ADVANCED COMPUTER NETWORKS

By: Mrs. Nidhi Divecha (ME CMPN)

(UNIT 1)

TCP/IP Protocol Suite

UNIT - I

TCP/IP Protocol suite

- **What is a Protocol ?**

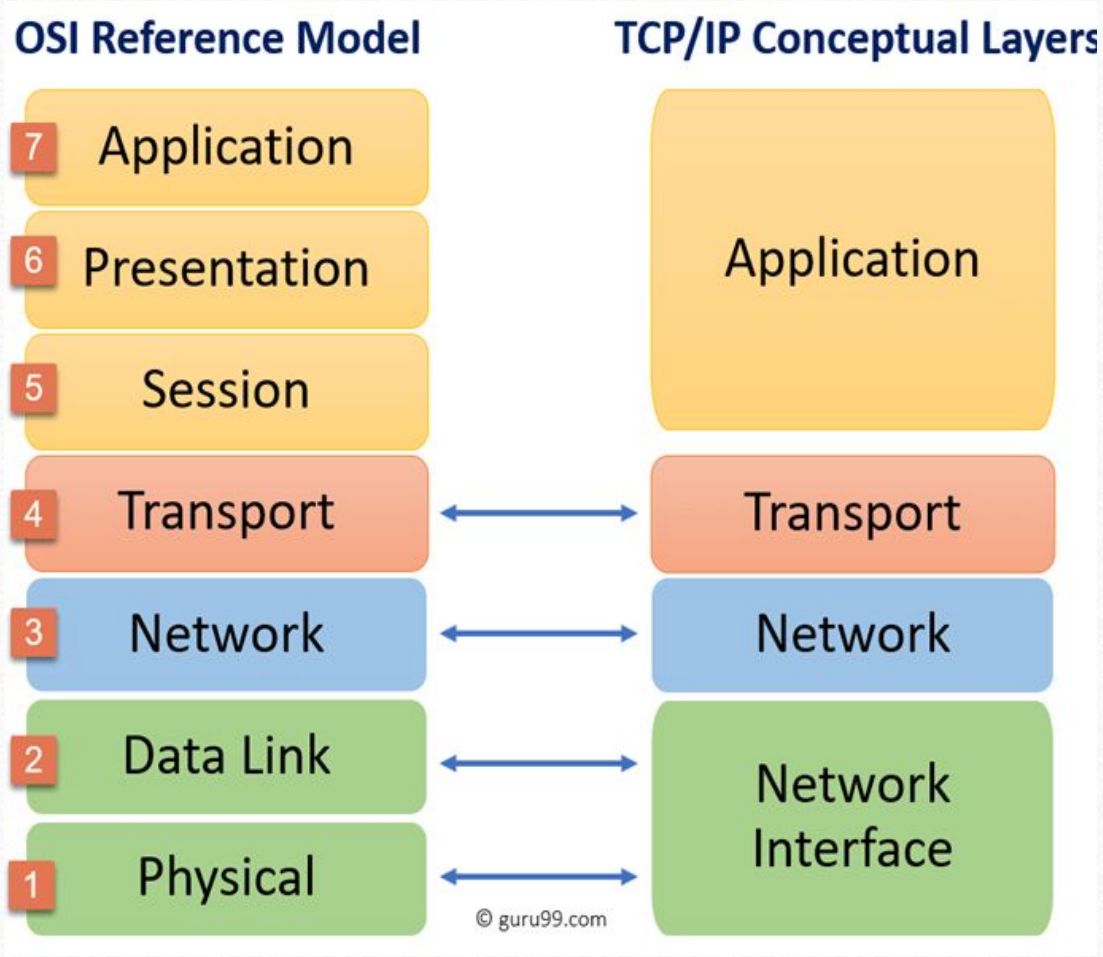
A protocol is a set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another.

- **What is a Protocol Suite ?**

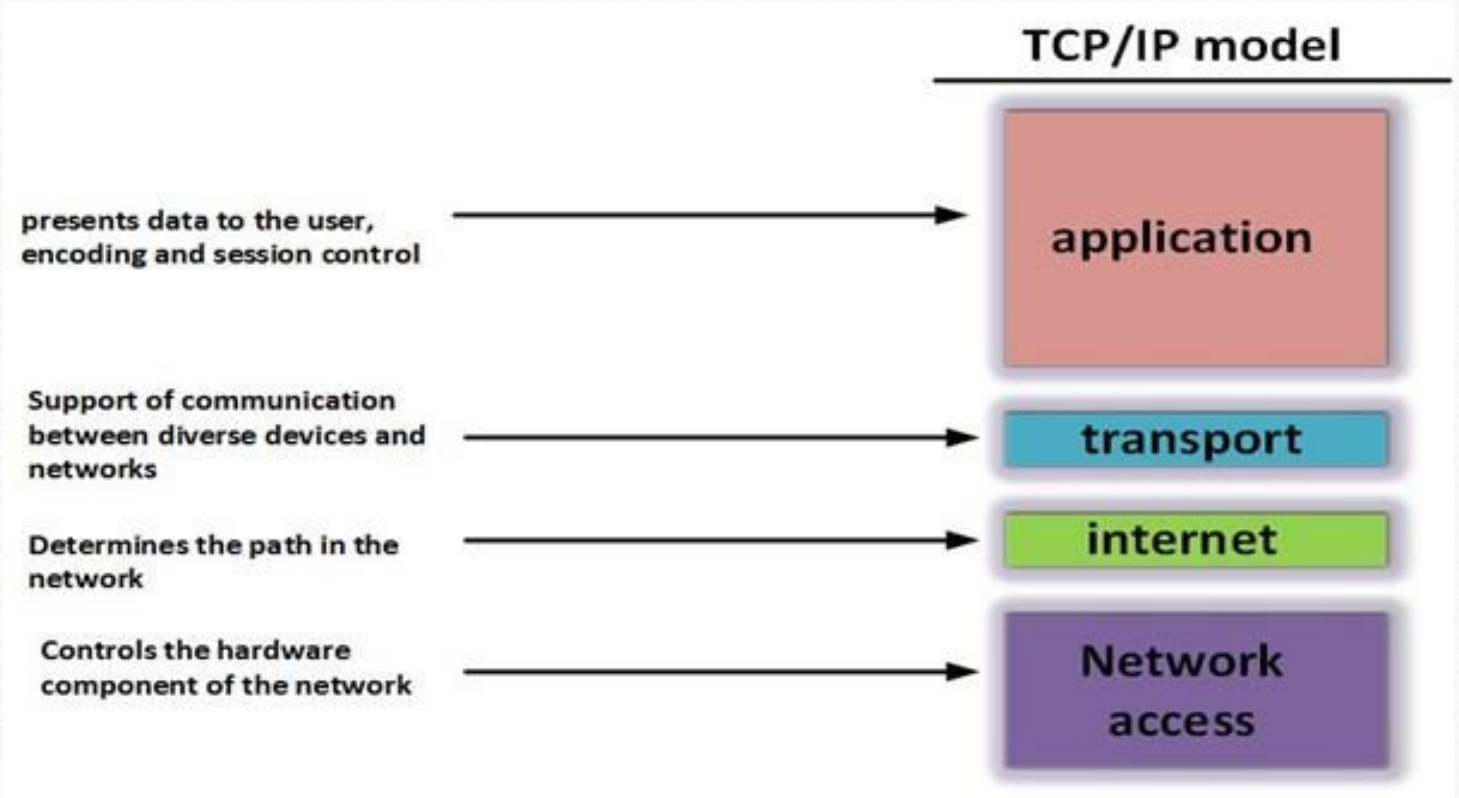
A protocol suite is a collection of protocols that are designed to work together.

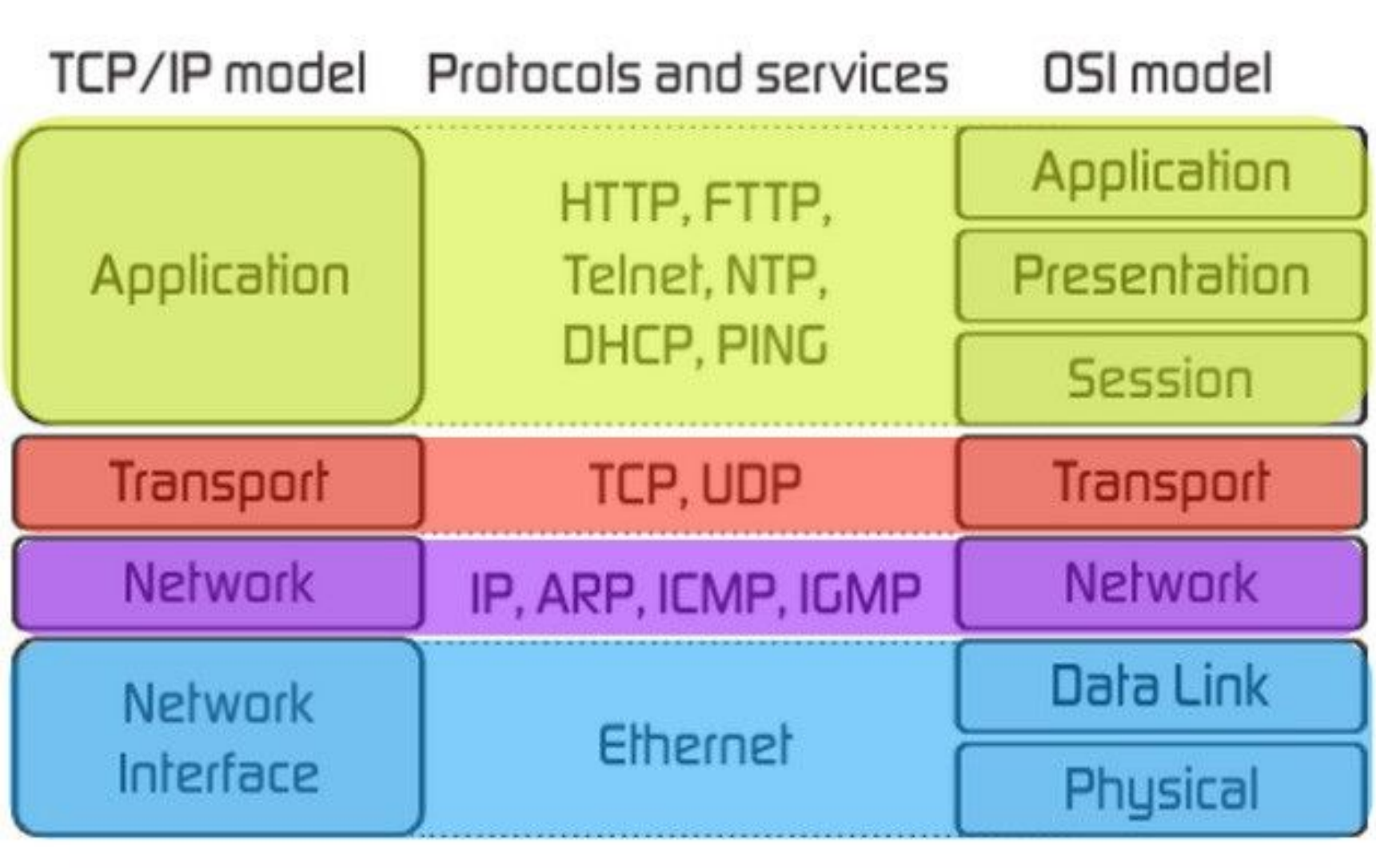
TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having **four layers**: network interface, internet, transport and application layer.
- However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made up of **five layers:** the application layer, transport layer, network layer, data link layer and physical layer.
- TCP/IP is a protocol made up of interactive modules, and each of them provides specific functionality.



