditional WAN Technologies

The following are traditional WAN technologies.

Leased Line

Figure 2 displays leased lines network:

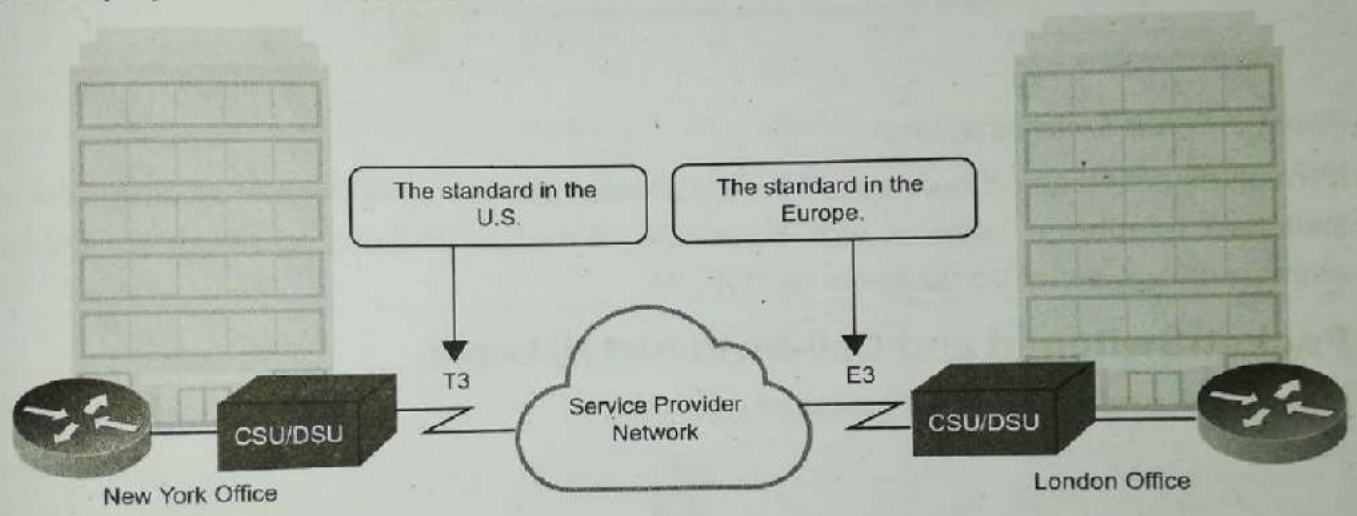


Figure 2: Leased Lines

It has point to point connection which is active all the time irrespective of the requirement. Businesses use leased lines to connect different geographical locations. A leased line uses either frequency division multiplexing or time division multiplexing (TDM). In leased line transmission, both sender and receiver are synchronised with each other.

Scanned by CamScanner

Circuit-Switched Network

Figure 3 illustrates a circuit-switched network:

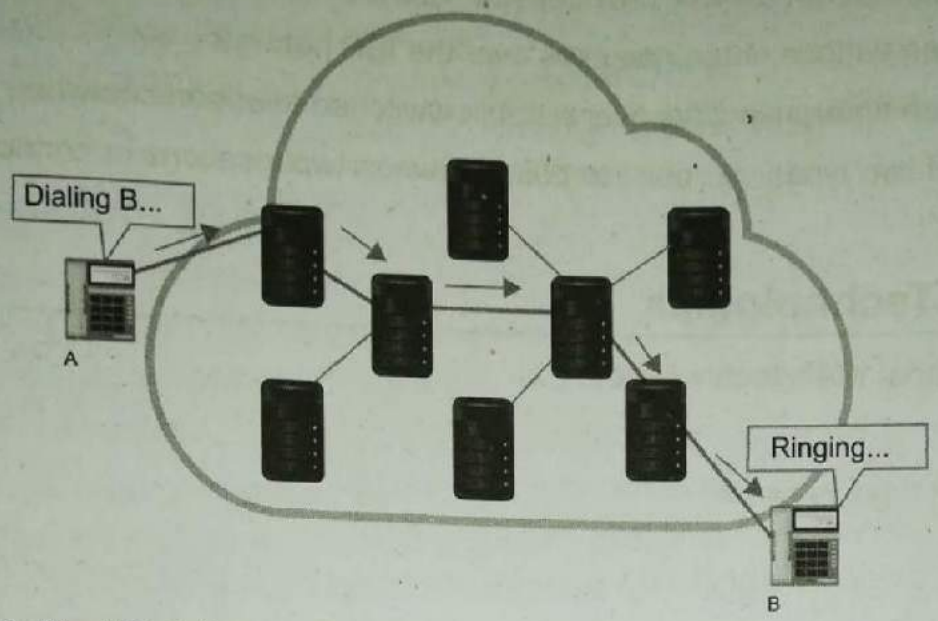


Figure 3: Circuit-Switched Network

It involves a dedicated connection for a particular point to point transfer of data. The public-switched telephone network (PSTN) is one of the circuit-switched networks. Others are asynchronous serial transmission and ISDN.

Packet-Switched and Cell-Switched Network

Figure 4 illustrates a packet-switched network:

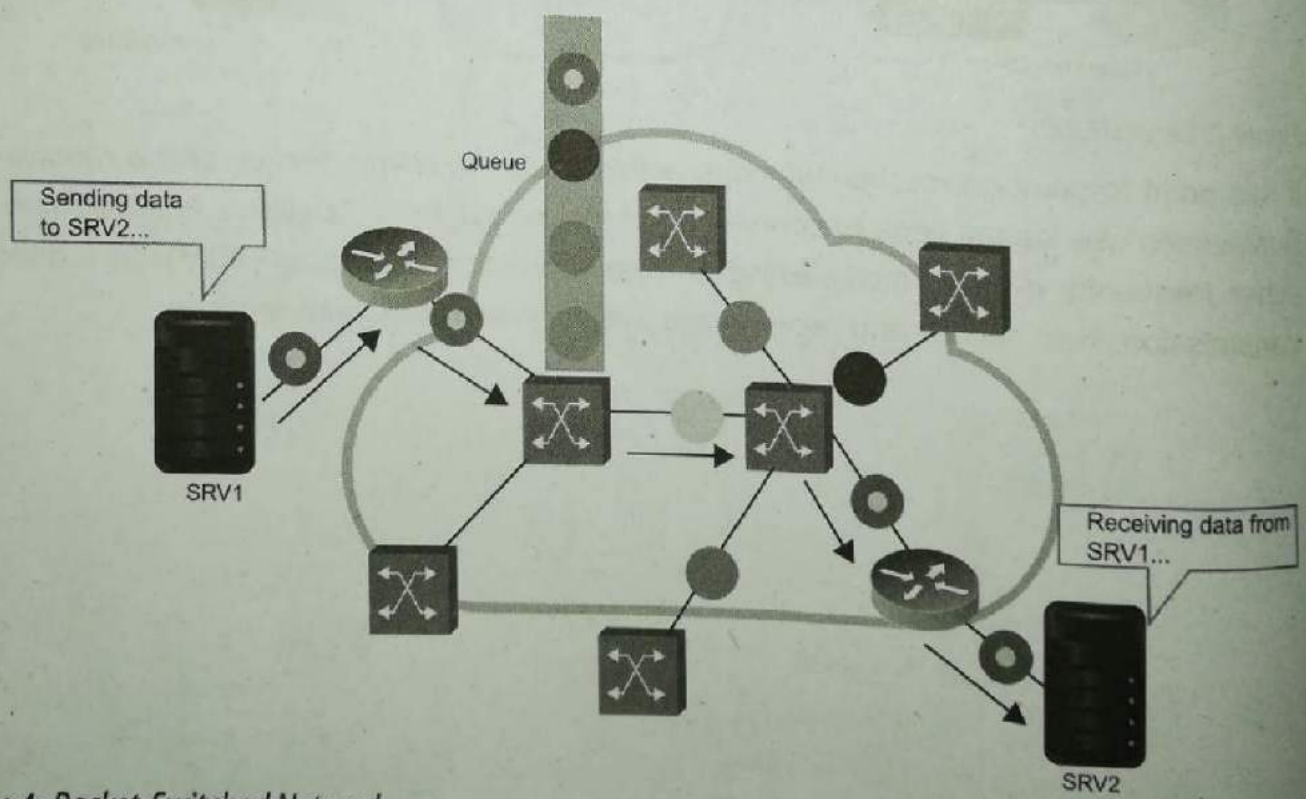


Figure 4: Packet-Switched Network

Scanned by CamScanner

It involves the transfer of packets between a sender and a receiver. In packet-switched networks, the same channel can be used by different connections leading to efficient use of resources. Cell switching provides low latency and high throughput by combining some features of packet switching and circuit switching. X.25, Frame Relay and Switched Multimegabit Data Service are some of the examples of packet-switched networks.

WAN Transport Technologies

Table 1 shows 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

Scanned by CamScanner

Figure 5 displays WAN access technologies:

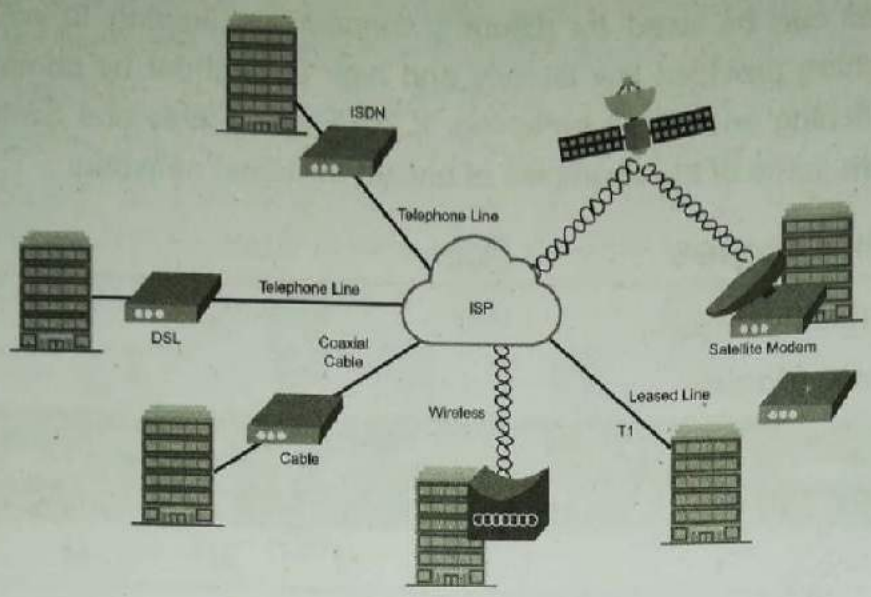


Figure 5: WAN Access Technologies

TDM (Leased Lines)

TDM stands for Time Division Multiplexing. In this technique, 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. Digital Signal level 0 (DS0), i.e. base channel bandwidth, is 64 Kbps. The same bandwidth is utilised for uncompressed digitised phone conversations. In TDM, the connection is established by dedicating a channel for a specific connection. As discussed, in a packet-switching network, a channel is not dedicated for a user, and hence users pay based on network usage. Consequently, due to dynamic channel allocation, the network bandwidth is more efficiently utilised in a packet-switched network.

Integrated Services Digital Network

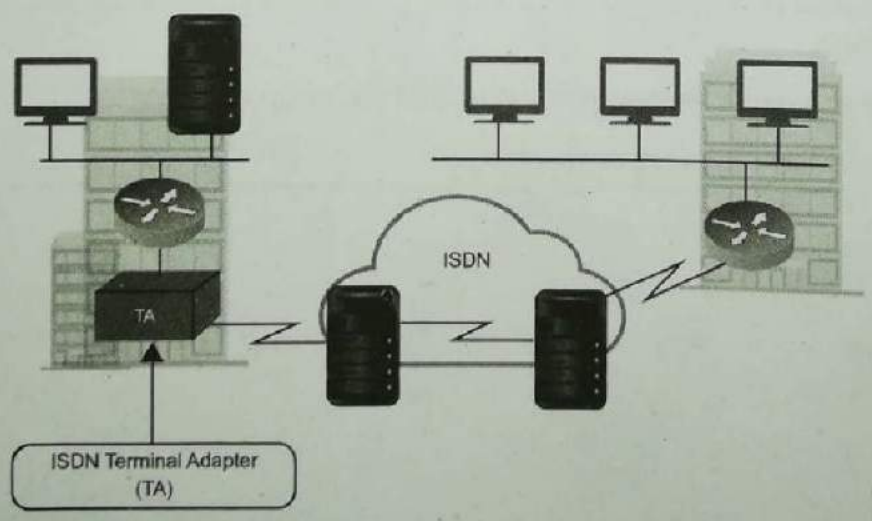


Figure 6: ISDN

Scanned by CamScanner

The traditional Plain Old Telephone Service (POTS) provides low-speed data connectivity over PSTN using an analogue modem. Integrated Services Digital Network (ISDN) is a circuit-switched technology that digitally transmits voice and data simultaneously over a 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 call setup time less than a second. The 64 Kbps bearer channel provides greater capacity than an analogue modem connection. Hence, as compared to the analogue dial up, ISDN provides better remote area connectivity with increased bandwidth, reduced latency, reduced call setup time, and lower signal to noise ratio.

Frame Relay

Figure 7 illustrates the working of Frame Relay network:

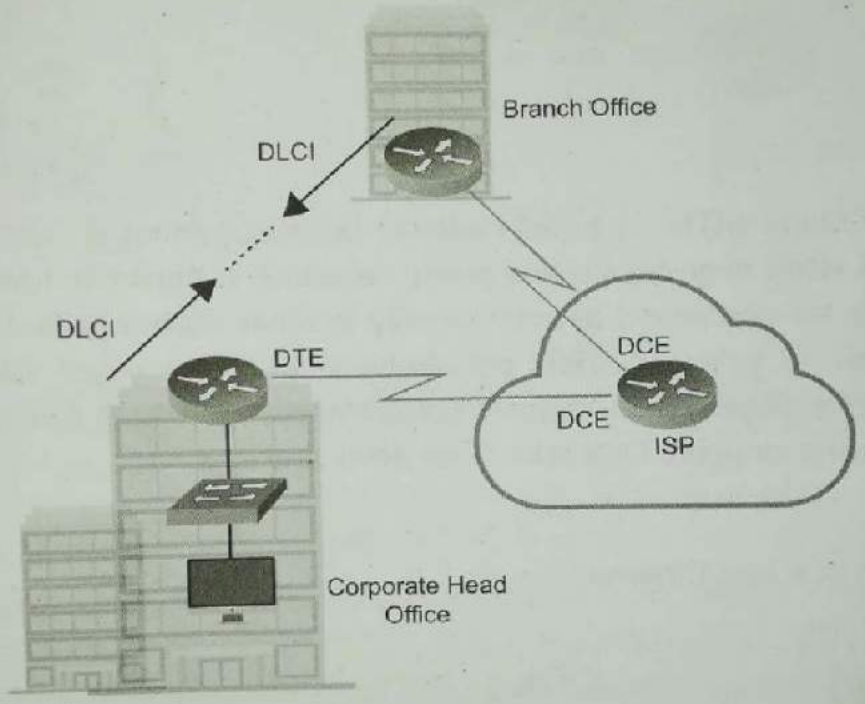


Figure 7: Frame Relay

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 4 Mbps 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). Bidirectional communication among two DTE devices is ensured by PVCs.

Scanned by CamScanner

Asynchronous Transfer Mode

Figure 8 displays the working of the ATM:

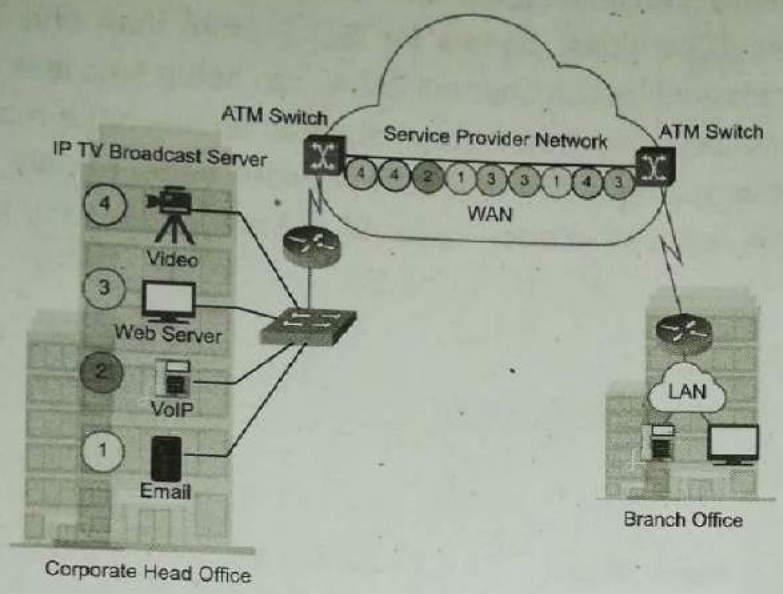


Figure 8: ATM

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 transmissions. Hence, an ATM is suitable for businesses and networks having stringent QoS criteria for delay and loss.

Metro Ethernet

Figure 9 displays the working of metro Ethernet:

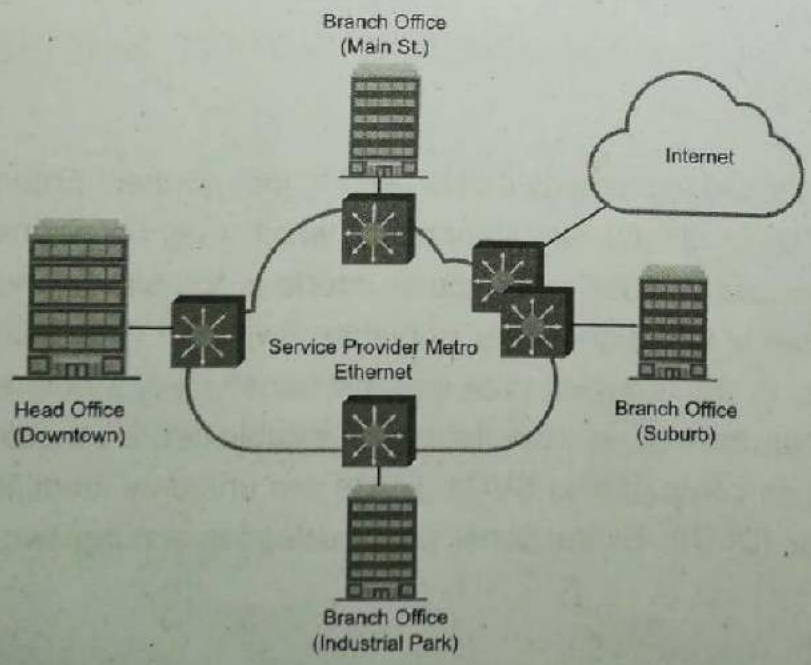


Figure 9: Metro Ethernet

Scanned by CamScanner

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. Enterprises can easily meet QoS requirements with high-performance network delivering converged data, voice, and video in a MAN using the metro Ethernet technology.

DSL Technologies

Figure 10 shows the working of DSL:

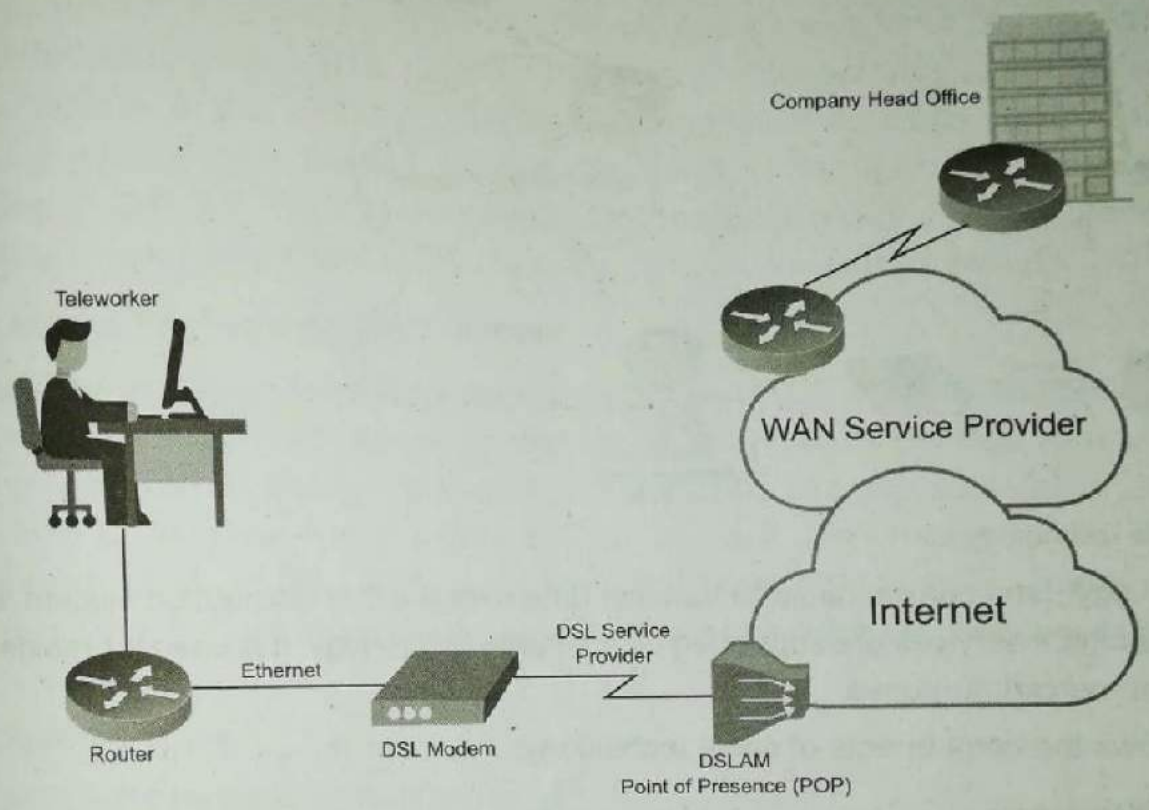


Figure 10: DSL

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.

Scanned by CamScanner

Cable Technology

Figure 11 illustrates cable technology:

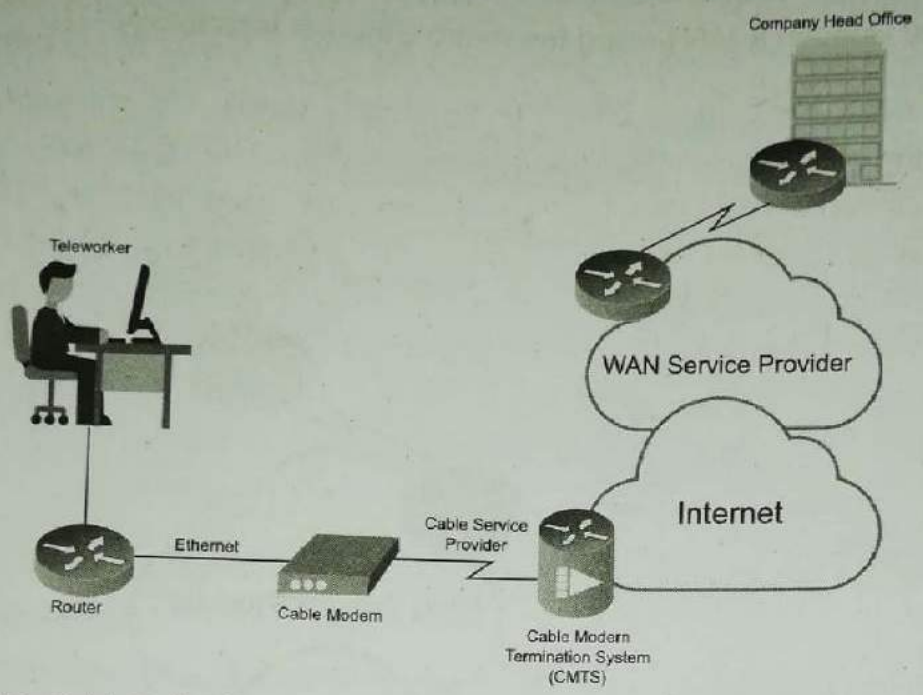


Figure 11: Cable Technology

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

Figure 12 shows the components of cable technology:

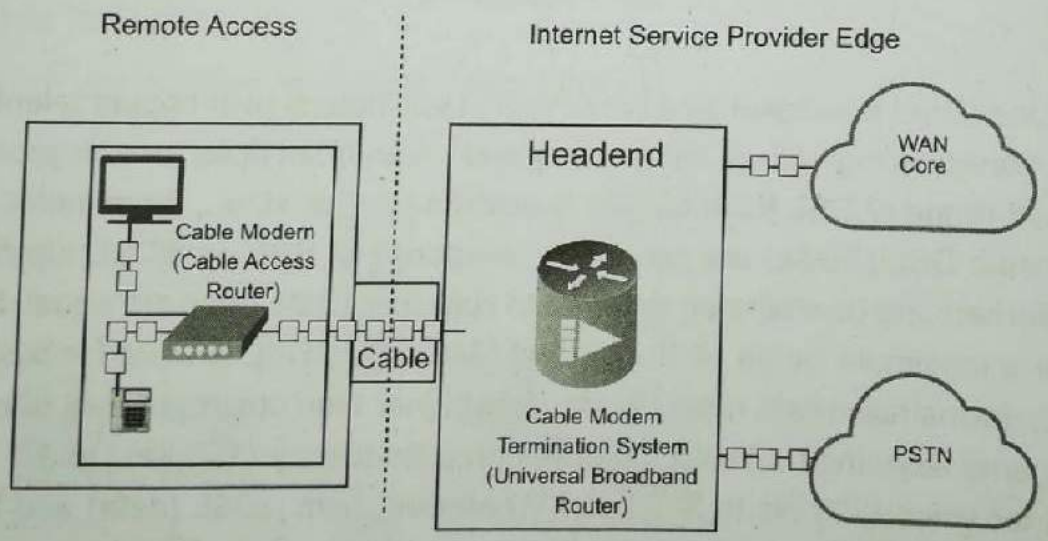


Figure 12: Cable Technology Components

Various components that are used for voice and data transmissions over the cable technology are shown in Figure 12. As depicted in the figure, the customer is at the remote access end and has a cable modem, also known as a cable access router, installed at his/her location. A cable modem supports voice, fax calls, and modem transmission over a cable network

Scanned by CamScanner

for small businesses, branch offices, and corporate telecommuters. At client's headend, a Universal Broadband Router terminates the cable modem system of the customer. Hence, the Universal Broadband Router is also known as the Cable Modem Termination System (CMTS). It provides high-speed connectivity to send upstream data to PSTN or the Internet.

A cable modem from the customer's end to CMTS at the client's headend is connected via an interface as per the Data over Cable Service Interface Specification (DOCSIS) Radio Frequency (RF) Interface Specification. Two channels are used for communication between the cable modem and CMTS. One channel is for the downstream signal from CMTS to the cable modem. In this, CMTS modulates the signal for transmission across a cable before sending it to the cable modem. Another channel is for the upstream signal from the cable modem to CMTS. In this, CMTS converts the received signal from the cable modem into IP packets before forwarding it to the router for transmission to the Internet.

Wireless Technologies

Wireless technology allows electromagnetic waves, which are used as transmission media, to carry radio frequency signals. Wires, cables or any other physical medium is not used for transmission in the wireless technology. Mobile phones, satellite TV, wireless LAN (WLAN), Global Positioning System (GPS), etc., are all examples of the applications of wireless technology. This technology can be implemented in three prominent ways, viz. bridged wireless, mobile wireless, and WLAN. Let us have an overview of each of these implementations.

Bridged Wireless

Figure 13 displays a bridged wireless network:

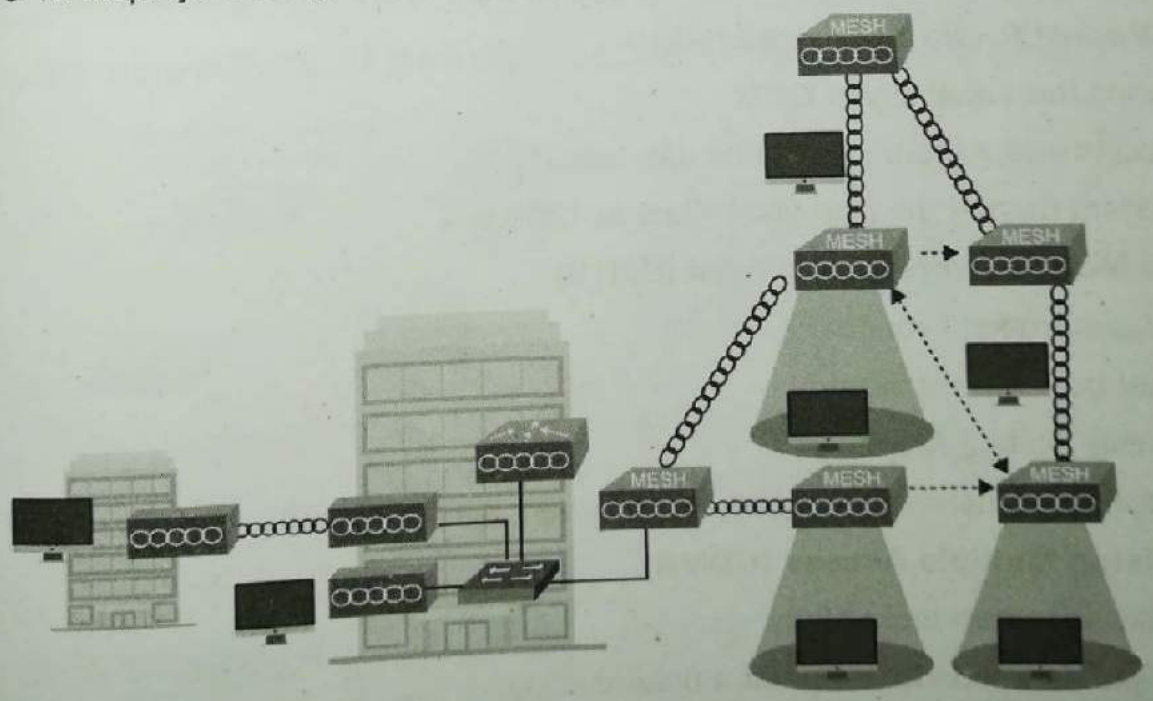


Figure 13: Bridged Wireless Network

Scanned by CamScanner

- Connects two or more networks
- Provides high-speed connectivity for data-intensive, line-of-sight applications
- Distant sites, hard to wire sites or non-contiguous floors can be connected as a single LAN by a series of wireless bridges or routers

Mobile Wireless

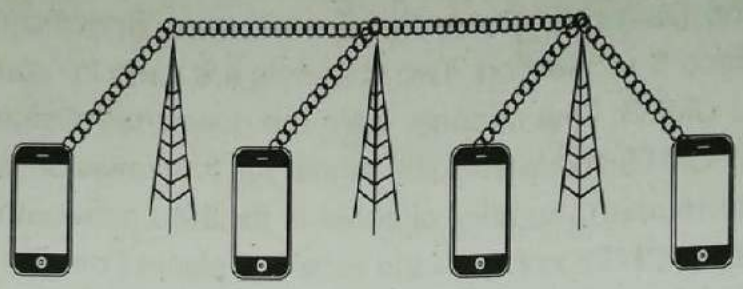


Figure 14: Mobile Wireless Network

- Connects cellular voice and data applications
- Provides better connectivity and higher speed
- **Global System for Mobile (GSM)**
  - A digital mobile radio standard.
  - It uses Time Division Multiple Access (TDMA) technology.
  - It has three different bands, i.e. 900, 1800, 1900 MHz.
  - Each band allows eight calls simultaneously.
  - It transfers data at the rate of 9.6 Kbps.
  - It supports international roaming through an agreement among operators.
- **General Packet Radio Service (GPRS)**
  - Extends the capability of GSM
  - Supports intermittent and bursty data transfer
  - Transfers data at the rate of 64 Kbps to 128 Kbps
- **Universal Mobile Telephone Service (UMTS)**
  - Third generation broadband
  - Packet-based transmission
  - Data rate up to 2 Mbps
  - Support for transmission of text, voice, video, and multimedia
- **Code Division Multiple Access (CDMA)**
  - Spread-spectrum technology
  - Each conversation is assigned a unique code
  - Pseudo-random digital sequence is used for encoding

Scanned by CamScanner

WLAN

Figure 15 displays a wireless LAN network:

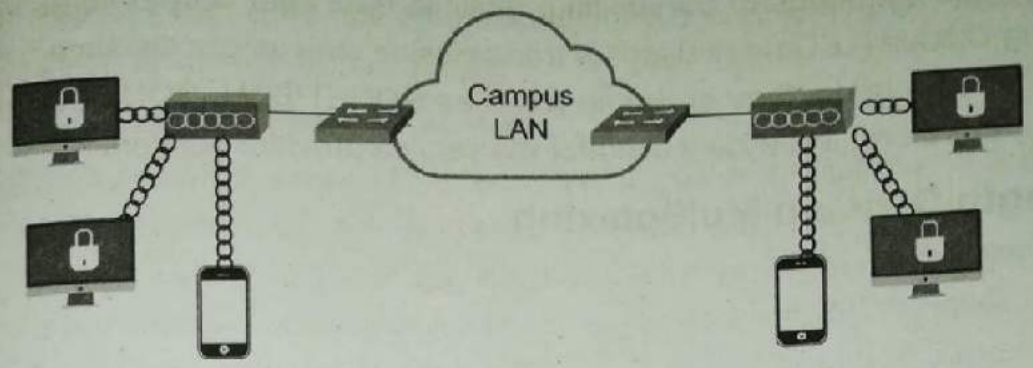


Figure 15: Wireless LAN

- Supports a LAN connection wirelessly
- Supports an intrabuilding wireless connection
- Extends the capabilities of a wired network
- Guest access and advanced security are examples of WLAN applications and services

Table 2 shows wireless LAN standards:

Table 2: Wireless LAN Standards

IEEE Standard	Band	Speed
IEEE 802.11a	5 GHz	54 Mbps
IEEE 802.11b	2.4 GHz	11 Mbps
IEEE 802.11g	2.4 GHz	54 Mbps

Synchronous Optical Network and Synchronous Digital Hierarchy

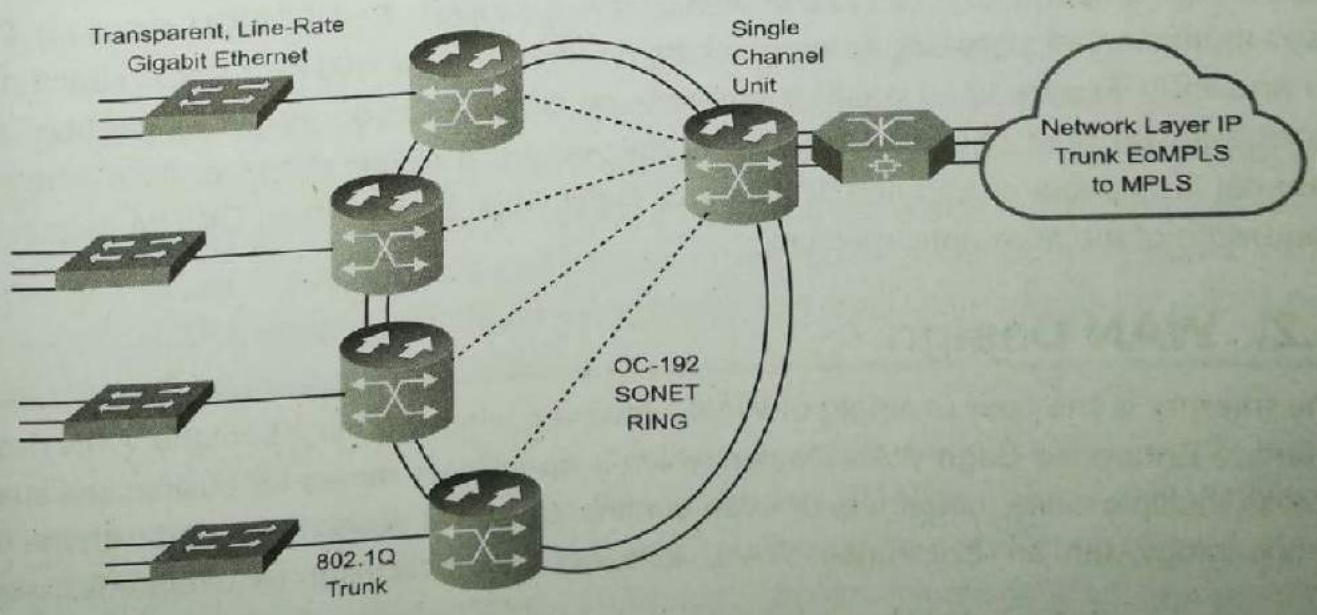


Figure 16: SONET/SDH

Scanned by CamScanner

Synchronous Optical Network (SONET) is an American-based ANSI standard whereas Synchronous Digital Hierarchy (SDH) is a European-based ETSI and ITU standard for SONET. Both refer to the standards of transmitting multiple data over optical fibres where laser or Light Emitting Diodes (LEDs) are used for transmission over longer distances. Since both refer to the same standards, they are often listed as SONET/SDH. SONET/SDH has self-healing capacity; therefore, it is widely used for the service provider network.

