2 November 2016

Internetworking

Assignment Report

Course: Computer Networks (CO300)

Instructor: Prof. K. Chandrasekaran

Degree / Semester: B.Tech. / Fifth

Department: Computer Science and Engineering

Submitted by

S. No	Reg. No	Name	Signature
1.	14co202	Alla Pranathi	
2.	14CO203	Anirudh Sriram	
3.	14CO204	Aparna R. Joshi	

4.	14C0205	Bairi Sandhya Rani	
5.	14CO206	Chinthapulusu Bugga Yuvaraj	
6.	14CO207	Chiranjeevi AR Hegde	
7.	14CO208	Deepak Srikanth	
8.	14CO209	Devanga Teja Sri	

Table of Contents

Internetworking

Assignment Report

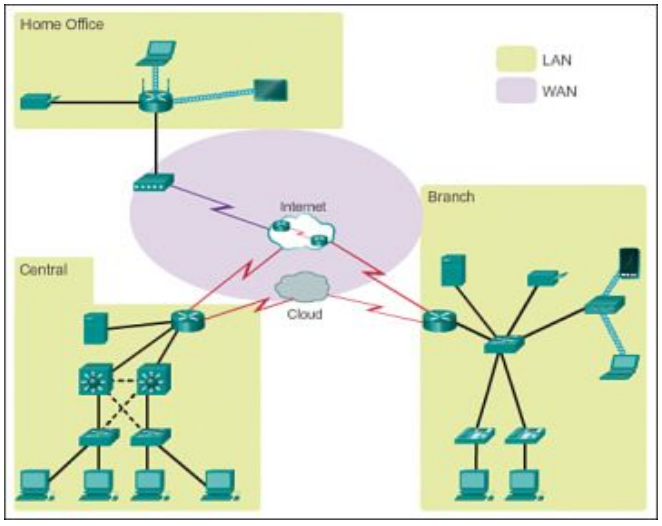
1. Introduction

1.1 LAN TECHNOLOGIES

Local-area networks (LAN) are a network infrastructure that spans a small geographical area. Specific features of LANs include

- LANs are used to interconnect end devices in a limited area such as home, school, office building, or campus.
- A single organization or individual usually administers LAN. The administrative control that governs the security and access control policies are enforced on the network level.
- LANs provide high-speed bandwidth to internal end devices and intermediary devices.

LAN networking comprises cables, switches, routers and other components that let users connect to internal servers, websites and other LANs via wide area networks.



1.2 WAN TECHNOLOGIES

A WAN is a data communications network which covers a broad geographic area relatively and often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. In order to interconnect the LANs at the different locations, the organization needs a Telecommunication Service Provider (TSP). TSPs transported voice and data communications on separate networks. These networks that connect LANs in geographically separated locations are referred to as **Wide Area Networks** (WANs).

Specific features of WANs include

- WANs interconnect LANs over wide geographical areas such as between cities, states, provinces, countries, or continents.
- WANs are usually administered by multiple service providers.
- WANs use serial connections of various types to provide access to bandwidth over large geographic areas.
- WANs typically provide slower-speed links between LANs.

A WAN can be as complex as the backbones that connect the Internet referred as switched WAN or as simple as a dial-up line that connects a home computer to the Internet known as point-to-point WAN. The switched WAN connects the end systems, consisting a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is leased line from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (lSP). This type of WAN is often used to provide Internet access.

Comparison between LAN and WAN:

Characteristic	Local Area Network	Wide Area Network
Geographic area of coverage	Localized to a building, group of buildings, or campus	Can span an area ranging in size from a city to the globe
Data transmission rate	Typically 4 Mbps to 16 Mbps, with some limited distance copper pair based and extended distance fiber optic-based networks operating at 100 Mbps	Normally operate at or below T1 and E1 transmission rates of 1.54 Mbps and 2.048 Mbps and T3 at 45 Mbps
Error rate	1 in 10^7 to 1 in 10^6	1 in 10^6 to 1 in 10^7
Ownership	Usually with the implementor	Communications carrier retains ownership of the facilities
Data routing	Normally follows fixed route or mesh structure for limited distance	Switching capability of network allows dynamic alteration of data flow for long distance
Topology	Usually limited to bus, ring, tree, and star	Virtually unlimited design capability
Type of information carried	Primarily data	Voice, data, and video commonly integrated