TCP/IP MODEL


TCP/IP model
presents data to the user, encoding and session control
application
Support of communication between diverse devices and networks
transport
Determines the path in the network
internet
Controls the hardware component of the network
Network access


TCP/IP model
Protocols and services
OSI model
Application
HTTP, FTTP, Telnet, NTP, DHCP, PING
Application
Presentation
Session
Transport
TCP, UDP
Transport
Network
IP, ARP, ICMP, IGMP
Network
Network Interface
Ethernet
Data Link
Physical

Protocol Data Unit (PDU)

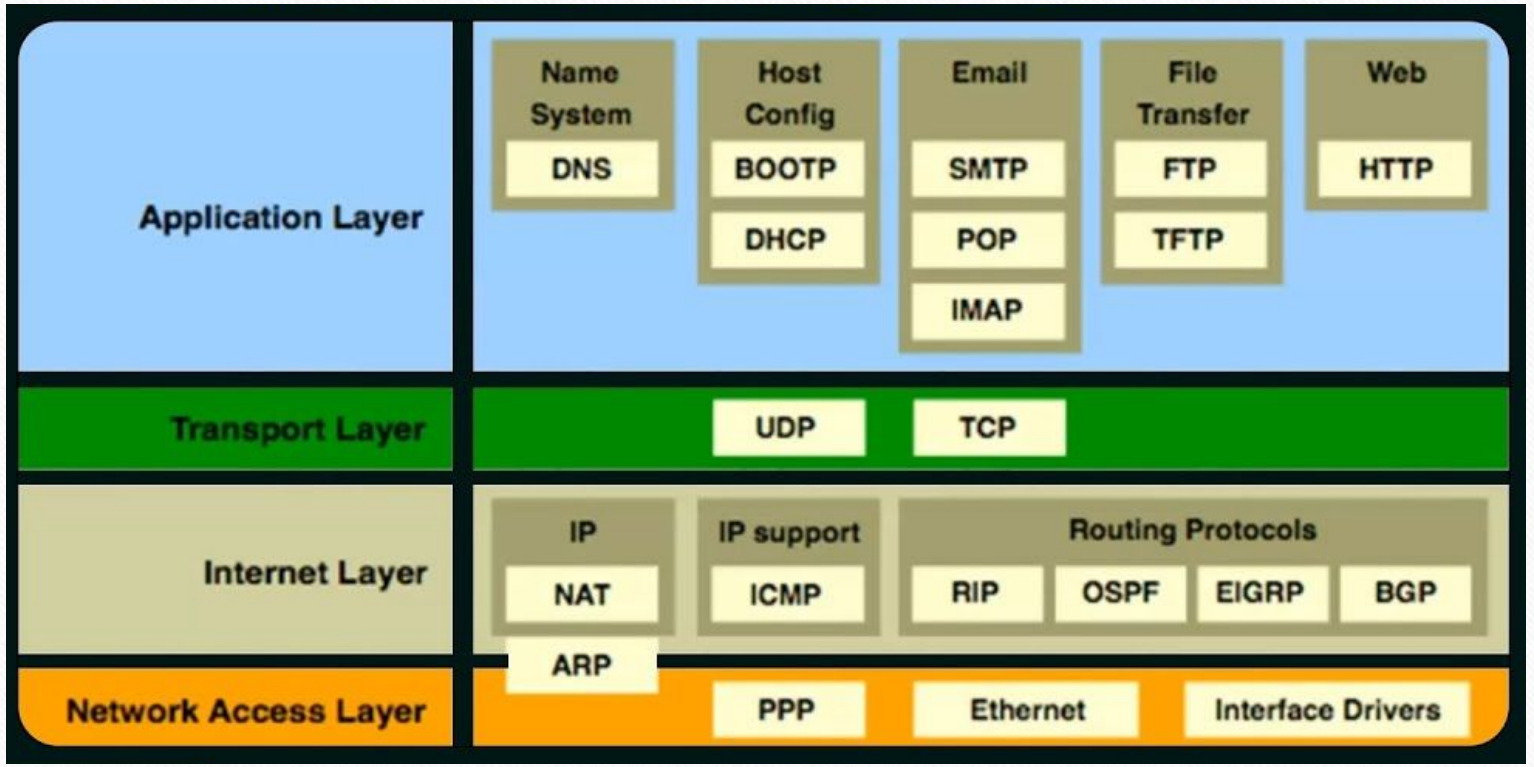
- Stands for **"Protocol Data Unit."**
- A PDU is a specific block of information transferred over a network.
- It is often used in reference to the OSI model, since it describes the different types of data that are transferred from each layer.

The PDU for each layer of the OSI model is listed below.

- **Physical layer** – **raw bits** (1s or 0s) transmitted physically via the hardware
- **Data Link layer** – a **frame** (or series of bits)
- **Network layer** – a **packet** that contains the source and destination address
- **Transport layer** – a **segment** that includes a TCP header and data
- **Session layer** – the **data** passed to the network connection
- **Presentation layer** – the **data** formatted for presentation
- **Application layer** – the **data** received or transmitted by a software application

OSI Model	PDU	TCP/IP Stack
Application	Data	Application
Presentation		
Session		
Transport	Segment	Transport
Network	Packet	Internet
Data Link	Frame	Network Access/Link
Physical	Bits	

TCP/IP Protocol Suite



Functions of TCP/IP layers

Network Access Layer

- A network layer is the **lowest layer** of the TCP/IP model.
- A network layer is the **combination of the Physical layer and Data Link layer** defined in the OSI reference model.
- It defines how the data should be sent physically through the network.
- This layer is mainly responsible for the **transmission of the data** between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet(Network) Layer

- An internet layer is the **second layer** of the TCP/IP model.
- An internet layer is also known as the **network layer.**
- The network layer is responsible for the **source-to-destination delivery of a packet**, possibly across multiple networks (links).
- IP is **an unreliable and connectionless protocol.**

Other responsibilities of the network layer include the following:

- **Logical addressing**
- **Routing**

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

Following are the protocols used in this layer are:

IP Protocol

- IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

ARP Protocol

- ARP stands for **Address Resolution Protocol.**
- ARP is a network layer protocol which is used for **logical to physical address conversion** i.e., it converts **IP address to physical address**.

The two terms are mainly associated with the ARP Protocol:

- **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
- **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

RARP

- RARP stands for **Reverse Address Resolution Protocol.**
- It is based directly on ARP and works in the same way, but in inverse.
- Thus, it is a protocol used to convert the **physical address to IP address.**

ICMP Protocol

- ICMP stands for **Internet Control Message Protocol**.
- ICMP is a mechanism used by routers to **send error or control messages** to other routers or hosts.

IGMP Protocol

- IGMP stands for **Internet Group Message Protocol.**
- IGMP enables the **transmission of messages to a group of recipients** simultaneously.

Transport Layer

- The transport layer is responsible for **process-to-process(communication) delivery of the entire message**.
- A process is an application program running on the host.
- The **two protocols** used in the transport layer are **User Datagram protocol and Transmission control protocol**.

User Datagram Protocol (UDP)

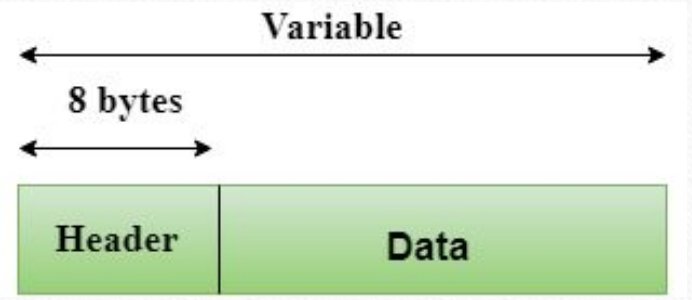
- It provides **connectionless service** and **end-to-end delivery** of transmission.
- It is an **unreliable protocol** as it discovers the errors but not specify the error.
- User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.

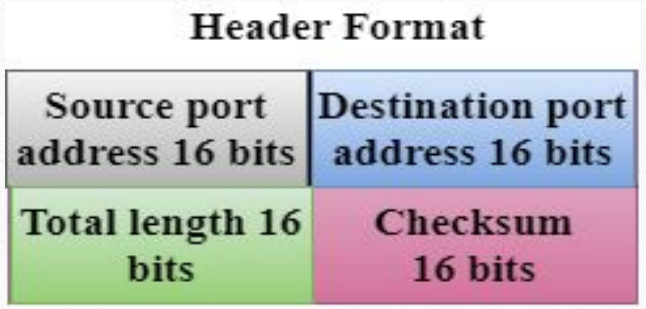
UDP consists of the following fields:

- **Source port address:** The source port address is the address of the application program that has created the message.
- **Destination port address:** The destination port address is the address of the application program that receives the message.
- **Total length:** It defines the total number of bytes of the user datagram in bytes.
- **Checksum:** The checksum is a 16-bit field used in error detection.
- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.

Transmission Control Protocol (TCP)

- It provides a full transport layer services to applications.
- It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
- TCP is called a **connection-oriented, reliable protocol.**
- TCP is a **reliable protocol** as it detects the error and retransmits the damaged frames.
- Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
- At the sending end, TCP divides the whole message into smaller units known as **segment**, and each segment contains a sequence number which is required for reordering the frames to form an original message.
- At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.





Application Layer

- An application layer is the **topmost layer** in the TCP/IP model.
- This layer allows the **user to interact with the application**.
- **When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.**
- There is an ambiguity occurs in the application layer.
- Every application cannot be placed inside the application layer except those who interact with the communication system.

For example:

- text editor cannot be considered in application layer while web browser using HTTP protocol to interact with the network where **HTTP protocol is an application layer protocol.**

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for **Hypertext transfer protocol**. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is a protocol which governs the dialog between the client and a server. **(port no 80)**
- **SNMP:** SNMP stands for **Simple Network Management Protocol**. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for **Simple mail transfer protocol**. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address**.(synchronous & asynchronous)**
- **DNS:** DNS stands for **Domain Name System**. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for **Terminal Network**. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for **File Transfer Protocol**. FTP is a standard internet protocol used for transmitting the files from one computer to another computer on the internet**.(port no 20 for data and 21 for control) (synchronous)**

Difference between OSI and TCP/IP model

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as **a communication gateway between the network and end user.**	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is **a communication protocol**, which allows connection of hosts over a network.
2. In OSI model the transport layer **guarantees the delivery of packets.**	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. OSI model has a **separate Presentation layer and Session** layer.	3. TCP/IP does not have a separate Presentation layer or Session layer.
4. **Transport Layer** is Connection Oriented.	4. Transport Layer is both Connection Oriented and Connection less.
5. **Network Layer** is both Connection Oriented and Connection less.	5. Network Layer is Connection less.
6. **OSI is a reference model** around which the networks are built. Generally, it is used as a guidance tool.	6. TCP/IP model is, in a **way implementation of the OSI model.**

7. OSI model has a **problem of fitting the protocols into the model.**	7. TCP/IP model does not fit any protocol
8. **Protocols are hidden** in OSI model and are easily replaced as the technology changes.	8. In TCP/IP **replacing protocol is not easy.**
9. It has **7 layers**	9. It has **4 layers**

What is Internet Protocol (IP) ?

- An IP stands for internet protocol.
- An IP address is assigned to each device connected to a network.
- Each device uses an IP address for communication.
- It defines the technical format of the packets.
- Mainly, both the networks, i.e., IP and TCP, are combined, so together, they are referred to as a TCP/IP.
- It creates a virtual connection between the source and the destination.
- To facilitate the routing of packets, TCP/IP protocol uses a 32-bit logical address known as IPv4(Internet Protocol version 4).
- An IP address consists of two parts, i.e., the first one is a **network address**, and the other one is a **host address**.

There are two types of IP addresses:

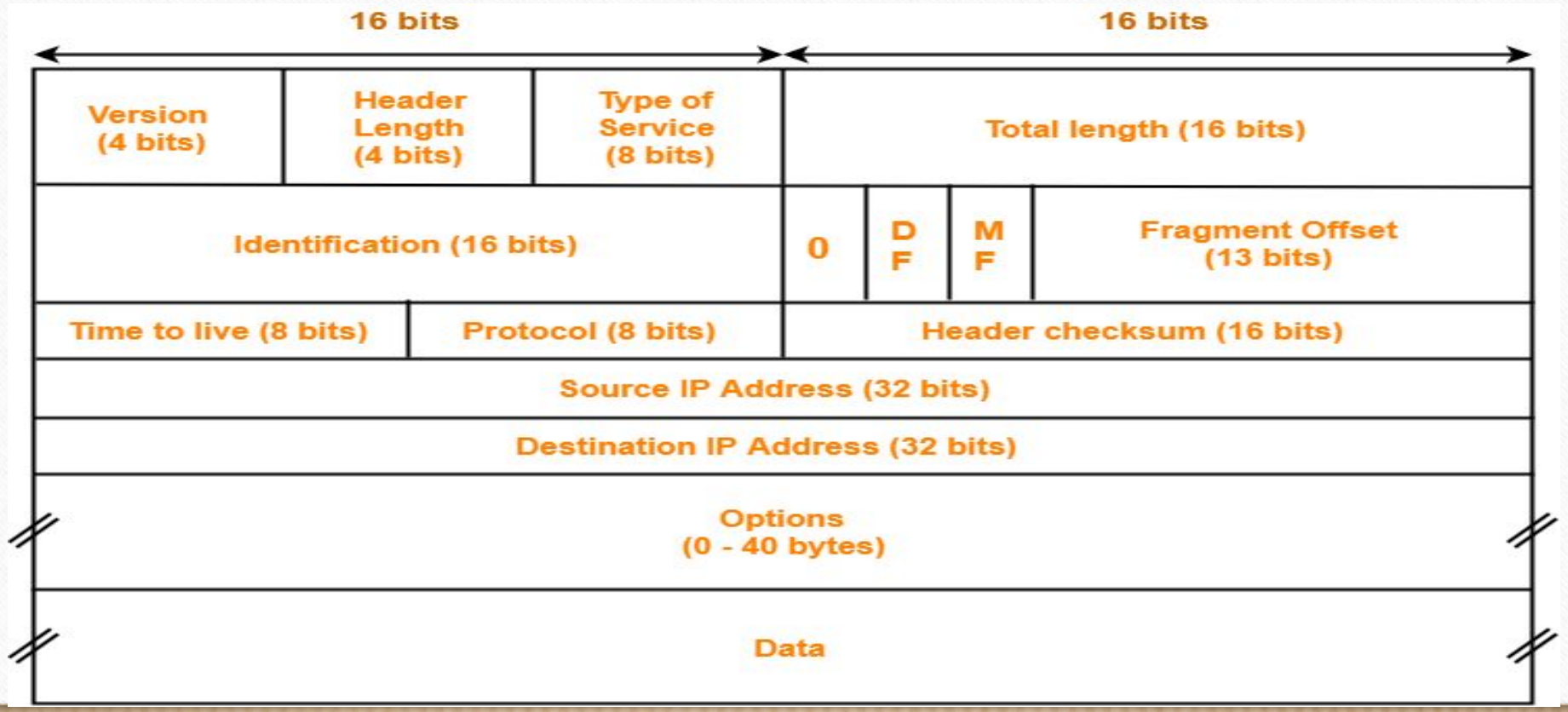
- **IPv4**
- **IPv6**

Differences between IPv4 and IPv6

- IPv4 and IPv6 are internet protocol version 4 and internet protocol version 6.
- IP version 6 is the new version of Internet Protocol.
- IPv6 is way better than IPv4 in terms of complexity and efficiency.
- For example, **66.94.29.13**

Points	IPv4	IPv6
Address size	32-bit Address space	128-bit Address space
	In IPv4, around 4 billion unique IP addresses are generated (2^{32})	In IPv6, around 340 trillion unique IP addresses are generated (2^{128})
Address format	Dotted Decimal Notation: 192.168.0.1	Hexadecimal Notation: 3FFE:F200:0204:AB00 0123:4567:8901:ABCD
Range	The range of IPv4 address is 0 to 255	The range of IPv6 address is 0 to FFFF(65535)
Checksum	Checksum field is available in header	Checksum field is not available in header
Packet Size	576 bytes	1280 bytes
Security	Provides less security as compared to IPv6	Uses authentication and encryption to provide security
Network configuration	Manual configuration is required	Provides Auto-configuration
Broadcast/Multicast	Uses both	No broadcast and has different forms of multicast
Mobility	No support	Provides support for Mobile IP
QoS support	Provides less QoS as compared to IPv6	Provides QoS for multimedia data
classes	It has total 5 classes	It doesn’t have any class
	IPv4 is a numeric address separated by .(dot)	IPv6 is alphanumeric number separated by colon (:)

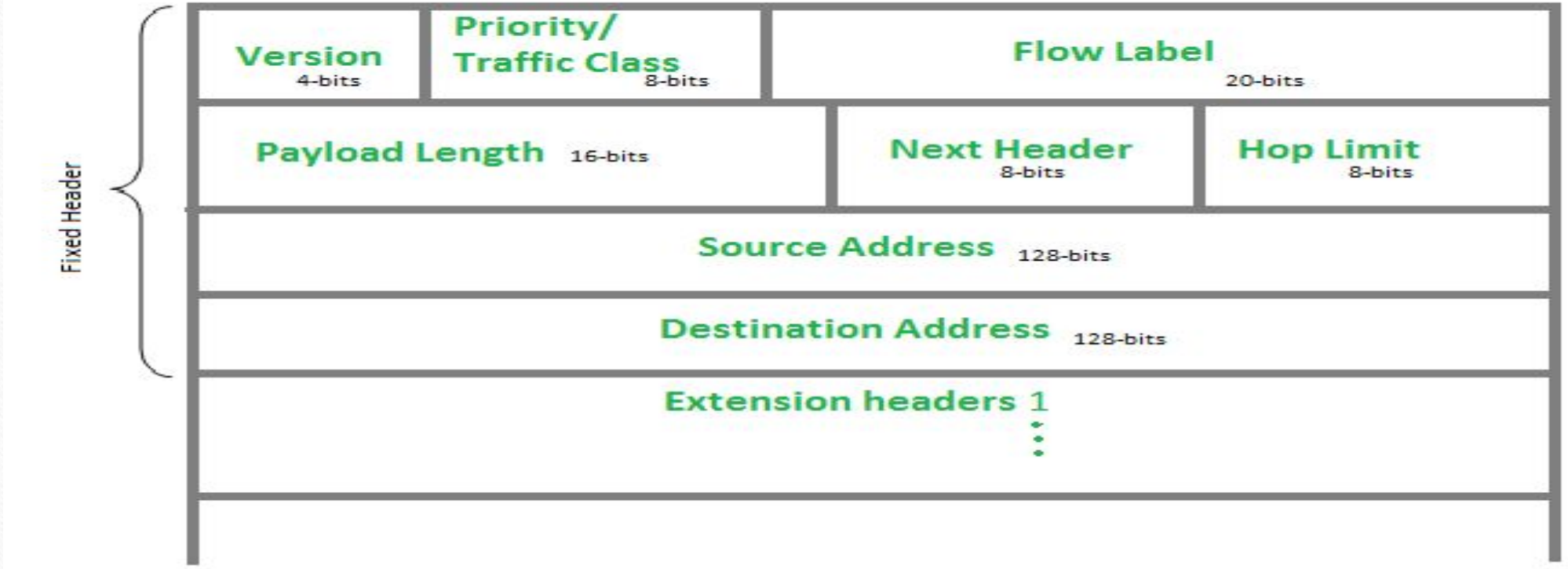
IPv4 Header Format



- **Version:** version no of Internet Protocol used (e.g IPv4)
- **HLEN:** Header length is a 4-bit field that contains the length of the IP header.
- **Types of Services:** Type of service is a 8-bit field that is used for Quality of Service (QoS).
- **Total Length:** Length of entire IP packet i.e 16 bits (Header + Data) = Datagram
- **Identification:** Identification is a 16-bit field. It is used for the identification of the fragments of an original IP datagram.
- **Flags:** If IP packet is too large to handle, these flags tells if they can be fragmented or not. In this 3-bit flag, the MSB always set to 0.

  DF Bit- DF bit stands for Do Not Fragment bit. Its value may be 0 or 1. When DF bit is set to 0, It grants the permission to the intermediate devices to fragment the datagram if required.
- **Fragment offset:** (13 bit) It indicates the position of a fragmented datagram in the original unfragmented IP datagram. The first fragmented datagram has a fragment offset of zero.
- **TTL:** Time to live (TTL) is a 8-bit field. It indicates the maximum number of hops a datagram can take to reach the destination.
- **Protocol:** (8-bit field) It tells the network layer at the destination host to which protocol the IP datagram belongs to. Protocol number of ICMP is 1, IGMP is 2, TCP is 6 and UDP is 17.
- **Header Checksum:** (16-bit field) The checksum value is used for error checking of the header.
- **Source Address:** 32-bits. It holds the address of the sender of the packet.
- **Destination Address:** 32-bits. It holds the address of the intended recipient of the packet.

IPv6 Header Format



- **Version:** 4-bit IP version number i.e., 6.
- **Traffic Class or Priority:** 4-bit priority value. It enables a source to identify the desired delivery priority of its packets.
- **Flow Label:** 24-bit field. It is used to give packets some special type of traffic, such as video messages.
- **Payload length:** 16-bit unsigned integer. Length of payload, i.e the rest of the packet following the IPv6 header, in octets.
- **Next Header:** 8-bit selector. It identifies the type of header immediately following the IPv6 header. It uses the same values as IPv4 field.
- **Hop Limit:** 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet will be discarded if Hop Limit is decremented to zero. Similar to IPv4 which contained time-to-live in seconds.
- **Source Address:** 128-bits. It holds the address of the sender of the packet.
- **Destination Address:** 128-bits. It holds the address of the intended recipient of the packet.

Difference between IPv4 & IPv6 Header Format

- IPv6 header is much simpler than IPv4 header.
- The size of IPv6 header is much bigger than that of IPv4 header, because of IPv6 address size. IPv4 addresses are 32bit binary numbers and IPv6 addresses are 128-bit binary numbers.
- In IPv4 header, the source and destination IPv4 addresses are 32-bit binary numbers. In IPv6 header, source and destination IPv6 addresses are 128-bit binary numbers.
- The fields in the IPv4 header such as IHL (Internet Header Length), identification, flags are not present in IPv6 header.
- Time-to-Live (TTL), a field in IPv4 header, typically used for preventing routing loops, is renamed to its exact meaning, "Hop Limit".

Mobile IP

- Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address.
- The goal of Mobile IP is to enable packet transmission efficiently without any packet loss and disruptions in the presence of host or destination mobility.

Terminologies:

- **Mobile Node (MN):**

It is the hand-held communication device that the user caries e.g. Cell phone.

- **Home Network:**

It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).

- **Home Agent (HA):**

It is a router in home network to which the mobile node was originally connected

- **Home Address:**

It is the permanent IP address assigned to the mobile node (within its home network).

- **Foreign Network:**

It is the current network to which the mobile node is visiting (away from its home network).

- **Foreign Agent (FA):**

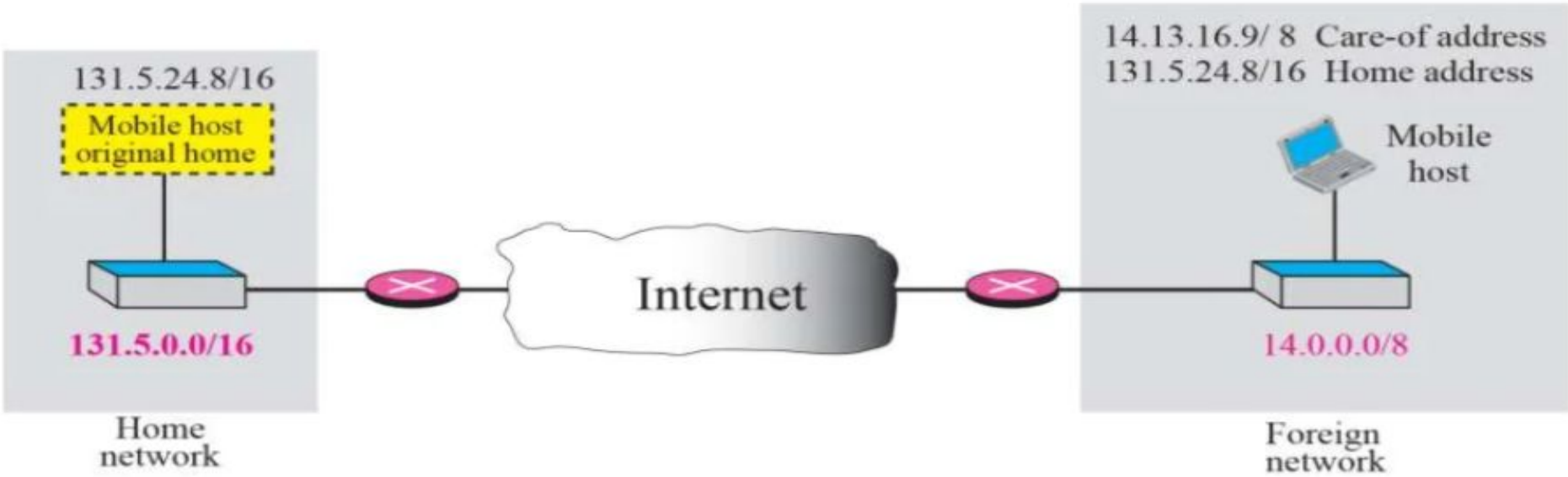
It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.