Dense Wavelength Division Multiplexing

Figure 17 illustrates DWDM:

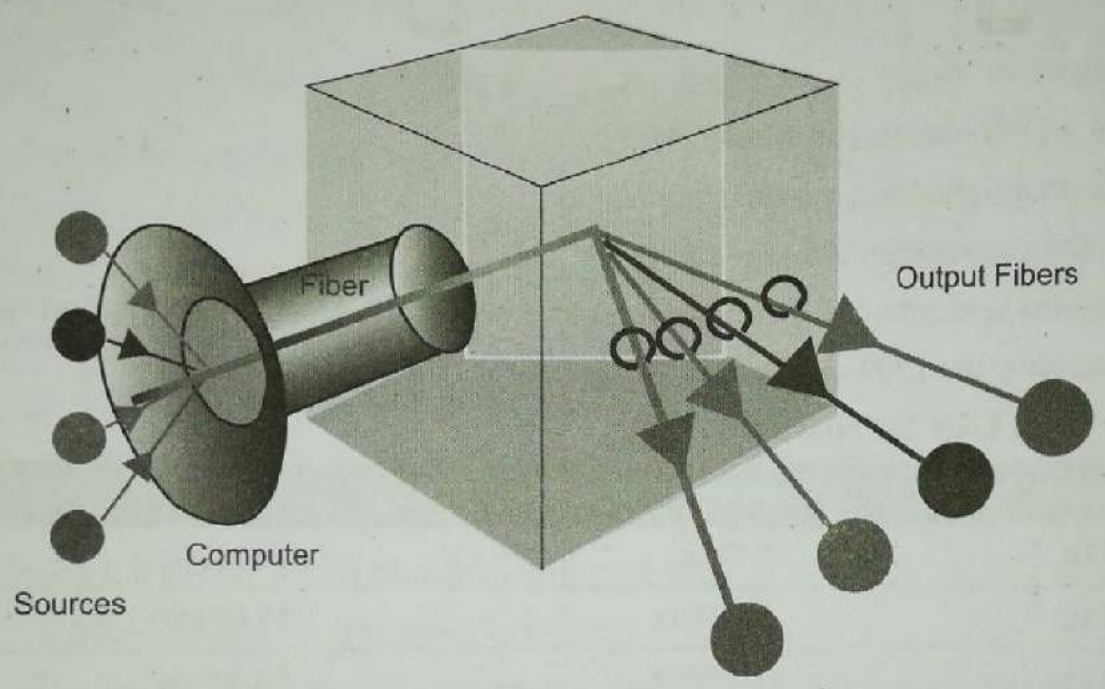


Figure 17: DWDM

Dense Wavelength Division Multiplexing (DWDM) is a technology working on fibre-optic media that supports long-range communication. It supports SONET/SDH standard. DWDM uses multichannel signalling to increase the bandwidth supported by a single strand of fibre, as shown in Figure 17. It enables bidirectional communication over a single fibre strand. More than 80 data channels can be multiplexed on a single strand of fibre where each channel is capable of carrying 10 Gbps of multiplexed signal. Thus, DWDM increases the bandwidth of the fibre-optic medium.

4.2. WAN Design

The Internet is the best example of WAN. However, when we talk about the WAN design, it refers to Enterprise Edge WAN Design which is specifically meant for businesses spanning across multiple cities, countries, or even continents. In this section, we start with the design methodology for an Enterprise WAN, followed by application requirements, technical

Scanned by CamScanner

requirements and cost consideration for the WAN design. The section concludes with bandwidth optimisation techniques for a WAN.

Based on PPDIOO methodology, described in Chapter 1, the following are the network design steps for an Enterprise WAN:

1. **Customer requirements analysis**

   This is the first step in Enterprise WAN design. It includes the analysis of business requirements and network requirements. Network applications, their types and importance level should also be considered while analysing customer requirements. Network infrastructure services such as high availability, bandwidth, security, QoS, and IP multicast required by the customers also need to be analysed. Also, based on the latest technologies and business trends, customer requirements keep on changing. All these factors need to be considered while designing an Enterprise WAN.

2. **Characterising existing network**

   The second step in designing Enterprise WAN design is to analyse the existing network and sites as the existing software, hardware and link capacity influence the network design. During this step, the existing documentation is to be reviewed along with network assessment and traffic analysis. This helps in getting an insight of the location and types of servers, network devices, power sources, redundancy, routing protocols, etc., which can be summarised as network interface, network topology, network services and network applications of the existing network. The summarised information can be used to determine whether the existing network can be extended to support new business requirements.

3. **Network topology and solution design**

   The last step in designing Enterprise WAN design is to design the network topology and solutions. The design document should brief about physical topology, routing protocol, network infrastructure services implementation, etc., while considering the existing network characteristics, customer requirements, and technical constraints.

While designing an Enterprise WAN, application requirements, technical requirements and cost of requirements serve as major trade-off factors. All these three factors are discussed further in this section. Also, the adoption of new technologies should not be restricted by network design. The network should be expandable and upgradable to easily adopt new technologies without substantial changes.

Application Requirements

Application requirements highly influence the Enterprise WAN design as they influence Enterprise Campus design, as discussed in Chapter 3. The number and types of applications form the basis of application requirements. Different applications have different requirements in terms of speed, bandwidth, memory, data storage, etc. All of these, along with high

Scanned by CamScanner

availability, throughput, reliability, and security requirements, highly influence the Enterprise WAN design. One of the most important customer requirements is application availability which is defined by throughput, response time, packet-loss and reliability. Let us discuss each of these in detail.

Table 3 shows the application requirements in 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→				

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

Scanned by CamScanner

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.

Technical Requirements

Along with application requirements, technical requirements also influence network design. Technical requirements in the network design refer to optimising network performance in terms of link utilisation and bandwidth utilisation.

Network Traffic

The end-user's requirements contradict with the network manager's requirements specifically when it comes to network performance. Response time of an application over a WAN link should be minimum as per the end-user's requirements. Contradictorily, link utilisation should be the maximum from the network manager's perspective. As discussed in the previous section, longer response time may indicate to a user that the application is down. Thus, the response time directly affects a user's experience. 120 ms response time may be considered as a delayed response by an end-user but does not hold any significance for the network manager. The network manager is concerned about link utilisation whereas the end-user is least bothered about it.

Scanned by CamScanner

Figure 18 shows the optimal network traffic:

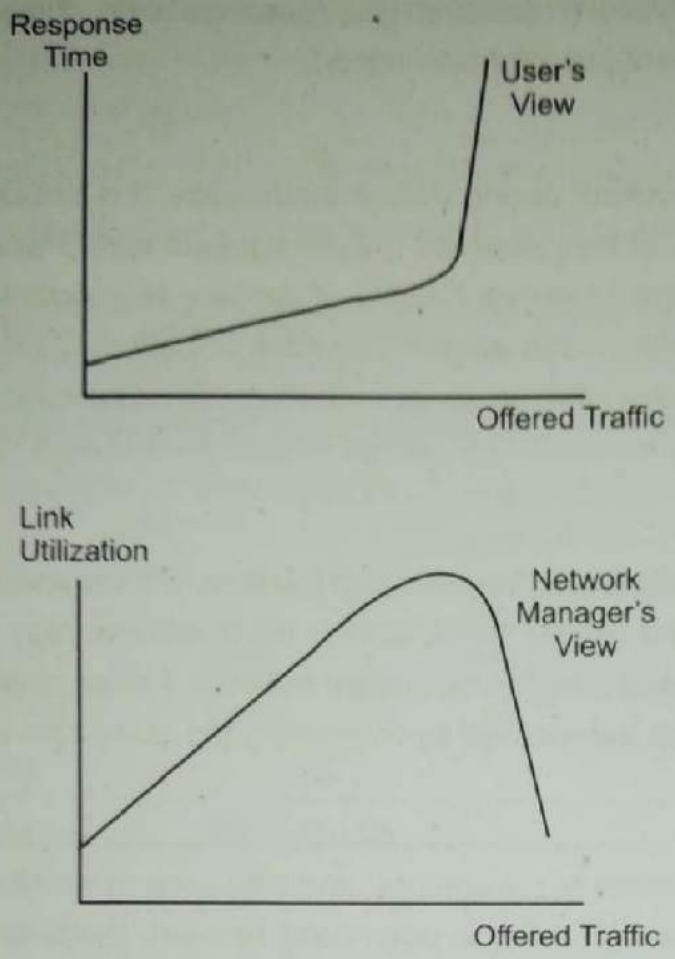


Figure 18: Optimal Network Traffic

Figure 18 contains two graphs. In the response time vs offered traffic graph, as the network traffic increases, response time also increases. At one point, the network traffic increases to such an extent that it leads to unacceptable response time. When it comes to link utilisation vs offered traffic, as the network traffic increases, link utilisation increases. However, after a certain point, the increase in network traffic results in link saturation. Thus, network traffic needs to be optimised so that the minimum response time can be offered to the end-users over a link that is optimally utilised. Link utilisation also serves as an indicator to increase WAN capacity. 50% link utilisation indicates that planning for additional WAN capacity should begin. 60% link utilisation indicates that additional WAN capacity should be purchased. 75% link utilisation indicates that its high time to increase the WAN capacity.

Scanned by CamScanner

Bandwidth

Table 4 shows the Bandwidth of WAN Media:

Table 4: WAN Media Bandwidth

WAN Media Type	Bandwidth			
	<=1.5/2 Mbps (Low)	From 1.5/2 Mbps to 45/34 Mbps (Medium)	From 45/34 Mbps to 100 Mbps (High)	From 100 Mbps to 10 Gbps (Higher)
Copper	Serial or asynchronous serial, ISDN, TDM (DSO, E1/ T1), X25, Frame Relay, ADSL	LRE (up to 15 Mbps), ADSL (8 Mbps downstream)		
Fiber		Ethernet, TDM (T3/E3)	Fast Ethernet, ATM over SONET/ SDH,POS[1]	Gigabit Ethernet, 10 Gigabit Ethernet, ATM over SONET/ SDH,POS
Coaxial		Shared bandwidth; 27 Mbps downstream, 2.5 Mbps upstream		
2.4 or 5 GHz WAN Wireless		Varies, based on distance and RF quality		

The bandwidth of a network is the quantity of data that can be transmitted or received per unit time. Bandwidth adequate for one application may not be sufficient for another application. This is because as the data complexity increases, bandwidth requirement increases. It takes more bandwidth to download a video than downloading a photograph in a specific time. Therefore, the selection of physical media for an Enterprise WAN is determined by data complexity. For less than 2 Mbps bandwidth, ADSL, ISDN, TDM, Frame Relay, X25 WAN transport technologies are preferred. Ethernet and TDM (T3/S3) can support a medium bandwidth requirement. The coaxial cable supports shared bandwidth with 27 Mbps downstream and 2.5 Mbps upstream data transfer. ATM over SONET/SDH, Packet over SONET/SDH support bandwidth in a range of 45 Mbps up to 10 Gbps. Fast Ethernet supports bandwidth up to 100 Mbps. For higher bandwidth requirements, Gigabit Ethernet and 10 Gigabit Ethernet can be

Scanned by CamScanner

used. Application requirements must be considered while selecting physical media for an Enterprise WAN.

WAN Ownership

WAN links can be private, leased, or shared. Let us have an overview of each one of them.

Private WAN

A private WAN provides high security and a better transmission rate. For a private WAN, the owner needs to buy physical media, such as copper, fibre, coaxial cable, or wireless, and configure the physical layer connectivity. Similarly, the terminal equipment also needs to be bought and configured by the WAN owner. Thus, building a WAN infrastructure is an expensive task. The WAN owner needs to maintain both the physical layer connectivity and terminal equipment, which is a labour-intensive task. Business changes may demand for WAN reconfiguration. This is a difficult job and needs to be carried out by the WAN owner.

Leased WAN

In this WAN, dedicated bandwidth is obtained from a carrier provider for a TDM or SONET circuit. However, the terminal equipment may be private or leased. Both configuration and maintenance of the circuit is provided by the provider. Operating costs in a leased WAN are high irrespective of the bandwidth utilisation; the company needs to pay for the allocated bandwidth.

Shared WAN

As in a leased WAN, in a shared WAN, the provider provisions and maintains the circuit; however, this circuit is shared by many users. In shared WANs, the circuits are circuit-switched or packet-switched transport networks. MPLS and Frame Relay are prominent examples of a shared WAN.

Bandwidth Optimisation

The overall performance of a network can be improved by optimising the bandwidth. Let us discuss few techniques to optimise bandwidth.

Data Compression

Data compression refers to the technique of reducing the data size for data transmission. As the size of data is reduced, the time required to transmit the data reduces, and hence the transmission time is saved. Also, the reduced data size results in the transmission of more data in a specified time. Thus, through data compression, the available yet limited bandwidth can be more efficiently utilised. As data compression increases, network latency decreases. Data compression can be in three ways, viz. header only, payload only, and entire packet (header + payload). Encoding techniques used to compress data include statistical compression and dictionary compression. The non-adaptive encoding method is used in the statistical compression technique. Therefore, statistical compression is preferable

Scanned by CamScanner

for applications having predictable or consistent data. However, this is a rare scenario in internetworks as the traffic is unpredictable and inconsistent. To handle unpredictable and inconsistent network traffic, the compression technique should be responsive to variations in data. One such technique is dictionary compression. The Lempel-Ziv algorithm is an example of dictionary compression. In this technique, codes are used to replace continuous streams of characters.

Real-Time Transport Protocol is used for applications demanding real-time transmission such as audio, video, etc. Compressed Real-Time Transfer Protocol (CRTP) compresses the headers of audio from 40 bytes to 2 or 4 bytes. Since the data size is reduced drastically, the bandwidth is optimally utilised. Data compression techniques can also be categorised as software-based and hardware-based. In software-based data compression techniques, compression is carried out by CPU. In hardware-based data compression techniques, the compression is carried out by circuits specially designed for compression. Therefore, a hardware-based data compression technique is faster than a software-based data compression technique.

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 the DSL internet service, PPPoE or PPPoA is used. When extra bandwidth is required between two computers, multiple physical communication links are connected by using Multilink PPP (MLP). The bandwidth of these 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.

Scanned by CamScanner

4.3. Using WAN Technologies

As discussed earlier, customer requirements influence the WAN design. The efficiency of the network can be increased by selecting an appropriate WAN technology. Various WAN technologies can be used for varied purposes such as remote access, VPNs, WAN backup, and the Internet as a backup WAN.

Remote Access Network Design

Access to a remote network can be provided using a data link or a network layer connection. The selection of remote access technologies depends on application requirements and service provider offerings. For connecting a remote site with Enterprise Edge network, data link layer WAN technologies are used. But it incurs high investment and operational costs. Interactive traffic including small to medium file transfer is supported. Remote teleworkers need to have either dedicated connection or provisioned service to the Enterprise Edge. Examples of remote access technology for permanent connection include cable, DSL and dialup. For mobile teleworkers, an on-demand connection is required. Examples include hotspot wireless service.

VPN Design

A Virtual Private Network refers to a private network over a shared infrastructure such as the Internet, Frame Relay Network, and ATM. **Access VPN** enables access to a corporate network over shared infrastructure without compromising security. Access VPNs can be client-initiated or Network Access Server (NAS)-initiated. In a client-initiated VPN, the client initiates the connection to the corporate network by establishing encrypted IP tunnel over shared infrastructure from the remote user to the corporate network. In NAS-initiated VPN, SP initiates encrypted tunnel establishment to the corporate network on receiving a request from the remote user. In **Intranet VPN**, the corporate network is extended across remote offices using the Internet or SP infrastructure. Since the Internet is used for connectivity, performance cannot be guaranteed but operational costs are reduced. To extend the corporate network to customers, suppliers and business partners, **Extranet VPN**s are used. Even in this VPN, the Internet or SP infrastructure is used for connectivity. Hence, security is a major concern.

VPN Connectivity Options

IP access through VPNs can be provided through three different options viz. Overlay VPNs, Virtual Private Dial-up Networks (VPDN) and Peer-to-peer VPNs. In Overlay VPNs, virtual point-to-point connection is provided over provider's network. For the implementation of Overlay VPN, different technologies at Layer 1 and Layer 2 such as Frame Relay, ATM, ISDN, and SONET/SDH are used. In Overlay VPNs, each individual virtual connection must

Scanned by CamScanner

be established along with providing sufficient bandwidth. Hence, maintenance of overlay networks is costly.

Figure 19 displays the Overlay VPN:

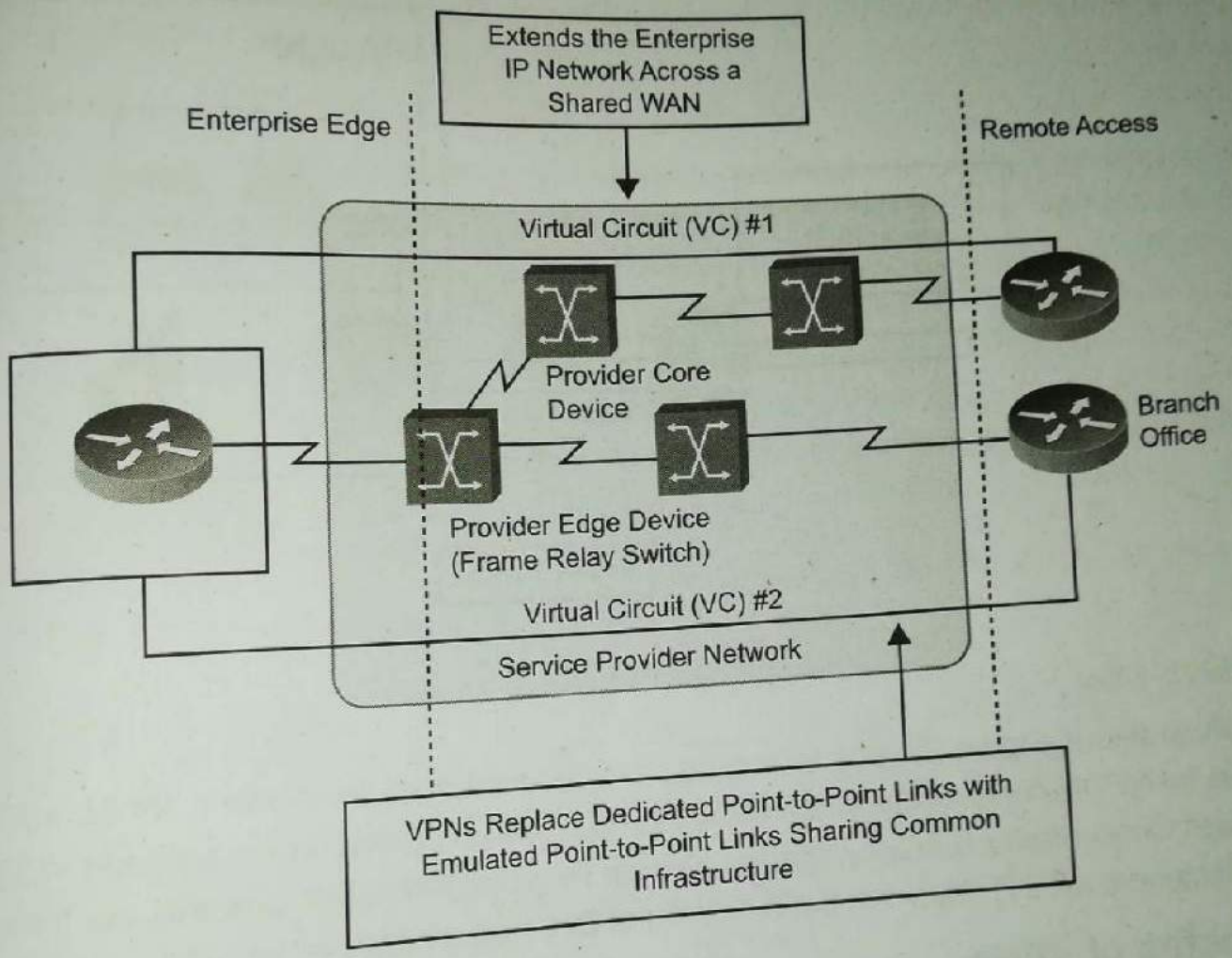


Figure 19: Overlay VPN

As depicted in Figure 19, Enterprise Edge router is directly connected to the Service Provider network. Also, Enterprise Edge is connected to the router on the top and the router of the Branch Office through Virtual Circuit 1 and Virtual Circuit 2, respectively, provisioned over Service Provider network.

VPDNs rely on SP for secure connectivity. VPDN has the capability of working on any access technology such as ISDN, xDSL, cable and modem. SP provides connectivity till the enterprise's gateway through a virtual tunnel or a point-to-point tunnel. Enterprise has the control of network configuration and security.

Scanned by CamScanner

Figure 20 displays a VPDN:

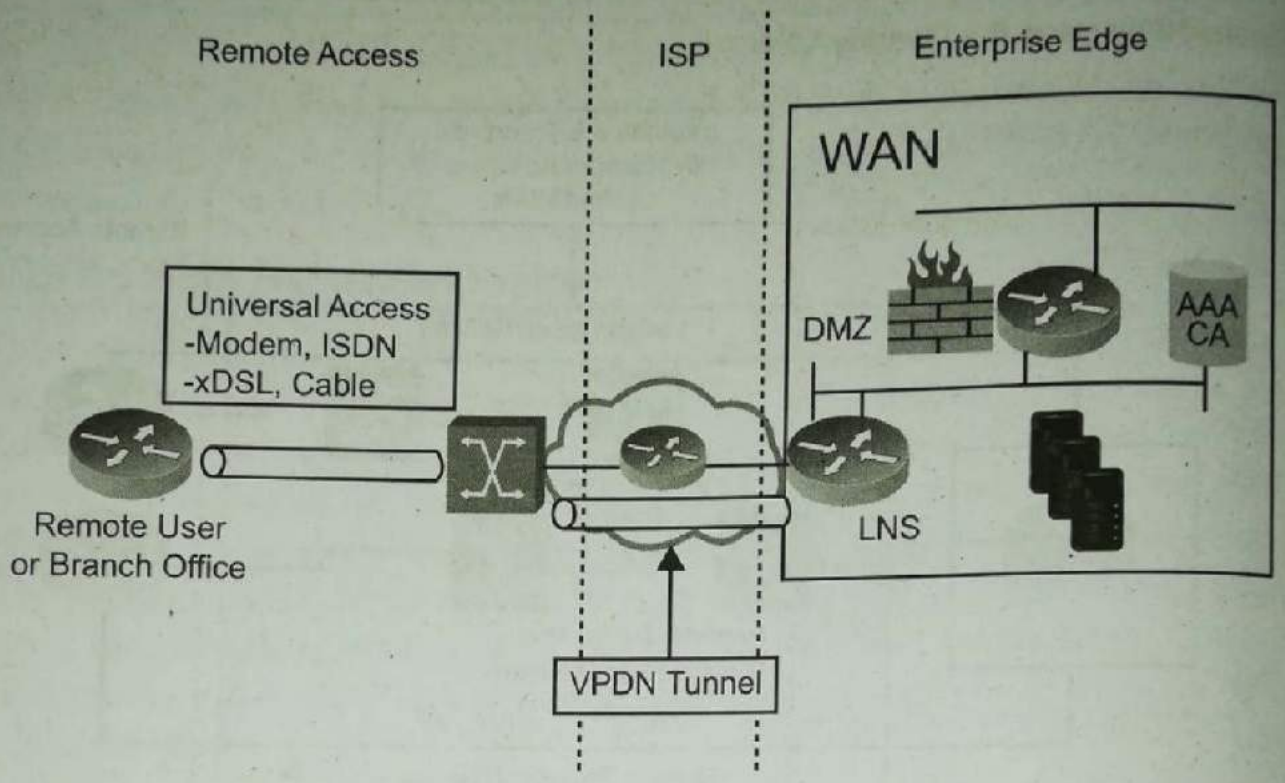


Figure 20: VPDN

As illustrated in Figure 20, any technology can be used such as modem, ISDN, xDSL and cable for VPDN connectivity at a remote site. But dial up connection is terminated at L2TP Access Concentrator (LAC) by Internet Service Provider (ISP). ISP forwards the traffic over VPDN tunnel to L2TP Network Server (LNS) at Enterprise Edge.

Benefits of VPNs

VPNs can quickly extend corporate network to the remote users over the existing infrastructure such as the Internet or SP network. Similarly, business partners, customers, suppliers can access corporate network using Extranet VPN. Thus, VPNs offer flexibility to setup quick yet secure connections for remote access. Security policies can be configured on VPN based on domain requirements. WAN is extended to remote users and teleworkers by the use of VPN over the Internet. Thus, a VPN easily offers scalability of WAN at lower costs.

WAN Backup Strategies

WAN links are unreliable and slower as compared to LAN links. To ensure high availability, strategies must be defined for WAN Backup through redundancy. The purpose is to minimise downtime in branch offices when the primary link fails. For backup, either dialup can be used to establish connection to a remote site, or a permanent secondary WAN link can be deployed.

Scanned by CamScanner

Dial Backup Routing

WAN connectivity to remote users is generally provided using a point-to-point or Frame Relay connection. When the primary link fails, the router detects link failure and subsequently initiates a dial up switched circuit connection. Once the primary link is up, this dial up connection is terminated.

Secondary WAN Link

Another option for WAN backup is to deploy a permanent secondary WAN link in the corporate network to connect remote sites. When the primary link fails, the secondary WAN backup link is activated. Routers automatically detect the primary link failure using routing protocols such as EIGRP and OSPF. On primary link failure, traffic is redirected to an alternative link. Thus, a permanent secondary WAN link makes the remote connectivity to the enterprise network fault tolerant and ensures high availability. Apart from primary link failure, the secondary WAN link can also be used to increase bandwidth of the network and hence, decrease application response time to the remote users. Load balancing is automatically performed by routing protocols.

Figure 21 shows the Secondary WAN Link:

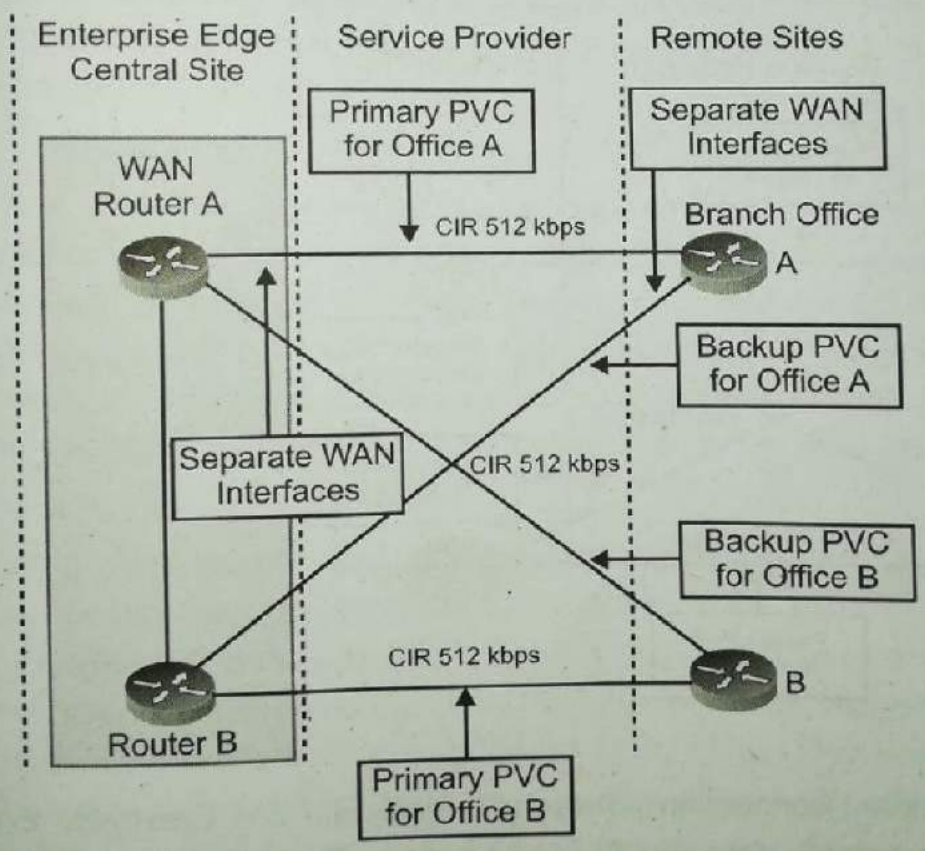


Figure 21: Secondary WAN Link

Scanned by CamScanner

As depicted in Figure 21, Branch Office A at the Remote Site is connected to WAN Router A at Enterprise Edge through Primary Permanent Virtual Circuit (PVC). Simultaneously, Branch Office A at the Remote Site is connected to WAN Router B at Enterprise Edge through Secondary PVC, i.e. Backup Primary PVC. This Backup Primary PVC adds redundancy to the WAN link. For load balancing, a routing protocol is used to increase utilisation. Load balancing can be done in two ways viz. per-packet load balancing and per-destination load balancing. Per-packet load balancing is preferred for WAN links having speed up to 56 kbps. For WAN links faster than 56 kbps, per-destination load balancing is used. One of the important points to note is that apart from fault-tolerance, availability and utilisation, the cost of the network is also increased.

Shadow PVC

Shadow PVC is an additional WAN link connecting the Branch Office of a Remote Site to the Enterprise Edge Central Site. Such a secondary PVC is provided by SP without any additional charge if the load on the shadow PVC does not exceed one-fourth of the load on Primary PVC. If the load on Shadow PVC exceeds the set traffic limit, SP charges for the additional load.

Figure 22 displays the Shadow PVC:

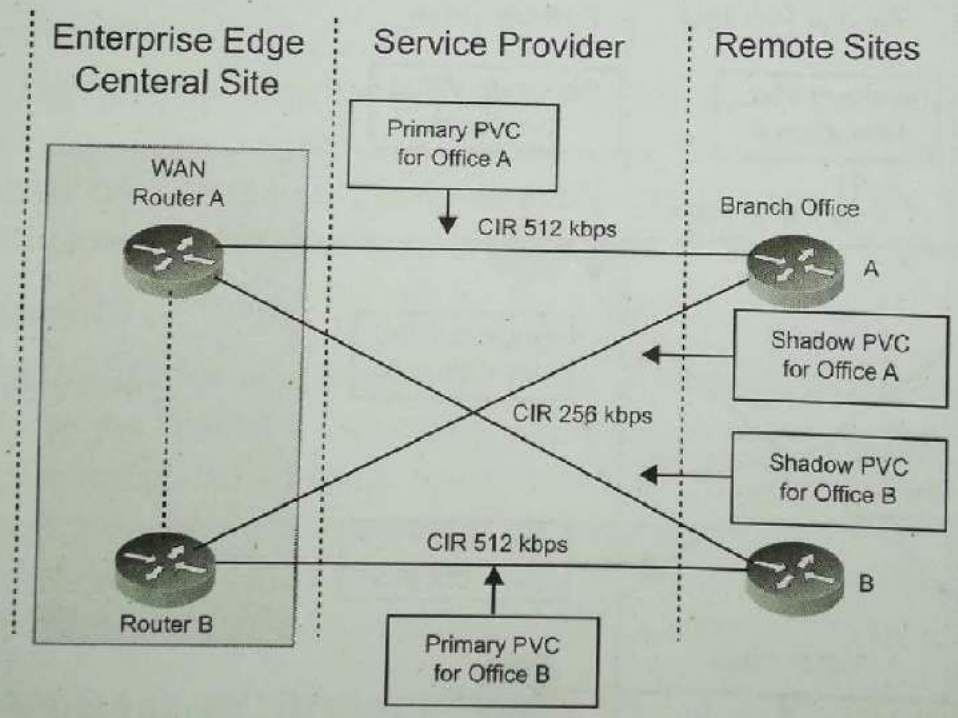


Figure 22: Shadow PVC

Shadow PVC for the redundant connection between Remote Site and Enterprise Edge is depicted in Figure 22. Unnecessary data should not be sent on Shadow PVC as extra load incurs additional charges.

Scanned by CamScanner

The Internet as a WAN Backup Technology

Apart from methods discussed in the previous section, the Internet is an alternative for WAN backup. A private network can be established over a public network by IP routing as well as Layer 3 tunnelling. In IP Routing without any constraint, the data is sent over the Internet in an unencrypted form. An enterprise needs to make its Internet Service Provider aware that the Internet is used as backup for Remote Site connectivity. Another approach is to use IPsec Layer 3 tunnelling to connect two non-contiguous private networks over the public infrastructure. IPsec is a security protocol for tunnel encapsulation. The sensitive data can be transmitted securely, in encrypted form, over the unprotected Internet by using IPsec. An IPsec sender encrypts the data before sending and the packet can be authenticated by the IPsec receiver that the data has not been altered with. Along with the content, the source of the packet can also be authenticated and checked for integrity. The IPsec receiver has the ability to detect and reject duplicate packets. Internet Key Exchange (IKE) is used for automated key management in IPsec. Also, IPsec is easily deployable without any changes in the intermediate system or existing applications.

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.

Scanned by CamScanner

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.