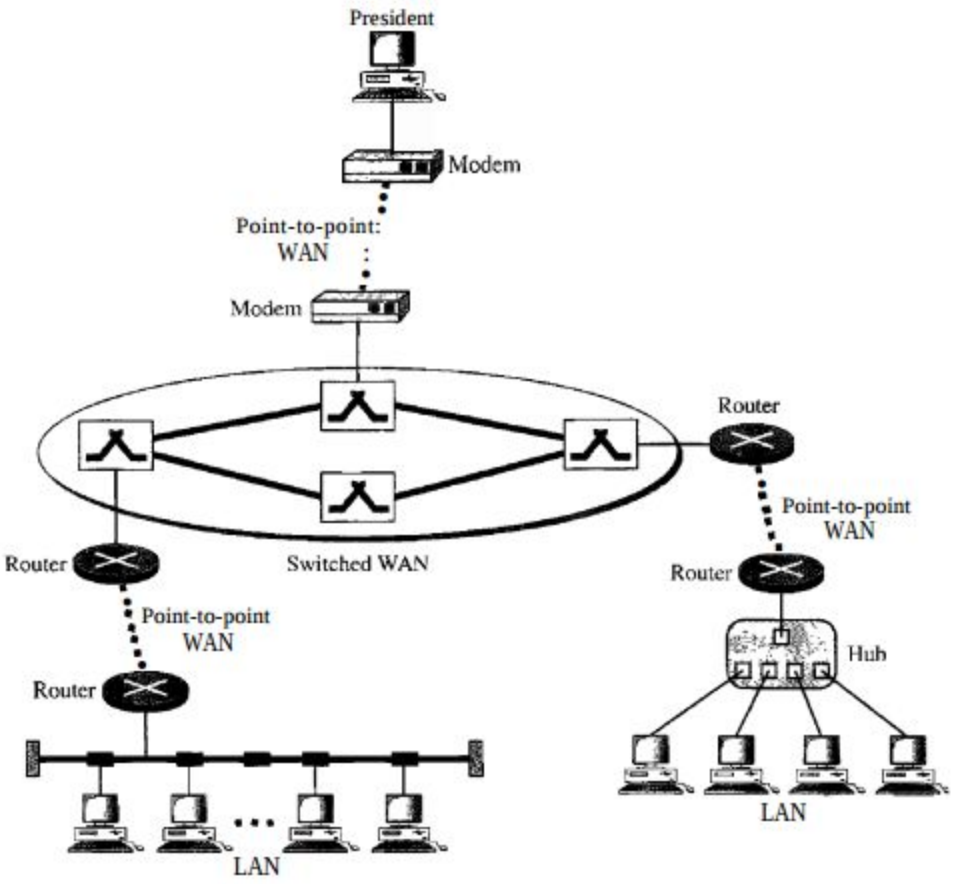
2. INTERNETWORKING

Interconnection of Networks: Internetwork

Today, it is very rare to see a LAN, a MAN, or a LAN in isolation; they are connected to one another. When two or more networks are connected, they become an internetwork, or internet.

As an example, assume that an organization has two offices, one on the east coast and the other on the west coast. The established office on the west coast has a bus topology LAN; the newly opened office on the east coast has a star topology LAN. The president of the company lives somewhere in the middle and needs to have control over the company from her horne.

To create a backbone WAN for connecting these three entities (two LANs and the president's computer), a switched WAN (operated by a service provider such as a telecom company) has been leased. To connect the LANs to this switched WAN, however, three point-to-point WANs are required. These point-to-point WANs can be a high-speed DSL line offered by a telephone company or a cable modem line offered by a cable TV provider.



There are two basic choices for connecting different networks: we can build devices that translate or convert packets from each kind of network into packets for each other network or we can add a layer of indirection and building a common layer on top of the different networks. In either case, the devices are placed at the boundaries between networks such as routers gateways,repeaters, hubs, switches, or bridges.

A committee (IEEE802.1) of IEEE identified the following possible internetworking scenarios.