- **Correspondent Node (CN):**

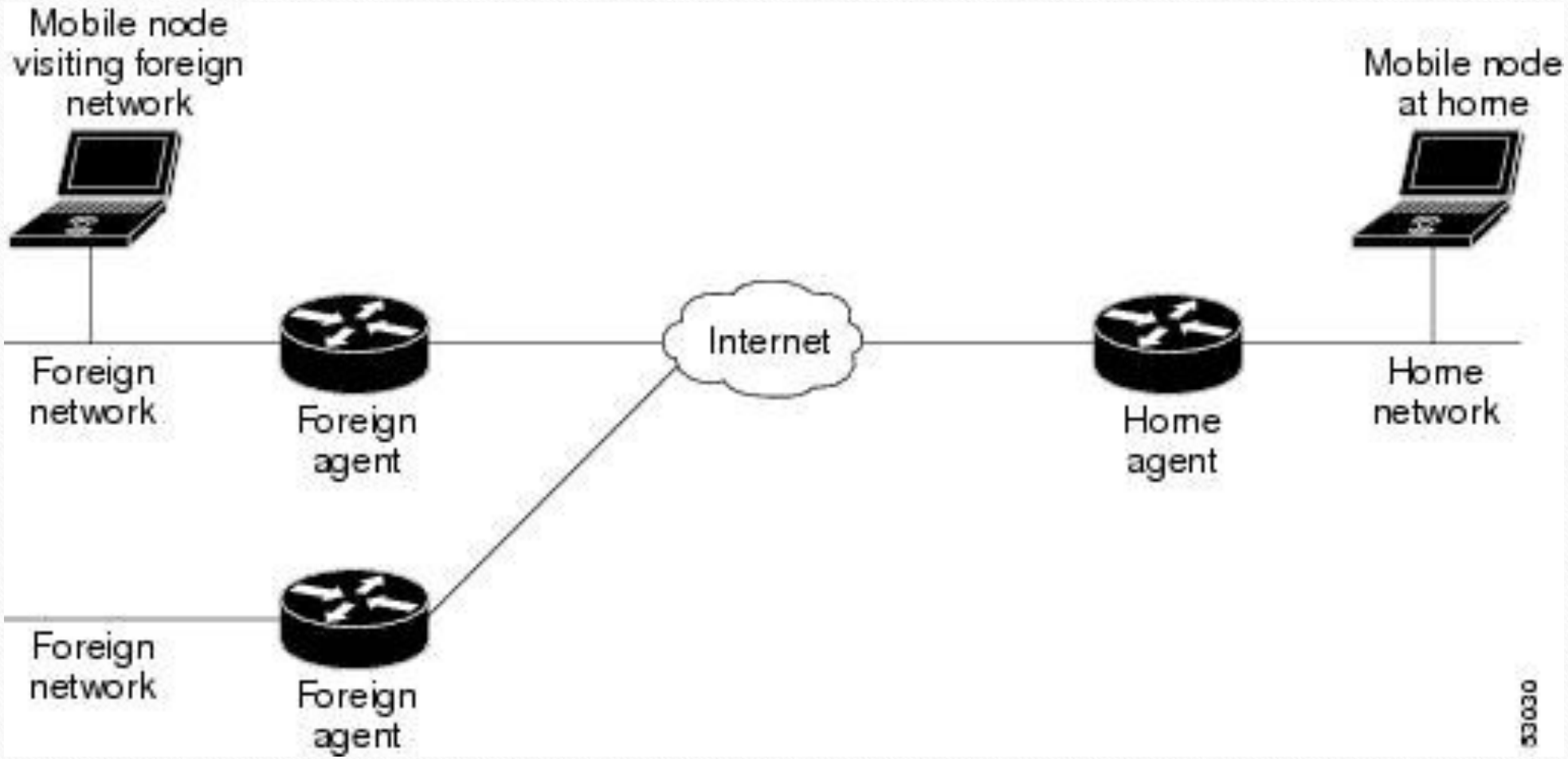
It is a device on the internet communicating to the mobile node.

- **Care of Address (COA):**

It is the temporary address used by a mobile node while it is moving away from its home network.


131.5.24.8/16
Mobile host original home
131.5.0.0/16
Home network
Internet
14.13.16.9/ 8 Care-of address
131.5.24.8/16 Home address
Mobile host
14.0.0.0/8
Foreign network


Home network
Mobile host original home
Home agent
Internet
Foreign agent
Foreign network
Mobile host


Mobile node visiting foreign network
Mobile node at home
Foreign network
Foreign agent
Internet
Home agent
Home network
Foreign network
Foreign agent
33030

Working of Mobile IP:

- Correspondent node sends the data to the mobile node.
- Data packets contains correspondent node's address (Source) and home address (Destination).
- Packets reaches to the home agent.
- But now mobile node is not in the home network, it has moved into the foreign network.
- Foreign agent sends the care-of-address to the home agent to which all the packets should be sent.
- Now, a tunnel will be established between the home agent and the foreign agent by the process of tunneling.
- Tunneling establishes a virtual pipe for the packets available between a tunnel entry and an endpoint.
- It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation.

Working of Mobile IP:

- The Mobile IP process has three main phases, which are discussed in the following sections.

Agent Discovery

- A Mobile Node discovers its Foreign and Home Agents during agent discovery.

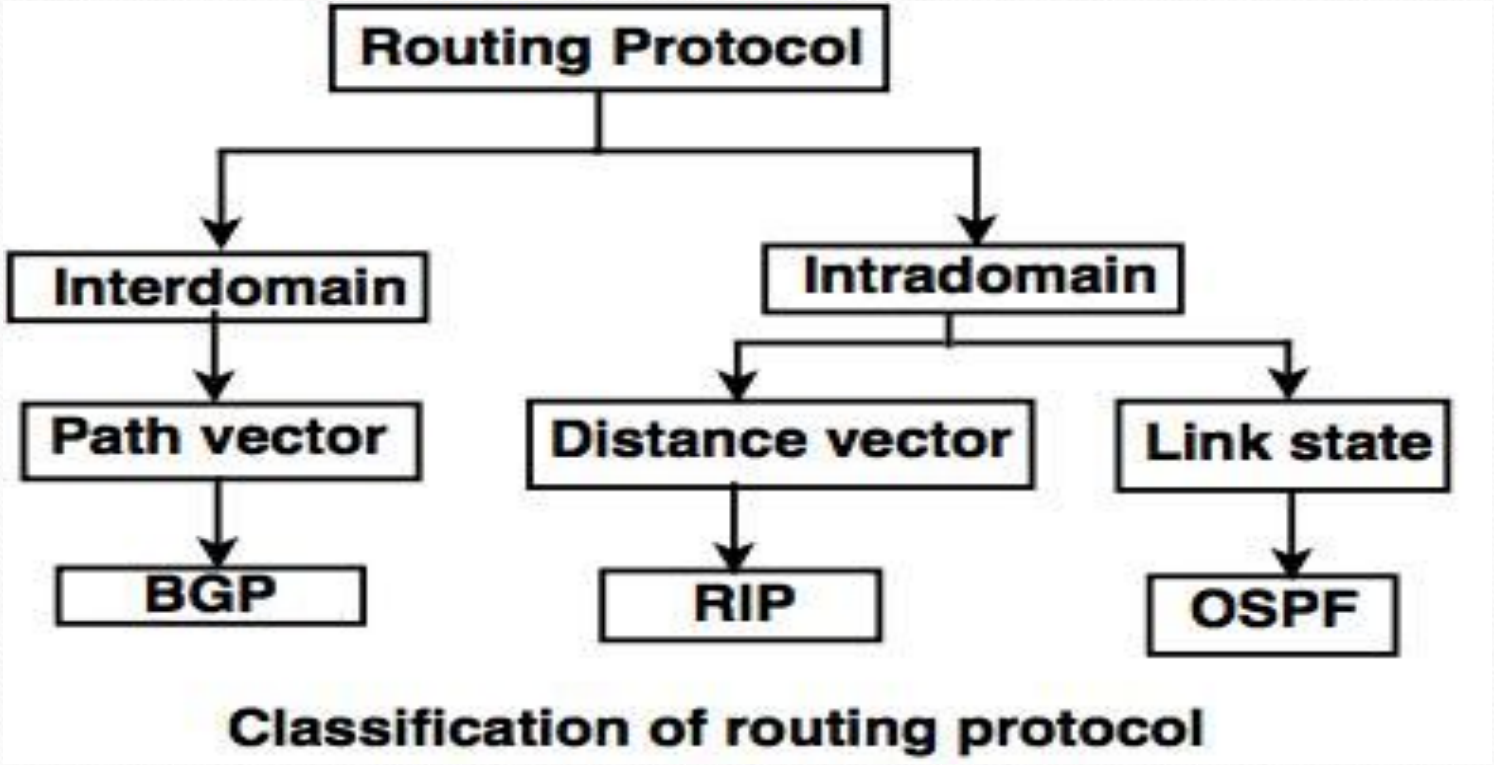
Registration

- The Mobile Node registers its current location with the Foreign Agent and Home Agent during registration.

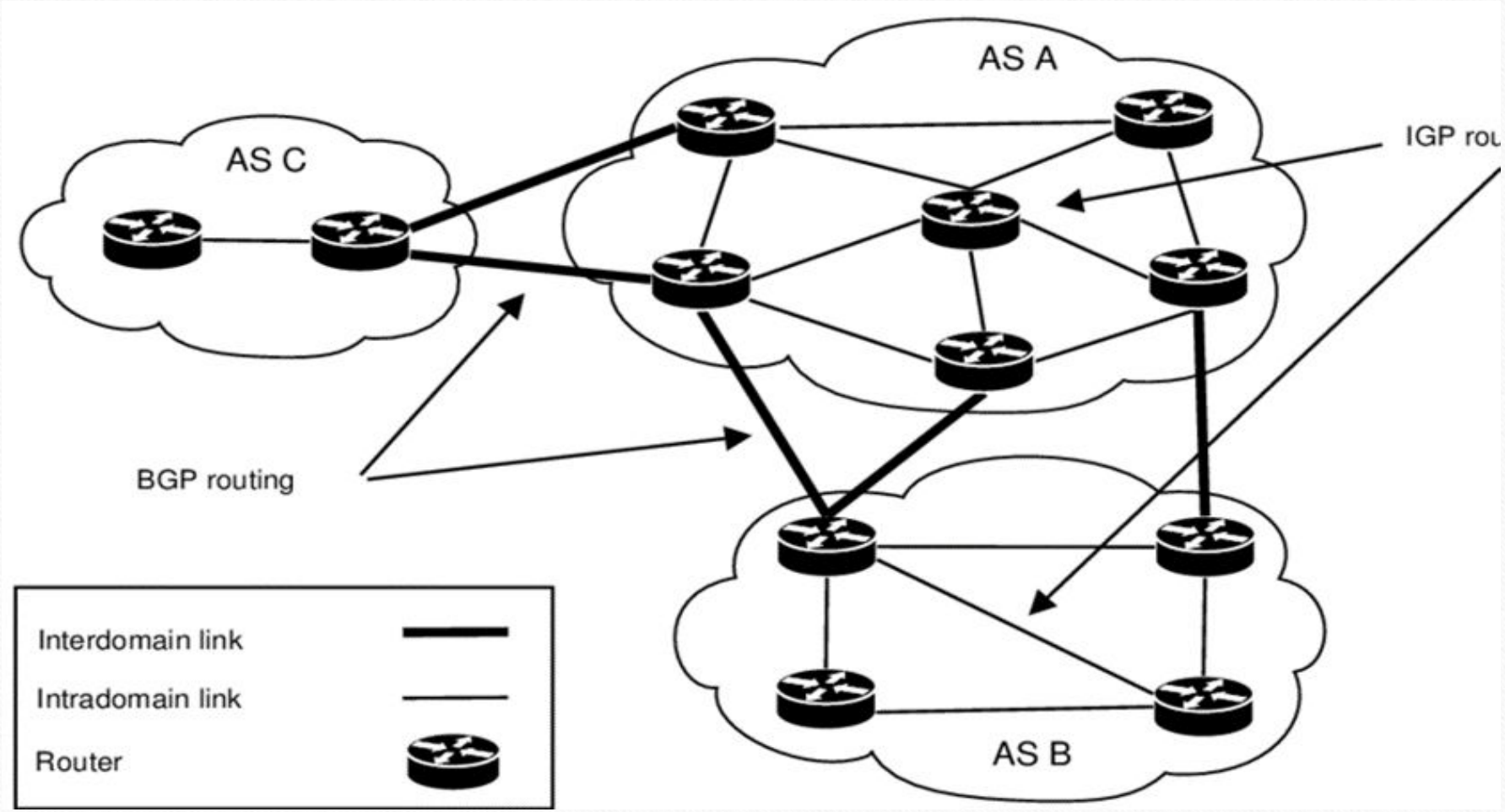
Tunneling

- A reciprocal tunnel is set up by the Home Agent to the care-of address (current location of the Mobile Node on the foreign network) to route packets to the Mobile Node as it roams.