Scanned by CamScanner

Table 5 shows Enterprise WAN architecture technologies:

Table 5: Enterprise WAN Architecture Technologies

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

Private WAN

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

Scanned by CamScanner

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

Scanned by CamScanner

Figure 23 shows a sample Enterprise WAN architecture:

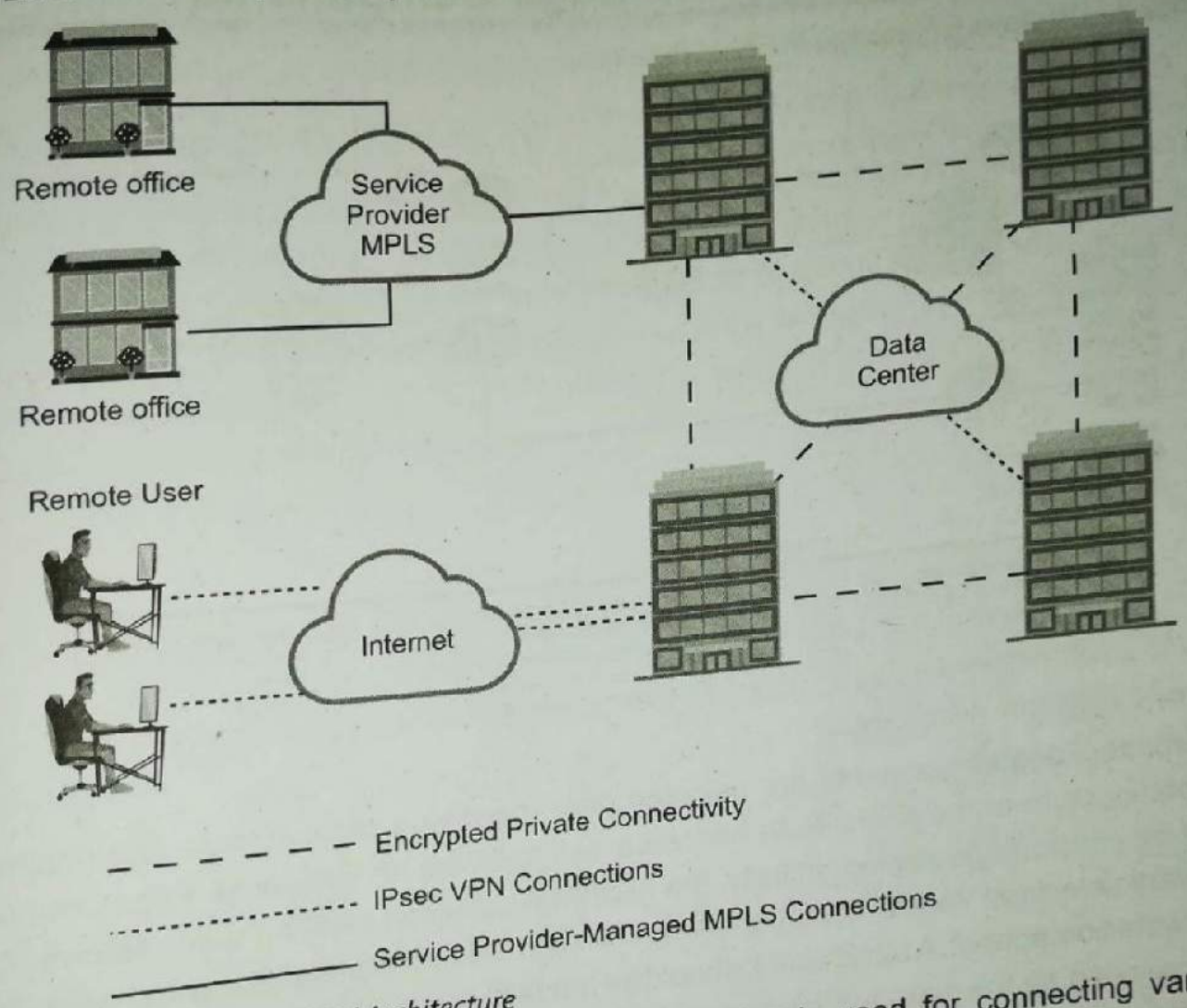


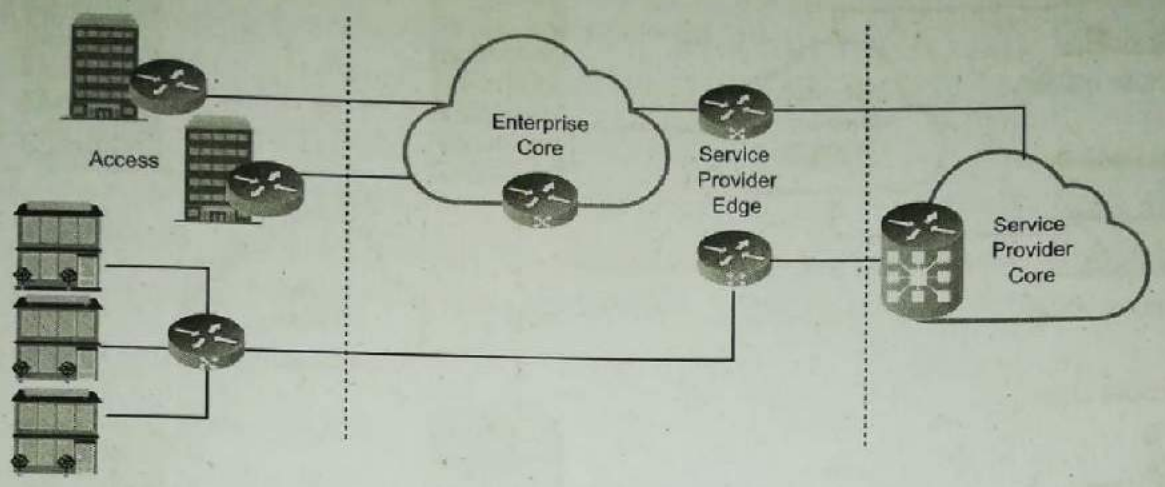
Figure 23: Sample Enterprise WAN Architecture

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

Scanned by CamScanner

4.5. Selecting Enterprise Edge Components

Figure 24 displays Enterprise WAN software:



- Broadband access
- Mobility and wireless
- Data centeer
- Security
- IP communications

- High-end enterprise core
- Service provider edge
- Virtual Private Networks (MPLS, Layer 2, and Layer 3)
- Video and content multicast

- Large-scale networks
- High availability
- In-service software upgrade

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.

Scanned by CamScanner

4.6. Enterprise Branch and Teleworker Design

This section provides insight on architecture design of Enterprise Branch and Teleworker.

Enterprise Branch Architecture

As discussed in Chapter 2, section 'Functional Areas of the Cisco Enterprise Architecture', Enterprise Branch and Enterprise Teleworker module extend services and applications at the head-office to all the branches and end-users at a remote location. The aim is to provide a single IP network for enterprises with improved productivity, increased security and reduced costs at all remote sites.

Figure 25 shows Enterprise Branch services:

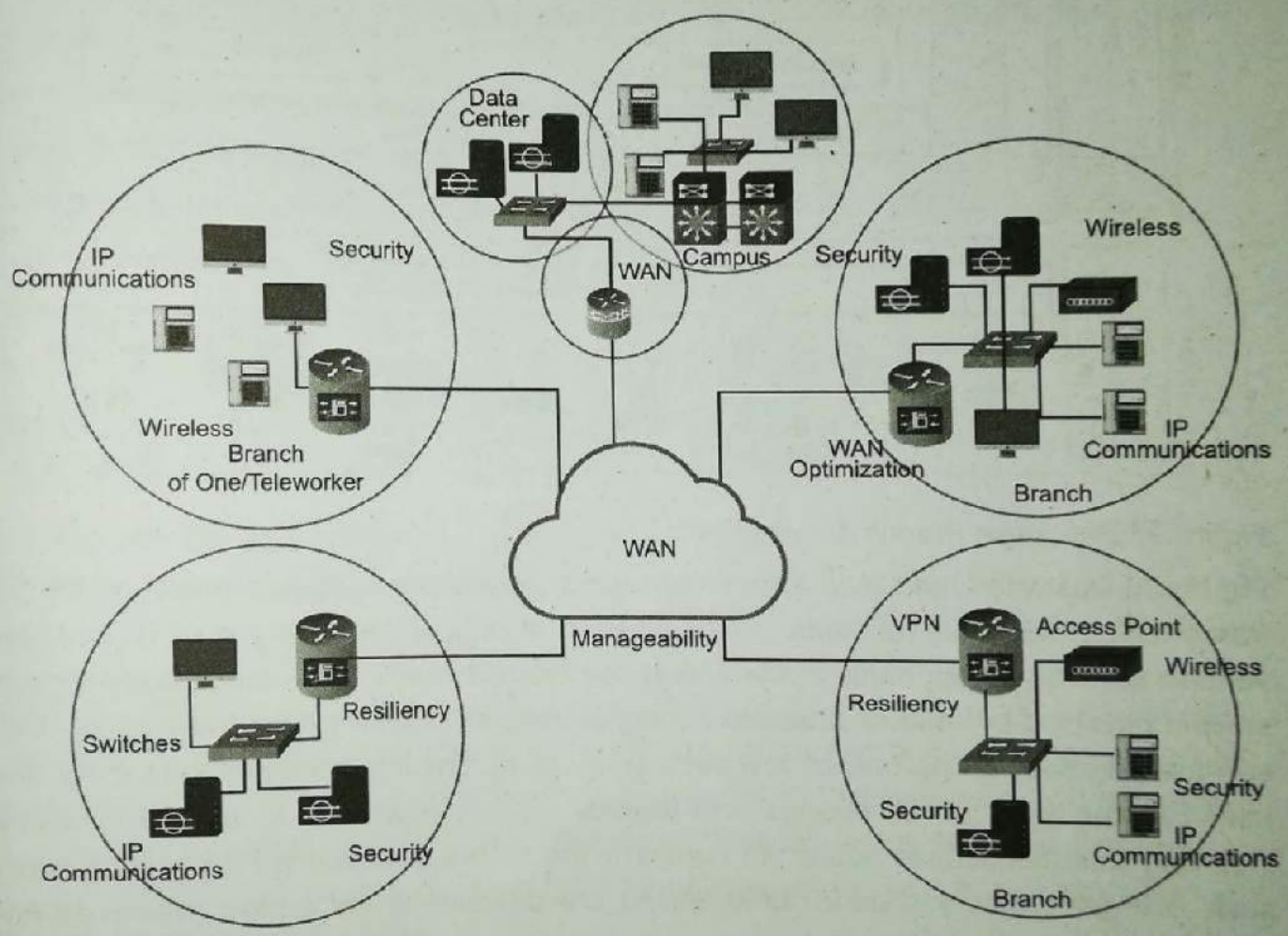


Figure 25: Enterprise Branch Services

Enterprise Branch architecture focuses on services to be provided at the Enterprise Branches irrespective of their distance and connectivity from the main location. Figure 25 illustrates different services, such as security, resiliency, manageability, and WAN optimisation, that are made available to Enterprise Branches over the WAN through VPN, wireless, IP communications and other connectivity options.

Scanned by CamScanner

Figure 26 shows the Enterprise Branch architecture:

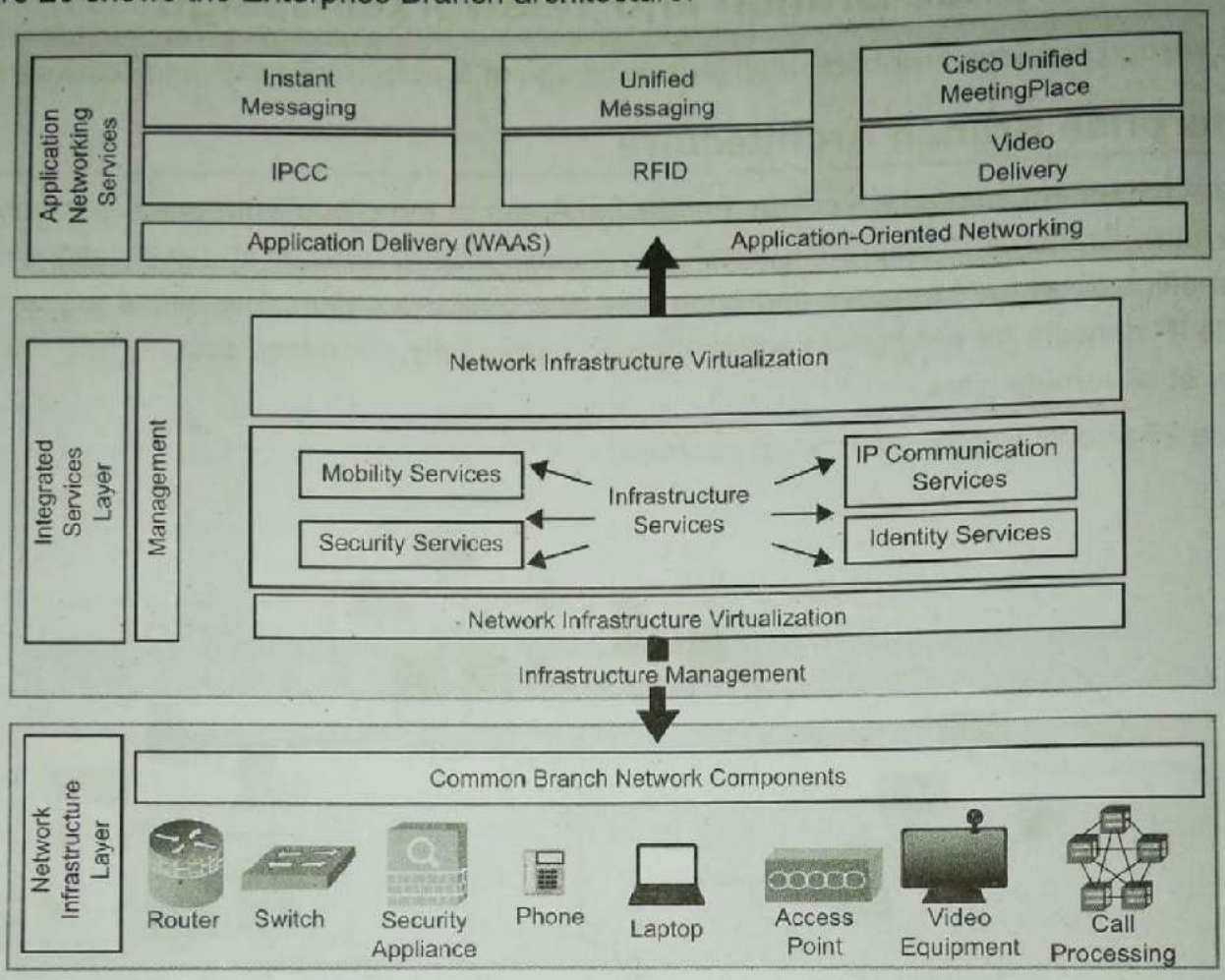


Figure 26:Enterprise Branch Architecture

Figure 26 illustrates the Cisco Enterprise Branch Architecture which is based on the SONA framework. It supports real-time communication at remote sites. This is made possible by various network components in the Enterprise Branch. WAN edge connectivity for remote sites is provided by routers where switching is used to support LAN infrastructure. Various end-user devices at the branch are secured by using security appliances. Mobility of end-user devices such as IP phones and laptops is also supported in remote locations by installing wireless access points. To consume the facility of advanced application services, such as IP telephony and video conferencing, call-processing and video equipment are used at Enterprise Branches.

Scanned by CamScanner

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.

Scanned by CamScanner

Small Branch Office Design

Figure 27 shows a Small Branch office:

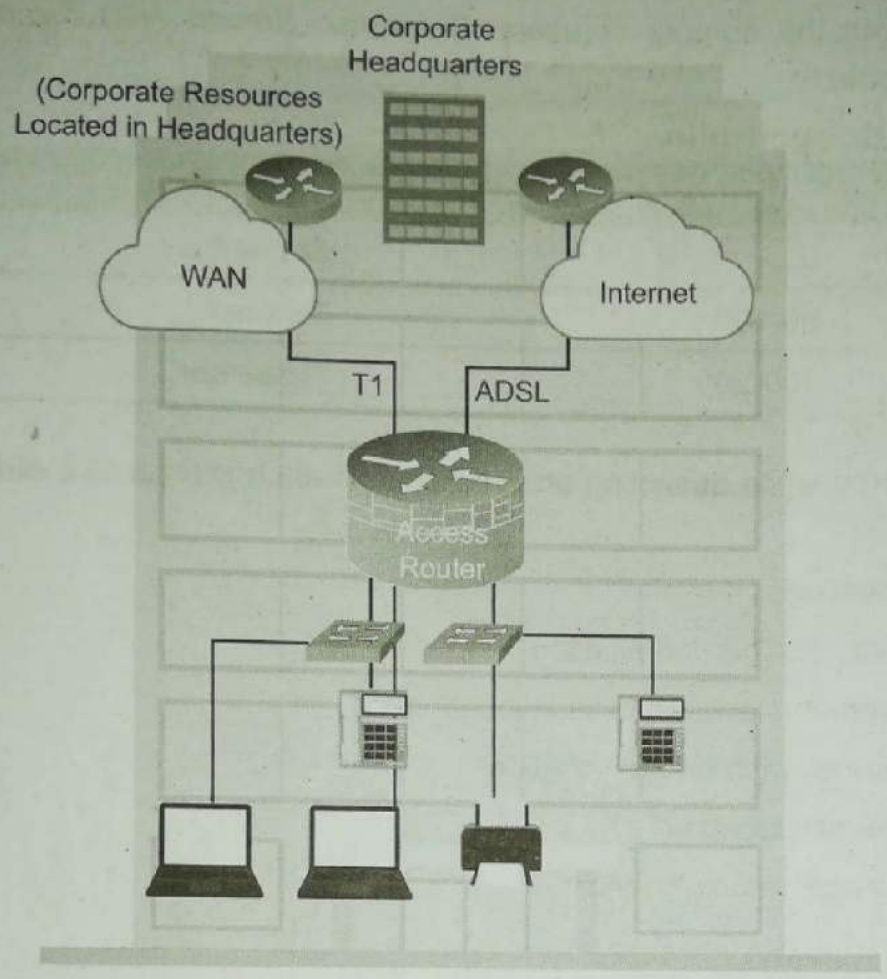


Figure 27: Small Branch Office

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.

Scanned by CamScanner

Medium Branch Office Design

Figure 28 displays a Medium Branch office:

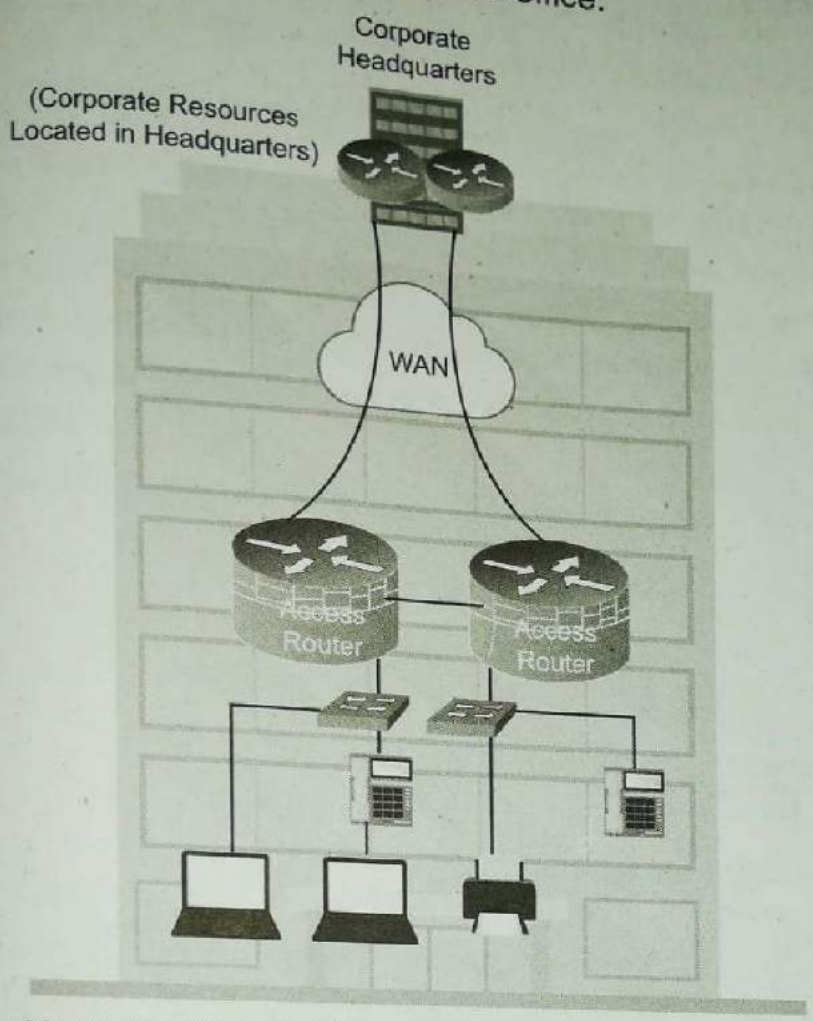


Figure 28: Medium Branch Office

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.

Scanned by CamScanner

Large Branch Office Design

Figure 29 displays a Large Branch office:

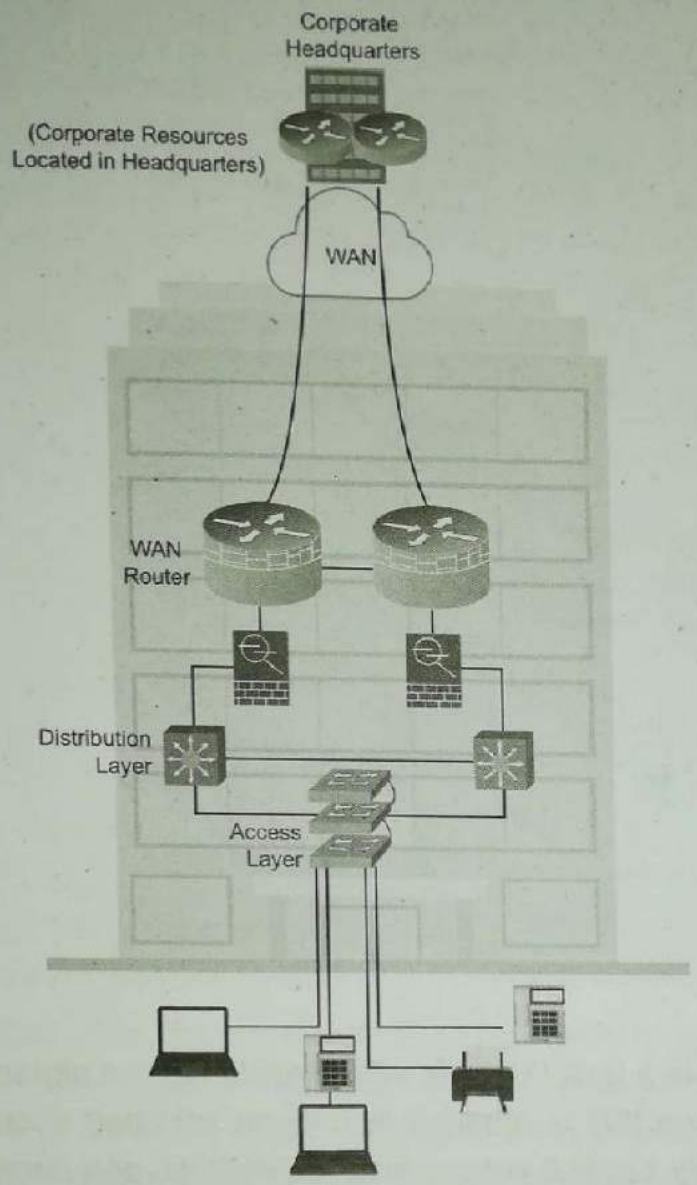


Figure 29: Large Branch Office

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

Scanned by CamScanner

is used to provide network services, and traffic shaping; policing along with scavenger class of traffic is used to provide QoS and routing redundancy protocols, such as HSRP, VRRP, GLBP, are used to ensure high availability in Large Branch offices.

Enterprise Teleworker Design

Enterprise Teleworker Design aims to provide fast and secure connectivity to employees so that they can work from their home. This helps the enterprise to retain valued customers having increased productivity and greater job satisfaction. Wireless hotspot is one of the widely used option for connectivity by occasional remote users. For Teleworkers constantly accessing all applications and services of the enterprise, the focus is on delivering seamless services.

Figure 30 displays comparison of Teleworkers:

	Occasional Users	Part-Time or Full-Time and Day Extenders
	Occasional Remote Worker	Teleworker
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
Video conferencing	Unlikely	High quality
Remote configuration and management	No	Yes
Integrated security	Basic	Full
Resiliency and availability	No	Yes

Figure 30: Teleworkers Comparison

Figure 30 illustrates the difference between Occasional Remote Workers and Teleworkers. Both have access to emails and web applications. Occasional users do not have the provision for configuration and management, resilience and availability. Nor do they get Video on demand or Videoconferencing services. On the other hand, Teleworkers working from home can configure and manage the network having high resiliency and availability. They have the provision for high-quality Voice over IP, Video on demand and Videoconferencing service.

Scanned by CamScanner

Figure 31 displays Teleworker Architecture:

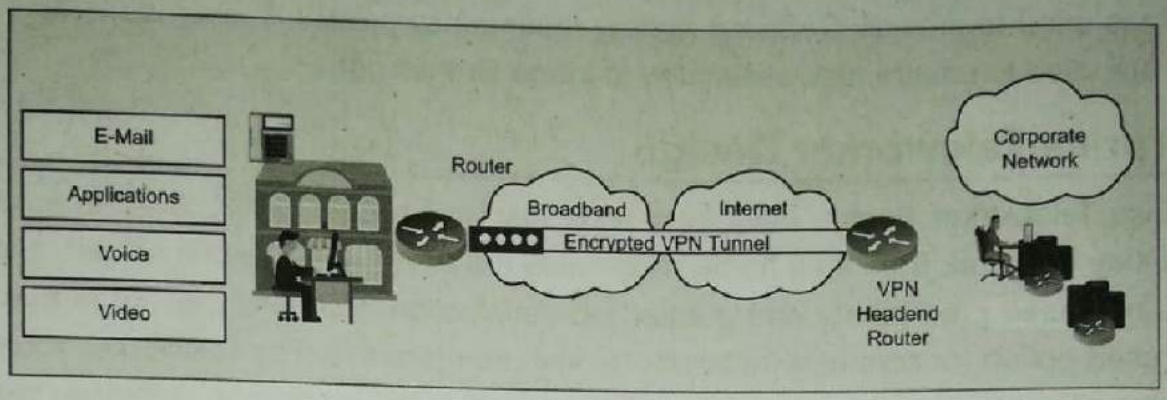


Figure 31: Teleworker Architecture

As shown in Figure 31, a teleworker has access to emails, web applications and other enterprise applications over the broadband cloud. The connection also supports advanced applications such as voice and video. The connection is centrally managed by enterprise as security policies are applied across the network. All the configurations are pushed on to the network and the connection is tested periodically. This helps in monitoring delay, latency and packet loss. QoS is maintained while transmitting data, voice, video and multimedia data.

4.7. Summary

This chapter focuses on remote connectivity network design. It starts with the basics of WAN interconnections and WAN transport technologies such as ATM, Leased Line, Frame Relay and many more. Response time, throughput, packet loss and reliability define application requirements of WAN design whereas traffic and bandwidth determine technical requirements. Enterprise Edge WAN and MAN considerations along with architecture are explained. The chapter concludes with insight on Enterprise Branch and Teleworker Design.

QUESTIONS

1. List and explain any 5 WAN transport technologies.
2. Justify the influence of application and technical requirements on WAN design.
3. What are the various techniques to optimise bandwidth? Explain.
4. Describe the use of various WAN technologies for remote access, VPNs, WAN backup, and connecting to the Internet as a backup WAN.
5. Explain Enterprise Edge WAN and MAN architecture along with technologies.
6. What are the design considerations for Enterprise Branch and Enterprise Teleworker? Explain.

Scanned by CamScanner

Designing IP Addressing in the Network & Selecting Routing Protocols

5

OBJECTIVES

After reading this chapter, the student will be able to:

- To design an IP Addressing Plan
- To introduce IPv6
- To learn Routing Protocol features
- To understand Routing Protocols for the Enterprise
- To deploy Routing Protocol
- To learn Route Redistribution and Route Filtering with BGP
- To learn Route Summarisation

Scanned by CamScanner

5.1. Designing an IP Addressing Plan

Determine the Size of the Network

IP address plan of an enterprise will depend on the size of the network. Based on the strategy for IP subnetting is to be formulated. Hence, we need to get an input on the following points:

- Number of locations in the network and IP address require in individual location
- Number of devices per location which includes PC, switches, router interface firewall devices, etc.
- Number of subnets require that are based on a plan network design and use of switches.

For example, XYZ Technology ltd. has its main office in Mumbai where the majority of users are located and have another three offices in Chennai, New Delhi and Kolkata. These three offices need to get connected to the main office which is in Mumbai for HR and account application.

Now, we need to identify the individual size of the network, to design the IP addresses for each location which includes the number of desktops/workstations, servers, routers/L3 interfaces, firewall interfaces, public servers in each location. This will be an approximate number and we need to add another 20 % as a future growth of the network. The designers need to get information of the growth from enterprise representatives.

IP address Hierarchy and Routing

As we have discussed in the previous section that IP address is in a hierarchy form as with telephone PSTN numbers. For example, PSTN number covers country code, area code and local exchange along with the actual line number. Here, in telephone network the routing or switching occurs based on a prefix number and switch the line based on area code and not worried about an actual line number within that area. It is a part of the telephone exchange of that area to connect to an actual line number and complete the call. Similarly, over the Internet, the router uses the Network ID (prefix part of the IP address) to reach to the next hop in best path and not worried about how to reach to the end node which is not local. So, all routers in between do indirect delivery of packet for destination IP address and once packet reaches, the last router where the local host is present whose IP address has been followed by every router for decision of forwarding of the packet, does direct delivery of the packet to that host.

Route Summarisation– Route Supernetting

Here, one route in the routing table represents many other routes. Due to summarisation technique, there are a smaller number of entries on routing tables, and hence reduce the routing update traffic. As a result, the number of routes in routing tables will be reduced

Scanned by CamScanner

which reduce overall overhead of the router. This is possible with classless interdomain routing (CIDR). The idea behind CIDR is to combine block of multiple addresses into a larger classless set of IP addresses. For example, Internet Service Provider has been allocated with blocks of class C network numbers. Internet service providers will allocate subset of these blocks to an enterprise who will become their client. Such multiple class C addresses which has been allocated to enterprises will combine or summarised in the routing table resulting in fewer entry in the routing table.

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.

Benefit of Hierarchical Addressing for large networks

For a large network having multiple locations, you need different prefixes of IP address per location. This will give burden on routers and size of the routing table. So, during design consideration of IP hierarchy of addresses help in route summarisation which has positive impact on routers performance. Even within single campus, careful consideration of network partition at department level of an organisation will improve overall network performance within the campus. So, IP address plans to support hierarchy and aggregation will enhance networks over all routing stability, service availability, support modular design of the network and network scalability.

Scanned by CamScanner

Summarisation Groups in Multilevel Hierarchical Network

Multilevel hierarchy of networks will help in reduce the routing overhead. The depth of the hierarchy depends on the size of networks and the usage of high level summarisation group. Figure 1 depicts the IP address hierarchy:

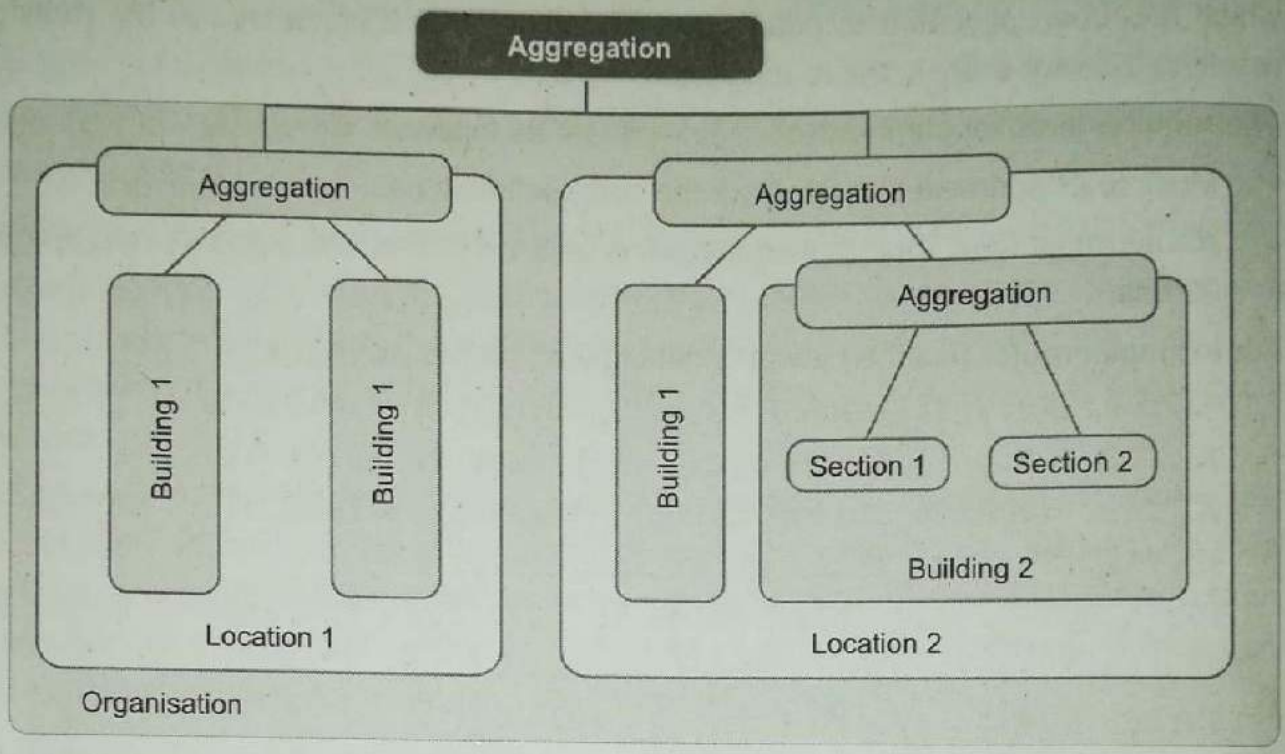


Figure 1: IP Address Hierarchy

As we have seen in past, typical enterprise has three levels of hierarchy in the network. Location of network acts as the first level. If we link to the summarisation group, then each location will represent groups of summarisation subnets. Second level of hierarchy is within the first level summarisation group. So, within large location now there is a division of summarisation group based on building of an enterprise. Third level of summarisation is within the second level summarisation group. Finally, it links to each department of floor within the building.

Disadvantages of Poorly Designed IP Addressing

A poorly designed IP addressing schemes are where IP addresses are randomly assigned when required. That is the range of IP addresses with different Network IDs (prefix) are assigned randomly as the network grows. Here, the allocation of IP addresses is dispersed through the network, and hence aggregation or summarisation is difficult to achieve.