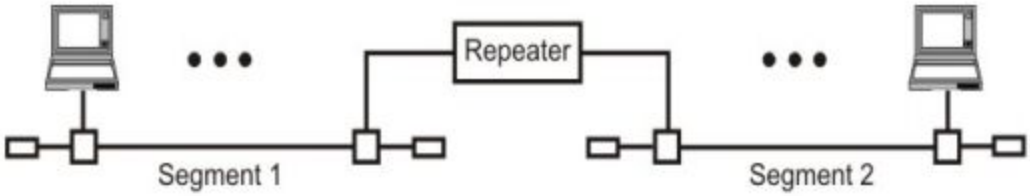
- A single LAN

- Two LANs connected together (LAN-LAN)
- A LAN connected to a WAN (LAN-WAN)
- Two LANs connected through a WAN (LAN-WAN-LAN)

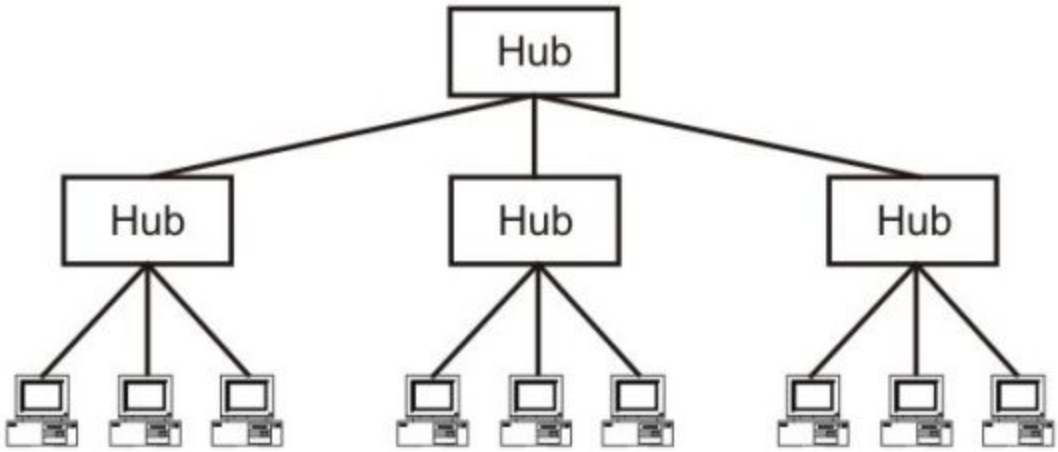
Numerous internetworking devices such as hubs, switches, bridges, routers and gateways are essential to connect these networks together detailed in section 2.1.

2.1 Internetworking Devices

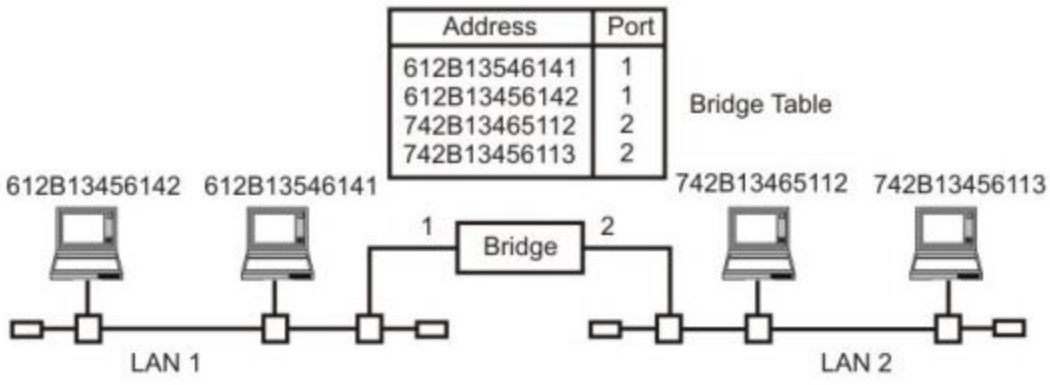
- **Repeaters**: One Ethernet segment has maximum length of 500m with a maximum of 100 nodes. Repeaters are used to extend the length of the network. Two transceivers connected together and to two distinct segments of coaxial cable functionally, forms a repeater. The digital signal is passed bit-by-bit in both directions by the repeater between the two segments. A repeater amplifies the signal and regenerates it at its other transceiver end. The repeater does not isolate one segment from the other, if there is a collision on one segment, it is regenerated on the other segment. Therefore, the two segments form a single LAN and it is transparent to rest of the system. Ethernet allows five segments to be used in cascade to have a maximum network span of 2.5 km. The repeater is merely used to extend the span of a single LAN. Some significant features of a repeater include connecting different segments of a LAN, forwarding every frame that it receives, regenerating the signals, and creating a single extended LAN.