Routing in the internet



Classification of routing protocol



Intradomain & Interdomain routing

Intra-domain Routing Protocols

- *Routing inside an autonomous system is referred to as **intradomain routing**.*

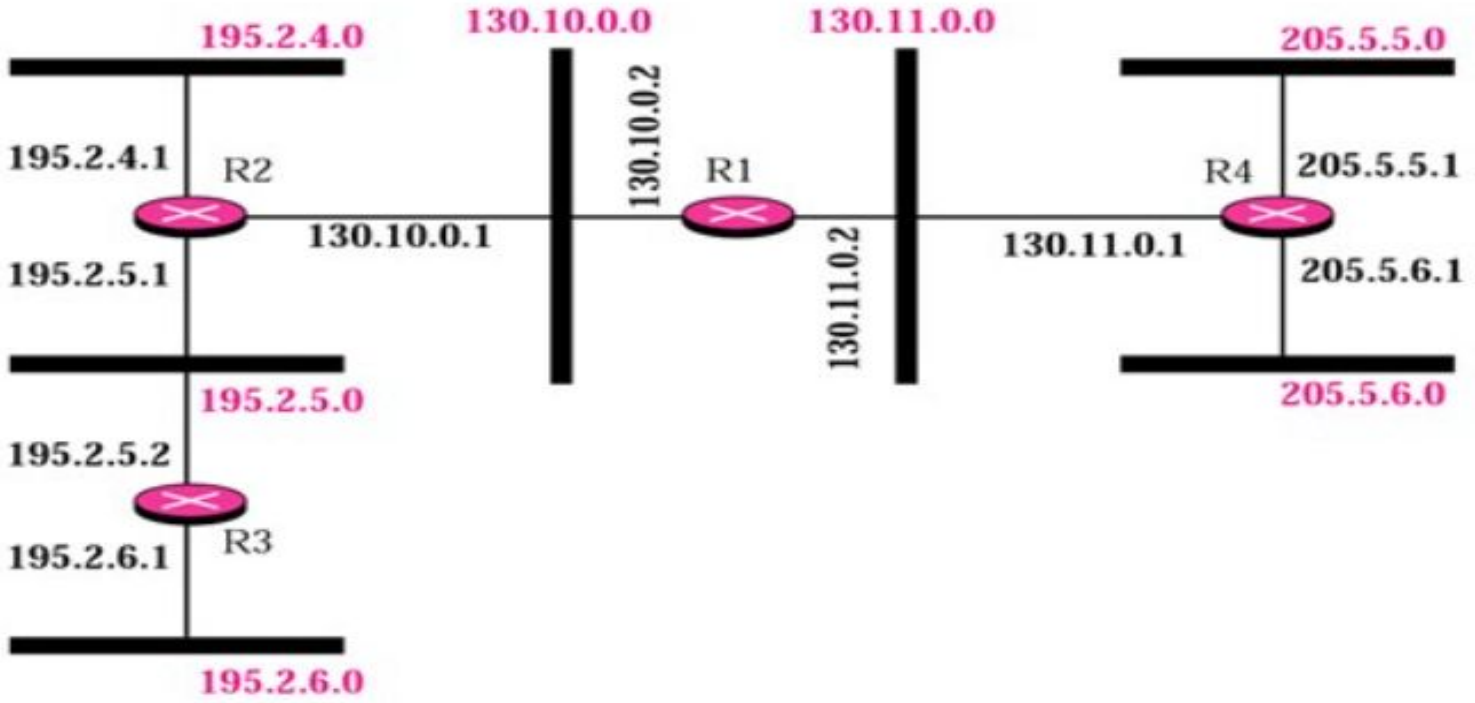
Distance vector

This algorithm communicates the current distance estimates of a node to every other node

RIP (unicast)

- The Routing Information Protocol (RIP) uses "hop count" to find the shortest path from one network to another, where "hop count" means number of routers a packet must pass through on the way. (When a packet goes from one network to another, this is known as a "hop."). Two versions of RIP are RIPv1 & RIPv2

Figure 14.8 *Example of a domain using RIP*



R1 Table

Dest.	Hop	Next
130.10.0.0	1	———
130.11.0.0	1	———
195.2.4.0	2	130.10.0.1
195.2.5.0	2	130.10.0.1
195.2.6.0	3	130.10.0.1
205.5.5.0	2	130.11.0.1
205.5.6.0	2	130.11.0.1

R2 Table

Dest.	Hop	Next
130.10.0.0	1	———
130.11.0.0	2	130.10.0.2
195.2.4.0	1	———
195.2.5.0	1	———
195.2.6.0	2	195.2.5.2
205.5.5.0	3	130.10.0.2
205.5.6.0	3	130.10.0.2

R3 Table

Dest.	Hop	Next
130.10.0.0	2	195.2.5.1
130.11.0.0	3	195.2.5.1
195.2.4.0	2	195.2.5.1
195.2.5.0	1	———
195.2.6.0	1	———
205.5.5.0	4	195.2.5.1
205.5.6.0	4	195.2.5.1

R4 Table

Dest.	Hop	Next
130.10.0.0	2	130.11.0.2
130.11.0.0	1	———
195.2.4.0	3	130.11.0.2
195.2.5.0	3	130.11.0.2
195.2.6.0	4	130.11.0.2
205.5.5.0	1	———
205.5.6.0	1	———

Link State

Link state routing is a technique in which each router shares the knowledge of its neighborhood with every other router in the internetwork. Based on this learned topology, each router is then able to compute its routing table by using the shortest path computation using Dijkstra's algorithm.

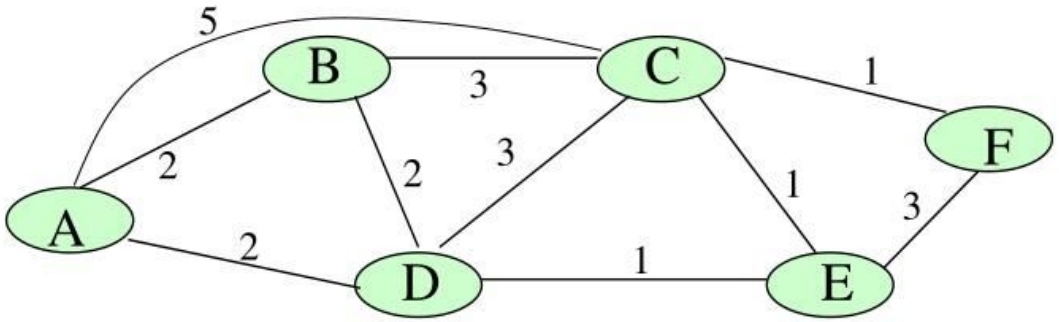
OSPF (unicast)

The Open Shortest Path First (OSPF) protocol is commonly used by network routers to dynamically identify the fastest and shortest available routes for sending packets to their destination.

- Discover the neighboring node. (send Hello message periodically)
- Measure the link costs to the neighboring nodes.
- Make the Link State packet.
- Broadcast the Link State packet to all nodes.
- After receiving the Link State packets from all other nodes, make the link state database.
- Compute the shortest paths to reach all other nodes based on the link state database.

Example of Link state routing

Step1: Collect the link state information from the neighboring nodes and make the link state packets.



Link state packets

A	
seq#	
age	
B	2
C	5
D	2

B	
seq#	
age	
A	2
C	3
D	2

C	
seq#	
age	
A	5
B	3
D	3
E	1
F	1

D	
seq#	
age	
A	2
B	2
C	3
E	1

E	
seq#	
age	
C	1
D	1
F	1

F	
seq#	
age	
C	1
E	1

Example of Link state routing

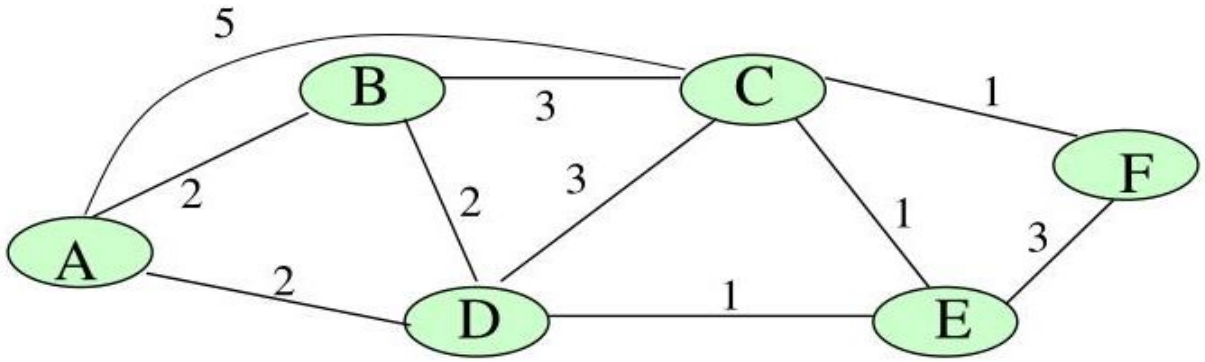
Step 2: Propagate the link state information to all other nodes.

- Make the link state packet.
- Use the flooding.

Step 3: Compute the shortest path.

- Based on the link state information, the node makes the link state database that represents the whole network topology.
- Compute the shortest path using the Dijkstra algorithm.

Link State Database



Link #	Cost	Link #	Cost	Link #	Cost
A-B	2	C-B	3	D-E	1
A-C	5	C-D	3	E-C	1
A-D	2	C-E	1	E-D	1
B-A	2	C-F	1	E-F	1
B-C	3	D-A	2	E-C	1
B-D	2	D-B	2	E-E	1
C-A	5	D-C	3		

Inter-domain Routing Protocols

- *Routing between autonomous systems is referred to as **interdomain routing**.*

Path Vector Routing

- This algorithm communicates the current estimates of preferred paths from a node to every other node.

BGP: (unicast)

- The Border Gateway Protocol (BGP) is an interdomain routing protocol using path vector routing.
- It is used to announce which networks control which IP addresses, and which networks connect to each other. (The large networks that make these BGP announcements are called autonomous systems.) BGP is a dynamic routing protocol.

path vector routing (BGP)

- Interdomain routing protocol
- A path vector protocol is essentially a distance vector protocol that does not rely on the distance to destination to guarantee a loop-free path but instead relies on the analysis of the path itself.
- In a path vector protocol, a router does not just receive the distance vector for a particular destination from its neighbor; instead, a node receives the distance *as well* as **path information** (aka BGP path attributes), that the node can use to calculate how traffic is routed to the destination AS.

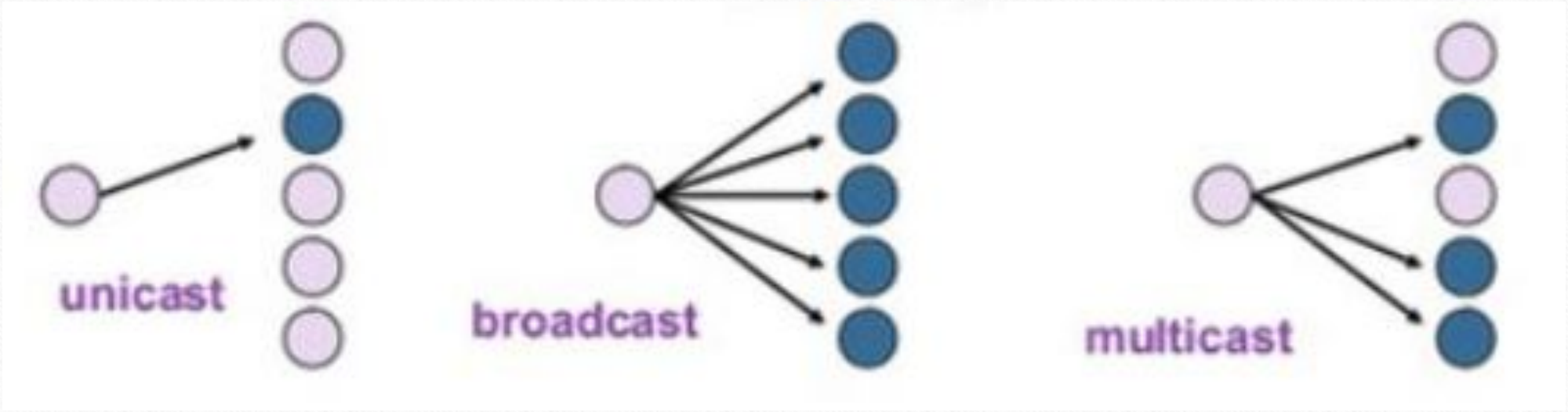
There is at least one node, called the speaker node, in each AS that creates a routing table and advertises it to speaker nodes in the neighboring ASs.

Only speaker nodes in each AS can communicate with each other.

Speaker node advertises the path, not the metric.

- **Sharing:**
  - A speaker in an autonomous system shares its table with immediate neighbors.
- **Updating:**
  - When a speaker node receives a table from its neighbor, it updates its own table by adding the nodes that are not in its routing table.
  - It also adds its own AS and the AS that sent the table.