Let us say that one of the links at the third layer i.e. at floor layer in building is not stable than all routers need to update that information about the link which is up or down as a continuous process and there is a lot of unnecessary traffic for updating routing tables of all the routers. But if IP address is designed in such a way that every layer is a part of

Scanned by CamScanner

aggregation group of IP address then only neighbour routers need to update it on the failure of the link. Aforementioned routers have no entry for particular link as they have only entry of/ for aggregated layers so need to update that routing table. Figure 2 depicts a poorly designed IP addressing scheme which results in excess routing traffic:

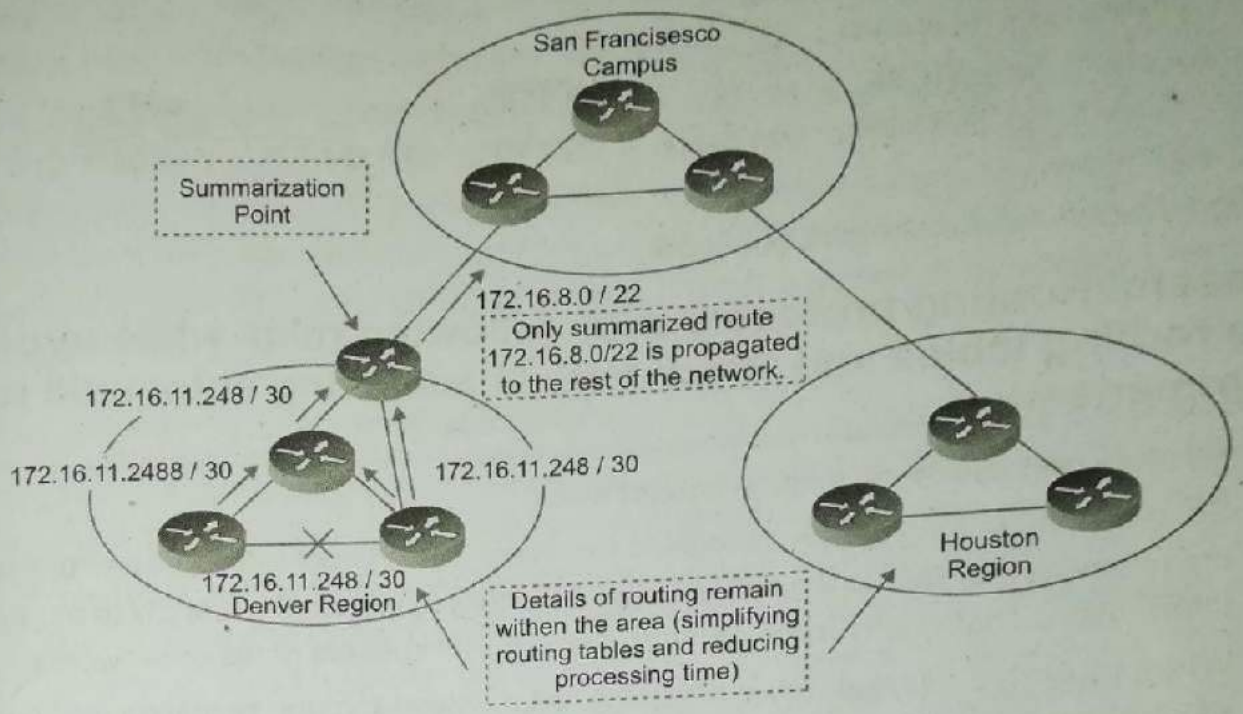


Figure 2: A Poorly Designed IP Addressing Scheme Results in Excess Routing Traffic

Fixed and Variable length Subnet mask and Routing Protocol Consideration

In earlier days when we needed to create a subnetwork as a part of the IP address hierarchy, then we had to decide the number of bits that are required for subnetwork and accordingly we had to change subnet mask from default to new subnet mask and that new subnet mask was applicable for entire network. This process is called as Fixed length subnet mask (FLSM). But, now to conserve the IP address, we use different subnet masks for different parts of the network. This is called as Variable length subnet mask. VLSM allows efficient IP address space allocation and also supports route summarisation. Classful Routing protocol only supports FLSM. The routing protocol should understand classless to support VLSM. In classful routing, the routing updates do not carry subnet mask. With classless routing, the routing updates carry the subnet mask. Figure 3 depicts fixed and variable length subnet mask:

Scanned by CamScanner

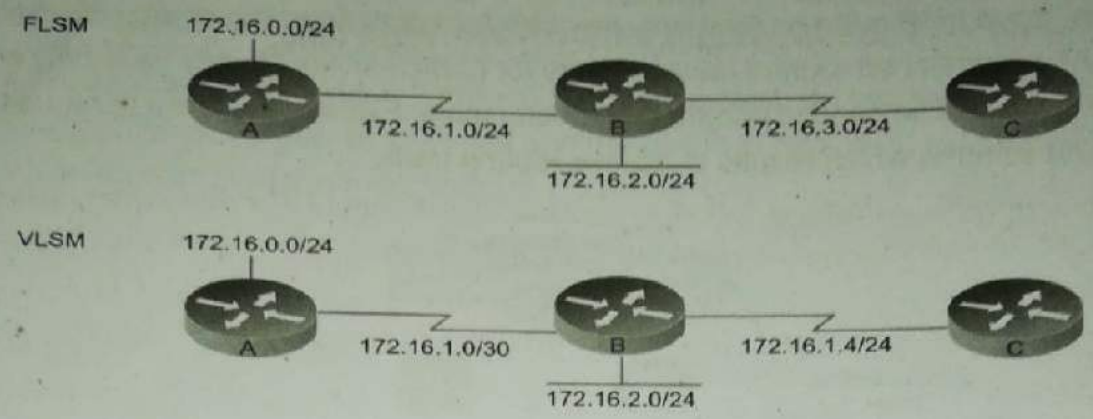


Figure 3: Fixed and variable length subnet mask

Classful Routing protocols uses following rules while updating the routing tables and which help 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:

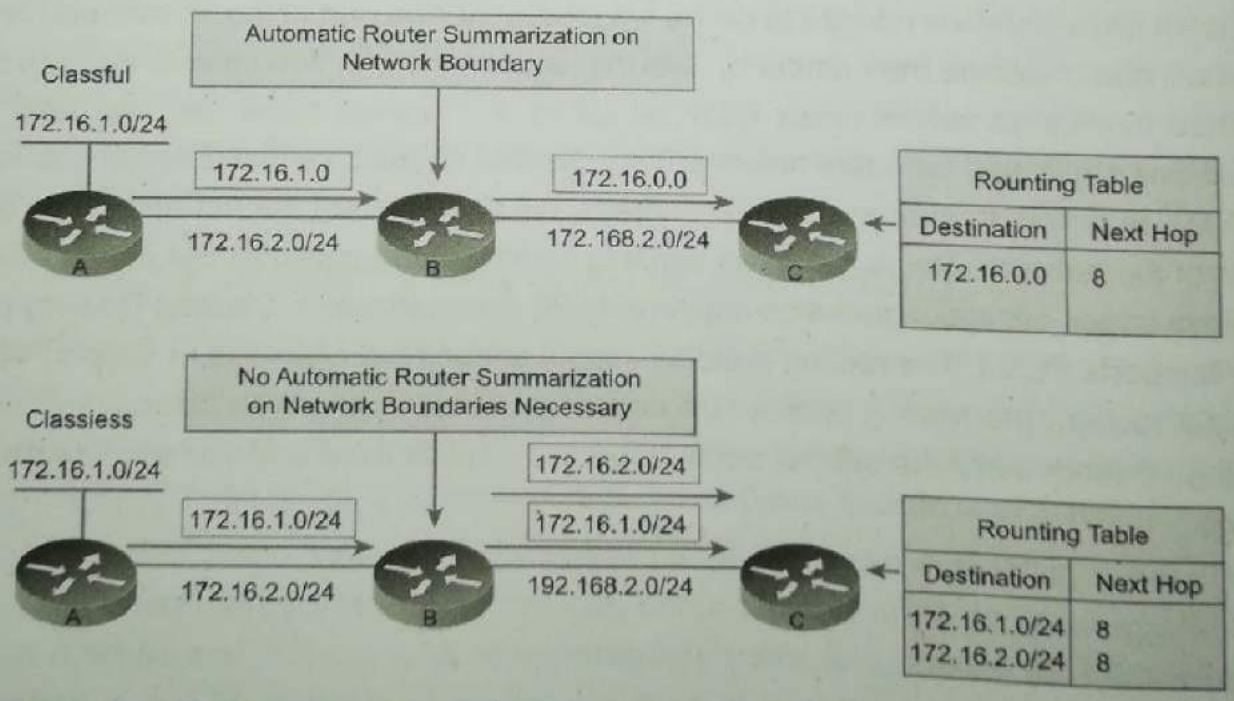


Figure 4: Example of Classful and Classless Routing

Scanned by CamScanner

Classless Routing Protocols

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

Today all latest routing protocols support classful and class less routing. For example, RIP v2 EIGRP OSPF BGP support class less routing. But they all do not behave same for summarisation. RIP v2 and EIGRP, by default, behave like classful by summarising at the network boundary. But they can configure to change their default behaviour to support classless mechanism. Whereas, OSPF, by default, cannot summarise at network boundary but can be configured to do so.

Method of Assigning IP addresses

We understand that as a part of TCP/IP network, every node /host/server needs to have a unique IP address in the network. But only providing IP address is not enough as it will make that host as network ready i.e. only able to communicate to the neighbouring node. To make it Internet ready, we need to specify gateway address and DNS servers address along with its own IP address. So, after getting the knowledge of gateway address and DNS servers address host can communicate to the outside world. Hence assigning an IP address and other details to an individual host in large network is a challenging task. We need to consider about how many devices in network require IP address along with other parameters and out of which the number of devices require static IP address which is not going to change in future. Figure 5 depicts a Lan card configuration network:

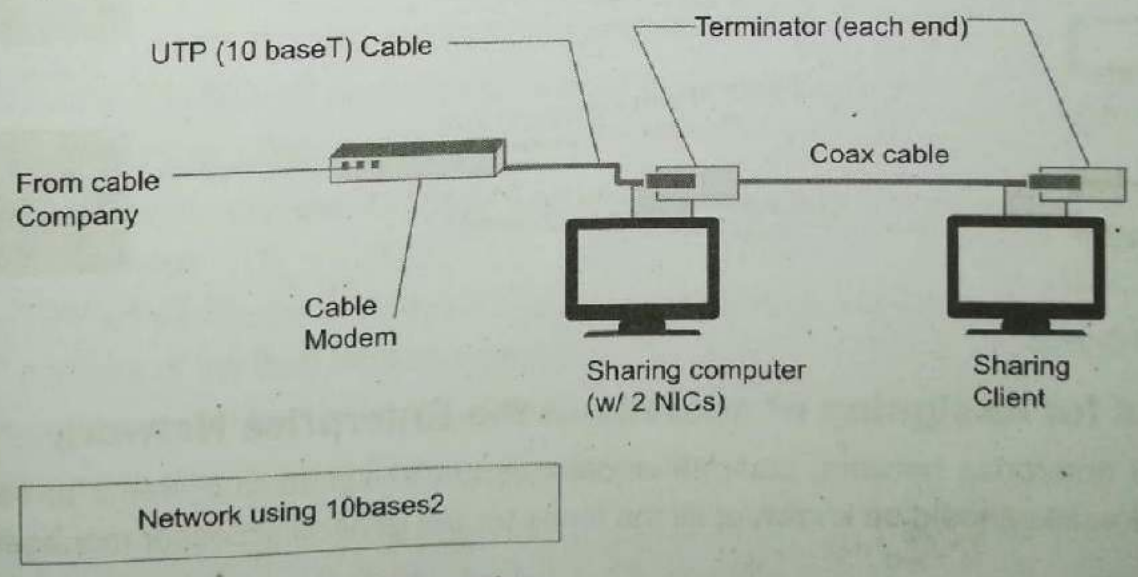


Figure 5: Small Lan Network with configurations

Scanned by CamScanner

Static and Dynamic IP address Assignment methods

Static IP address assignment means network administrator needs to manually configure LAN card and provides IP address along with the address of gateway and DNS server. In a large network, it is going to be an extra burden to the network administrator. Due to manual assignment of IP address, network administrator can assign IP address in sequence in one of the rooms so that it becomes easy to track and troubleshoot the connection. But it has security issues as others also can identify IP address remotely based on verifying sequence.

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:

Figure 6: DHCP Operation

Guidelines for Assigning IP address in the Enterprise Network

In the typical enterprise network, static IP addresses are assigned to systems or servers where IP addresses should be known at all the times for the general accessor management.

Scanned by CamScanner

The static IP address should be given to various network infrastructure devices, servers in server farm, at the enterprise edge for public servers or for VPN, whereas dynamic IP addresses are assigned to various end-user devices.

5.2. Introduction To IPV6

The IPv6 (Internet Protocol version 6)is an upgrade of IP version 4 (IPv4) and a set of specifications from the Internet Engineering Task Force (IETF). The basics of IPv6 are similar to those of IPv4, with some slight variations. The improvement in IPv6 over IPv4 is the scalability of the IP addresses from 32 bits to 128 bits. This scalability causes considerable future growth of the Internet and provides a fix to the shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4 and has integrated security and mobility features. Figure 7 shows the IPV6 address structure:

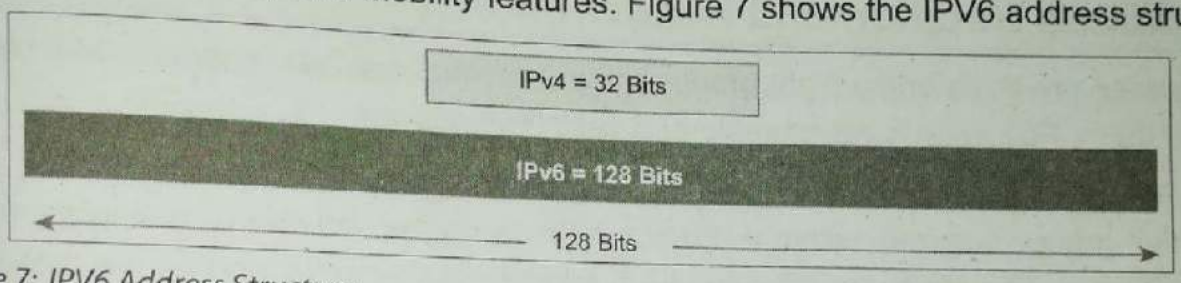


Figure 7: IPV6 Address Structure

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

Scanned by CamScanner

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 Notation and Header Format

IPv6 addresses are denoted by eight groups of hexadecimal quartets, separated by colons in between them. Following is an example of a valid IPv6 address:

```
2002: cadb:0000:0000:0000:0000:3257:8745
```

Any four-digit group of zeroes within an IPv6 address may be reduced to a single zero or omitted altogether. Therefore, the following IPv6 addresses are similar and equally valid.

```
2002:cadb:0000:0000:0000:0000:3257:8745
2002:cadb:0:0:0:0:3257:8745
2002:cadb::3257:8745
```

IPv6 Packet Header

IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow. Figure 8 shows the IPV6 header format:

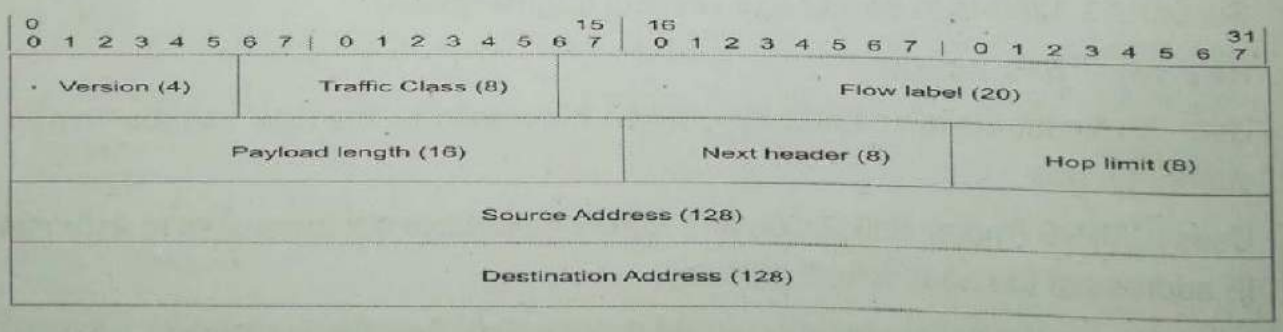


Figure 8: IPV6 Header Format

IPv6 fixed header is 40 bytes long and contains the following information:

- **Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
- **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for the type of service to let the router known what services should be provided

Scanned by CamScanner

to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).

- **Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps to avoid re-ordering of data packets. It is designed for streaming/real-time media.
- **Payload Length** (16-bits): This field is used to tell the routers that how much information a particular packet contains in its payload. Payload is composed of the Extension Headers and the Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
- **Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
- **Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0, the packet is discarded.
- **Source Address** (128-bits): This field indicates the address of the originator of the packet.
- **Destination Address** (128-bits): This field provides the address of the intended recipient of the packet.

Address Assignment Strategies

IPv6 has two address assignment strategies: static and dynamic.

Static IPv6 Address Assignment

The administrator must enter the IPv6 address configuration manually on every device in the network in static address assignment.

Dynamic IPv6 Address Assignment

IPv6 dynamic address assignment strategies allow dynamic assignment of IPv6 addresses, as follows:

- **Link-local address**: Using the link-local prefix FE80::0/10 and a 64-bit identifier for the interface, in an EUI-64 format, the host configures its own link-local address autonomously.
- **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

Scanned by CamScanner

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

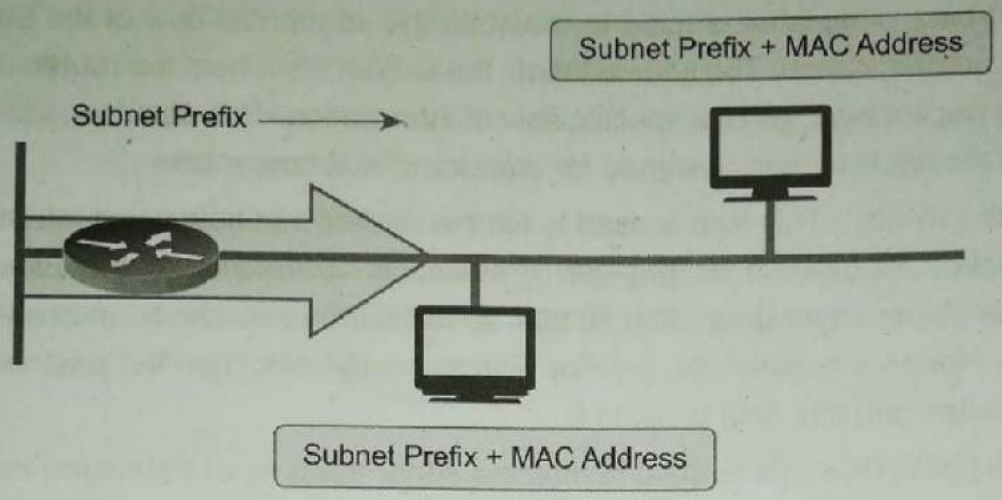


Figure 9: IPv6 Stateless Auto Configuration

- **IPv6 Stateless Address Autoconfiguration (SLAAC):** This mode is always used and configures a Dynamic Address. 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).

IPv6 Name Resolution

Static and Dynamic IPv6 Name Resolution

The following two-name resolutions are:

- **Static name resolution:** Accomplished by manual entries in the host's local configuration files
- **Dynamic name resolution:** Accomplished using a DNS server that supports IPv6, usually along with IPv4 support

An IPv6-aware application requests the destination hostname's IPv6 address from the DNS server using a request for an A6 record; an A6 record is a new DNS feature that contains an address record for an IPv6 host. The task of querying for the address is done with the name resolver, which is usually a part of the operating system. The network administrator must set up the appropriate DNS server with IPv6 support and connect it to the IPv6 network with a valid IPv6 address. Figure 10 displays the IPv6 name resolution:

Scanned by CamScanner

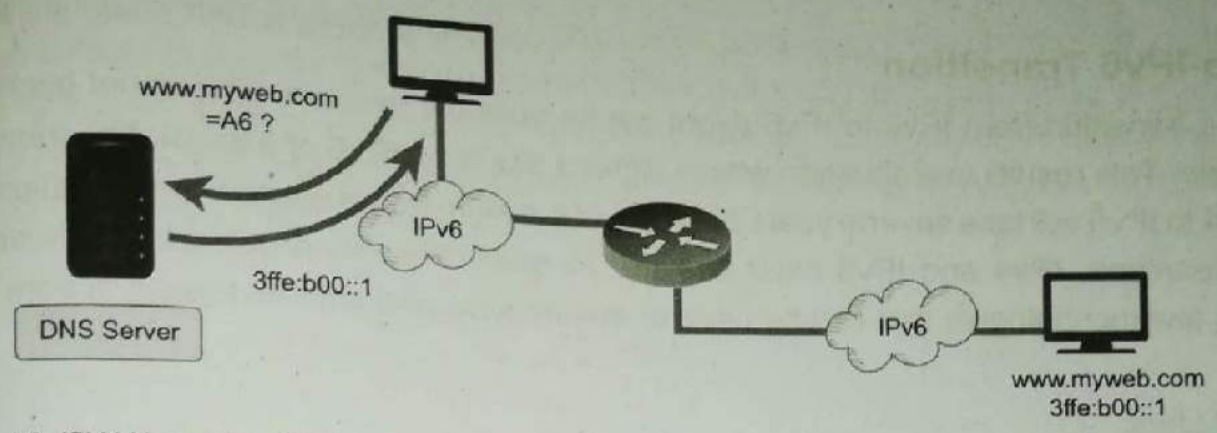


Figure 10: IPV6 Name resolution

IPv4-to-IPv6 Transition Strategies and Deployments

There is no automatic transition from IPv4-to-IPv6. Let us start with the comparison between IPV4 and IPv6. The possible transition strategies and deployments are discussed later.

Comparison Between IPv4 and IPv6

IP version 6 is the new version of Internet Protocol, which is much better than IP version 4 in terms of complexity and efficiency.

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 4.29×10^9 addresses	Can produce quite large number of addresses, i.e. 3.4×10^{38}
Type of addresses	Unicast, broadcast, multicast	Unicast, multicast, anycast
Address representation	Decimal	hexadecimal
Checksum field	Not available	Available
Fragmentation	Fragmentation is done by sending and forwarding routes	Fragmentation is done by the senders

Scanned by CamScanner

IPv4-to-IPv6 Transition

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

- Dual stack
- Tunneling
- Translation

- Dual Stack Mechanism

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

Figure 11 depicts the dual stack mechanism:

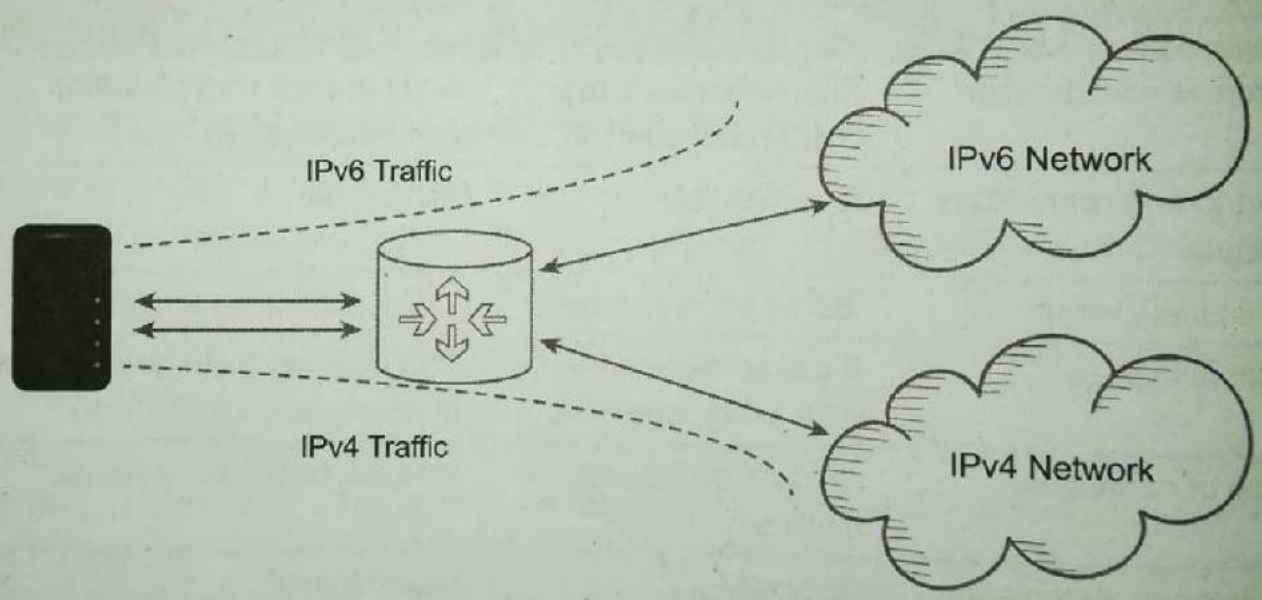


Figure 11: Dual Stack Mechanism

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

- **Tunneling Mechanism**

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

Scanned by CamScanner

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

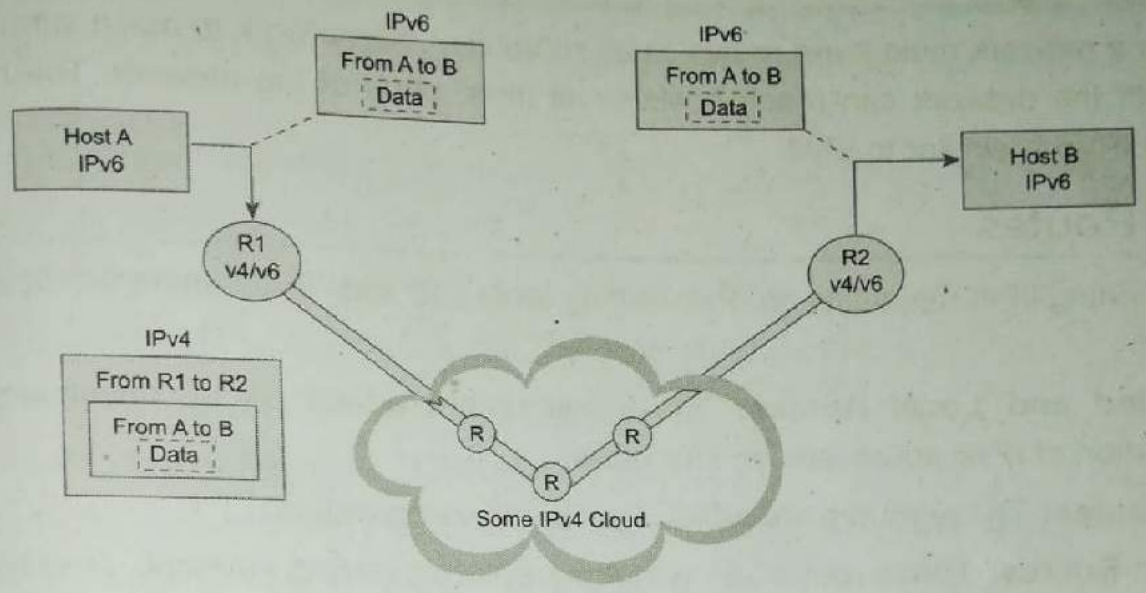


Figure 12: Tunneling Mechanism

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

- Configured tunnels between two routers
- Automatic tunnels that terminate at the dual hosts
- **NAT Protocol Translation**

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

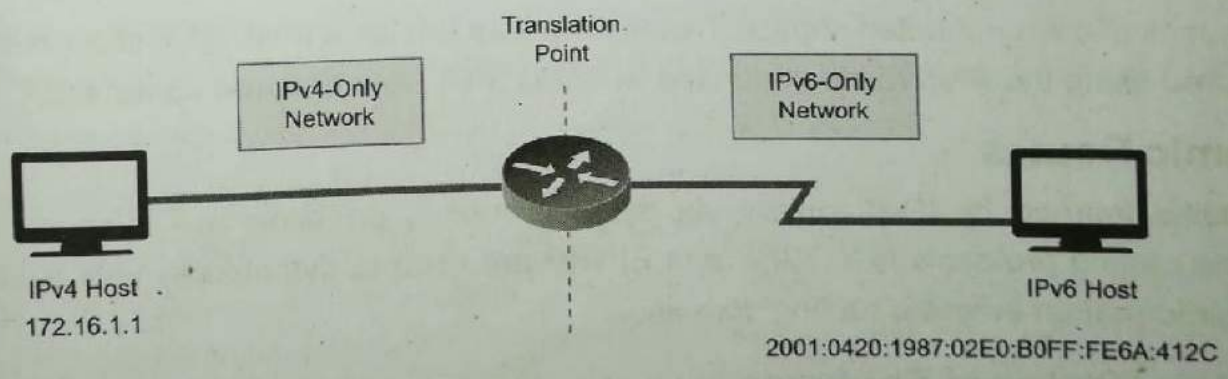


Figure 13: NAT Protocol Translation

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

Scanned by CamScanner

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 for the IPv4 host, the router does vice versa.

5.3. Routing Protocols

All routers in a network must learn routes to all subnets in the network to make sure a host in one part of the network can reach hosts in all other parts of the network. The routing procedure in IPV6 is similar to IPv4.

Types of Routes

Any router running IPv6 maintains an IPv6 routing table and adds IPv6 routes to it based on the following:

- **Connected and Local Routes:** These routes are added as a consequence of configuration of IPv6 addresses on interfaces.
- **Static Routes:** These routes are added by manual configuration.
- **Dynamic Routes:** These routes are added by dynamic routing protocols like OSPFv3 and EIGRP for IPv6.

Connected and Local Routes

The most efficient and scalable way to achieve end-to-end connectivity is to use a dynamic IPv6 routing protocol, like OSPFv3 (Open Shortest Path First version 3) and EIGRP (Enhanced Interior Gateway Routing Protocol) for IPv6. These dynamic routing protocols for IPv6 are good at what they do but are complex to understand and configure. There are other simpler ways that routers can add IPv6 routes to their routing tables namely, connected, local, and static routes.

Static Routes

IPv6 makes use of connected and local routes in a way similar to IPv4. IPv6 static routes are configured using the **IPv6 route** command whereas IPv4 uses **IP route** command.

Dynamic Routes

The routes learned by IPv6 routers via dynamic routing protocols are dynamic routes. Dynamic routing protocols like OSPF and EIGRP are used to dynamically propagate IPv6 routing information across a routing domain.

Routing Protocol Features

A routing protocol specifies that how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network. The routers perform the 'traffic directing' functions on the Internet; data packets are

Scanned by CamScanner

forwarded through the networks of the internet from router to router until they reach their destination computer. Routing algorithms determine the specific choice of route. Each router has a prior knowledge only of networks that are attached to it directly. A routing protocol shares this information first amongst the immediate neighbours, and then throughout the network. This way, routers gain knowledge of the topology of the network. Routing is a process to forward routable data choosing the best route amongst several available routes or path to the destination. A router is a device that forwards data that is not explicitly destined to it.

There are many ways to characterize routing protocols which are as follows:

- ■ Static versus dynamic routing
- ■ Interior versus exterior routing protocols
- ■ Distance vector versus link-state versus hybrid protocols
- ■ Flat versus hierarchical routing protocols
- **Static versus 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.

- **Interior and Exterior Routing protocols**

Interior Routing Protocol:

Interior Gateway Protocols (IGPs) handle routing within an Autonomous System (one routing domain). In general, IGPs figure out how to get from place to place between the routers you own. These dynamic routing protocols keep track of paths which are used to move data from one end system to another, inside a network or set of networks that one administrates.

There are two forms of Interior Routing Protocols which are as follows:

- Distance Vector Protocols:
  a. Routing Information Protocol (RIP)

Scanned by CamScanner

b. Interior Gateway Routing Protocol (IGRP)

- Link State Protocol
  a. Open shortest Path First (OSPF)
  b. Intermediate System to Intermediate system (IS-IS)
- **Distance Vector Routing Protocol**: In a distance vector routing algorithm, routes are selected based on the distance between networks. The distance metric is something simple enough to allow consistent values across the domain. A router running distance vector protocol advertises its connected routes and learns new routes from its neighbours. The routing cost to reach a destination is calculated by the means of hops between the source and destination. A router generally relies on its neighbour for best path selection, also known as 'routing-by-rumors'. RIP and IGRP are the examples of distance vector protocols. Figure 14 shows the example of distance vector routing protocol:

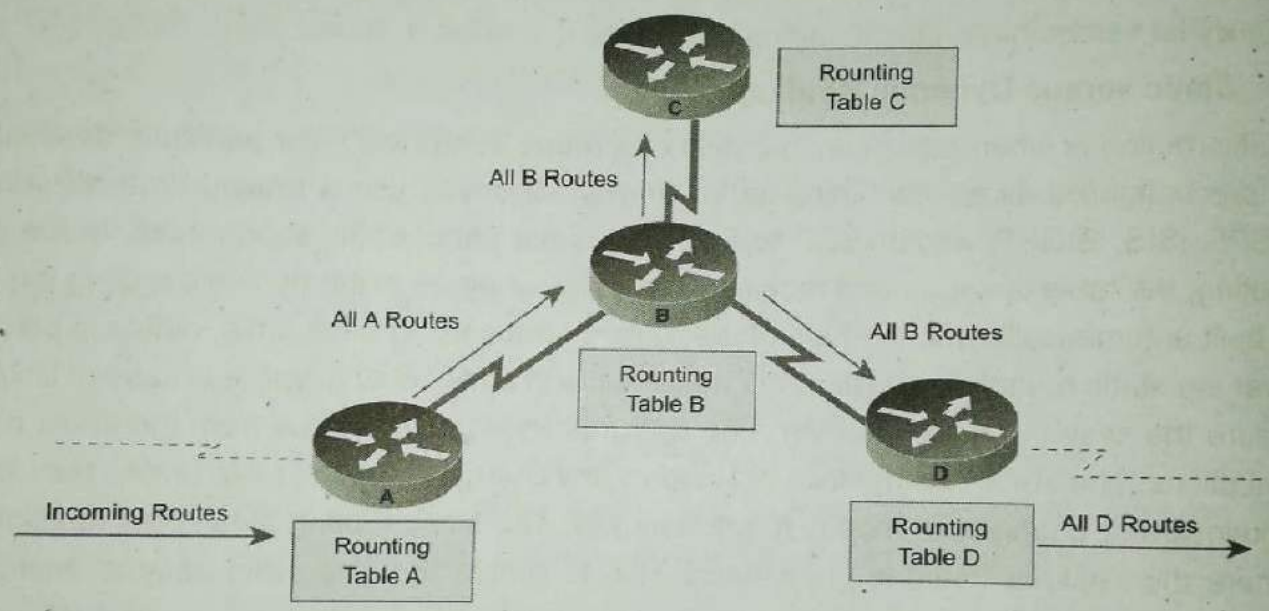


Figure 14: Example of Distance Vector Routing

(a) RIPng

RIPng stands for Routing Information Protocol Next Generation. This is an interior routing protocol and a distance vector protocol. RIPng has been upgraded to support IPv6 to determine the best route to a destination, using hop count as the metric. RIPng exchanges routing information used to compute routes and is intended for IP version 6 (IPv6)-based networks. RIPng is disabled by default.

(b) Interior Gateway Routing Protocol (IGRP)

The Interior Gateway Routing Protocol (IGRP) was created in response to the limitations in Routing Information Protocol (RIP), which handles a maximum hop count of 15. IGRP supports a maximum hop count of up to 255. The primary two purposes of IGRP are to:

Scanned by CamScanner

- communicate routing information to all connected routers within its boundary or autonomous system.
- continue updating whenever there is a topological, network or path change occurs.