- **Hubs:** Hub refers to a multiport repeater. It can be used to create multiple levels of hierarchy of stations. The stations are linked to the hub with the RJ-45 connector having maximum segment length as 100m. This type of interconnected set of stations is easy to maintain and diagnose.

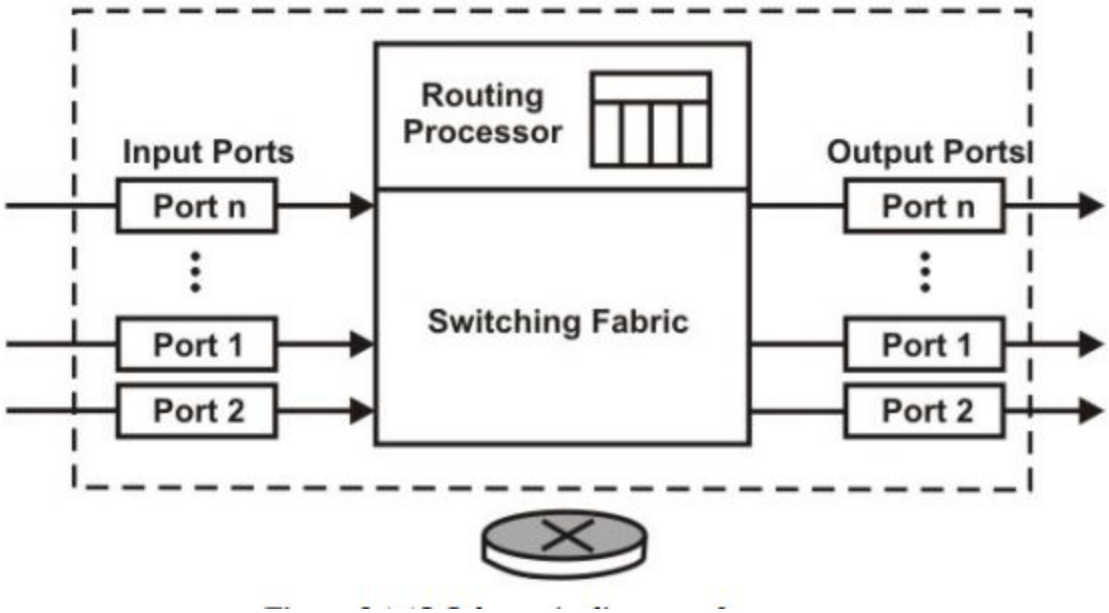


- **Bridges**: The device that can be used to interconnect two separate (similar or dissimilar) LANs is known as a bridge. The bridge operates in layer 2, that is data-link layer and that is why it is called level-2 relay with reference to the OSI model. Designed to store and forward frames, it is protocol independent and transparent to the end stations. Use of bridges offer a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage. Key features of a bridge include operation both in physical and data-link layer, use of table for filtering/routing, retaining the MAC addresses in a frame. The two types of bridges are **transparent bridges** and **source routing bridges.** Transparent bridges are produced as an extension of IEEE 802.1 and are applicable to all IEEE 802 LANs. Source routing bridges are developed for the IEEE 802.5 token rings, and are based on source routing approach. It applies to many types of LAN including token ring, token bus and CSMA/CD bus.



- **Switches:** A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames. Some of important functionalities are ports provided with buffer, a directory that is maintained by the switch #address - port#, frame forwarding after examining the #address to the proper port#, three forwarding approaches: Cut-through, Collision-free and Fully buffered. A switch that forwards a frame immediately after receiving the destination address is a **cut-through switch**. As a consequence, the switch forwards the frame without collision and error detection. When the switch forwards the frame after receiving 64 bytes, which allows detection of collision, it is a **collision-free switch**. However, error detection is not possible because switch is yet to receive the entire frame. A **fully buffered switch** forwards the frame only after receiving the entire frame. So, the switch can detect both collision and error free frames are forwarded.
- **Routers:** A router is considered as a layer-3 relay that operates in the network layer, that is it acts on network layer frames. It can be used to link two dissimilar LANs. A router isolates LANs into subnets to manage and control network traffic. However, unlike bridges it is not transparent to end stations. A router has four basic components: Input ports, output ports, the routing processor and the switching fabric. Input port performs physical and data-link layer functions of the router. Output ports perform the same functions as the input ports, but in the reverse order. The routing processor performs the function of the network layer. The process involves table lookup. The switching fabric moves the packet from the input queue to the output queue by using specialized mechanisms. The switching fabric is realized with the help

of multistage interconnection networks.