Unicast and Multicast Routing Protocol



IP Routing

- IP Routing is a process that sends packets from a host on one network to another host on a different remote network.
- It helps you examine the destination IP address of a packet, determine the next-hop address, and forward it.
- IP routers use **routing tables** to determine the next-hop address to which the packet should be delivered.

Routing Metrics

Routing metric are the value that allows the routers to decide the **best route for the data packet**

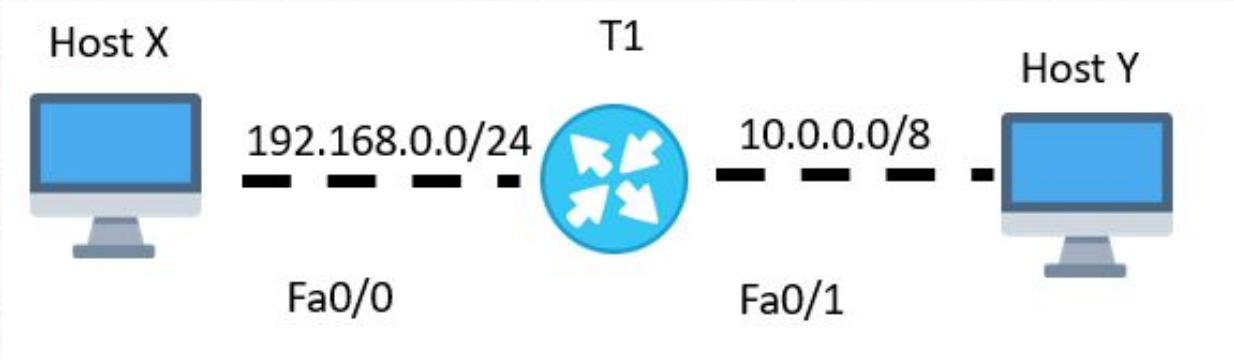
- **Hops:** the path with the least hop count will be considered as the best path to move from source to the destination.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link.
- Load:
- Cost
- Reliability

What is the Default gateway?

- A default gateway is a router that hosts use to communicate with other hosts on remote networks.
- A default gateway is used when a host does not have a route entry for the remote network and does not know how to reach that network.
- Hosts should be configured to send all packets destined to the default gateway's remote networks, which has a route to reach that specific network.

How does IP routing work?

- Host X has an IP address of the router T1 configured as the default gateway address.
- Here, host X is trying to communicate with host Y, which is a host on another remote network.
- This host looks up in its routing table to check if there is an entry for the destination network address.
- If the entry is found, the host will send all data to the router T1.
- Router T1 then receives the packets and forwards them to host Y.

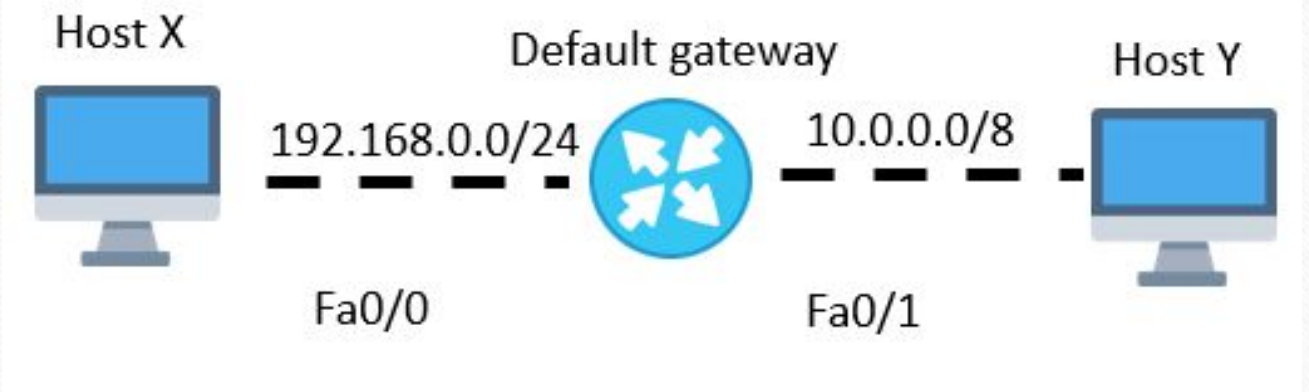


Default gateway

Routing Table

- Every router maintains a routing table which is stored in its RAM. A routing table is widely used by routers to decide the path to the destination network. There are mainly three different methods for populating a routing table:

- Directly connected subnets
- Using static routing (manually)
- Using dynamic routing (automatic)



Functions of Router

- Creates a local area network (LAN).
- It allows you to split your internet connection to all of your devices.
- Connect different media and set of devices
- The routers determine where to send information from one computer to another
- Packet Forwarding, switching, and filtering.
- Router also makes sure that information does make it to the intended destination.
- Connect to a VPN (allows you to connect a private network across a public network)

ADVANCED COMPUTER NETWORKS

By: Mrs. Nidhi Divecha (ME CMPN)

(Unit 2)