IGRP sends a notification of any new change, and information about its status, to its neighbours every 90 seconds. IGRP manages a routing table with the most optimal path to respective nodes and to networks within the parent network. Since it is a distance vector protocol, IGRP uses several parameters to calculate the metric for the best path to a specific destination. These parameters include delay, bandwidth, reliability, load and maximum transmission unit (MTU).Figure 15 represents a network support with EIGRP:

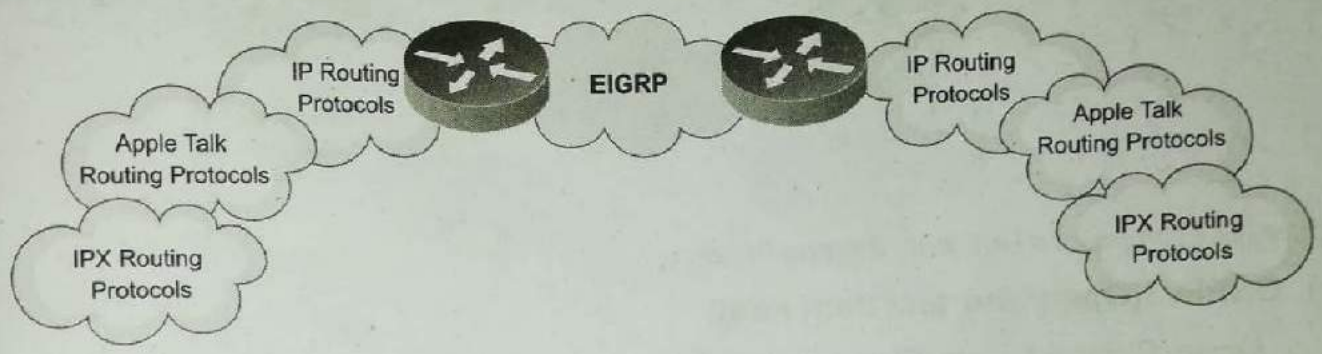


Figure 15: Network Support with EIGRP

- **Link-State Routing Protocol**: This protocol acknowledges the state of a link and advertises to its neighbours. Information about new links is learnt from peer routers. After all the routing information has been converged, the link-state routing protocol uses its own algorithm to calculate the best path to all available links. The main advantage of a link-state routing protocol is that the complete knowledge of topology allows routers to calculate routes that satisfy a particular criterion. This can be useful for traffic engineering purposes, where routes can be constrained to meet particular quality of service requirements. The main disadvantage of a link state routing protocol is that it does not scale well as more routers are added to the routing domain. Increasing the number of routers increases the size and frequency of the topology updates, and also the length of time it takes to calculate end-to-end routes. This lack of scalability means that a link-state routing protocol is unsuitable for routing across the Internet at large, which is the reason why IGPs only route traffic within a single AS. OSPF and IS-IS are link-state routing protocols and both of them use Dijkstra's Shortest Path First algorithm. Figure 16 depicts the example of a link state routing protocol:

Scanned by CamScanner

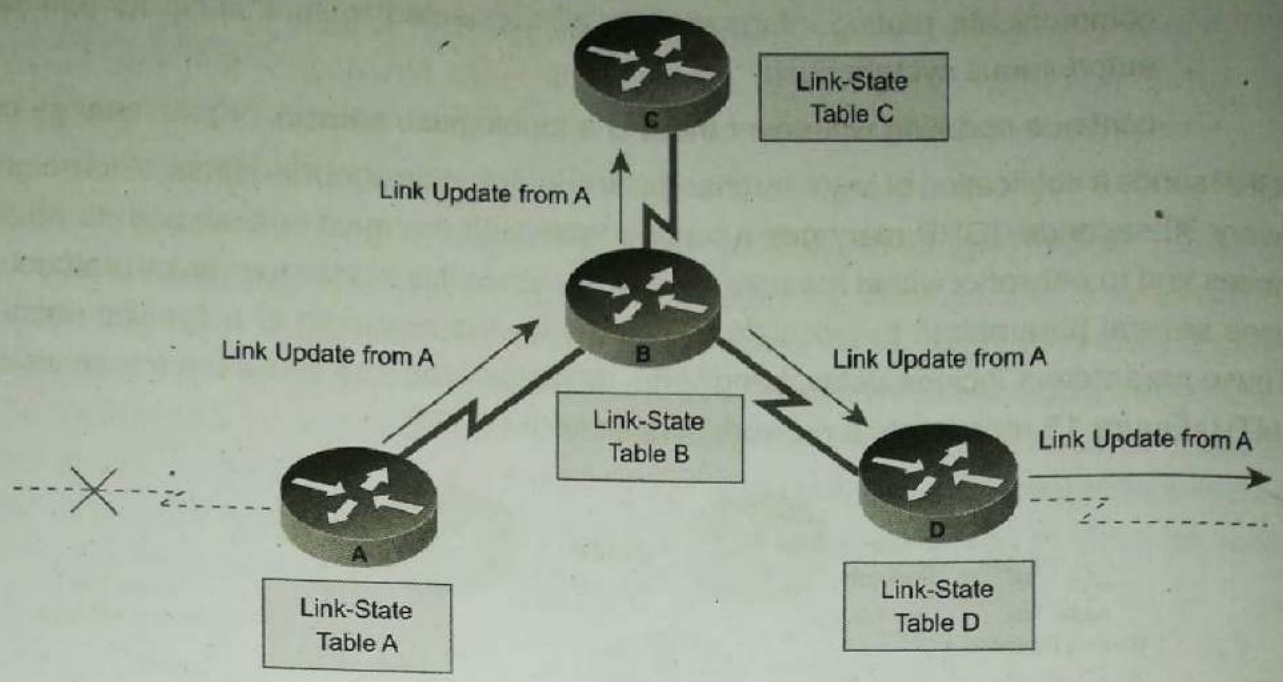


Figure 16: Example of a Link State Routing Protocol

(c) OSPFv3(Open Shortest Path First)

Open Shortest Path First version 3 is an interior routing protocol which is modified to support IPv6. This is a link-state protocol and uses Djikrasta's shortest path first algorithm to calculate best path to all destinations. OSPF and IS-IS protocol will be discussed in detail in the later part of the chapter.

Hybrid Routing Protocol

A third type of protocol is the hybrid interior gateway protocol, which is the Cisco EIGRP. EIGRP has characteristics of both distance vector and link-state protocols. It combines distance vector behavior with some link-state characteristics and some proprietary features. EIGRP is a fast-converging and scalable routing protocol.

The following table 2 summarises interior gatewayrouting protocols:

Table 2: IP Routing Protocols

Category	Routing Protocol
Distance Vector	RIPv1, RIPv2, IGRP
Link-State	OSPF, Integrated IS-IS
Hybrid	EIGRP

- **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

Scanned by CamScanner

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).

- **BGPv4(Border Gateway Protocol)**

  BGP stands for Border Gateway Protocol. It is the only open standard exterior gateway protocol available. BGP is a distance vector protocol which takes an autonomous system as calculation metric, instead of the number of routers as hop. BGPv4 is an upgrade of BGP to support IPv6 routing. Figure 17showsan integration of interior v/s exterior routing protocols:

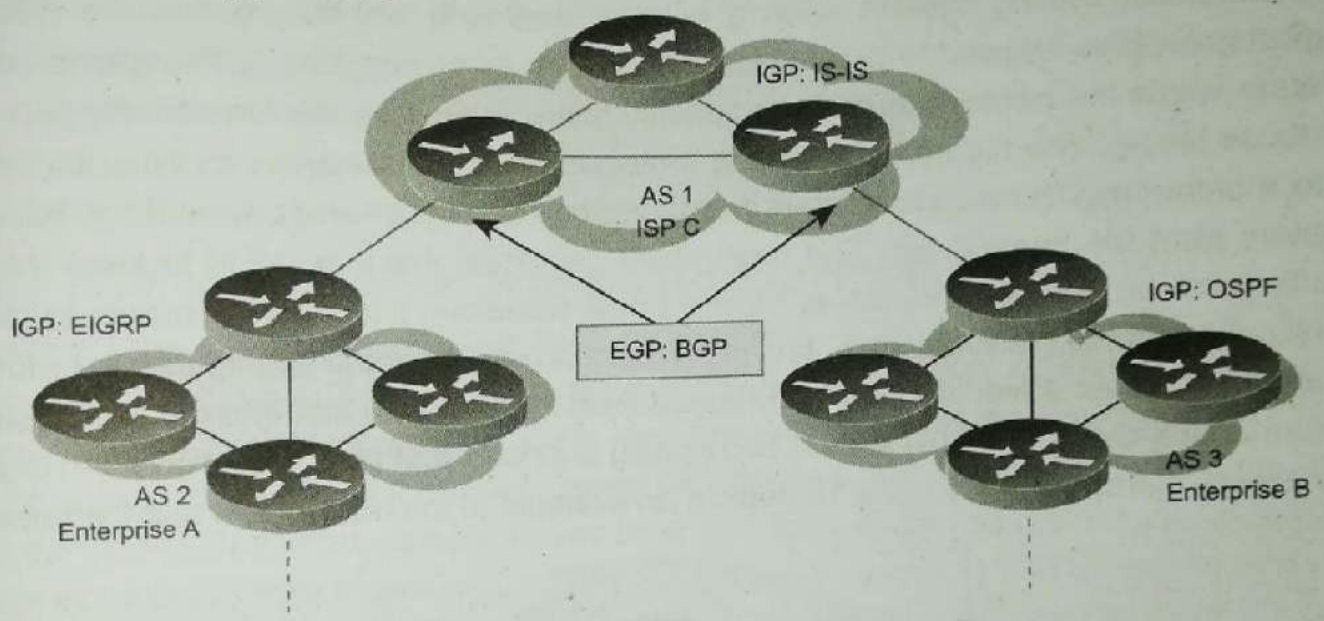


Figure 17: Integration of Interior and Exterior Routing Protocols

Protocols Changed to Support IPv6

- **ICMPv6**: Internet Control Message Protocol version 6 is an upgraded implementation of ICMP to accommodate IPv6 requirements. This protocol is used for diagnostic functions, errors and information messages, and statistical purposes. ICMPv6's Neighbour Discovery Protocol replaces ARP and helps to discover neighbour and routers on the link.
- **DHCPv6**: Dynamic Host Configuration Protocol version 6 is an implementation of DHCP. IPv6 enabled hosts do not require any DHCPv6 server to acquire IP address as they can be autoconfigured. They do not need DHCPv6 to locate DNS server as DNS can be discovered and configured via ICMPv6 Neighbor Discovery Protocol yet can be used to provide this information.
- **DNS**: There has been no new version of DNS, but it is now equipped with extensions to provide support for querying IPv6 addresses. A new AAAA (quad A) record has been

Scanned by CamScanner

added to reply IPv6 query messages. Now the DNS can reply with both the IP versions (4 & 6) without any change in the query format.

- **Flat and Hierarchical 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.

Hierarchical routing protocols

A hierarchical routing system uses a layered approach wherein routers are placed in logical groupings referred to domains, areas, or autonomous systems. This allows different routers within the network to perform specific tasks, optimizing the functionality performed at those layers. The hierarchical routing protocols often group routers together by function into a hierarchy. The access routers form the first tier of the hierarchy, and the backbone routers form the second tier. The hierarchical protocols make an effort to keep the local traffic local, i.e. they will not forward traffic to the backbone if it is not necessary to reach a destination. Some hierarchical routing protocols also perform route aggregation to reduce the number of routes advertised. Open Shortest Path First (OSPF) and Intermediate-system to Intermediate-System (IS-IS) are the two routing protocols that can be configured to organise a network hierarchically. Figure 18 depicts an example of the hierarchical and flat network:

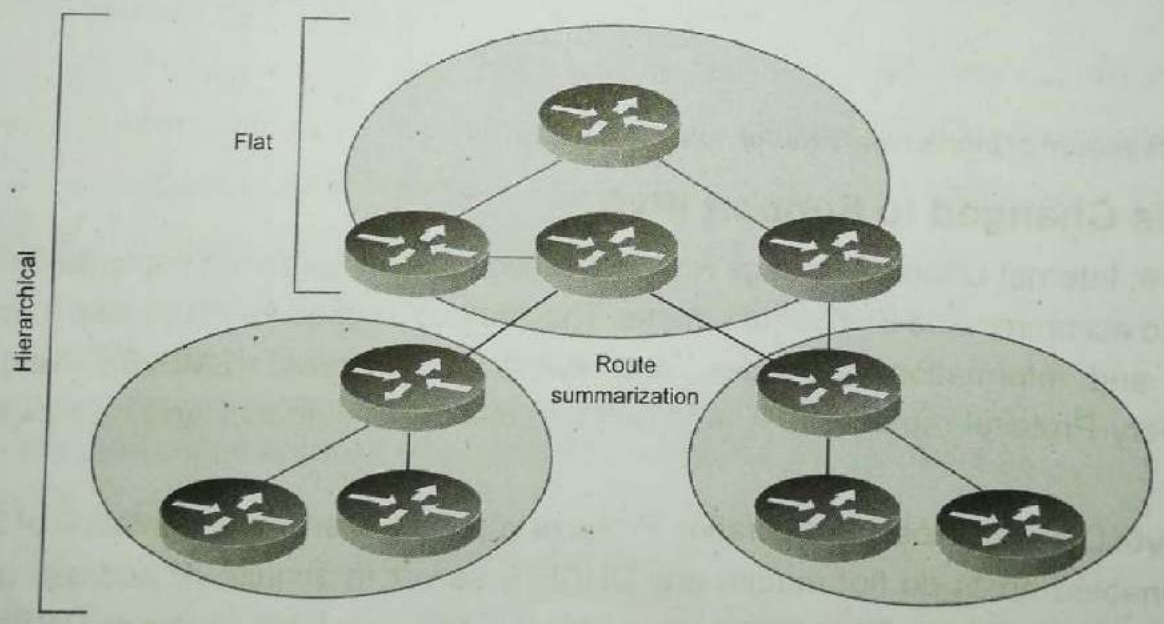


Figure 18: Example of Hierarchical and Flat Network

Scanned by CamScanner

5.4. Routing Protocols for Enterprise

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

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

EIGRP (Enhanced Interior Gateway Routing Protocol)

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

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

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

Scanned by CamScanner

EIGRP supports the following features:

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

EIGRP Metrics

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

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

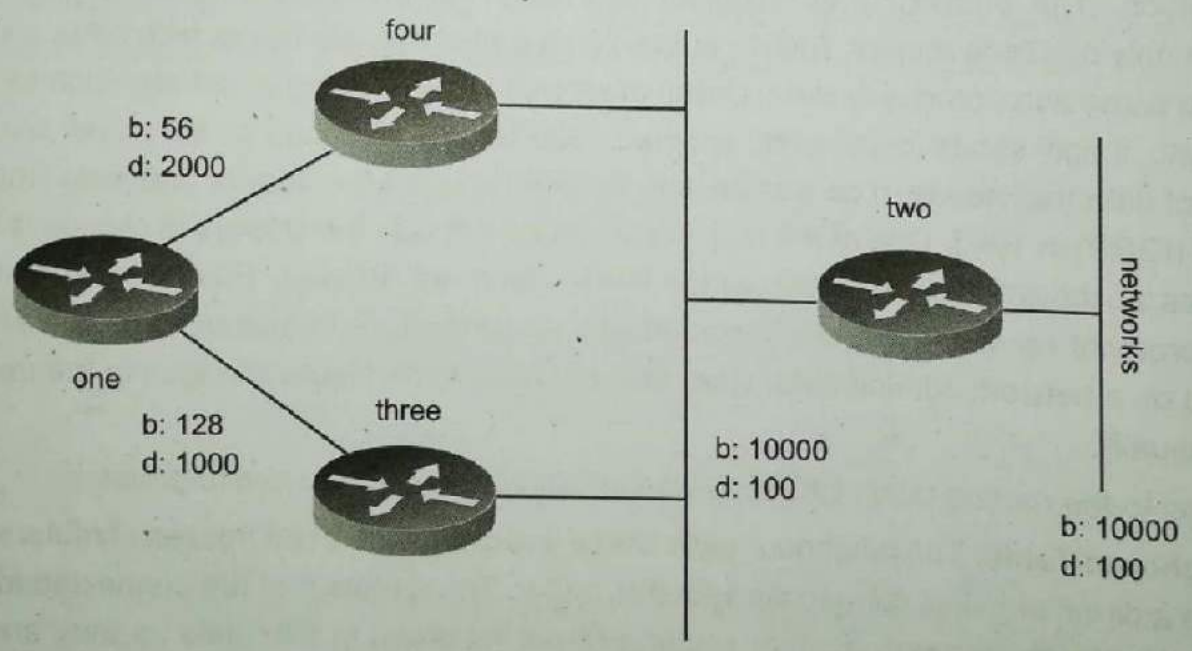


Figure 19: Example of EIGRP Network

It starts with the two advertisements for this network: one through Router Four, with a minimum bandwidth of 56 and a total delay of 2200; and the other through Router Three, with a minimum bandwidth of 128 and a delay of 1200. Router One chooses the path with the lowest metric.

Scanned by CamScanner

Let us compute the metrics. EIGRP calculates the total metric by scaling the bandwidth and delay metrics. EIGRP uses the following formula to scale the bandwidth:

- bandwidth = (10000000/bandwidth(i)) * 256

  where bandwidth(i) is the least bandwidth of all outgoing interfaces on the route to the destination network represented in kilobits.

  EIGRP uses the following formula to scale the delay:

- delay = delay(i) * 256

  where delay(i) is the sum of the delays configured on the interfaces, on the route to the destination network, in tens of microseconds. The delay as shown in the **show IPEIGRP topology** or **show interface** commands is in microseconds, so you must divide by 10 before you use it in this formula. Throughout this paper, we use delay as it is configured and shown on the interface.

  EIGRP uses these scaled values to determine the total metric to the network:

  metric = ([K1 * bandwidth + (K2 * bandwidth) / (256 - load) + K3 * delay] * [K5 / (reliability + K4)]) * 256

Note: These **K** values should be used after careful planning. Mismatched **K** values prevent a neighbour relationship from being built, which can cause your network to fail to converge.

Note: If K5 = 0, the formula reduces to Metric = ([k1 * bandwidth + (k2 * bandwidth)/(256 - load) + k3 * delay]) * 256.

The default values for **K** are:

K1 = 1

K2 = 0

K3 = 1

K4 = 0

K5 = 0

For default behaviour, you can simplify the formula as follows:

metric = bandwidth + delay

Cisco routers do not perform floating point math, so at each stage in the calculation, you need to round down to the nearest integer to calculate the metrics properly. In this example, the total cost through Router Four is:

minimum bandwidth = 56k

total delay = 100 + 100 + 2000 = 2200

[(10000000/56) + 2200] x 256 = (178571 + 2200) x 256 = 180771 x 256 = 46277376

And the total cost through Router Three is:

minimum bandwidth = 128k

Scanned by CamScanner

total delay = 100 + 100 + 1000 = 1200

[(10000000/128) + 1200] x 256 = (78125 + 1200) x 256 = 79325 x 256 = 20307200

So, to reach Network A, Router One chooses the route through Router Three.

OSPF (Open Shortest Path First)

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

Figure 20 depicts the example of OSPF network:

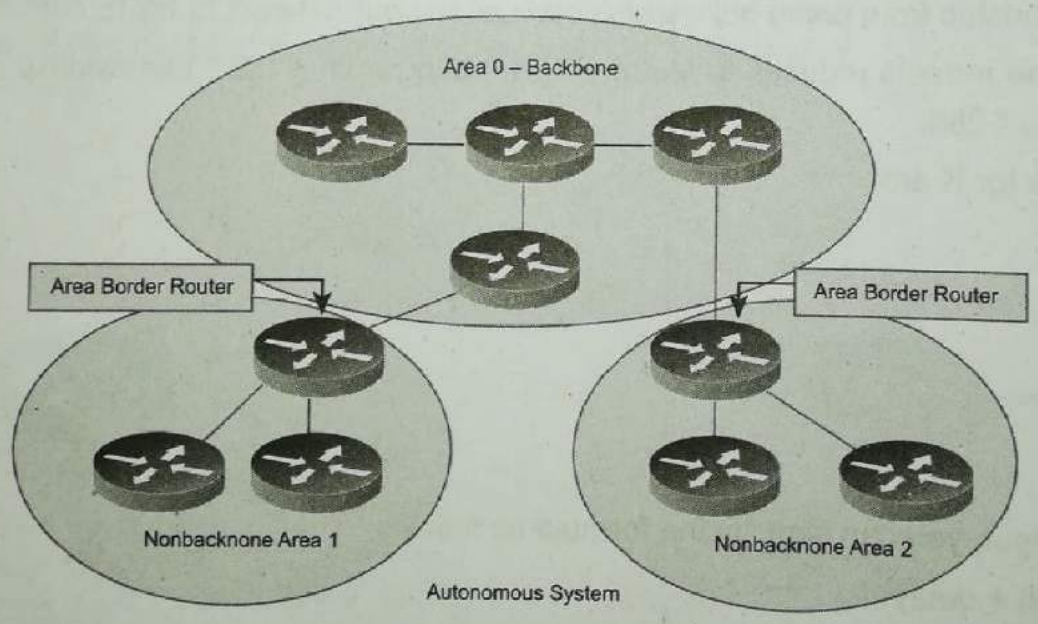


Figure 20: Example of OSPF Network

OSPF has the following features:

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

Scanned by CamScanner

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

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

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

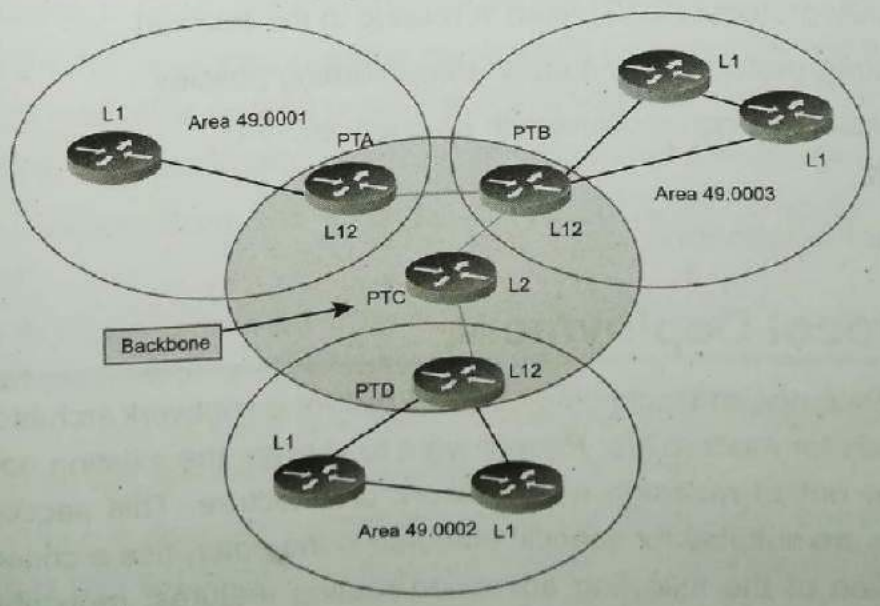


Figure 21: IS-IS Network

Scanned by CamScanner

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:

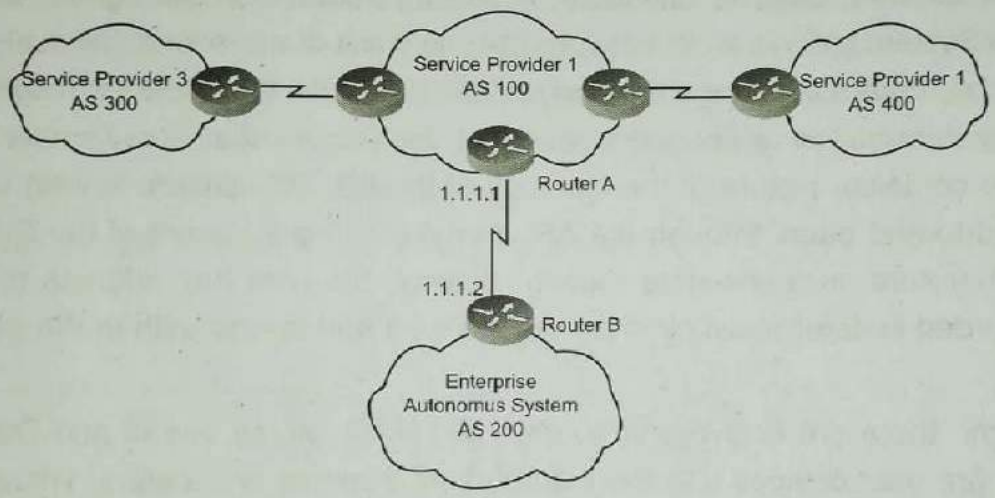


Figure 22: Example of BGP Network

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.

5.5. Routing Protocol Deployment

With the rapid development of science and technology, the old-fashioned network architectures cannot meet the various needs for modern life. People want to change the existing network architecture urgently and set out to redesign new network architecture. This section will discuss why certain protocols are suitable for specific modules in the enterprise architecture. After that there is a discussion of the following advanced routing features: redistribution, filtering and summarisation.

Scanned by CamScanner

Example of Routing in the Campus Core

Both small and large enterprise campuses require a highly available and secure, intelligent network infrastructure to support business solutions such as voice, video, wireless, and mission-critical data applications. The use of hierarchical design principles provides the foundation for implementing campus networks which meet these requirements. Connectivity is very critical and hence in case of a link failure, it must immediately adapt to change to provide a seamless transport service. EIGRP and OSPF both adapt quickly to changes and have short convergence times. Therefore, they are suitable for use in the Campus Core. The underlying physical topology, IP addressing, equipment used, and possible issues related to the routing protocol in a particular situation are the deciding factors to use certain protocols. Figure 23 depicts the routing protocols in the Enterprise Architecture:

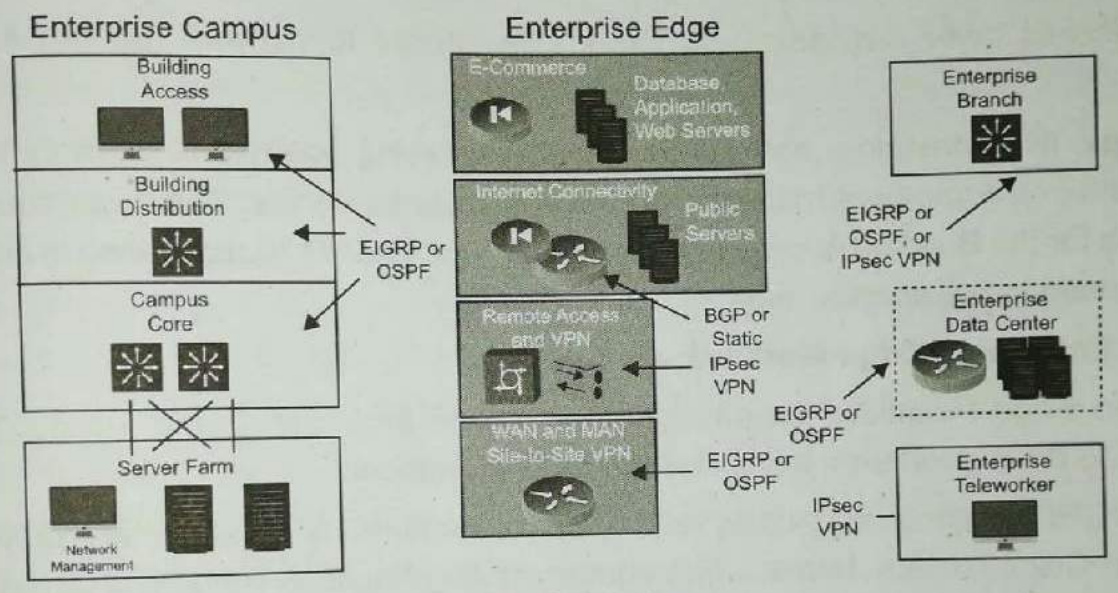


Figure 23: Routing protocols in the Enterprise Architecture.

In the Campus Core, the following points are considered for choosing the routing protocol:

- As EIGRP is a Cisco-proprietary protocol, hence restricted to use EIGRP in the Campus Core and other routing protocols in the non-Cisco parts of the network.
- OSPF imposes a strict hierarchical design and should map to the IP addressing plan.

In the Campus Core, the following points are considered for not choosing other routing protocol:

- IS-IS requires detailed knowledge of the OSI protocol suite for proper configuration, and that knowledge is not widely available.
- In the Campus Core, since static routing requires administrative intervention for changes and on link failures, static routing is not an option.
- RIP has a slow convergence because of its periodic transmission of the entire routing table, and is based on hop count, hence not recommended as a Campus Core routing protocol.

Scanned by CamScanner

Routing in the Building Distribution Layer, Building Access Layer and Enterprise Edge Modules

It is a standard proposal that the same routing protocol should be used in all three layersof the Enterprise Campus.

Routing in Building Distribution layer

In Building Distribution layer if multiple routing protocols are used, then redistribution is done. EIGRP and OSPF are the suggested routing protocols in the Building Distribution layer.

The Building Distribution layer is the middle point between the core and the access layers. Hence, the choice of routing protocol depends on the routing protocols used in the core and the access layers.

Routing in the Building Access layer

The Building Access layer provides local users with access to network resources. The underlying

physical topology, IP addressing, and the available processing power and memory in the Building Access layer equipment influence the routing protocol choice. The recommended routing protocols for the Building Access layer are OSPF and EIGRP. Static routing is also an option which is used in the access layer.

Routing in the Enterprise Edge Modules

In the Enterprise Edge modules, the physical topology, IP addressing, and the deployed equipment are the driving features to choose the routing protocol.

As we know, EIGRP protocol was designed by Cisco Systems as a proprietary protocol, available only on Cisco routers, hence when equipment from multiple vendors is part of the overall design, the use of EIGRP is restricted to only where Cisco devices exist. However, EIGRP gives an administrator more influence on routing and is suitable for NBMA (A non-broadcast multiple access network) environments in which there is a split-horizon issue because EIGRP split-horizon can be turned off.

OSPF is appropriate in environments such as LAN, NBMA, and dialup. The limitations of using OSPF as an Enterprise Edge routing protocol are due to its high memory, processing power requirements and strict hierarchical design. The high memory and processing power requirements can be reduced using summarisation and careful area planning. OSPF also requires significant configuration expertise. However, if multiple exit points exist and on redundancy requirements, static routes or BGP are used for the Internet connectivity.

5.6. Route Redistribution

This section discusses about the route redistribution and administrative distance and the process to select the best route.

Scanned by CamScanner

The following are the possible reasons why one might need multiple routing protocols running at the same time within your network:

- Migrating from an older IGP to a new IGP. Multiple redistribution boundaries might exist until the new protocol has displaced the old protocol completely.
- Use another protocol but have to keep the old routing protocol because of the host system's needs.
- Some departments might not want to upgrade their routers to support a new routing protocol.
- In a hybrid-vendor environment, one can use the EIGRP routing protocol in the Cisco portion of the network and also uses a common standards-based routing protocol, such as OSP, to communicate with non-Cisco devices.

Redistribution of the routes is required when one or both of the following occur:

- Multiple routing protocols are used in the network, for example, RIPv2, EIGRP, and OSPF.
- Multiple routing domains are used in the network, for example, two EIGRP routing processes.

When any of these situations arises, routers allow internetworks using different routing protocols to exchange routing information through a feature called route redistribution. This causes hosts in one part of the network to reach hosts in another part.

Redistribution occurs on the boundaries between routing protocols and between domains. Figure 24shows the redistribution occurs on a router with interfaces that participate in multiple routing protocols or routing domains:

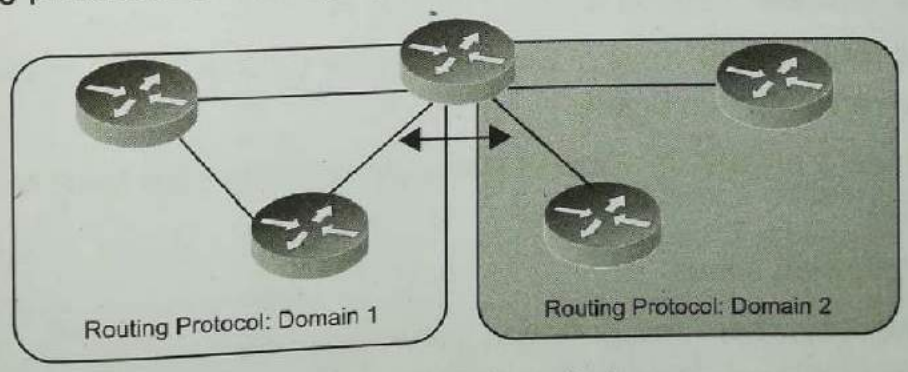


Figure 24: Route Redistribution in domain boundaries

Selecting the Best Route

Routers use the following two parameters to select the best path to the destination:

- **Administrative distance**: The administrative distance issued to rate a routing protocol's believability.
- **Routing metric:** The routing metric is a value representing the path between the local router and the destination network, according to the routing protocol being used.

Scanned by CamScanner

Route Redistribution Direction

Redistribution is possible in two ways which are as follows:

- **One-way route redistribution**: Routing information is redistributed from one routing protocol or domain to another, but not vice versa.
- **Two-way route redistribution**: Routing information is redistributed from one routing protocol or domain to another, and vice versa. Figure 25 shows the route redistribution direction:

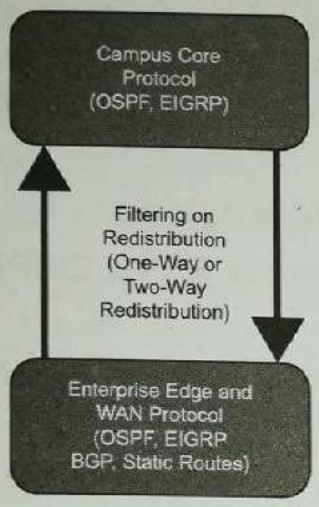


Figure 25: Route Redistribution Direction

5.7. 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

5.8. Redistributing And Filtering With Bgp

During a normal BGP operation, peer routers redistribute routes from each other. However, in some specific situations it may be best not to advertise routes from one peer, such as if the peer is redundant with another peer (they share the same routes exactly), if it might be

Scanned by CamScanner

unreliable in some or the other reason. An enterprise border router running BGP typically announces only the major network to the external domains. This is done using the BGP **network** router configuration command, which allows BGP to advertise a network that is already a part of its IP routing table.

If IGP routes are redistributed into BGP, make sure that only local routes i.e. Those that originate within the AS, are redistributed.

Private IP addresses must not be redistributed, so they should also be filtered. Configuring this filtering can be complex.

In the other direction, either a default route or a default route plus a few other specific routes is

passed into an enterprise AS. These can then be redistributed into the IGP running in the AS. Redistributing all BGP routes into an IGP is not advised, because non-BGP participating routers

do not require full Internet routing tables, and IGP protocols are unable to process large numbers

of advertised routes. Unnecessary routes should be filtered. Figure 26 depicts Route Redistribution in the enterprise network from the selected building access protocols, between campus core and WAN routers, between campus core and WAN routers, static routes or BGP routes into enterprise IGP:

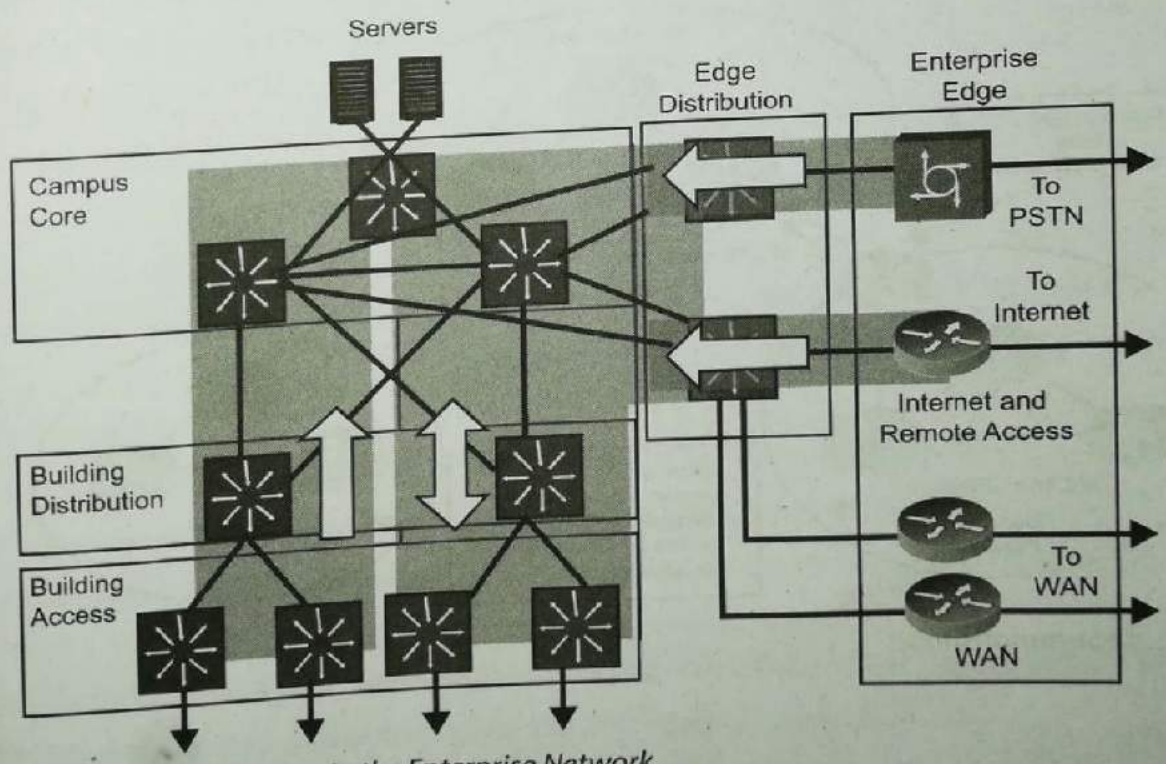


Figure 26: Route Redistribution in the Enterprise Network

Scanned by CamScanner

5.9. Route Summarisation

Route summarisation is also called route aggregation or supernetting. In route summarisation, a single summary address in the routing table represents a set of routes. Summarisation reduces the routing update traffic, the number of routes in the routing table, and the overall router overhead in the router receiving the routes.