- **Gateways:** A gateway works above the network layer, such as application layer. As a consequence, it is known as a Layer-7 relay. The application level gateways can look into the content application layer packets such as email before forwarding it to the other side.

2.2 LAN-WAN Internetworking

WAN is the most used network type in the Enterprise world. With growing importance to local area networks as the media for data communication has lead to increasing interest in interconnections between the LAN and WAN. The demand for LAN-WAN only keeps increasing. Several strategies exist to provide this LAN-WAN internetworking capabilities. But each internetworking device has significant performance issues. The devices in comparison are bridges and routers.

Bridges operate on the Medium Access Control layer (MAC) of the LAN Open Systems Interconnection(OSI) protocol stack. The simplest bridge is a 2 port device with each port connecting to a similar LAN. The purpose of the bridge is to examine the frames arriving at the bridge and through internal routing table forward it to the corresponding LAN it was meant for. Bridges are capable of supporting a number of possible destination or ports for the forwarded frames. Thus bridges restrict traffic to remain within a separate physical network but still provide connectivity to stations on other adjacent LANs.

Routers can be found to operate on the network layer. The are designed to support the LAN stations wishing to communicate over a WAN or even a LAN. Since several network layer protocols coexist in a LAN, multiple network layer protocols must be supported by the router. Major functions of the interconnecting device are

1. To handle network layer address mapping between the LAN and WAN network layer protocols.

2. To handle error conditions and help in congestion control in the network.

3. They route data arriving from the LAN to Virtual circuit networks

4. It also segments and rearranges LAN packets.

Bridges and routers are used to interconnect LANs and WANs. But both have significant performance differences in different scenarios that shall be addressed in the following

MAC Address Phenomenon:

Bridges rely on a unique MAC address to be assigned to the entirety of the bridged LAN. Although this isn't a pressing issue, the MAC addresses can be changed in a LAN station implementation and because bridges require LAN address to be unique, these changes could cause negative scenarios.

Routers,on the other hand, ensure that MAC addresse are a local matter to the LAN.

Routing Flexibility:

Since all IEEE MAC protocols operate in connectionless service mode, each MAC frame processed is treated as a separate entity .Whether the next sublayer LLC is providing connectionless or connection-oriented service, this is immaterial to the Bridges operation.This connectionless nature of the bridges help them to potentially deal with the inter-bridge traffic.

Whereas, a router encapsulates the LAN network protocol in x.25 packets(an ITU-T standard protocol suite for **packet** switched wide area network (WAN) communication), can manage numerous packets on one single virtual link.

Bandwidth Efficiency:

Bridges encapsulate the MAC layer frame for transmission over WAN. Since the MAC header takes up 15 octets and the checksum another 4 octets, this results in the inefficient use of the network facility. Routers in this regard are more bandwidth efficient, because MAC layer is terminated in the routers and no MAC headers are transmitted over the network thus making it more efficient.

Topology Flexibility:

Bridges operate in a point to point transmission fashion. It is safe to say that the network via bridges is not fully connected because it would require point to point links between each bridge and would become highly expensive to implement. This means, some LANs might have to communicate to the other LAN/WAN in the network via another network, this might lead to drawbacks in performance. Whereas routers are capable of communicating over a wide variety of WAN services simultaneously utilizing both circuit and packet switching.

Higher layer Protocol Dependence:

Bridges operation is independent of the higher layer protocols being implemented including the LLC sublayer and the protocols incorporated in the 3 and 4 th layers, as bridges deal with the IEEE 802 MAC protocols which operate in connectionless service mode.

In case of routers this transparency is not seen.The routers should have the knowledge of the protocols being implemented in the higher layers and be able to support each protocol's(TCP/IP or XNS or ISO CLNP) network layer.

Security:

Bridges base routing decisions are based on the LAN addresses of the MAC stations and it is possible to emulate MAC address of some other end system and thereafter receive all the data meant for that end system. Data security becomes a concern in such scenarios.

Routers are managed by routing tables and are less prone to security attacks. The network will not allow end users to emulate its subscribers so data cannot be "hacked" into, thus making routers a reliable interconnecting device of choice for corporate networks.

Taking everything into account, routers have more advantages over bridges. But depending on the performance issues, cost, flexibility and security of the network, bridge or router can be chosen accordingly.