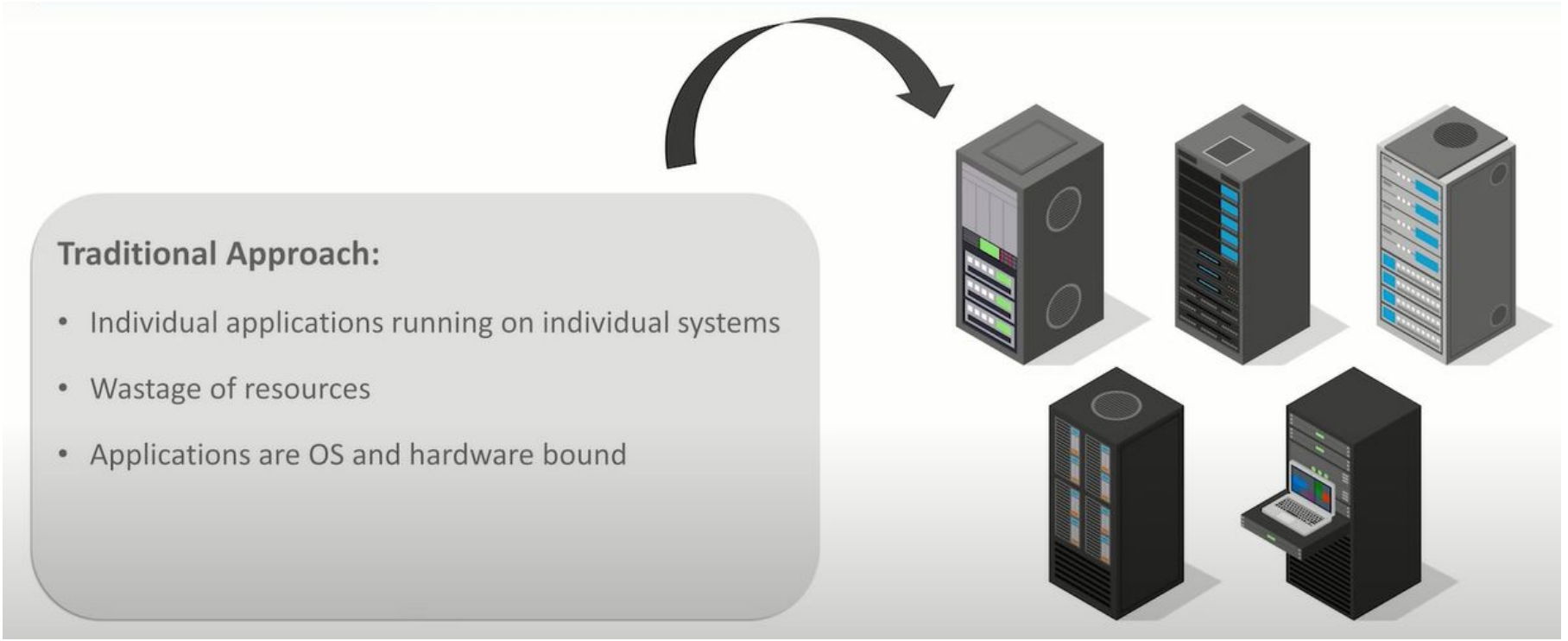
NETWORK VIRTUALIZATION

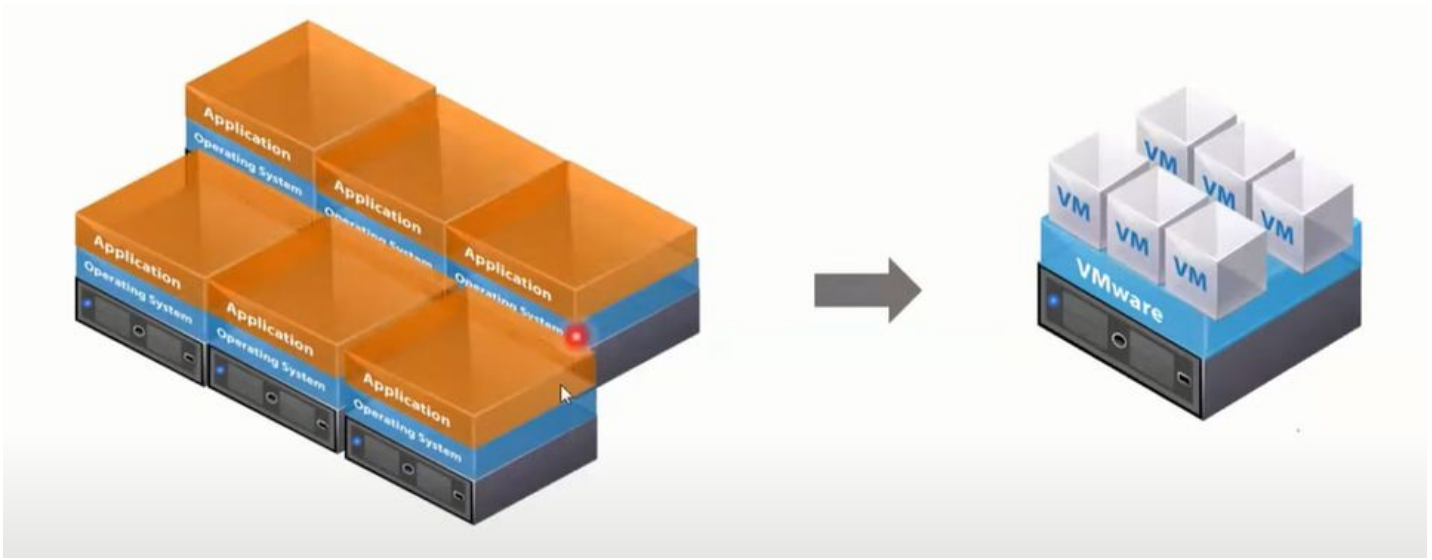
NEED FOR VIRTUALIZATION

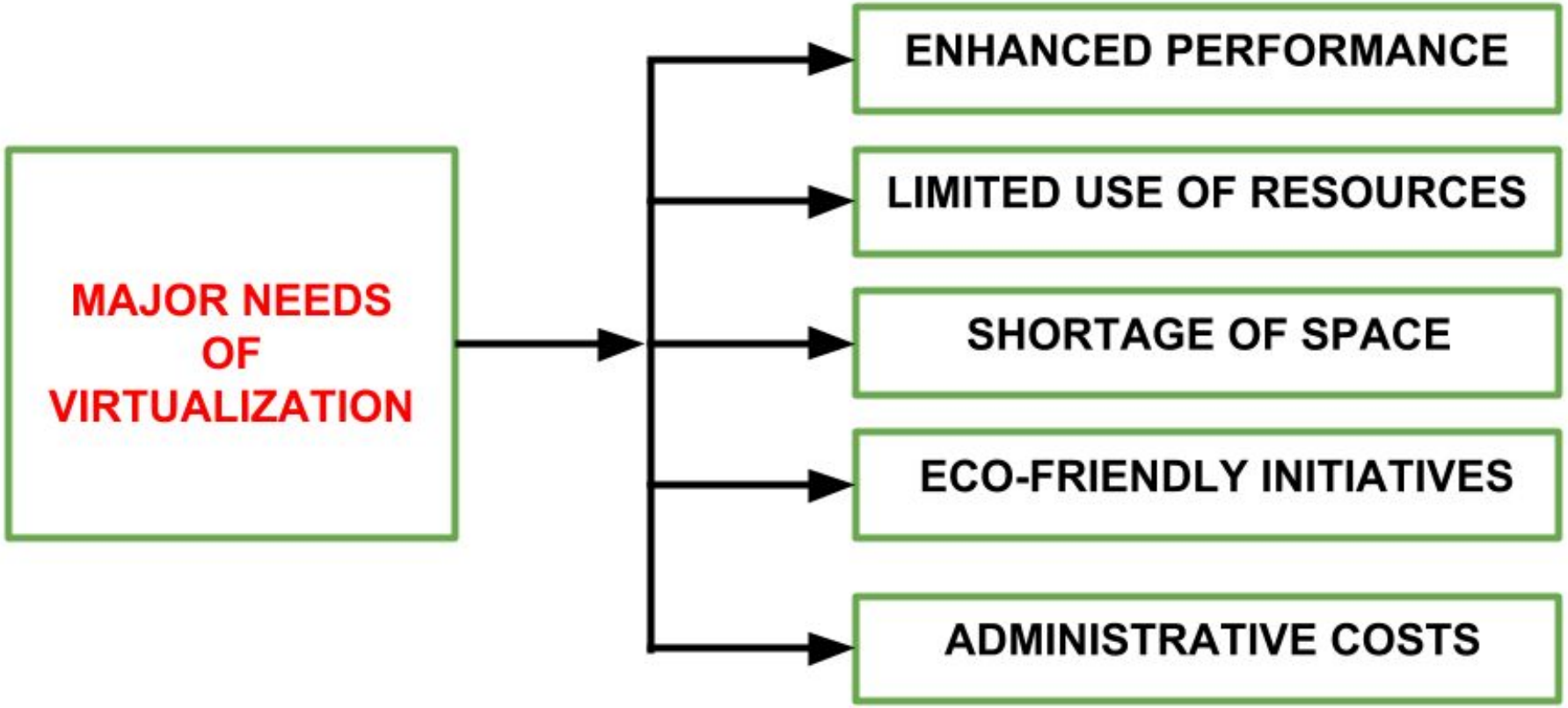
- No need to maintain thousands of servers in a server room.
- No need to buy lots of PCs for the work force of your organization.
- No need to buy individual storage space for your apps.
- With the growing and scaling technology, the complexity to manage IT Infrastructure has also increased to a challenging level.
- To solve this technical issue, a technology comes into play, which is Virtualization.
- With Virtualization, there is no need of following the old approach of one-app & one-server.
- The goal of visualization is to centralize the major and administrative tasks with parallel improvisation in scalability and workload.

Traditional Approach:

- Individual applications running on individual systems
- Wastage of resources
- Applications are OS and hardware bound






MAJOR NEEDS OF VIRTUALIZATION
ENHANCED PERFORMANCE
LIMITED USE OF RESOURCES
SHORTAGE OF SPACE
ECO-FRIENDLY INITIATIVES
ADMINISTRATIVE COSTS

What is Network Virtualization?

- Network virtualization describes **hardware, software, and network functionality** combined into a single, **virtual network.**
- It divides one physical network into seperate, independent virtual networks.
- This allows developers and engineers to test software that is under development or in the simulation stage.
- By implementing network virtualizing, the network administrator can **automate many of the tasks** previously performed manually, making the network much easier to scale.
- Network virtualization software allows network administrators to move virtual machines across different domains **without reconfiguring the network.**
- Network virtualization is intended to **optimize network speed, reliability, flexibility, scalability and security.**

Benefits of Network Virtualization

Lower hardware costs:

- With network virtualization, overall hardware costs are reduced, while providing a bandwidth that is more efficient.
- Also, thanks to automation and centralized control, most operational processes that are required to manage the network are reduced, allowing for reduced operational costs.

Dynamic network control:

- Network virtualization offers centralized control over network resources and allows for dynamic provisions and reconfiguration.
- Also, computer resources and applications can communicate with virtual network resources directly. This also allows for optimization of application support and resource utilization.

Rapid scalability:

- Network virtualization created an ability to scale the network rapidly either up or down to manage and create new networks on demand.
- Allows resources to be scaled elastically to address changing network demands.

Why Network Virtualization?

Advantages:

- More productive IT environments (i.e., efficient scaling).
- Improved security and recovery times.
- Faster in application delivery.
- More efficient networks.
- Reduced overall costs.
- Achieves greater operational efficiency by automating manual processes
- Improves network security within the data center

Types of Network Virtualization

- **Internal Virtualization**

Provides network-like functionality to the software containers on a single system.

- **External Virtualization**

Combines many networks, or parts of networks, into a virtual unit.

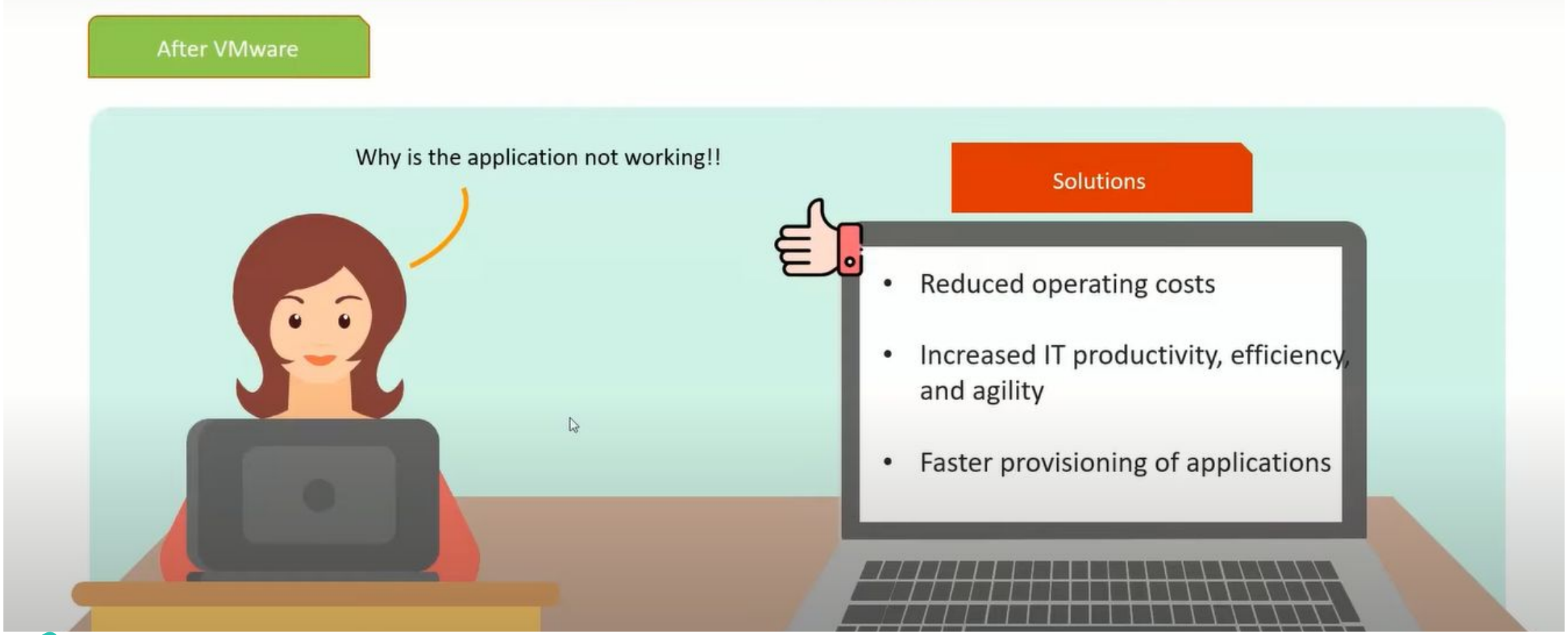
What is VMware?

In simple terms, VMware builds virtualization software.

Virtualization software generates an abstraction layer over computer hardware

This layer allows the hardware elements (like RAM, memory, storage, and more) to be categorized into multiple virtual machines

What is the need of VMware ?

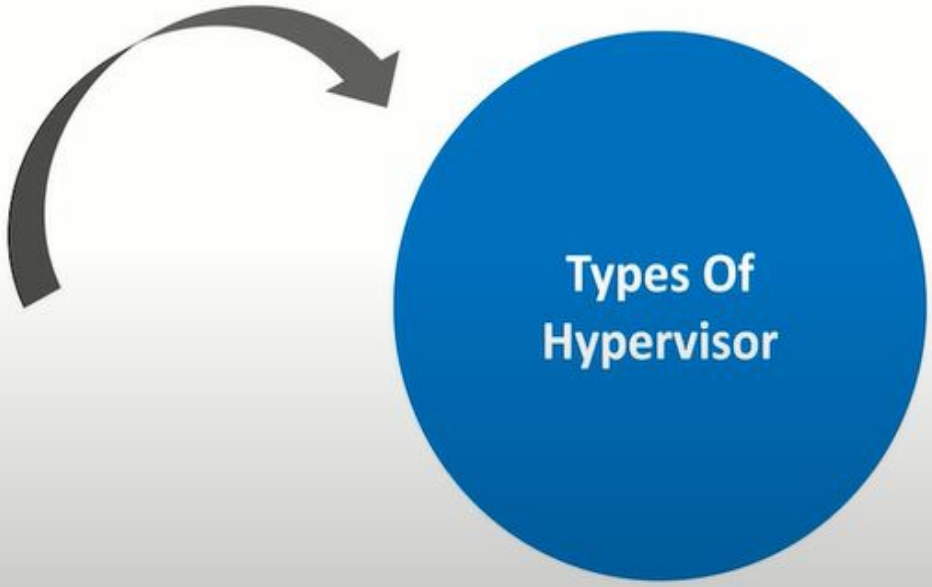


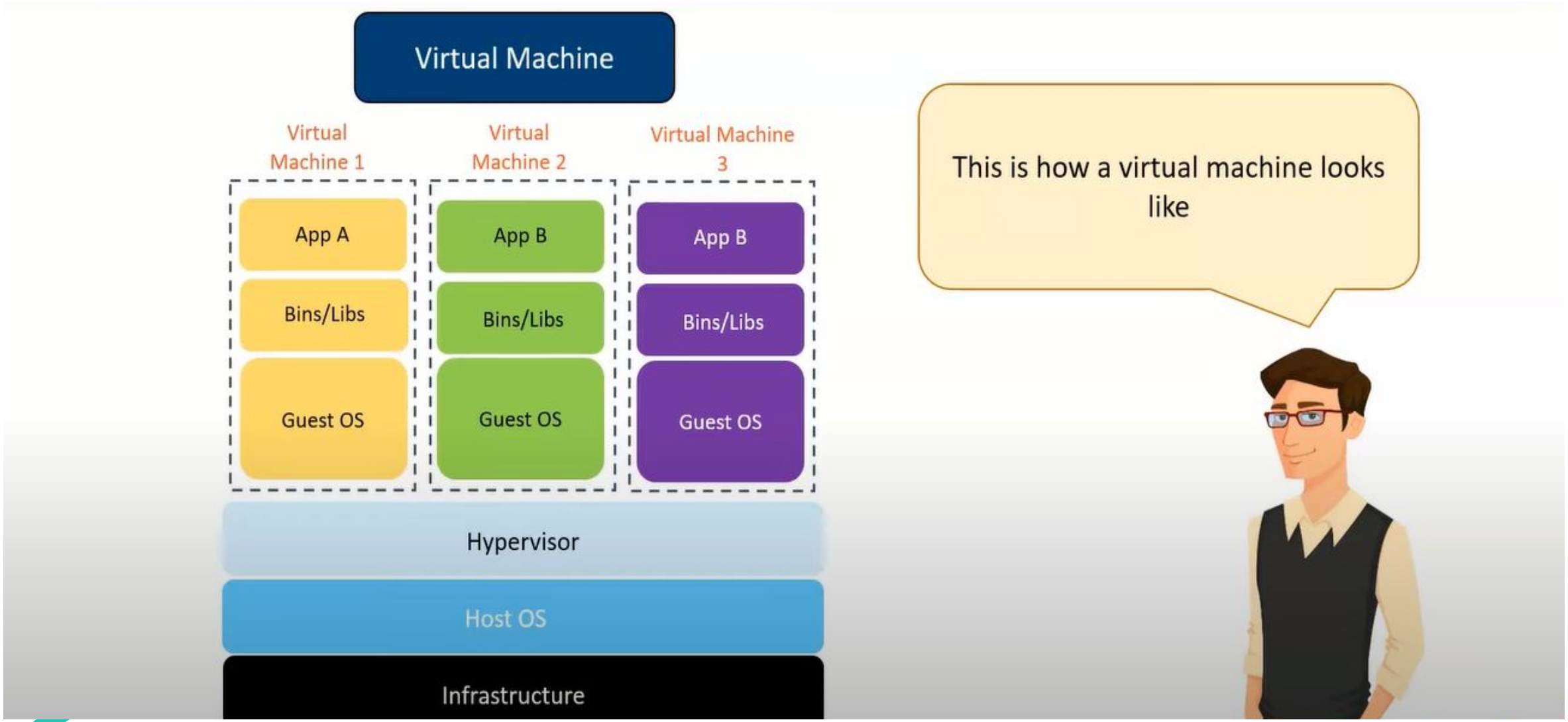
What is Hypervisor ?