The Benefits of Route Summarisation

A large flat network is not scalable because routing traffic consumes considerable network resources. When a network change occurs, it is propagated throughout the network, which requires processing time for route recomputation and bandwidth to propagate the routing updates.

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.

Summarisationis configured manually, or occurs automatically at the major network boundary 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:

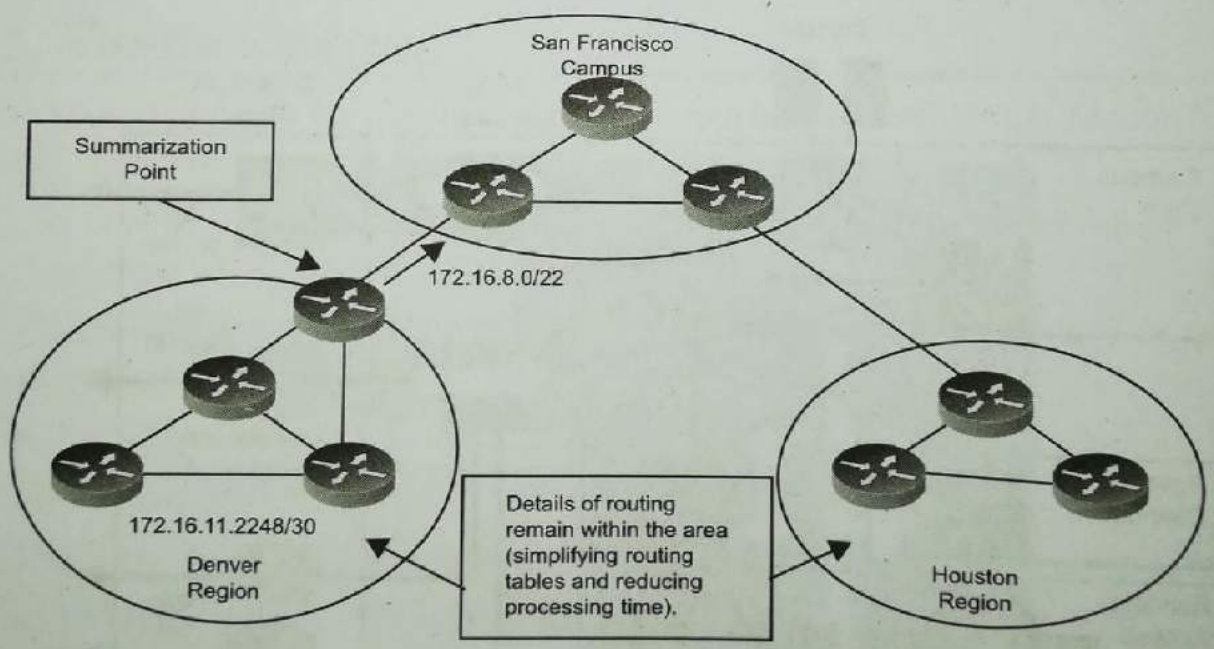


Figure 27: Route Summarisation

Scanned by CamScanner

5.10. Summary

This chapter highlights IPv4 and IPv6 addressing and routing Algorithms. It starts with topics as Private and Public IP addresses, steps in designing an IP address, hierarchical addressing, Static and Dynamic (DHCP) address assignment, Static and dynamic (DNS) name resolution, features of IPv6, types of IP address, and IPv4-to-IPv6 transition strategies. Later, we discussed routing i.e. different IPv6 routing protocols, static versus dynamic routing, distance vector versus link-state versus hybrid routing protocols, Routing protocol metrics and flat versus hierarchical protocols in detail. Finally, we concluded the chapter with the detailed explanation of route summarisation.

Questions

1. For the address 168.23.5.237/24:
   - What is the mask?
   - What class is the address?
   - What is the host part?
   - What is the network part?
   - How many hosts can reside on this subnet?
2. What characteristics determine the size of the network?
3. What type of routing protocol can support VLSM?
4. Assume that a router has the following subnets behind it:
   - 12.7.16.0/24
   - 12.7.17.0/24
   - 12.7.18.0/24
   - 12.7.19.0/24

   What summary route can the router advertise to represent these four subnets?
5. What factors lead to a poorly designed IP addressing scheme and what are its disadvantages?
6. What are some advantages of a hierarchical IP addressing scheme?
7. Differentiate between classless and classful routing protocols.
8. Differentiate between DHCP and static address assignment. Why is dynamic method better?
9. What is the advantage of using dynamic name resolution over static name resolution?
10. With the help of a neat diagram give the IPv6 packet header.
11. Which is the valid way of writing the following IPv6 address:

    2044:0000:178A: 0000:0000:069C: 0001:006D?

Scanned by CamScanner

a. 2044: 178A:069C: 1:006D

b. 2044: 178A: 69C:1: 6D

c. 2044:0: 178A:069C: 1:006D

d. 2044::178A: 0:0: 69C:1: 6D

e. 2044::0: 178A: 69C:1: 6D

12. Specify the address assignment strategies available in IPv6?
13. Which feature allows DNS to support IPv6? Can a host support IPv4 and IPv6 simultaneously?
14. Describe briefly the mechanisms for transitioning from IPv4 to IPv6.
15. Which IPv6 routing protocols are supported on Cisco routers?
16. What multicast address is used for RIPng?
17. In which situations can static routing be preferred over dynamic routing?
18. How do distance vector and link-state routing protocols differ?
19. What parameters do the following routing protocols use in their metric calculation by default?
    - RIP
    - EIGRP
    - OSPF
    - BGP
    - IS-IS
20. How does a hierarchical network differ from a flat network?
21. Describe features of EIGRP in brief.
22. What is the difference between an Integrated IS-IS backbone and an OSPF backbone? Write advantages of each.
23. What is the main use of BGP?
24. Which routing protocols are likely to be used in an enterprise Campus Core?
25. Describe route redistribution.
26. What is route filtering and why is it required?
27. What is route summarization?

Scanned by CamScanner

Software Defined Networking

6

OBJECTIVES

After reading this chapter, the student will be able to:

- To understand Software Defined Networking (SDN)
- To implement Open Flow Switch
- To understand the working of Open Flow Controller
- To understand the working of Open Flow in Cloud Computing
- To evaluate a case-study- Effect of SDN on Traditional Enterprise Network Design

Scanned by CamScanner

6.1. Understanding Software Defined Networking [SDN]

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

SDN focuses on the key features are listed as follows:

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

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

Networking the Traditional Way:

Traditional network architectures are increasing inadequately to face the growing complexity, variability, and high volume of data, in spite of the greater capacity of transmission schemes and greater performance of network devices. The traditional internetworking approach is based on the TCP/IP protocol architecture. The characteristics of the traditional approach are as follows:

- **Complex Architecture:** To respond for demands such as high and fluctuating traffic load, differing levels of QoS and security requirements, the complexity of networking technology has grown. This has resulted in a number of independently defined protocols each of which addresses a portion of networking requirements.
- **Variable Policies:** In a huge and complex network, when a new machine is activated, it can take hours or even days to reconfigure the entire network. To implement a network-wide security policy, the staff may have to make configuration changes to thousands of devices and mechanisms.
- **Scalability Issue:** Demands on networks are growing rapidly, both in volume and variety. Adding network devices and transmission capacity, involving multiple vendor equipment, is difficult because of the complex and, static nature of the network.
- **Vendor Dependence:** Lack of open interfaces for network functions leaves the enterprises limited by the relatively slow product cycles of the vendor equipment. Due to the nature of today's traffic demands on networks, enterprises need to deploy new capabilities and services rapidly in response to changing business needs and users' demands.

Scanned by CamScanner

Today the networking environment faces various limitations in the era of computing. The difficulty is the lack of integration between applications and network infrastructure. As demonstrated in the previous section, traditional network architectures are inadequate to meet the demands of the growing volume and variety of traffic. The centralised control of the network can work to solve the drawbacks of traditional networks, hence there is a growing demand for Software Defined Networking (SDN).

In traditional networks, as shown in Figure 1(a), the control and data planes are combined in a network node. The control plane is responsible for configuration of the node and programming the paths to be used for data flows. Once these paths have been determined, they are pushed down to the data plane. Data forwarding at the hardware level is based on this control information. In this traditional approach, once the flow management (forwarding policy) has been defined, the only way to make an adjustment to the policy is via changes to the configuration of the devices. This has proven restrictive for network operators who are keen to scale their networks in response to changing traffic demands, increasing use of mobile devices, and the impact of 'big data'.

Networking the SDN Way

SDN has emerged from service-focused requirements, Control moves out of the individual network nodes and goes into the separate, centralised controller. SDN switches are controlled by a network operating system (NOS) that collects information, using the API as shown in Fig. 1(b) and manipulates their forwarding plane, providing an abstract model of the network topology to the SDN controller hosting the applications. In Figure 1, the traditional network view is compared with the SDN network view

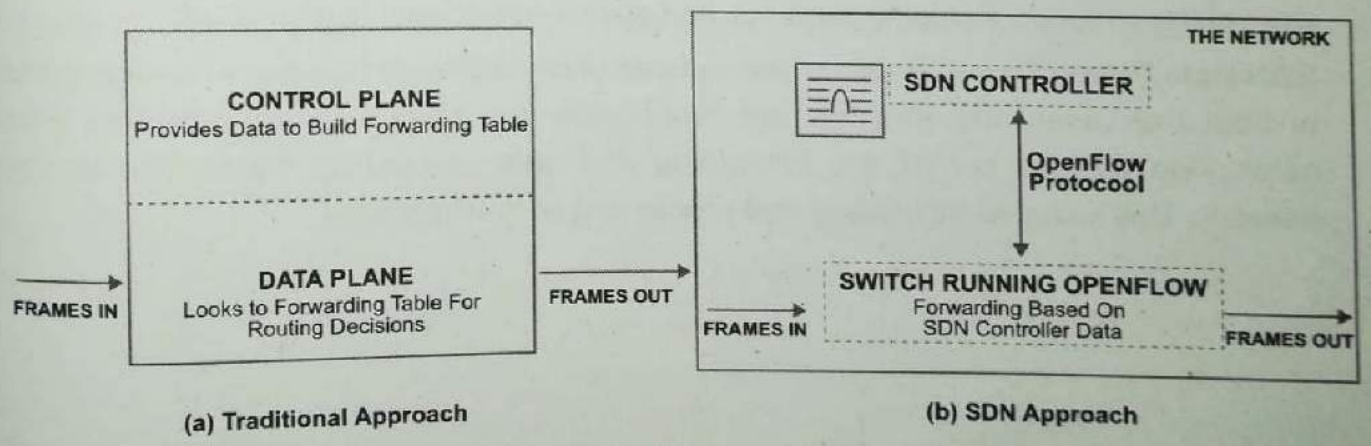


Figure 1: Traditional network view compared with SDN network view: a) Traditional approach (each network node has its own control and management plane); b) SDN approach (the control plane is extracted from the network node)

Scanned by CamScanner

The main concept of SDN lies in the notion of decoupling the control and data planes that is shown in Figure 1 (b). In SDN, the control plane is no longer distributed amongst network nodes, as in the traditional network, instead it is centralised at the controller which communicates with network nodes to setup the data plane through a southbound SDN protocol. The data plane is simply responsible for forwarding packets, whereas the control plane provides the 'intelligence' in designing routes, setting priority and routing policy parameters.

SDN Architecture

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

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

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

Scanned by CamScanner

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

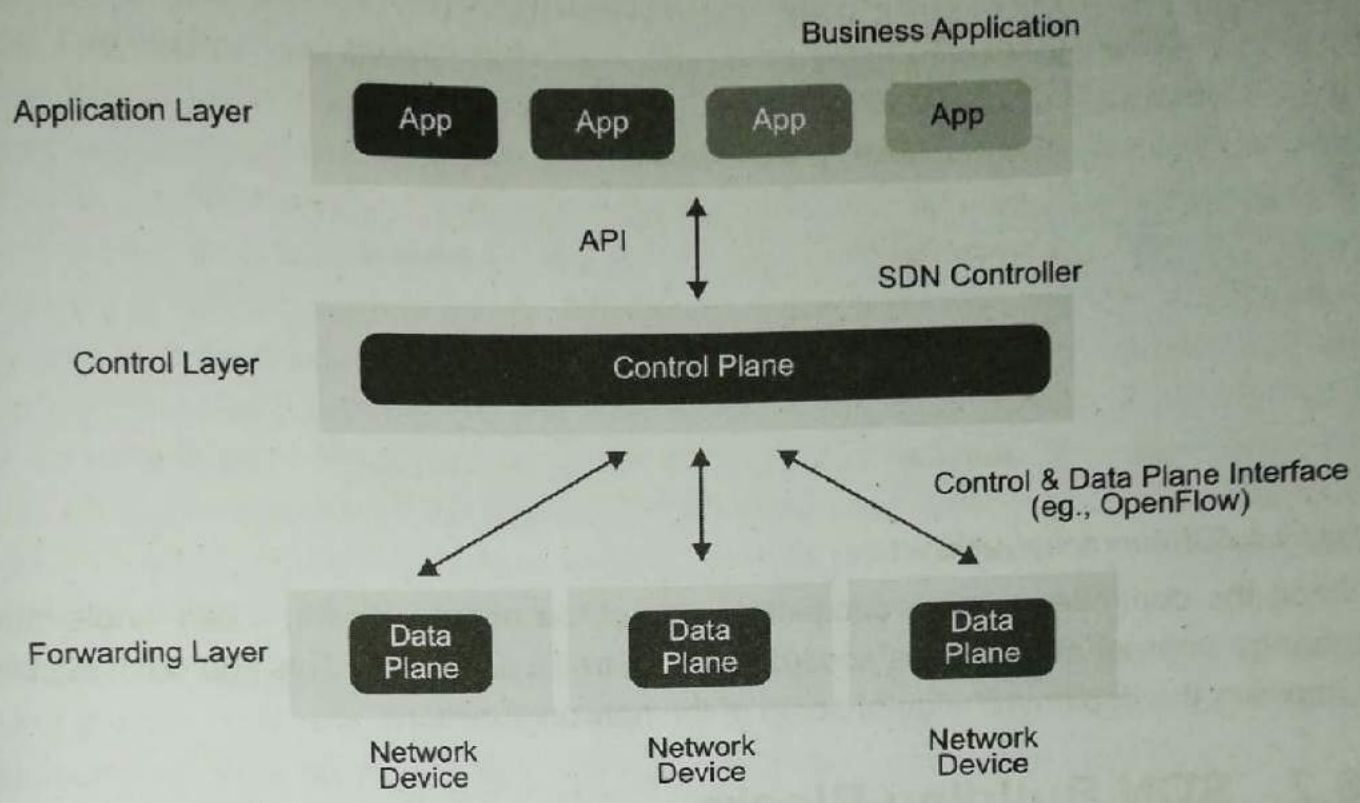


Figure 2: Software-Defined Network Architecture

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

Scanned by CamScanner

Figure 3 shows the SDN functional architecture:

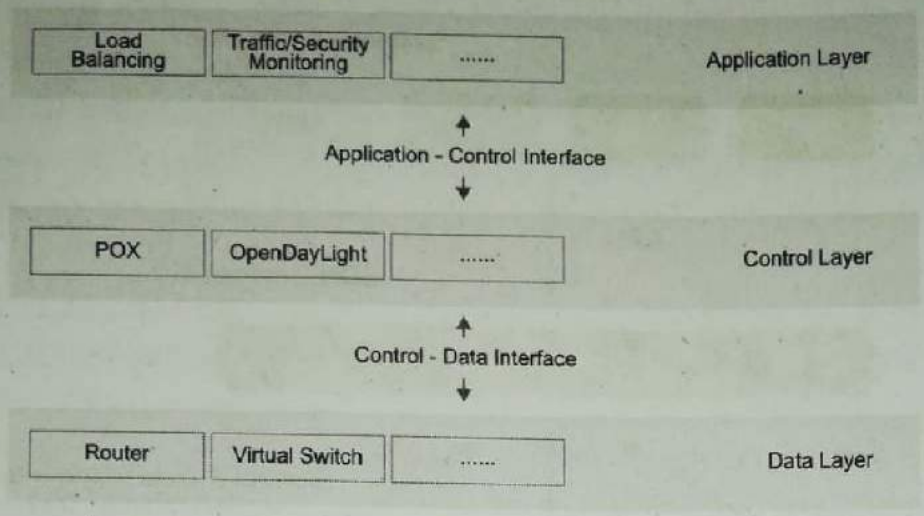


Figure 3: SDN Functional Architecture

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

6.2. SDN Building Blocks

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

Figure 4 describes the building blocks of SDN:

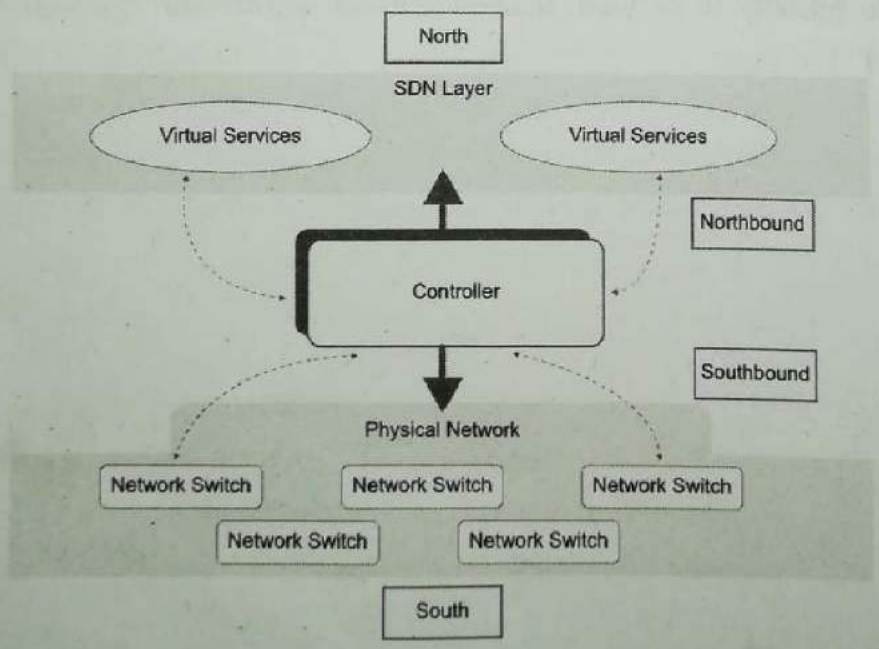


Figure 4: SDN Building Blocks and Interfaces

Scanned by CamScanner

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

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

6.3. Open Flow Protocol

OpenFlow protocol is the most well-known SDN protocol that has been chosen as the standard bearer in software defined networking. OpenFlow is a protocol that allows a server to tell network switches where to send packets. In a conventional network, each switch has proprietary software that tells it what to do. With OpenFlow, the packet-moving decisions are centralised, so that the network can be programmed independently of the individual switches .An OpenFlow protocol enables network controllers to determine the path of network packets across a network of switches. The controllers are distinct from the switches. This separation of the control from the forwarding allows for more sophisticated traffic management and is feasible using access control lists (ACLs) and routing protocols. Also, OpenFlow allows switches from different vendors to be managed remotely using a single, open protocol, hence can consider OpenFlow as an enabler of the software defined networking (SDN).

In a conventional switch, packet forwarding (the data path) and high-level routing (the control path) occur on the same device. An OpenFlow switch separates the data path from the control path. The data path portion resides on the switch itself; a separate controller makes

Scanned by CamScanner

high-level routing decisions. The switch and the controller communicate by means of the OpenFlow protocol. Figure 5 displays the structural view of an OpenFlow protocol.

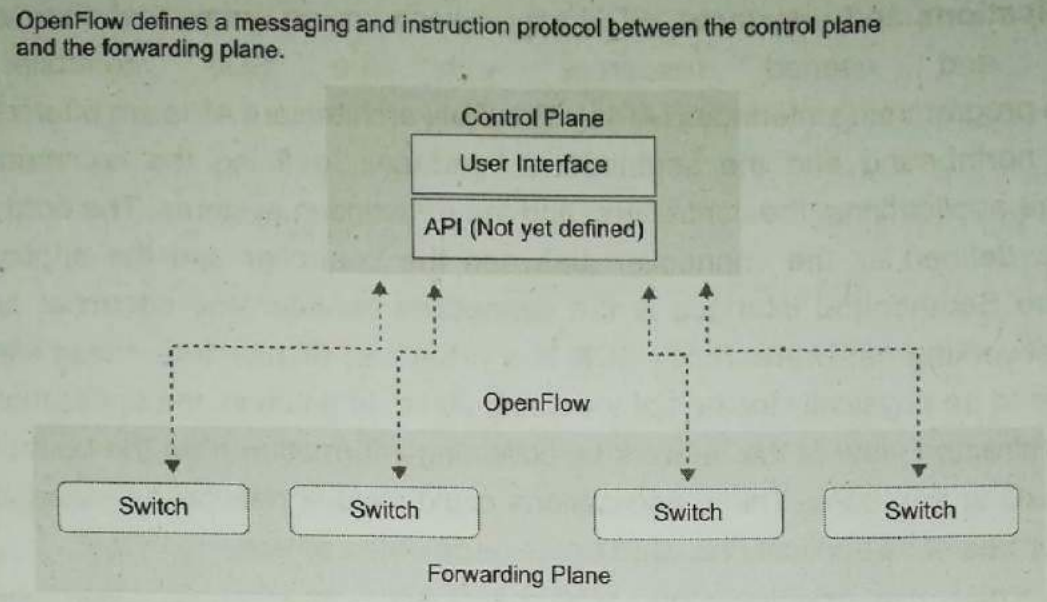


Figure 5: Structural view of Open Flow Protocol

6.4. Openflow Message Types

OpenFlow protocol consists of a number of message types that are used for communication between the switch and the controller. These messages can be classified into three groups: controller to switch messages, asynchronous messages and symmetric messages.

Controller-to-switch messages are initiated by the controller and used to manage directly or inspect the state of the switch. Asynchronous messages are initiated by the switch and used to update the controller of network events and changes to the state of the switch. The symmetric messages are initiated by either the switch or the controller and sent without solicitation. The message types used by OpenFlow are described below.

Controller-to-Switch Messages:

The controller/switch messages are initiated by the controller and may or may not require a response from the switch.

- **Features:** The controller may request the capabilities of the switch by sending a features request; the switch must respond with a features reply that specifies the capabilities of the switch. This is commonly performed upon establishment of the OpenFlow channel.
- **Configuration:** The controller is able to set and query configuration parameters in the switch. The switch only responds to a query from the controller.
- **Modify-State:** The modify-state messages are sent by the controller to manage state of the switches. Their primary purpose is to add, delete and modify the flow/group entries in the OpenFlow tables and to set switch port properties.

Scanned by CamScanner

- **Read-State:** The read-state messages are used by the controller to collect various information from the switch, such as current configuration, statistics and capabilities.
- **Packet-out:** These are used by the controller to send packets out of a specified port on the switch, and to forward packets received via packet-in messages. The packet-out messages must contain a full packet or a buffer ID referencing a packet stored in the switch. The message must also contain a list of actions to be applied in the order in which they are specified; an empty action list drops the packet.
- **Barrier:** The barrier request/reply messages are used by the controller to ensure message dependencies have been met or to receive notifications for completed operations.
- **Role-Request:** The role-request messages are used by the controller to set the role of its OpenFlow channel, or query that role. This is mainly useful when the switch connects to multiple controllers.
- **Asynchronous-Configuration:** The asynchronous-configuration messages are used by the controller to set an additional filter on the asynchronous messages that it wants to receive on its OpenFlow channel, or to query that filter. This is mostly useful when the switch connects to multiple controllers and commonly performed upon establishment of the OpenFlow channel.

Asynchronous Messages

The asynchronous messages are sent without a controller soliciting them from a switch. The switches send asynchronous messages to controllers to denote a packet arrival, change in switch state, or an error. The four main asynchronous message types are described below:

- **Packet-in:** It transfers the control of a packet to the controller. Other processing, such as TTL checking, may also send packets to the controller using packet-in events
- **Flow-Removed:** It informs the controller about the removal of a flow entry from a flow table. It is generated as a result of the controller flow delete requests or the switch flow expiry process, when timeout of one of the flows is exceeded.
- **Port-status:** It informs the controller of a change on a port. The switch is expected to send port status messages to controllers as a port configuration or change in a port state.

Symmetric Messages:

The symmetric messages are sent without solicitation, in any direction.

- **Hello:** The hello messages are exchanged between the switch and the controller upon a connection start-up.

Scanned by CamScanner

- **Echo:** The echo requests/reply messages can be sent from either the switch or the controller, and must return an echo reply. They are mainly used to verify the liveness of a controller-switch connection, and may as well be used to measure its latency or bandwidth.
- **Experimenter:** The experimenter messages provide a standard way for OpenFlow switches to offer additional functionality within the OpenFlow message type space.

6.5. Implementing Openflow Switch

OpenFlow Reference Switch:

An OpenFlow Switch consists of one or more flow tables and a group table, which performs packet lookups and forwarding, and an OpenFlow channel to an external controller. Figure 6 shows the components of an OpenFlow switch:

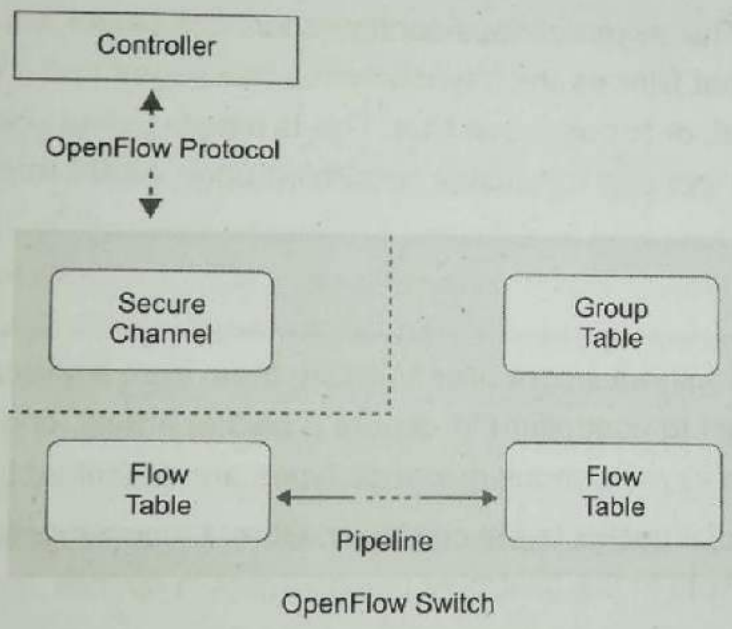


Figure 6: Components of an OpenFlow Switch

The switch communicates with the controller and the controller manages the switch via the OpenFlow protocol. The OpenFlow protocol allows the switches to be controlled by an independent controller. The communication between the switch and the controller is often over a Transport Layer Security (TLS) enabled channel. According to the specification each switch must contain one or more flow tables which will keep the flow entries specified by the controller. Using the OpenFlow protocol, the controller can add, update, and delete flow entries in the flow tables, both reactively (in response to packets) and proactively. Each flow table in the switch contains a set of flow entries; each flow entry consists of the match fields, counters, and a set of instructions to apply to matching packets. The flow entries match packets in their priority order, with the first matching entry in each table being used. If a matching entry is found, the instructions associated with that specific flow entry are

Scanned by CamScanner

executed. If no match is found in a flow table, the outcome depends on the configuration the table-miss flow entry: For example, the packet may be forwarded to the controller ov the OpenFlow channel, dropped, or may continue to the next flow table.

Structure of a Flow-table

The basic building block of the logical switch architecture is the flow table. Each packet that enters a switch passes through one of more flow tables. Each flow table consists of a number of rows, called entries. A flow entry includes a header that identifies the individual flow that the packets are matched against and a set of actions that are to be taken by the switch for the matched packets. The matching is made on the packet header fields. The actions that are taken can vary from packet forwarding, drop, further lookups in other flow tables, rewriting of the header fields.

Figure 7 displays the Open Flow table entry:

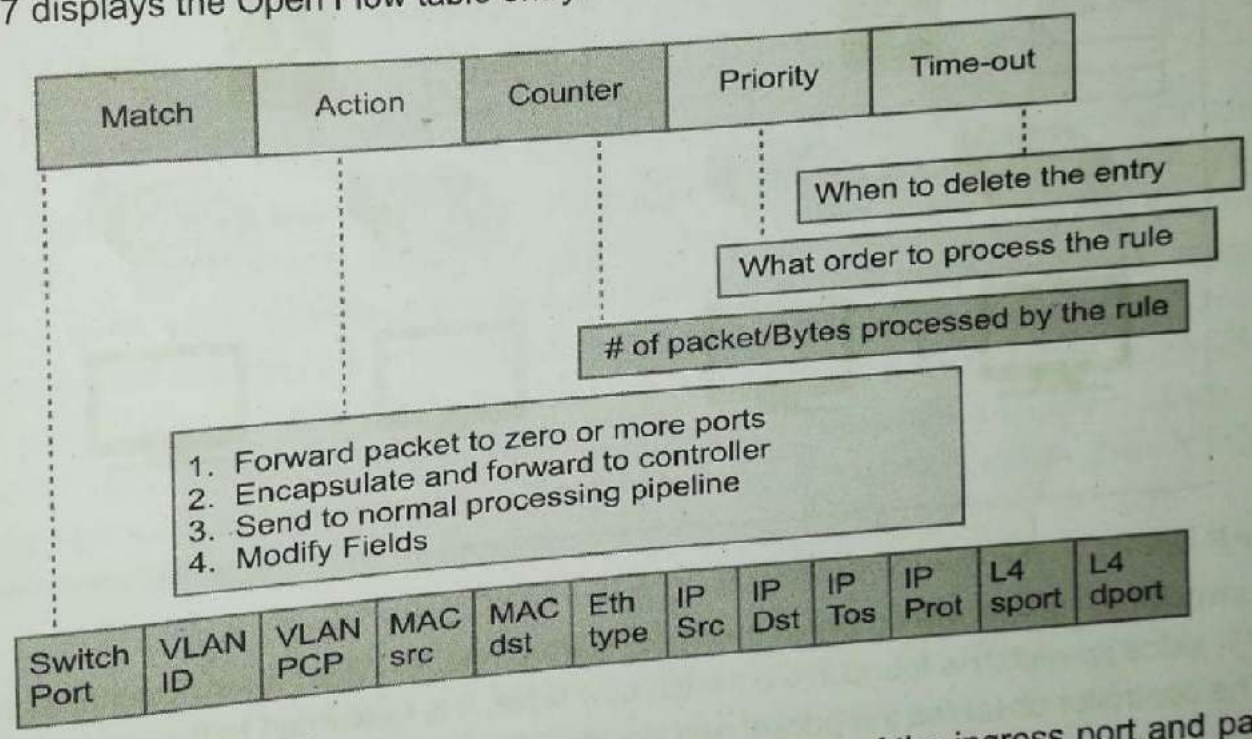


Figure 7: Open Flow Table Entry

- **Match fields:** To match against packets. These consist of the ingress port and packet headers, and optionally metadata specified by a previous table.
- **Priority:** Matching precedence of the flow entry
- **Counters:** To update for matching packets
- **Timeouts:** Maximum amount of time or idle time before flow is expired by the switch
- **Cookie:** Opaque data value chosen by the controller. May be used by the controller to filter flow statistics, flow modification and flow deletion, not used when processing packets.

Scanned by CamScanner

A flow table entry is identified by its match fields and priority: the match fields and the priority taken together identify a unique flow entry in the flow table. The flow entry that wildcards all fields (all fields omitted) and has priority equal to 0 is called the table-miss flow entry. Per table, per flow, per port and per queue counters are the four available statistic scopes kept in the flow table. The controller could query the switch to forward the statistics.

Open Flow Operation

The Figure 8 describes the steps taken in routing a flow between two hosts across two switches in SDN network:

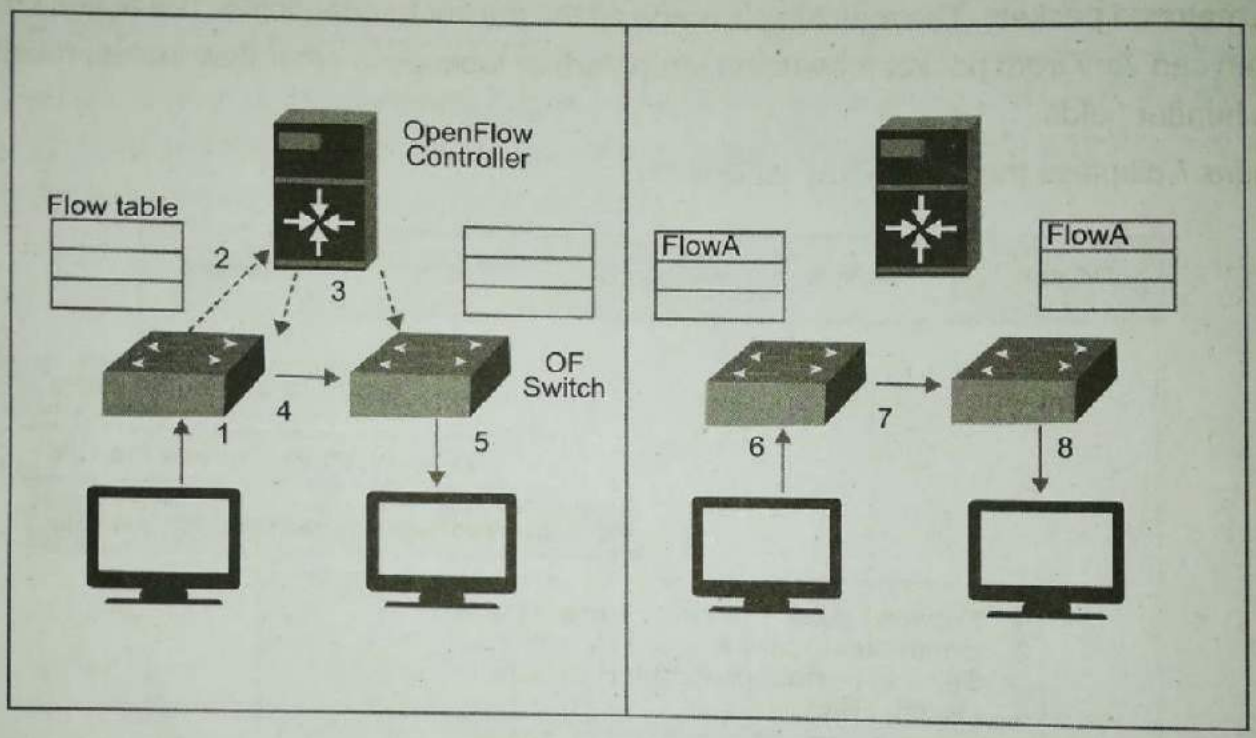


Figure 8: OpenFlow Flow Processing Procedure

The switch flow tables are empty in the initial startup phase. When a new packet arrives in step 1, since no match is found in the switch flow table, it is forwarded to the controller (step 2). The controller observes the packet and decides the action that should be taken (forward or drop) and creates a flow entry accordingly. This flow entry is sent to the switches in the path that the packet will traverse (step 3). Then, the packet is sent through to the receiving host in steps 4 and 5. In steps 6, 7, and 8 any of the new packets belonging to the same flow are routed directly since they would match the new entry in the flow tables.