2.3 WAN-WAN Internetworking

Network Load Balancing:

Network load balancing is the ability to balance traffic across two WAN links without using complex routing protocols like BGP. The amount of bandwidth available is literally increased when this capability balances network sessions like Web, email, etc. over multiple connections in order to spread out the amount of bandwidth used by each LAN user.

Software-defined Networking has unique approaches in both LANs and WANs.

SD-LAN refers to extending software-defined techniques into the access layer of switches, APs, and via drivers, eventually into client devices.

SD-LAN and SD-WAN: Differentiating Criteria

- Topology: LAN has a predictive topology with layers of switches and interconnects them and each of them aggregate bandwidth for the below layer. WAN infrastructures lead to unpredictability in the routing of traffic from one site to another due to the usage of mesh topologies, regional aggregation, traffic-engineered paths etc.
- Network Security: LAN authentication serves as the primary security mechanism; encryption is considered unconventional. WAN requires authentication of end-point devices and encryption of bits on the wire.
- Loss, Latency and Jitter: Avoidance of these conditions requires use of acceleration and optimization of applications. LAN faces no such problems since bandwidth and latency are assumed to be not issues.
- Flow Characteristics: The use of SDN in the LAN depends on the number of LAN traffic flows which is proportional to the number of users and applications whereas operating the network based on user and application population alone is impractical.
- Quality of Service: SD LAN focuses on classification and marking. On the other hand, SD-WAN focuses on shaping, prioritizing, and selective dropping. These are based on QoS.

SD-WAN:

In order to expand WANs and their coverage over multiple network service providers, WAN to WAN connections must be provided. However, most of these types of networks face operational challenges like packet loss, jitter and network connection. Furthermore, many real time applications such as VoIP, video conferencing, etc. require low latency and high bandwidth. SD-WANs are designed to address these network problems. Routers can be upgraded or even replaced with virtualization appliances that can control application level policies and offer network overlay, less expensive consumer grade internet links which can act more like a dedicated circuit.

Software-defined WAN (SD-WAN) is a concept that attempts to combine the benefits of WAN optimization and software-defined networking by virtualizing the WAN. SD-WAN helps in design and deployment of an enterprise wide area network that uses software-defined networking (SDN) and determines the most effective way to route traffic to remote locations including branch offices and data centers over large geographic distances.

The main goal of SD-WAN is to deliver a reliable, secure and simple WAN connection with as much open and software-based technology as possible which is useful to deliver basic WAN connectivity, and WAN optimization. SD-WAN is used to enable network managers in companies to aggregate multiple Internet connections so that they function as a single virtual overlay so that it provides a level of performance and reliability on par with private WAN connectivity.

The management and operation of a WAN is simplified by separating the networking hardware from its control mechanism and thus reducing provisioning times and minimizing or eliminating the need to manually configure traditional routers in branch locations. This is similar to how software-defined networking implements virtualization technology to improve data center management and operation.

Due to SD-WAN, traffic monitoring and management are shifted from physical devices to the application itself, thereby benefiting on SDN's flexibility and agility. The need for overprovisioning is reduced due to the flexibility of SD-WAN, reducing overall WAN expenses.

The main goal of SD-WAN technology is to deliver a business-class, secure, and simple cloud-enabled WAN connection with as much open and software-based technology as possible. This can be used to deliver basic WAN connectivity, or it can be used for premium business services such as VPN, WAN optimization, and applications delivery control (ADC).

SD-Wan also removes expensive routing hardware by improving connectivity and services through cloud.

Many of the new SD-WAN services can be used to improve and secure Internet connectivity, making it more competitive with more expensive legacy WAN technologies such as T-1 or MPLS. In some cases, SD-WAN technology uses Internet broadband connections to replace more expensive solutions. Virtualization technology can apply security and virtual private networking (VPN) technology to broadband Internet connections, making them more secure.

Carrier Ethernet over WAN:

Nowadays, communication and management tools such as mobility and collaboration are critical for Enterprise success.Therefore a new set of challenges must be addressed by the network connectivity and wan services.Following are some challenges:

- **Dynamic Business Environment:**
- Efficiently handle site additions and bandwidth upgrades.
- Quick adaption for new applications.
- Fast reaction to organizational changes.
- **Budget Constraints:**

Meet budget constraints by increasing IT operations' efficiency and productivity, lowering operating expenses.