Scanned by CamScanner

Figure 9, shows the flow of an OpenFlow processing:

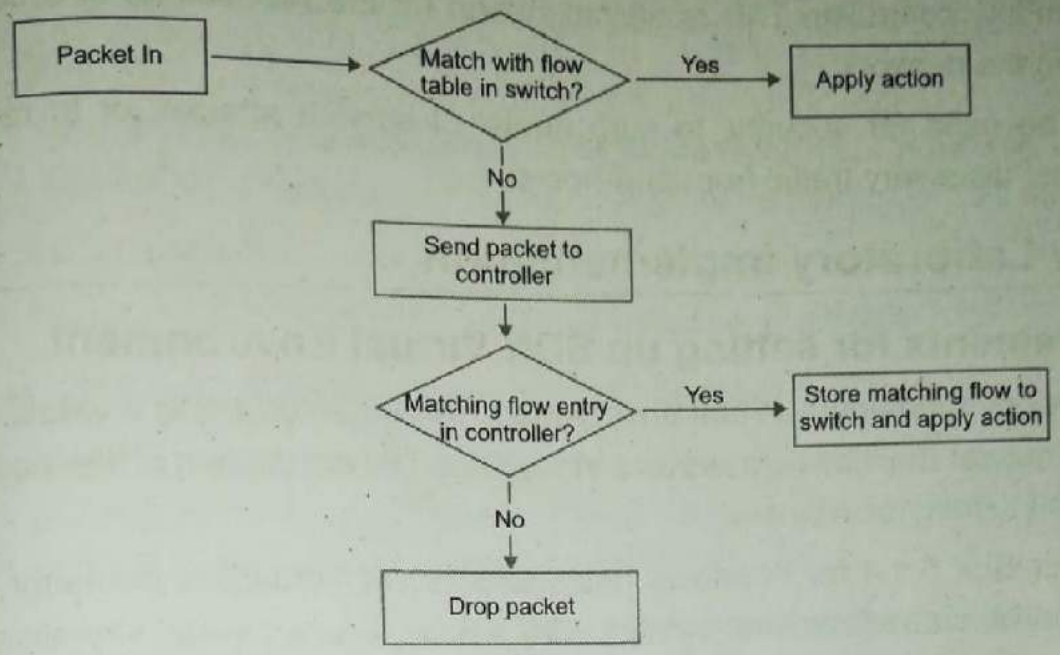


Figure 9: Flow Chart detailing packet flow in an Open Flow

In this once the first packet arrives at the switch, the flow table is checked for a matching flow rule. If a match is found, then the flow actions specified by the flow rule will be executed and the flow statistics are updated otherwise the packet header is forwarded to the controller over a secure channel. The controller processes the packet according to the defined algorithm in the controller and specifies the actions that are to be taken by the switches along the chosen path between the source and the destination. The new flow rule will be sent to the switches in the path to be installed in their flow tables. The switch will start taking appropriate actions on the data packets of the flow based on the new flow rule. If no matching flow entry is found in the controller the packets will be dropped.

Flow Table Entry Field

The basic OpenFlow switch and, the OpenFlow Type-0 switch, classify packets into flows that are based on a 10- tuple. The 10-tuple entails of the following fields:

Ingress Port	Ether source	Ether dst	Ether type	VLAN id	VLAN priority	IP src	IP dst	IP proto	IP Tos bite	src port	dst port

Figure 10: OpenFlow table entry header field

Figure 10 shows the header fields used as the match structure. If any of the fields are wild carded that field will be ignored while matching against the incoming packets.

The Flow table entries are matched by using a 10-tuple to find the corresponding actions associated with the flow. The OpenFlow Type-0 switch has three required actions:

- **Forward to a specified set of output ports:** This is used to move the packet across the network.

Scanned by CamScanner

- **Encapsulate and send to the controller:** The packet is sent via the secure channel to the remote OpenFlow controller. This is typically used for the first packet of a flow to establish a path in the network.
- **Drop:** This can be used for security, to curb denial of service attacks, or to reduce spurious broadcast discovery traffic from end-hosts.

SDN OpenFlow Laboratory Implementation

Software Requirements for setting up SDN Virtual Environment

To implement an SDN environment, a virtual environment can be setup using a virtual box. Mininet is a network emulator that can be used as a VirtualBox. The description of the required software installation is as described below:

- **Virtual Box:** VirtualBox 5.1.4 for Windows hosts Oracle VM VirtualBox (formerly Sun VirtualBox, Sun xVM VirtualBox and Innotek VirtualBox) is a software virtualisation package that installs on an operating system as an application. VirtualBox may be installed on a number of host operating systems, including: Linux, OS X, Windows, Solaris, and OpenSolaris. VM has two network interfaces. One is a NAT interface that can be used to access the Internet, and the other one is a host-only interface to enable it to communicate with the host machine. For example, NAT interface could be eth0 and have a 10.x IP address, and your host-only interface could be eth1 and have a 192.168.x IP address. Both the interfaces should be configured using DHCP.

  `Download: http://www.virtualbox.org/wiki/Downloads`
- **Mininet:** Mininet 2.2.1 on Ubuntu 14.04

  Mininet is a network emulator, which creates virtual networks using process-based virtualisation and network name spaces. It runs a collection of end-hosts, switches, routers, and links on a single Linux kernel .It uses lightweight virtualisation to make a single system look like a complete network, running the same kernel, system, and user code. A Mininet host behaves just like a real machine; you can ssh into it (if you start up ssh and bridge the network to your host) and run arbitrary programs (including anything that is installed on the underlying Linux system.) The programs that you run can send packets through seems like a real Ethernet interface, with a given link speed and delay. Packets get processed by what looks like a real Ethernet switch, router, or middlebox, with a given amount of queueing. The switches in Mininet are software based switches like Open vSwitch. Links are virtual Ethernet pairs, which live in the Linux Kernel and connect our emulated switches to emulated hosts.

  `Download: http://mininet.org/download/`
- **Wireshark:**

  The wireshark is a free and open source packet analyser.

Scanned by CamScanner

- **Hping:**

  A network scanner that uses spoofed source address packets.

- **MiniEdit:**

  The Mininet network simulator includes MiniEdit, a simple GUI editor for Mininet. MiniEdit is an experimental tool created to demonstrate how Mininet can be extended.

- **SDN Controller**

  Various SDN controller have to be installed, e.g. POX, NOX, Ryu, Floodlight, etc.

Installation of Mininet on a Virtual Box

- **Step 1:** Installation of Virtual Box. It can be downloaded from the http address given in the previous section. Figure 11 and 12 displays the snapshot of the installation of VirtualBox and virtual machine respectively.

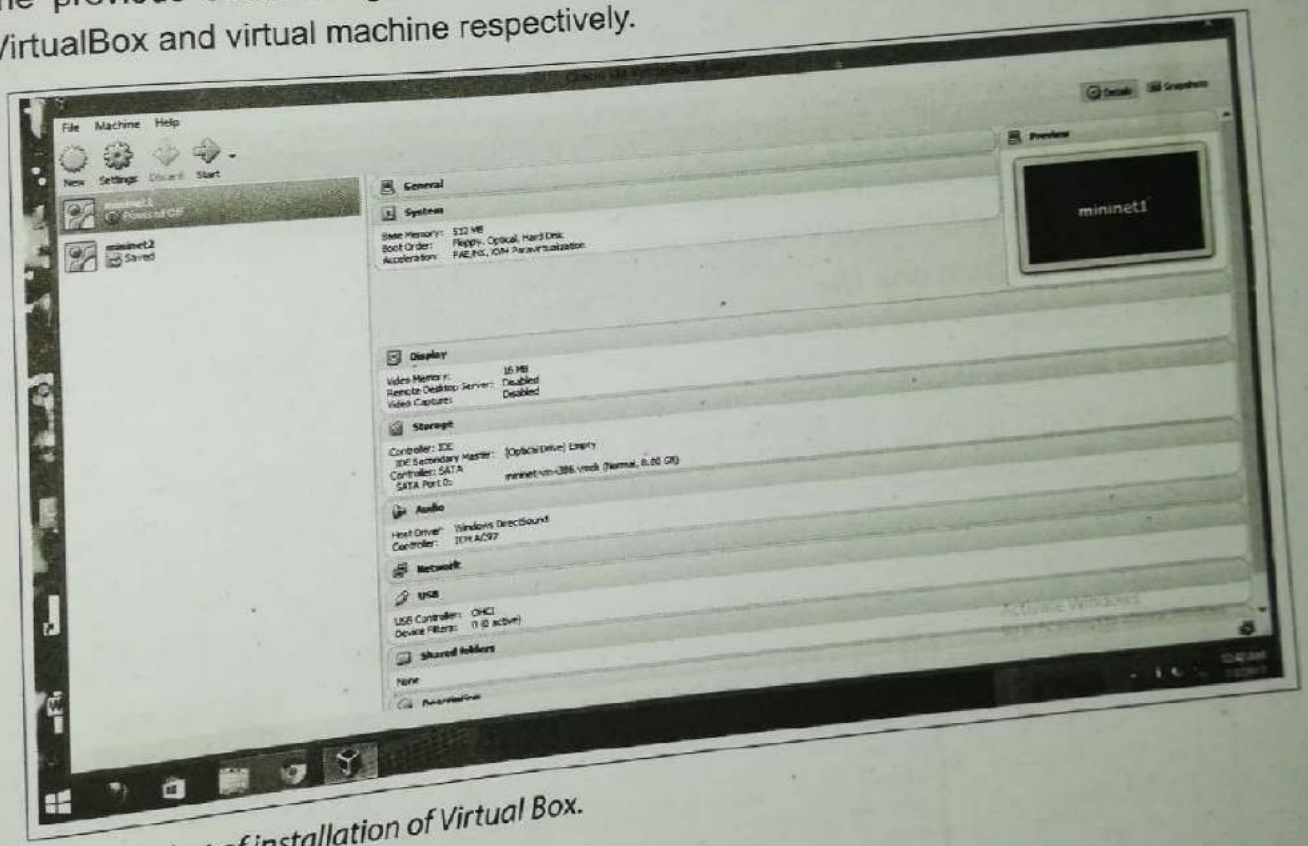


Figure 11: Snapshot of installation of Virtual Box.

Scanned by CamScanner

- **Step 2:** Installation of Virtual Machine and Mininet GUI

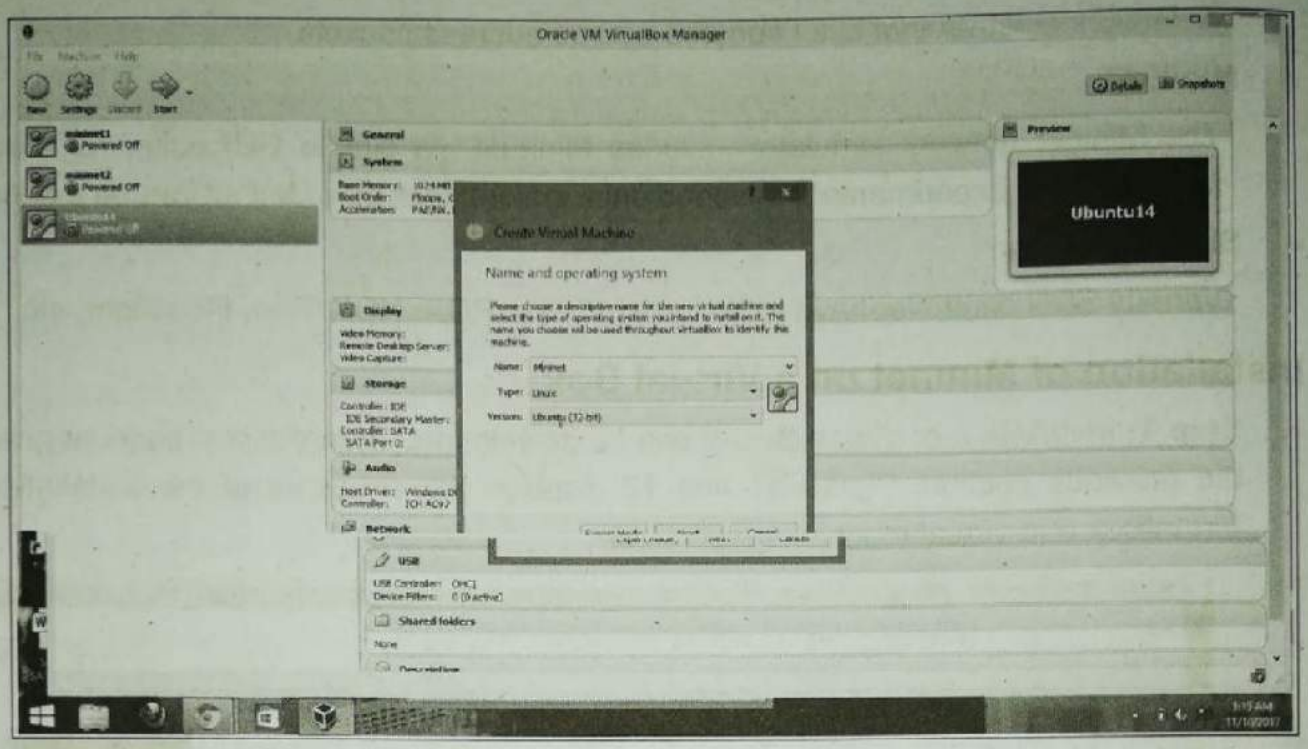


Figure 12: Snapshot of installation of Virtual machine

- **Step 3:** Select hard disk file.
- **Step 4:** Create
- **Step 5:** Add new interface from Virtual Box Setting

Figure 13 displays the snapshot of configuration of a virtual machine

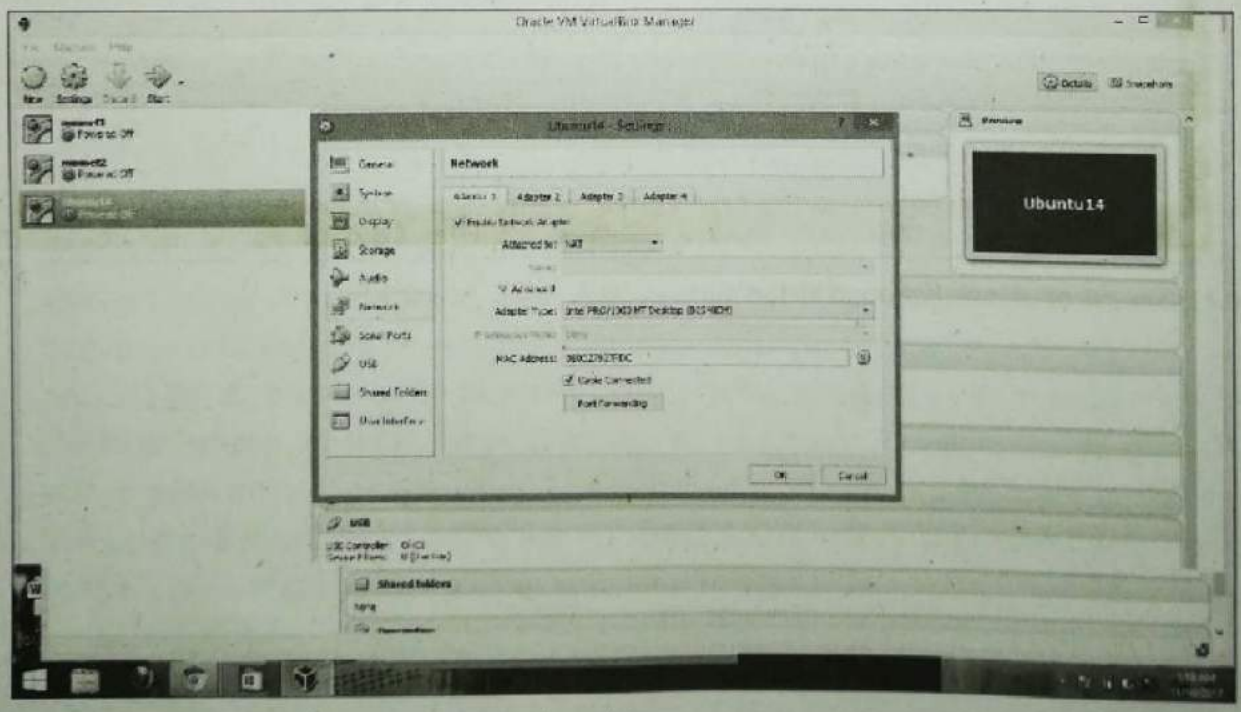


Figure 13: Snapshot of configuration of a Virtual machine

Scanned by CamScanner

- Steps to Run Mininet

Step 1: Start Mininet from Virtual Box.

Username: mininet

Password: mininet

Step 2: Configure Mininet interface with the local host interface using the following command:

$ sudodhclient.eth1

Step 3: Note the IP of interface eth1 through the following command:

$ sudoifconfig eth1

Step 4: Enter command prompt of the windows device and executeputty.exe to run Mininet on a local machine

>putty.exe –X mininet@ <IP Address of eth1>

Step 5: Run Mininet from putty.exe as follows:

Sudo mn

Step 6: Exit Mininet:

Mininet> exit

Step 7: Clear Mininet

```
$ sudo mn -c
```

Different topologies can be created using Mininet which are given below:

```
Command: $ sudo mn -topo minimal
```

The command will create a Minimal topology as given in figure 14

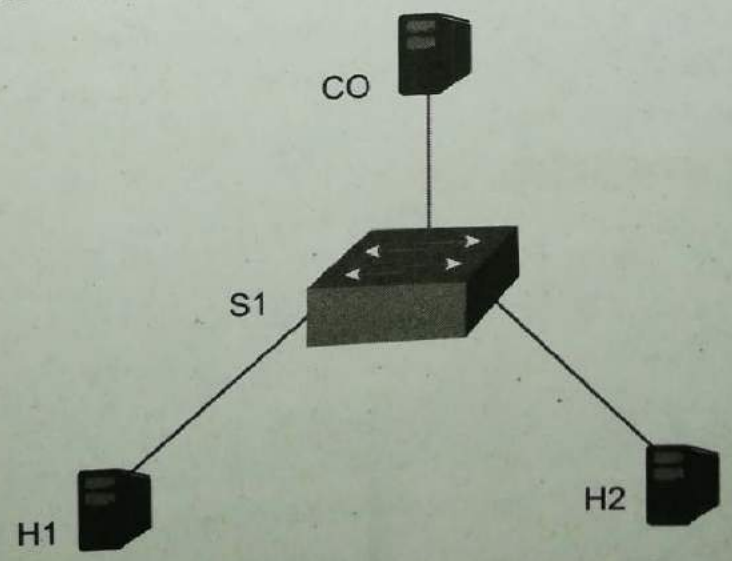


Figure 14: Minimal topology

Scanned by CamScanner

- **Steps to Run MiniEdit**

The Mininet network simulator includes MiniEdit, a simple GUI editor for Mininet. MiniEdit is an experimental tool created to demonstrate how Mininet can be extended.

Step 1: Set Up Network Access

Log in to the VM from the virtual machine console, then enter:

```
$ ifconfig -a
```

This will show three interfaces (eth0, eth1 and, lo), Both eth0 and eth1 should have assigned IP address. If this is not the case, type:

```
$ sudo dhclient ethX
```

Step 2: In order to use X11 applications such as xterm and wireshark, the Xming server must be running

```
2.1 Start Xming
2. 2Open a terminal
2.3 Change to the directory where putty is saved.
C:> cd <dir>
2.4 Run:
C:> putty.exe -X openflow@ [Guest IP Here]
```

Step 3: Start MiniEdit

The MiniEdit script is located in Mininet's examples folder. To run MiniEdit, execute the following command:

```
$ sudo ~/mininet/examples/miniedit.py
```

Step 4: Create a custom network topology using MiniEdit

First add some hosts to network scenario. Then click on the Host icon and, move the pointer to the location on the MiniEdit. Finally add controller, switch and, links. Figure 15 displays the snapshot of MiniEdit Interface

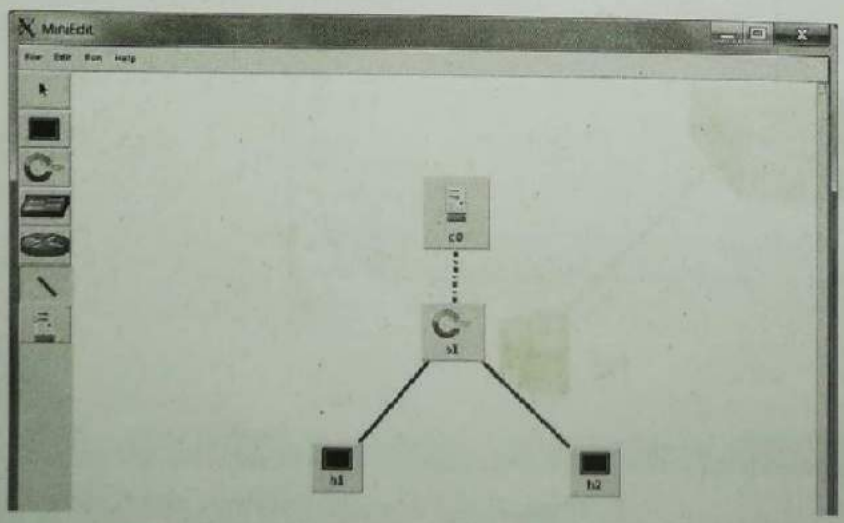


Figure 15: Snapshot MiniEdit Interface

Scanned by CamScanner

Step 5: Set MiniEdit Preferences

To set MiniEdit preferences, use the MiniEdit menu command, Edit → Preferences

By default, the MiniEdit console window does not give the user access to the Mininet command line interface. If you want to be able to use the Mininet CLI when a simulation is running, check the Start CLI box.

Step 6: Save topology file

To save the Mininet Topology file (*.mn), click on File in the top menu bar and select Save from the drop-down menu. Then type in a file name and save the file.

Step 7: Save custom Mininet script

To save the Mininet Custom Topology (*.py) file, click on File in the top menu bar and select Save Level 2 Script from the drop-down menu. Type in the file name and save the file.

Step 8: Run the MiniEdit network scenario

To start the simulation scenario, click the Run button on the MiniEdit GUI. In the terminal window from which you started MiniEdit, you will see some messages showing the progress of the simulation startup and then the Miniedit CLI prompt (because we checked Start CLI box in the MiniEdit preferences window). Figure 16 displays the snapshot of MiniEdit vm file output.

Figure 2.11 Snapshot of Mininet.vm output

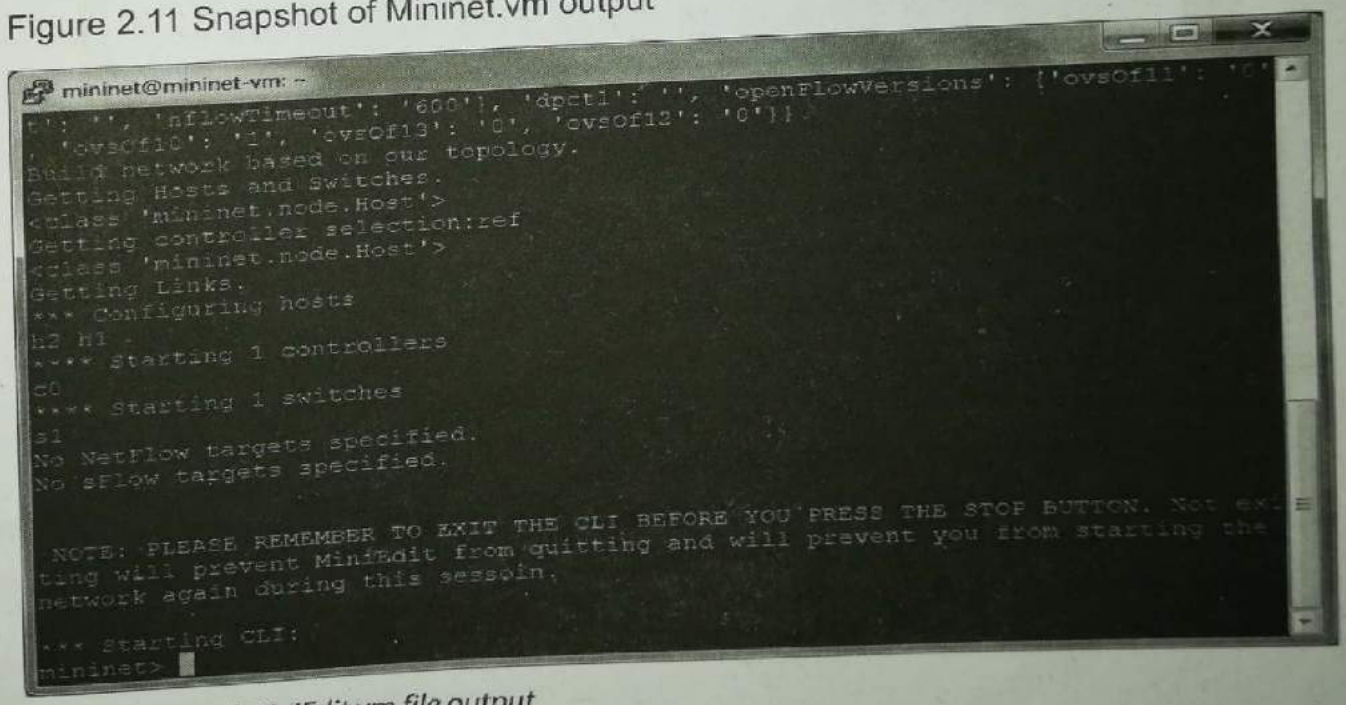


Figure 16: Snapshot of MiniEdit vm file output

Scanned by CamScanner

Experiment with the network-to check the contents of switch flow tables

Step 1: View Open vSwitch configurations

Run the MiniEdit menu command, Run → Show OVS Summary to see listing of switch configurations and verify that each switch is listening to the correct controller on the correct port.

Step 2: Check switch flow tables

Use MiniEdit to open an xterm connected to the host computer by using the MiniEdit menu command, Run → Root Terminal

In the root terminal window, first change the user id from root to mininet, so you can view the switches running in the mininet account.

Command: **# su mininet**

Then, check the flow table on switch s1 using the commands below. It should be empty.

Command: **$ sudo ovs-ofctl dump-flows s1**

Figure 17 displays that the Switch flow entries are initially empty

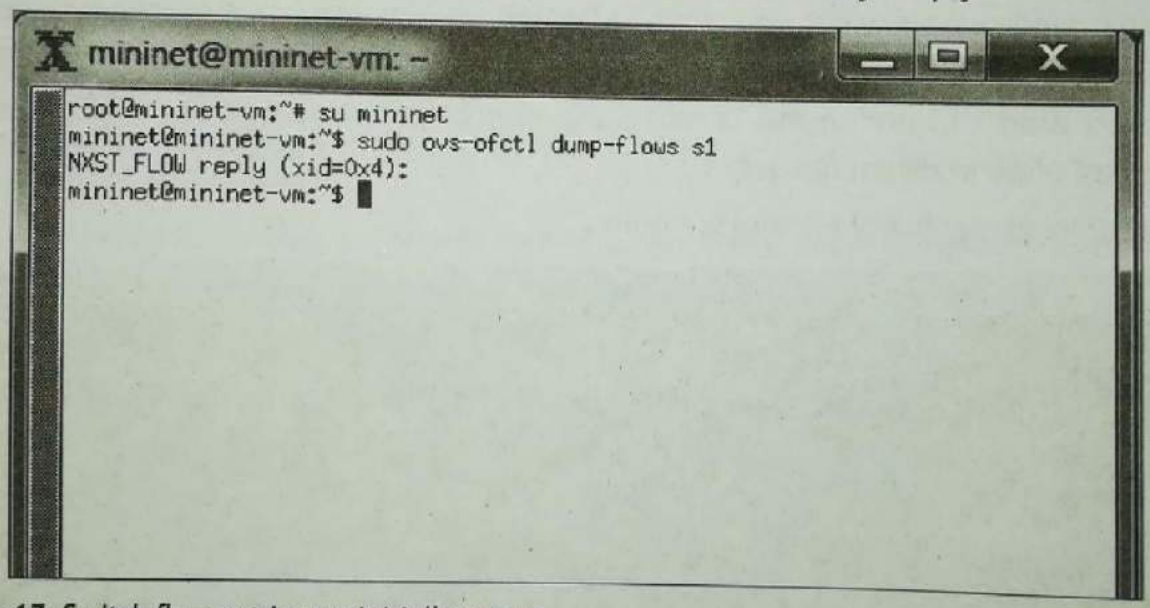


Figure 17: Switch flow entries are initially empty

Step 4: Run programs to generate and monitor traffic

Run a ping command to send traffic between host h1 and h8. On the MiniEdit console window, enter the following command:

```
mininet> h1 ping h2
```

Figure 18 displays the snapshot of the connection between two hosts:

Scanned by CamScanner

```
mininet@mininet-vm: ~
NOTE: PLEASE REMEMBER TO EXIT THE CLI BEFORE YOU PRESS THE STOP BUTTON. Not ex-
ting will prevent MiniEdit from quitting and will prevent you from starting the
network again during this seessoin.

*** Starting CLI:
mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=60.0 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=5.13 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.09 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=1.84 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.746 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=0.837 ms
64 bytes from 10.0.0.2: icmp_seq=7 ttl=64 time=4.31 ms
64 bytes from 10.0.0.2: icmp_seq=8 ttl=64 time=0.755 ms
64 bytes from 10.0.0.2: icmp_seq=9 ttl=64 time=1.40 ms
64 bytes from 10.0.0.2: icmp_seq=10 ttl=64 time=0.689 ms
64 bytes from 10.0.0.2: icmp_seq=11 ttl=64 time=1.38 ms
64 bytes from 10.0.0.2: icmp_seq=12 ttl=64 time=0.928 ms
64 bytes from 10.0.0.2: icmp_seq=13 ttl=64 time=0.720 ms
64 bytes from 10.0.0.2: icmp_seq=14 ttl=64 time=0.663 ms
64 bytes from 10.0.0.2: icmp_seq=15 ttl=64 time=1.57 ms
64 bytes from 10.0.0.2: icmp_seq=16 ttl=64 time=0.719 ms
64 bytes from 10.0.0.2: icmp_seq=17 ttl=64 time=1.22 ms
```

Figure 18: Snapshot of the connection between two hosts

Step 5: Check flow tables again

Check the flow table on switch s1 again. You should see flows installed for ICMP packets. On the root terminal window, enter the following command as shown in figure 19:

```
$ sudo ovs-ofctl dump-flows s1
```

```
mininet@mininet-vm: ~
root@mininet-vm:~# su mininet
mininet@mininet-vm:~$ sudo ovs-ofctl dump-flows s1
NXST_FLOW reply (xid=0x4):
 cookie=0x0, duration=651.041s, table=0, n_packets=24, n_bytes=1008, idle_timeou
t=60, idle_age=10, priority=65535,arp,in_port=1,vlan_tci=0x0000,dl_src=6a:17:b6:
df:52:ae,dl_dst=ce:27:8f:95:0f:4d,arp_spa=10.0.0.1,arp_tpa=10.0.0.2,arp_op=2 act
ions=output:2
 cookie=0x0, duration=651.058s, table=0, n_packets=24, n_bytes=1008, idle_timeou
t=60, idle_age=10, priority=65535,arp,in_port=2,vlan_tci=0x0000,dl_src=ce:27:8f:
95:0f:4d,dl_dst=6a:17:b6:df:52:ae,arp_spa=10.0.0.2,arp_tpa=10.0.0.1,arp_op=1 act
ions=output:1
 cookie=0x0, duration=656.08s, table=0, n_packets=654, n_bytes=64092, idle_timeo
ut=60, idle_age=1, priority=65535,icmp,in_port=1,vlan_tci=0x0000,dl_src=6a:17:b6
:df:52:ae,dl_dst=ce:27:8f:95:0f:4d,nw_src=10.0.0.1,nw_dst=10.0.0.2,nw_tos=0,icmp
_type=8,icmp_code=0 actions=output:2
 cookie=0x0, duration=656.065s, table=0, n_packets=654, n_bytes=64092, idle_time
out=60, idle_age=1, priority=65535,icmp,in_port=2,vlan_tci=0x0000,dl_src=ce:27:8
f:95:0f:4d,dl_dst=6a:17:b6:df:52:ae,nw_src=10.0.0.2,nw_dst=10.0.0.1,nw_tos=0,icm
p_type=0,icmp_code=0 actions=output:1
mininet@mininet-vm:~$
```

Figure 19: The switch flow entries showing ICMP Packets

Step 6: Stop the simulation

1. Press the Stop button on the MiniEdit GUI.
2. Quit the Mininet CLI by typing exit at the mininet> prompt.

Scanned by CamScanner

6.6. Openflow Controllers

The controllers are the focal point in the SDN networks and are also known as the brain of the network. The controller is the core of a software-defined network. It resides between network devices at one end of the network and applications at the other end. Any communication between applications and network devices must go through the controller. The controller communicates with applications -- such as firewalls or load balancers -- via northbound interfaces. The controller talks with individual network devices using a southbound interface, traditionally one like the OpenFlow protocol.

Different jobs are performed by the controller using a variety of modules. Some of these tasks include identifying the devices within the network and their capabilities, gathering network statistics, etc. Add-ons can be installed on the controller that will improve and widen the controller functionalities such as network monitoring and traffic anomaly detections.

An SDN controller is an application in a software-defined networking architecture that manages flow control for improved network management and application performance. The SDN controller platform typically runs on a server and uses protocols to tell switches where to send packets .The SDN controllers direct traffic according to forwarding policies that a network operator puts in place, thereby minimising manual configurations for individual network devices. By taking the control plane off of the network hardware and running it instead as software, the centralised controller facilitates automated network management and makes it easier to integrate and administer business applications. In effect, the SDN controller serves as a sort of operating system for the network.

Currently a number of well-known controller implementations are available that are open source and are written with different programming languages such as python, C++ and Java. Table 1, summarises the current implementations of different available controllers. The table1 provides a brief overview of the controller characteristics.

Table 1: Current Controller Implementations with the OpenFlow Standard

Controller	Implementation	Open Source	Developer	Overview
POX	Python	Yes	Nicira	General, open-source SDN controller written in Python.
NOX	Python/C++	Yes	Nicira	The first OpenFlow controller written in Python and C++

Scanned by CamScanner

Controller	Implementation	Open Source	Developer	Overview
MUL	C	Yes	Kulcloud	OpenFlow controller that has a C-based multi-threaded infrastructure at its core. It supports a multi-level north-bound interface (see Section III-E) for application development.
Maestro	Java	Yes	Rice University	A network operating system based on Java; it provids interfaces for implementing modular network control application and for them to access and modify network state.
Trema	Ruby/C	Yes	NEC	A framework for developing OpenFlow controllers written in Ruby and C.
Beacon	Java	Yes	Stanford	A cross-platform, modular, Java-based OpenFlow controller that supports event-based and threaded operations.
Jaxon	Java	Yes	Independent Developers	a Java-based OpenFlow controller based on NOX.
Helios	C	No	NEC	An extensible C-based openFlow controller that provides a programmatic shell for performing integrated experiments.

Scanned by CamScanner

Controller	Implementation	Open Source	Developer	Overview
Floodlight	Java	Yes	BigSwitch	A Java-based OpenFlow controller (supports vl. 3), based on the Beacon implementation, that works with physical- and virtual- OpenFlow switches.
SNAC	C++	No	Nicira	An OpenFlow controller based on NOX-0.4, which uses a web-based, user-friendly policy manager to manage the network, configure divices, and monitor events.
Ryu	Python	Yes	NTT, OSRG group	An SDN operating system that aims to provide logically centralized control and APIs to create new network management and control applications. Ryu fully supports OpenFlow v1.0, vl.2, vl.3 and the Nicira Extensions.
NodeFlow	JavaScript	Yes	Independent Developers	An OpenFlow controller written in JavaScript for Node JS[65]

Scanned by CamScanner

Controller	Implementation	Open Source	Developer	Overview
ovs-controller	C	Yes	Independent Developers	A simple OPenFlow controller reference implementation with Open vSwitch for managing any number of remote switches through the OpenFlow protocol; as a result the switches function as L2 MAC-learning switches or hubs.
Flowvisor	C	Yes	Stanford/ Nicira	Special purpose controller implementation.
RouteFlow	C++	Yes	CPqD	Special purpose controller implementation.

A number of both commercial and open source SDN controller implementations are recently developed. NOX and POX are the few prominent ones which are described in the next section.

6.7. NOX

NOX is an open source development platform for C++based software-defined networking control applications. NOX is the original OpenFlow controller. It serves as a network control platform, that provides a high-level programmatic interface for the management and the development of network control applications. Its system-wide abstractions turn networking into a software problem. NOX — initially developed by Nicira Networks and now, owned by VMware, along with Open Flow — was first introduced to the community in 2009. This was later divided into multiple different lines of development which are as follows:

1. **NOX classic:** This is the version that has been available under the GPL since 2009.
2. **NOX:** The 'new NOX.' only contains support for C++ and has lesser applications than the classic; however, this version is faster and has better codebase.
3. **POX:** It is typically termed as NOX's sibling that provides Python support.

Scanned by CamScanner

NOX Architecture

Figure 20 depicts the architecture of NOX.

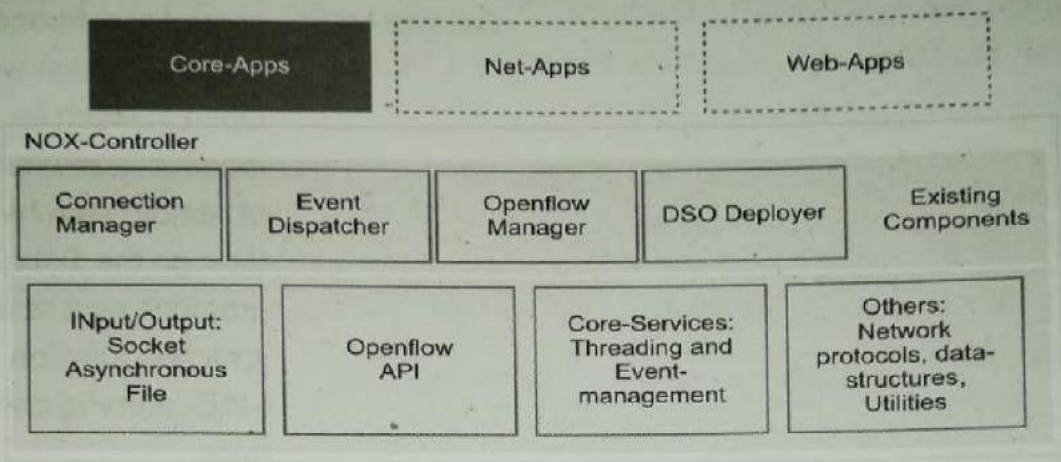


Figure 20: NOX Architecture

The NOX core provides helper methods, such as network packet process, threading and event engine, in addition to OpenFlow APIs for interacting with OpenFlow switches, and I/O operations support. At the upper layer, we have applications: Core, Net and Web. However, with the current NOX version, there are only two core applications: OpenFlow and switch, and both network and web applications are missing. The middle layer shows the in-built components of NOX. The dynamic shared object (DSO) deployer basically scans the directory structure for any components being implemented as DSOs.

6.8. POX

An open source OpenFlow controller has been implemented by a number of SDN developers and engineers. POX is a lightweight OpenFlow controller that is a suitable platform for SDN research, academic work, education, and experimentation. POX is a networking software platform that is written in Python.POX started life as an OpenFlow controller, but now it can also function as an OpenFlow switch, and can be useful for writing networking software in general. POX officially requires Python 2.7 (though much of it will work fine with Python 2.6), and should run under Linux, Mac OS, and Windows.POX currently communicates with OpenFlow 1.0 switches and includes special support for the Open vSwitch/Nicira extensions.

It also provides a web-based graphical user interface (GUI) and is written in Python, which typically shortens its experimental and developmental cycles compared to some other implementation languages, such as C++.

Scanned by CamScanner

Running POX Application

Step 1: Create the network scenario using Mininet

We will use the Mininet network emulator to create a test network that we will control using POX. We will use the MiniEdit GUI for Mininet to create the network.

Step2: Log into the Mininet VM

The Mininet VM should be running on your computer and should be accessible at the IP address assigned by the VirtualBox host-only interface. In this example, the VirtualBox host-only adapter's IP address *192.168.56.101*. Check the interface on the Mininet VM to see which IP address is assigned in your case.

Access the Mininet Vm with the command from a terminal window on your host computer:

```
trups: ~$ ssh -X mininet@192.168.56.101
```

Enter the password, *mininet*. The prompt will show that you are now logged into the Mininet VM:

```
mininet@mininet-vm:~$
```

Repeat this at least three times so you have three terminal windows open and logged into the Mininet VM.

Step 3: Create the network

We will use MiniEdit to create the network scenario. The MiniEdit script is located in Mininet's *examples* folder. To run MiniEdit, execute the following command:

```
$ sudo ~/mininet/examples/miniedit.py
```

Remember that Mininet needs to run with *root* privileges so use the *sudo* command.

Using the MiniEdit GUI, create a network that includes hosts, switches, and a controller. Add redundant links between switches, which creates loops in the network. In the example, we create a network topology as shown in figure 21 below:

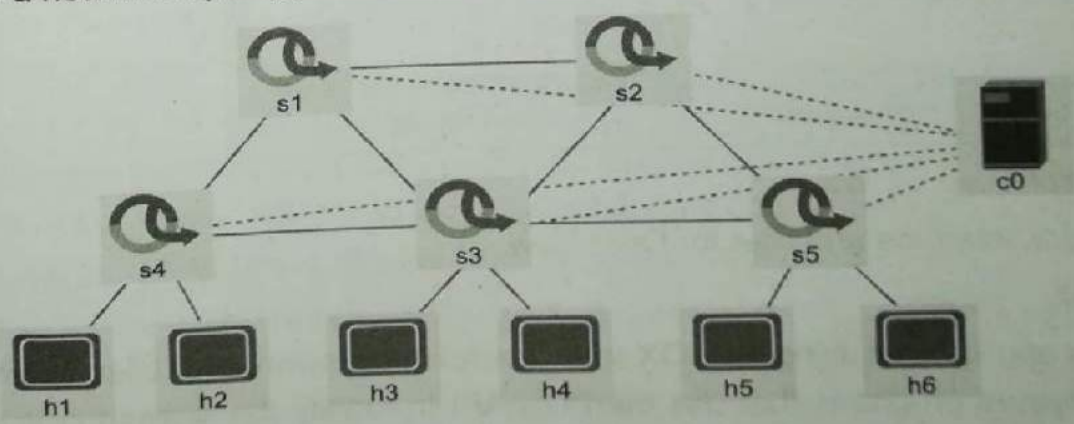


Figure 21: Snapshot of topology created using MiniEdit

Remember to configure the MiniEdit preferences so that the *Start CLI* function is enabled. Also, configure the controller as a *Remote Controller*.

Scanned by CamScanner

Step 4: Start the simulation

To start the simulation scenario, click the *Run* button on the MiniEdit GUI. The Mininet prompt will appear in the terminal window you used to start MiniEdit.

Step 5: Start Wireshark

Next, we start Wireshark and start capturing packets on the Mininet VM's loopback interface. We start Wireshark now, before starting the POX controller, because we need to capture the switch setup messages sent by the POX controller in order to learn which switch uses which port address.

In one of the terminal windows, start Wireshark with the command:

```
$ sudo wireshark &
```

Then select the *loopback interface* interface and start capturing. Then enter the text `of` in the filter box and click the *Apply* button. Now you will see only OpenFlow messages which are captured on the interface.

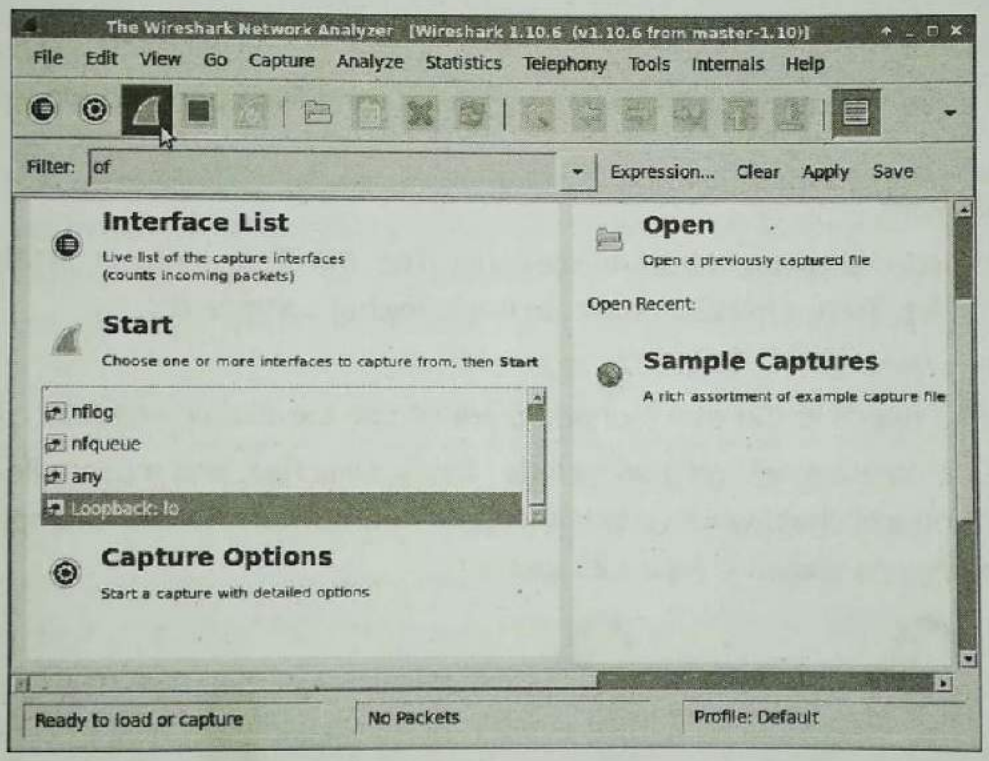


Figure 22: Snapshot of Wireshark Tool

Select the loopback interface and filter for OpenFlow

Step 6: Start POX

To create network applications using the POX software defined network controller, developers create and run Python programs that use the POX API to modify the state of switches in the network and to respond to the information those switches send to the POX controller. Programmers can write standalone programs that use the POX API or they can write programs that add functionality to POX directly. The latter type of program is called a *POX component*.

Scanned by CamScanner

The latest version of NOX and POX can be installed with the following commands:

```
$ git clone http://noxrepo.org/git/nox
$ git clone http://www.github.com/noxrepo/pox
```

Download the POX into your VM:

```
$ git clone http://github.com/noxrepo/pox
$ cd pox
```

Open a new terminal session. In the new terminal window (or tab), we will run the POX SDN controller. We will call this window the *POX console*.

The following command is used to start POX:

```
$ sudo ~/pox/pox.py forwarding. 12_learning \
  openflow.spanning_tree --no-flood --hold-down \
  log.level --DEBUG samples.pretty_log \
  openflow.discovery host_tracker \
  info.packet_dump
```

This starts POX and invokes POX components that create a network application that performs switching based on Ethernet MAC addresses and provides redundant links in the network while preventing packet storms due to loops. It also implements functions that will display more network events to the POX console and sets up *debug mode* in the console so we can see those network events

Step 7: Run Mininet

Run Mininet on a terminal window using the following command.

```
$ sudo mn --topo single,3 --mac --controller remote --switch ovsk
```

This starts a network emulation environment to emulate 5 switches and 6 hosts. The switch tries to connect to port 6633 on localhost. Initially, there is no controller listening.

- Since POX does not support OpenFlow 1.3 yet, it is best to statically set the OpenFlow version of the OVS

```
$ sudo ovs-vsctl set bridge s1 protocols=OpenFlow10
```

- Next, start the POX Controller. Assuming that the main folder where POX is installed is /home/ubuntu/pox, the command given as follows below starts the controller by initiating the OpenFlow Protocol Handler and the tutorial_hub application.

```
$ cd /home/ubuntu/pox &&. /pox.py log.level --DEBUG forwarding.
tutorial_12_hub
```

- The aforementioned command runs POX controller in DEBUG mode. This prints additional output of messages exchanged with the switch

```
POX 0.1.0 (betta) / Copyright 2011-2013 James McCauley, et al.
DEBUG:core:POX 0.1.0 (betta) going up...
DEBUG:core:Running on CPython
```


Scanned by CamScanner

```
DEBUG:core:Platform is Linux-3.5.0-30-generic-x86_64-with-Ubuntu-
12.10-quantal
INFO:core:POX 0.1.0 (betta) is up.
DEBUG:openflow.of_01:Listening on 0.0.0.0:6633
INFO:openflow.of_01:[00-00-00-00-00-01 1] connected
```

- Next, check if hosts in the Mininet topology can reach each other

```
mininet> h1 ping h2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_req=1 ttl=64 time=49.1 ms
64 bytes from 10.0.0.2: icmp_req=2 ttl=64 time=46.3 ms
64 bytes from 10.0.0.2: icmp_req=3 ttl=64 time=29.1 ms
64 bytes from 10.0.0.2: icmp_req=4 ttl=64 time=42.9 ms
64 bytes from 10.0.0.2: icmp_req=5 ttl=64 time=26.2 ms
```

6.9. Open Flow in Cloud Computing

OpenStack and Neutron

Software Defined Networking and OpenFlow are used for the facilitation of data centers and a cloud computing infrastructure .Hence, it is important to understand the usage of OpenFlow in data centers and in particular OpenStack ,since it is used as control and management software for cloud computing. A brief introduction to OpenStack and its networking component (which is called Neutron) and its overall architecture will be discussed in this chapter.

OpenStack's modular architecture and its building blocks (and their code names) are shown in figure 23.

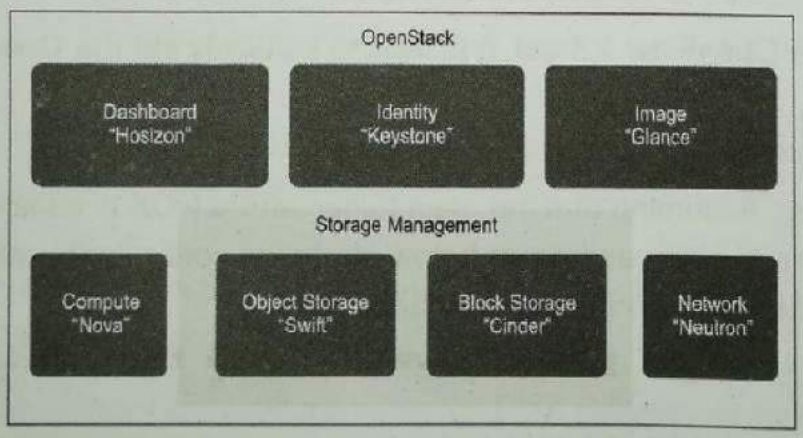


Figure 23: Components of OpenStack

- **OpenStack Compute (Nova):** OpenStack compute (codename: Nova) is the component which allows the user to create and manage virtual servers using the machine images.

Scanned by CamScanner

It is the brain of the cloud. The OpenStack compute provisions and manages large networks of virtual machines.

- **Block Storage (Cinder):** This component provides persistent block storage to running instances. The flexible architecture helps creating and managing block storage devices easily.
- **Object Storage (Swift):** This component stores and retrieves unstructured data objects through the HTTP based APIs. Further, it is also fault tolerant due to its data replication and scale out architecture.
- **OpenStack Networking (Neutron)**: It is a pluggable, scalable and API-driven system for managing networks. OpenStack networking is useful for VLAN management, management of IP addresses to different VMs and management of firewalls using these components.
- **Identity Service (Keystone)**: This provides a central directory of users mapped to the OpenStack services. It is used to provide an authentication and an authorisation service for other OpenStack services.
- **OpenStack Image Service (Glance):** This provides the discovery, registration and delivery services for the disk and server images. It stores and retrieves the virtual machine disk image.
- **OpenStack Telemetry Service (Ceilometer)**: It monitors the usage of the cloud services and decides the billing accordingly. This component is also used to decide the scalability and obtain the statistics regarding the usage.
- **Dashboard (Horizon)**: This component provides a web-based portal to interact with all the underlying OpenStack services, such as NOVA, Neutron, etc.
- **Orchestration Heat:** This component manages multiple cloud applications through an OpenStack-native REST API and a CloudFormation-compatible Query API.
- **Database as a Service (Trove):** Trove is database as a service for OpenStack. It is designed to run entirely on Open Stack, with the goal of allowing users to quickly and easily utilise the features of a relational database without the burden of handling complex administrative tasks. Cloud users and database administrators can provision and manage multiple database instances as needed. Initially, the service will focus on providing resource isolation at high performance while automating complex administrative tasks including deployment, configuration, patching, backups, restores and monitoring.
- **Messaging as a Service (Marconi):** Marconi is a cloud messaging and notification service for developers building applications on top of OpenStack. This service features a web-friendly HTTPAPI, which developers can use to send messages between the various components of their SaaS and mobile applications, using a variety of communication

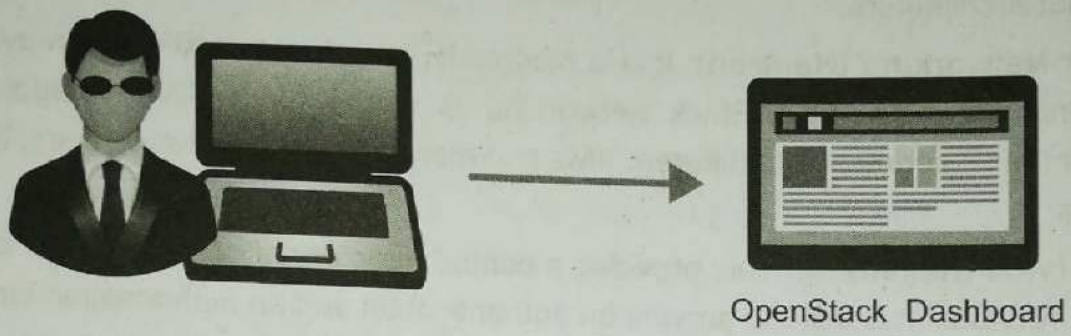
Scanned by CamScanner

patterns. Underlying the API is an efficient messaging engine designed with scalability and security in mind.

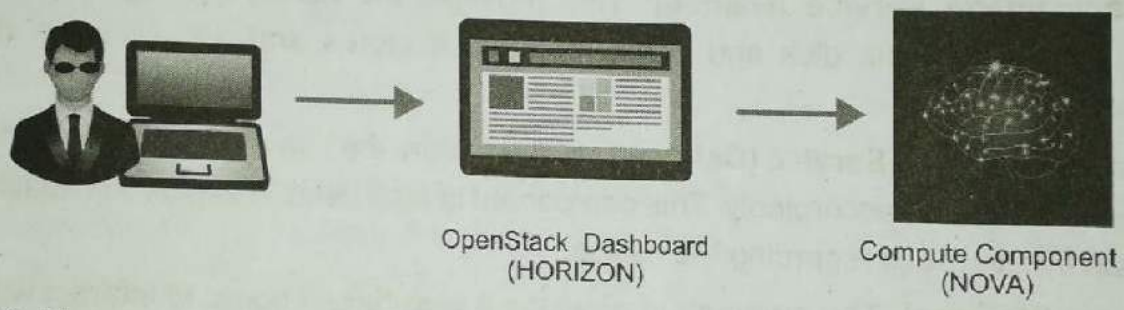
OpenStack Process Workflow

Here, is an example of a user who wants to host SUSE Linux. The workflow diagrams which describe the flow of process in OpenStack are as follows:

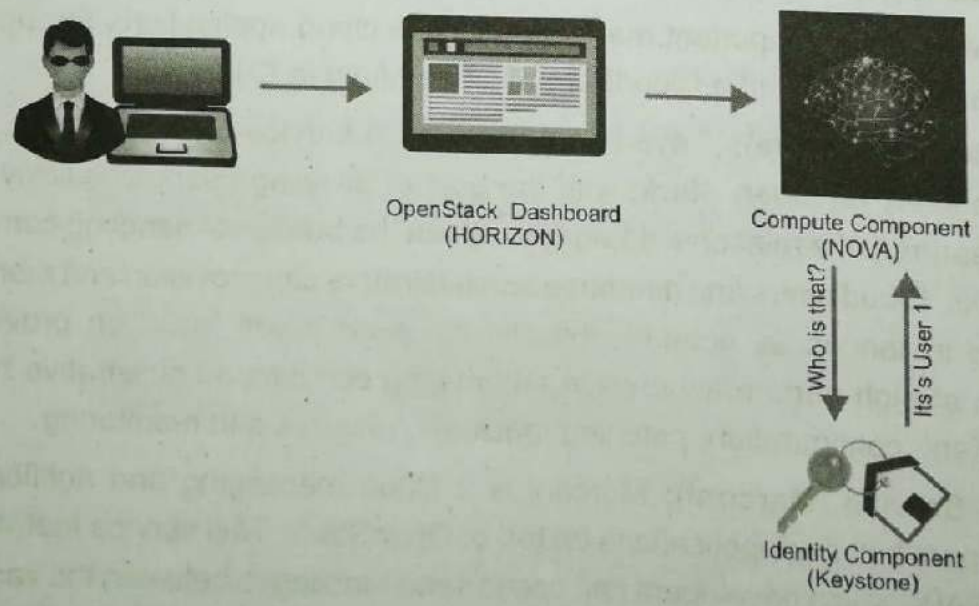
Step 1: User requests a VM running SUSE Linux



Step 2: The Dashboard (horizon) passes the request to the Compute Component(NOVA)

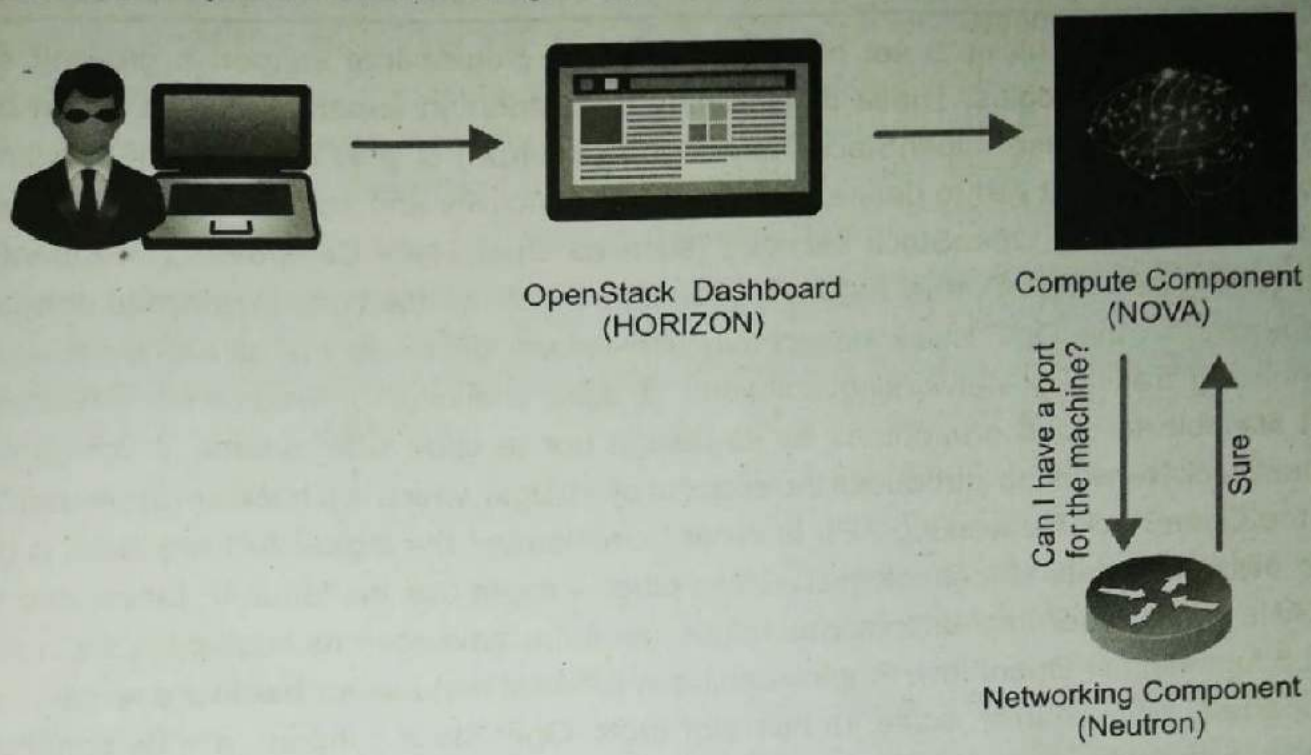


Step3: The request goes to Identity Component (Keystone) for the authentication

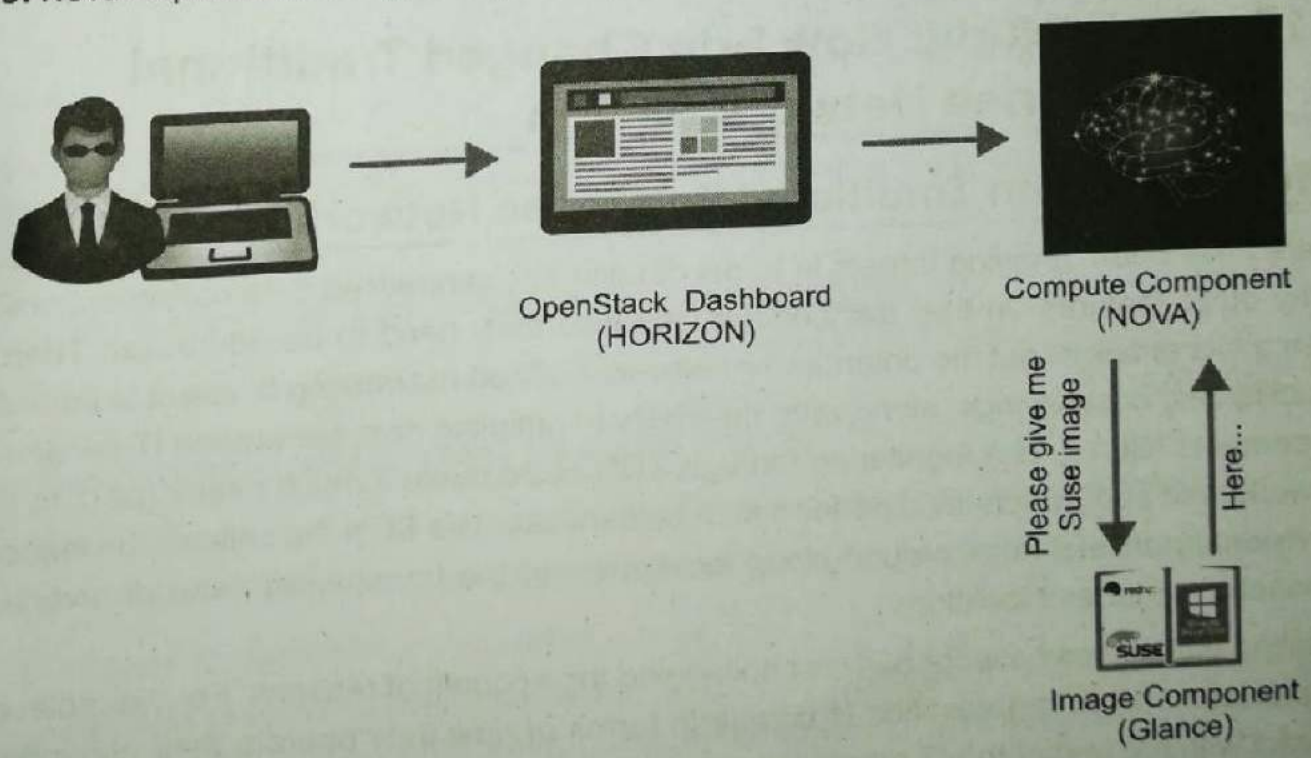


Scanned by CamScanner

Step 4: NOVA requests the Networking Component (Neutron)for an IP Address



Step 5: Nova requests the image component (Glance) for an image of SUSE linux



Finally after getting the image, Nova mounts it on a VM host. During the boot process of the VM, it requests Neutron (DHCP component) for an IP address.

Scanned by CamScanner

Neutron Plugins

Neutron is able to utilise a set of backends called plugins that support a growing set of networking technologies. These plugins may be distributed separately or as a part of the main Neutron release. OpenStack Networking (Neutron) is a virtual network service that provides an efficient API to define the network connectivity and addressing, that is used by devices from other OpenStack services (such as OpenStack Compute). The OpenStack Networking API utilises virtual network, subnet, and port abstractions to describe networking resources. In the OpenStack networking ecosystem, providing rich cloud networking by enhancing traditional networking solutions is quite challenging. Traditional networking is not scalable to cloud proportions by its design nor to cope with automatic configuration. OpenStack Networking introduces the concept of a plugin, which is a backend implementation of the OpenStack Networking API. In order to implement the logical API requests, a plugin can utilise a variety of technologies. Some plugins might use the Linux IP tables and basic VLANs, while other implementations might use more advanced technologies, such as L2-in-L3 tunneling or OpenFlow. Plugins can have different features for hardware requirements, properties, performance, scale, or operator tools. OpenStack supports a wide spectrum of plugins; therefore, the cloud administrator is able to consider different options and decide which networking technology fits a particular use case scenario.

6.10. Case Study: How Sdn Changed Traditional Enterprise Network Design

Effect of SDN on Traditional Enterprise Network Design

There have been growing threats in terms of security , centralised data collection, cost and many other features in the traditional enterprises that need to be addressed.There has been a lots of talk about the potential for software-defined networking to result in operational flexibility and cost savings, along with the ability to optimise next-generation IT service-level agreements (SLAs).SLA monitoring through SDN could make it much easier for IT to detect network- and application-level performance bottlenecks. The SDN then allows the immediate provisioning of resources around cloud locations and the transparent network diversion of transactions to these locations.

Creating a business case for SDN is challenging for a couple of reasons. For example, every Enterprise network organisation is unique in terms of how they operate their networks and interact with the rest of the IT organisation and the enterprise's business unit managers. Due to the variability in SDN use cases and enterprise IT environments, it is not possible to create a single SDN business case that has a perfect fit for all situations. It is, however, possible to create a template that can serve as the basis of a case study that is applicable to the vast

Scanned by CamScanner

majority of enterprise IT organisations. This chapter will discuss the features considered to compare the traditional enterprise with enterprise using SDN for network design.

Table 2 contains the primary advantages that are associated with adopting SDN in traditional network design and assessment of the likely impact of those advantages which are based on the experiences of some enterprises which have adopted SDN.

Table 2: SDN advantages over Traditional Network Design

SDN advantages over Traditional Network Design	Likely Impact
Efficiency in operational Activities	• 80% reduction in operational expense • 72% reduction in the labor to do configuration changes • Make moves, adds in changes in minutes, not days or weeks
Unification of Resources	• Reduce the number of switches by 70% • Reduce the number of server racks by 605% • Reduce power consumption by 75%
Business Scalability	• Deploy new business services more rapidly
Network Availability and Performance	• Visualisation of the entire network
Enhanced management and Transparency	• Equipment and virtual networks can be added via a GUI

The Features considered in case study

Considering an enterprise IT organisation to build a business case for implementing SDN is not very difficult. The Use Case discussed will highlight the following features.

- **Efficiency in operational Activities**

  Reduction of cost and time is one of the primary advantages of SDN .Reduction in tasks such as configuration and provisioning by centralising control and allowing network organisations to configure and provision hundreds of devices as if they were one device can cause considerable reduction.

Scanned by CamScanner

- **Unification of Resources**

  IT organisations can significantly reduce the number and the cost of the required physical resources. By virtualising and pooling compute, storage and network resources. One of the primary benefits of server virtualisation is being able to move virtual machines (VMs) between physical servers. This is not possible in a traditional network environment without costly and, time-consuming manual labor. SDN dynamically moves VMs resulting in considerable operational savings.

- **Business Scalability:**

  SDN enables optimisation and security in network functions with required policies.

  Enabling the enterprise network design to support new business services notably faster than in a traditional environment in which each device has to be manually added and configured.

- **Network Availability and Performance**

  Network availability can be improved by enabling enterprises to make changes to the physical network, by scaling devices, without impacting the current flows or closing down the network.

  Another way to do the same is that an SDN can result in increased availability i.e. the way traffic is

  routed. In a traditional network there is a single data path from origin to destination, and if the path fails, the entire network is down. However, in SDN, the controller has an ability to discover multiple paths to the destination and split the traffic for a given flow across multiple links.

- **Enhanced Management and Visibility**

  One of the principal reasons why IT organisations are often unaware of degraded application

  performance is that in the traditional enterprise network lack visibility into the

  end-to-end network flows. One of the key advantages of an SDN enabled enterprise network

  organisations is to have end-to-end network flow transparency since SDN simplifies tasks such as configuration management.

  Apart from this, SDN enabled enterprise network design also provides the following features:

- **Improved Security**

  There are a number of ways that a SDN can result in improved security. Since in most organizations, there is a need to keep the data generated by one set of users isolated from other

Scanned by CamScanner

users. This can be accomplished by adopting SDN that provides virtual networks that are

fully isolated from one another. Other security applications built on OpenFlow controller can

match suspicious flows to databases of malware signatures or divert DDoS attacks.

Use Cases:

Due to the sensitive nature of the information, the identity of the company is not revealed.

Hospital Use Case

In traditional network design the hospital management noted that daily operations were challenging. Doctors often try connecting new equipment to the network which change in settings and verifying connections, and sometimes even rewiring, causing increase on the hospital's budget. A network that requires setting changes and rewiring every time a new piece of equipment is connected cannot be called stable. The other issue was the slow reconfiguration of the network due to the processes in place. Adding a new piece of equipment could take three months including time to initiate the contract for the add/move/change."

The hospital decided that in order to overcome these challenges, it had to implement centralised LAN whose primary goal was to integrate the departmental LANs. By incorporating SDN network design, hardware was roughly the same as that of a traditional network, the operational and maintenance cost was reduced markedly. There is an estimated savings of 80 percent on its operational expenses, including reduction in the staff hours required to manage the network.

Manufacturing Company Use Case

The network issues that the manufacturing company faced was that their production network and their admin networks were not separated, and this lack of separation created serious concerns about the security of their manufacturing network. In addition, in order to add edge switches they had to install optical cables to connect the new edge switches with their core switches. The manufacturing company, in order to deal with this, decided to implement an SDN-based LAN because the capital costs of the SDN-based LAN were lower than the capital costs of a traditional LAN and in part as the operational costs were significantly less.

In the case of a traditional network, each configuration change requires:

- A week's time for design with changes
- 3 days to create the configuration files;
- 2 days to perform the configuration work.

Scanned by CamScanner

With the SDN they installed, each configuration change requires:

- 1 day for design;
- 0.5 of a day to create the configuration files;
- 1 day to perform the configuration work.

By reducing the time to make the configuration changes for 11days to 2,5 days, a labour reduction of 82%, which is in line with the operational savings.

6.11. Summary

This chapter begins with the fundamentals of Software Defined Networking concepts. Basics of SDN and OpenFlow is studied along with the difference between the traditional and SDN networks. The building blocks of SDN architecture are explained. The OpenFlow Operation along with Open flow Message Types are summarised. The laboratory implementations give a hands-on practice to readers. The various OpenFlow controllers are discussed in the chapter specifically, POX and NOX. Lastly, the chapter discusses the role of OpenFlow in cloud computing with an emphasis on OpenStack & Neutron, OpenStack process workflow and neutron plugins.

Questions:

1. Differentiate between traditional and software defined networking.
2. Briefly explain the SDN architecture and its building blocks.
3. Define the importance of OpenFlow protocol and the message types.
4. Describe the OpenFlow table format.
5. State the different OpenFlow controllers and explain their working.
6. Explain the role of OpenFlow in Cloud computing.
7. Write short notes on OpenStack and neutron plugins.
8. Write a short note on effect of SDN in Enterprise Design Network.

Cell:98696 42636
TSEC BOOK STALL
• Books to be returned within First 10 days after College reopens Jan / July 20
• Only if no new edition of book is expected
• Final decision on receiving books will be ours

Scanned by CamScanner