- Distance learning vs. costly on-site training
- Lower price per Mbps
- Help extend (budgetary) planning horizons to avoid expensive overhauls
- **Satisfying user expectations:**
- Ensure user QoE (quality of experience) for critical applications
- Enable speedy fault resolution and performance accountability
- Ensure service resiliency for BC/DR (e.g., for data center connectivity)
- Get more bandwidth on-demand
- **Enable remote user/locations:**
- Support distributed communications and Web-based applications for disparate locations, workforce on the move, etc.,
- Ensure system integrity and data security

How carrier ethernet can be used for addressing the wan enterprise service requirements?what are the benefits by using carrier ethernet in wan enterprises?

What is the reason carrier ethernet services are booming?

- Because the fastest growing segment in telecom industry today is carrier ethernet.
- Many enterprises need high-speed network connectivity wherever the business is going which carrier ethernet can offer at affordable and reasonable costs.
- Because of the growing popularity of distributed datacenters and cloud services.
- Most service providers are adding various Carrier Ethernet “flavors” to their WAN service offerings.

One can observe by all the reasons mentioned above, Carrier Ethernet is best equipped to meet current and future enterprise communications challenges.

Now, let us see how carrier ethernet can be used for addressing the wan enterprise service requirements:

- **Value –get more for less:**

Carrier Ethernet provides higher throughput at much lower price per Mbps than Frame Relay and other legacy services.Carrier Ethernet is scalable and rates upto 10 gbps with guaranteed throughput which ensures as much bandwidth as you need.

- **Reliability and Simplicity:**

Carrier ethernet is a mature technology which is standardised by reputed organizations such as IEEE,IETF etc.Since carrier ethernet technology is not new to the networking and almost present everywhere now-a-days no new training is required.

- **Flexibility:**

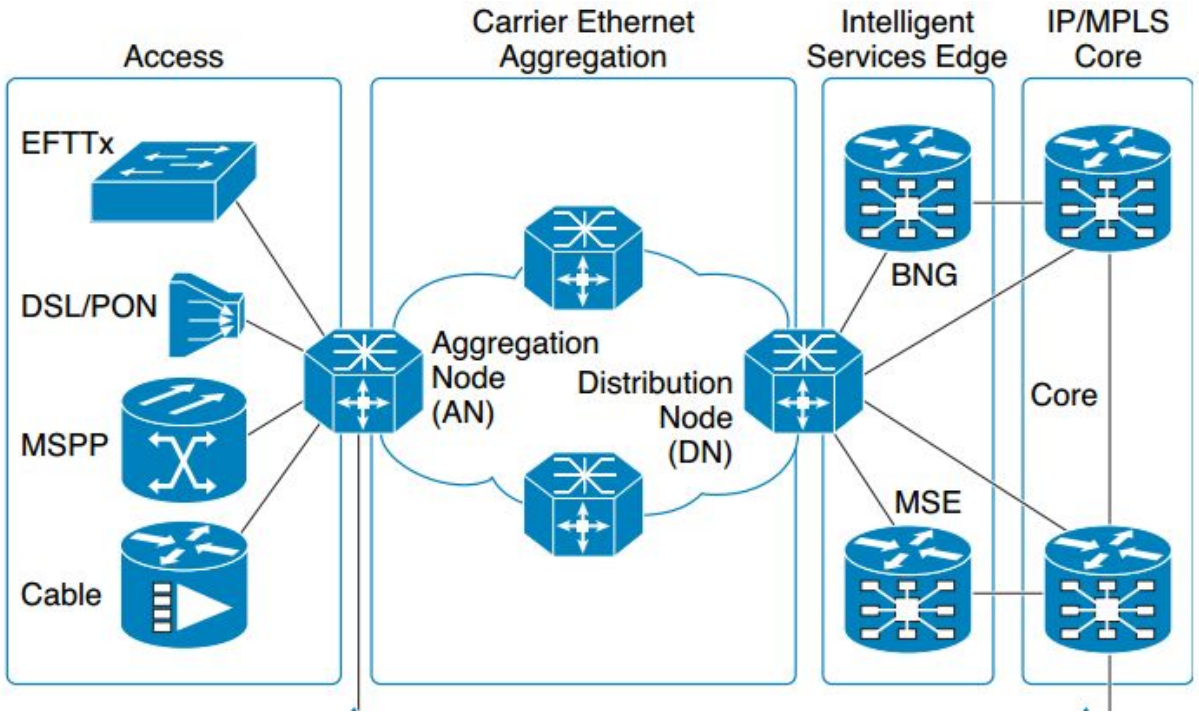
Carrier Ethernet provides flexible connectivity site-by-site and non-disruptive site addition.Carrier Ethenet is easy to adjust when more bandwidth is required.It enables IP applications such as MPLS VPN and Dedicated Internet Access (DIA).

Benefits of Carrier ethernet WAN

- Carrier ethernet offers low price when compared with private line services thus increasing its value for data centers,enterprises.Recent trend shows an increased demand for carrier ethernet for WAN.
- Carrier ethernet WAN services are flexible and can carry multiple type of traffics.It is Layer-2 solution providing an alternative to Layer-3 IP VPNs and helps to maintain control over routing
- Carrier ethernet with its software provisioning tools helps in controlling large scale networks from single platform thus simplifying monitoring and troubleshooting.

Carrier Ethernet: LAN-WAN interconnection

The general architecture of a Carrier Ethernet network is shown below. It is the Cisco IP Next-Generation Network (NGN) Carrier Ethernet Design architecture.



Architecture of Carrier Ethernet network [9]

As seen in the figure, there are multiple access mechanisms which allow the connection of LANs to the aggregation node i.e. the LANs to WAN. These include:

- Passive Optical Network: PON is a single to multi point architecture used to enable a single optical fibre to serve multiple endpoints. This is done by the use of unpowered fibre optic splitters to serve multiple customers without providing individual fibres to each customer. A PON consists of an optical line terminal (OLT) at the service provider's central office (hub) and a number of Optical Network Terminals (ONTs), near end users. Individual Ethernet LANs can be connected to these ONTs, which are connected to an OLT and the Aggregation Node.
- Digital Subscriber Line : This is a commonly used technology used to transmit digital data over telephone lines. A standard DSL modem can be used to connect a LAN to the Aggregation node.
- MultiService Provisioning Platform : Add Drop Multiplexers allow multiple low bandwidth signals to be sent concurrently on a single optical fibre. MSPP is an extension of ADMs that also allow direct connections of Ethernet LANs to the optic fibre backbone. These are then sent along an optic fibre to an aggregator node.
- Fibre to the x: FTTx is a generic description of all broadband architectures using optical fibre for all connections, upto the final stop where they are connected to the LAN. Fibre to the X can be FTTB/FTTH/FTTP (Fibre to the Building/Home/Premises).

3. Members Contributions

S. No	Reg. No	Name	Contribution(s)
1.	14CO202	Alla Pranathi	LAN-WAN internetworking performance issues with bridges and routers
2.	14CO203	Anirudh Sriram	SD-WAN and Carrier Ethernet
3.	14CO204	Aparna R. Joshi	LAN, WAN technologies and Internetworking, Internetworking devices
4.	14CO205	Bairi Sandhya Rani	Introduction of LAN and WAN technologies and description of SD-LAN and SD-WAN
5.	14CO206	Chinthapulusu Bugga Yuvaraj	Carrier Ethernet and how it is used in WAN enterprises

6.	14CO207	Chiranjeevi AR Hegde	Carrier Ethernet over WAN
7.	14CO208	Deepak Srikanth	
8.	14CO209	Devanga Teja Sri	LAN-WAN internetworking performance issues with bridges and routers

4. References

[1] http://nptel.ac.in/courses/Webcourse-contents/IIT%20Kharagpur/Computer%20networks/pdf/M6L1.pdf

[2] Data Communications and Networking, Behrouz A. Forouzan

[3] Computer Networks, Andrew S. Tanenbaum

[4] http://www.nojitter.com/post/240170988/the-same-but-different-sdlan-v-sdwan

[5] http://www.lan2lan.com/software-defined-lan/

[6] http://searchsdn.techtarget.com/definition/SD-WAN-software-defined-WAN

[7] https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=10&cad=rja&uact=8&ved=0ahUKEwjFyaXA54fQAhUlSY8KHR0nDIwQFghzMAk&url=http%3A%2F%2Fdocshare01.docshare.tips%2Ffiles%2F7158%2F71583421.pdf&usg=AFQjCNHI-6nNwXcZL1h8PobbkMWde3YZVg&sig2=O5qekbuUtPel--wY5WVL4A

[8] http://blog.globalcapacity.com/blog/bid/387330/The-Top-Three-Benefits-of-Carrier-Ethernet-WAN-for-Business

[9] http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/fulfillment/6-2/theory/operations/guide/theory/l2ce.pdf