*A **hypervisor** or **virtual machine monitor** (**VMM**) is computer software, firmware or hardware that creates and runs virtual machines.*

A computer on which a hypervisor runs one or more virtual machines is called a *host machine*, and each virtual machine is called a *guest machine*.

The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems.




Virtual Machine
Virtual Machine 1
Virtual Machine 2
Virtual Machine 3
App A
Bins/Libs
Guest OS
App B
Bins/Libs
Guest OS
App B
Bins/Libs
Guest OS
Hypervisor
Host OS
Infrastructure
This is how a virtual machine looks like

Benefits of Hypervisor

Cost-efficient

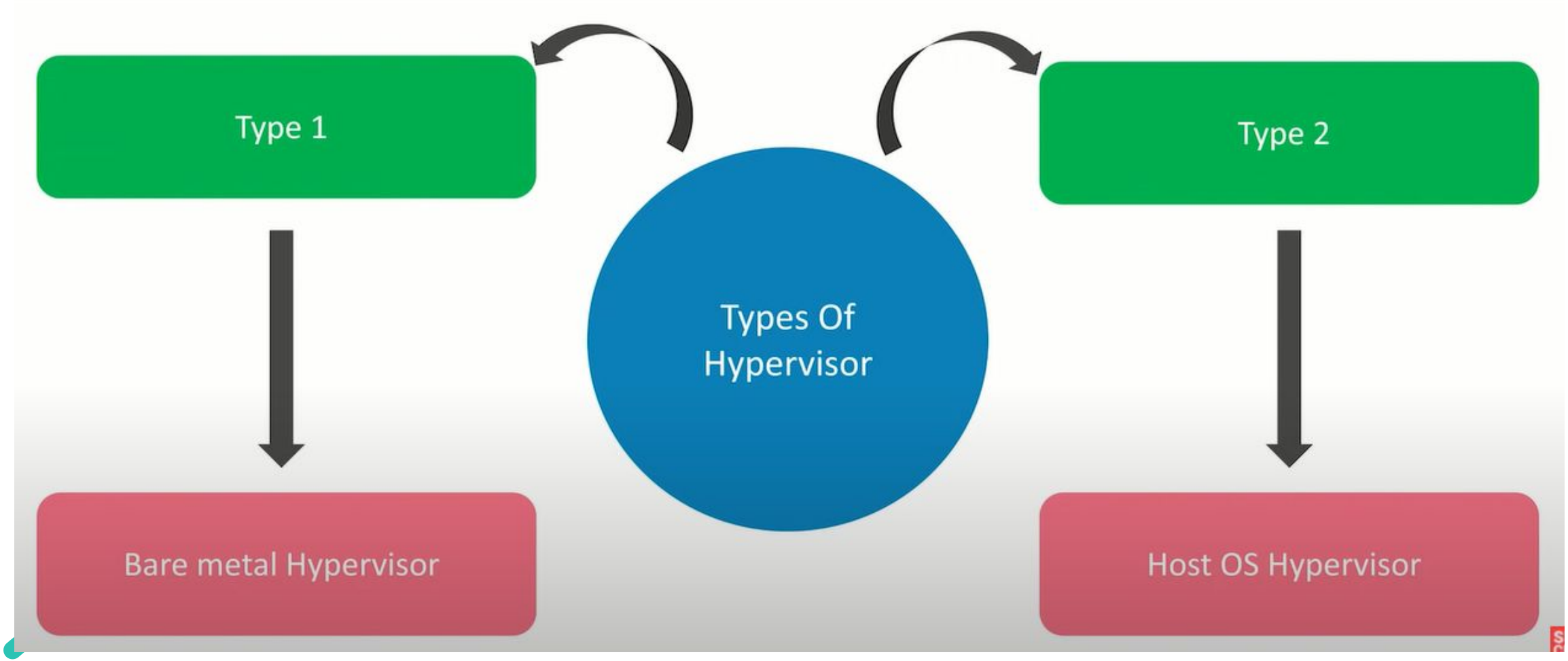
Flexibility

Portability

Easy setup and maintenance

Better resource allocation

Types of Hypervisor



How does Network Virtualization work?

- Network virtualization decouples network services from the underlying hardware and allows virtual provisioning of an entire network.
- Physical network resources, such as switching, routing, firewalling, load balancing, virtual private networks (VPNs), and more, are pooled, delivered in software, and require only Internet Protocol (IP) packet forwarding from the underlying physical network.
- Network and security services in software are distributed to a virtual layer (hypervisors, in the data center) and “attached” to individual workloads, such as your virtual machines (VMs) or containers, in accordance with networking and security policies defined for each connected application.
- When a workload is moved to another host, network services and security policies move with it.
- And when new workloads are created to scale an application, necessary policies are dynamically applied to these new workloads, providing greater policy consistency and network agility.

Network Virtualization Example

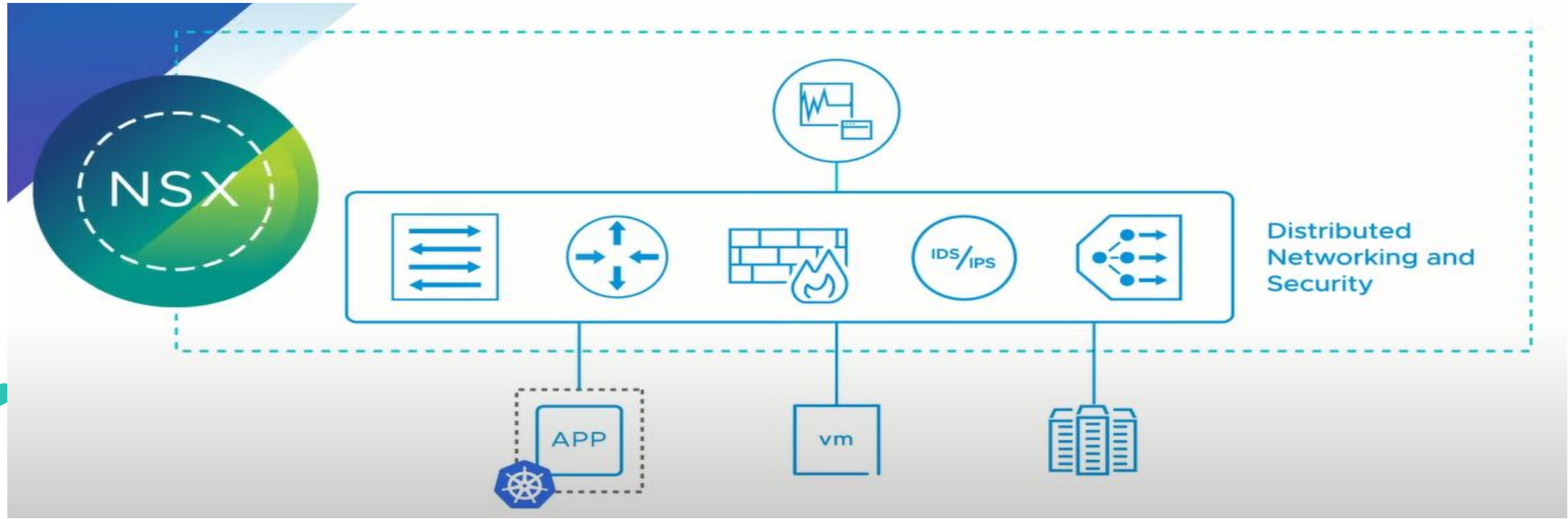
- One example of network virtualization is **virtual LAN (VLAN).**
- A VLAN is a subsection of a local area network (LAN) created with software that combines network devices into one group, regardless of physical location.
- VLANs can improve the speed and performance of busy networks and simplify changes or additions to the network.
- Another example is **VMware NSX Data Center – Network Virtualization Platform.**
- It is a network virtualization platform that delivers networking and security components like firewalling, switching, and routing that are defined and consumed in software. NSX takes an architectural approach built on scale-out network virtualization that delivers consistent, pervasive connectivity and security for apps and data wherever they reside, independent of underlying physical infrastructure.

VMware NSX Data Centre – Network Virtualization Platform

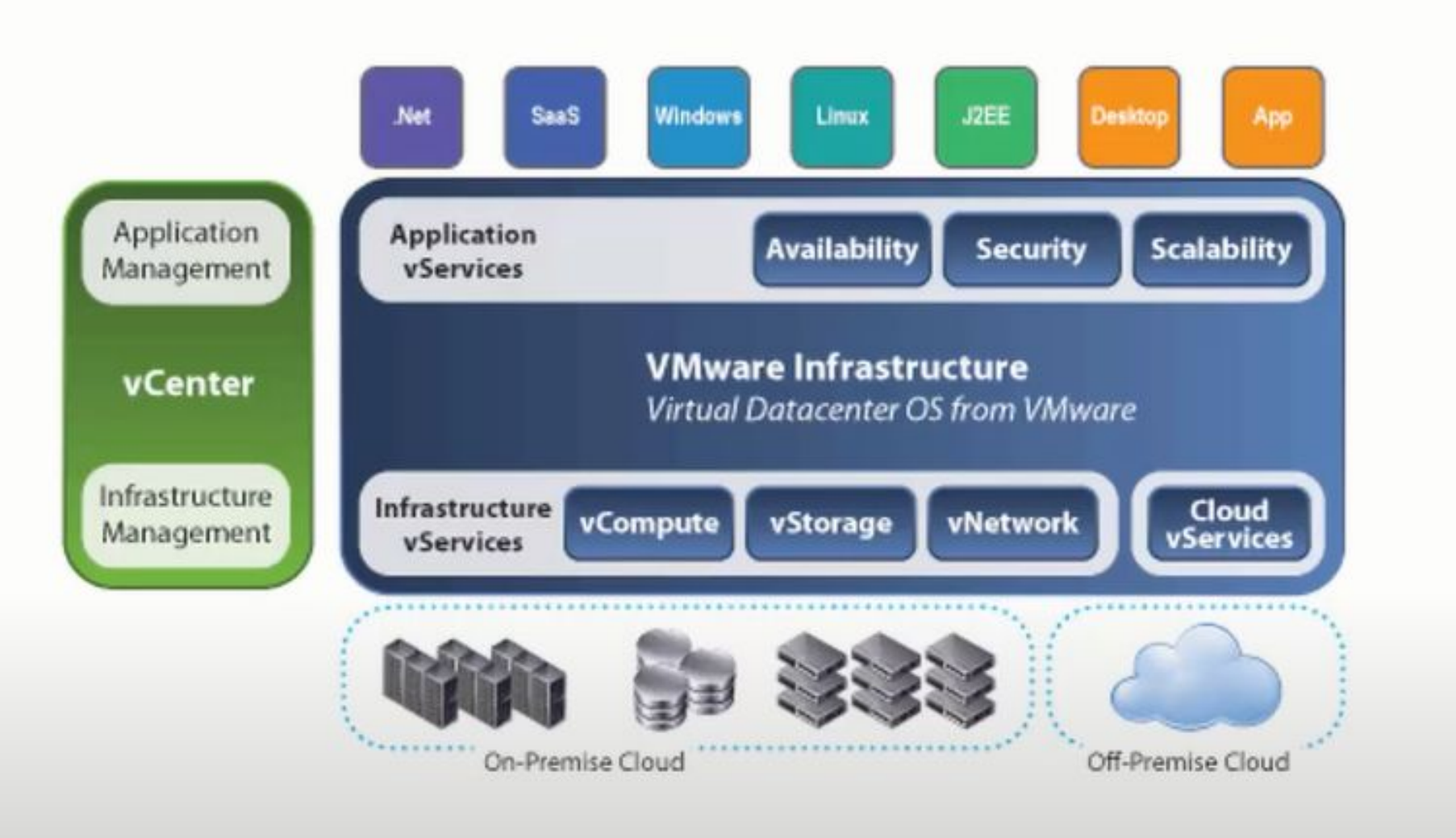
- **VMware NSX Data Center** transports the components of **networking and security** such as **switching, firewalling and routing** that are defined and consumed in software.
- It transports the operational model of a **virtual machine (VM)** for the network.
- VMware NSX is a **full-stack layer 2 to layer 7 network virtualization** & security platform that uses a software-defined approach to extend networking and security across data centers, clouds, & various application frameworks.
- By virtualizing network functions in the infrastructure, **NSX brings networking & security closer to where the applications run**, whether it's virtual machines (VMs), containers, or bare metal servers.

Introduction to VMware NSX

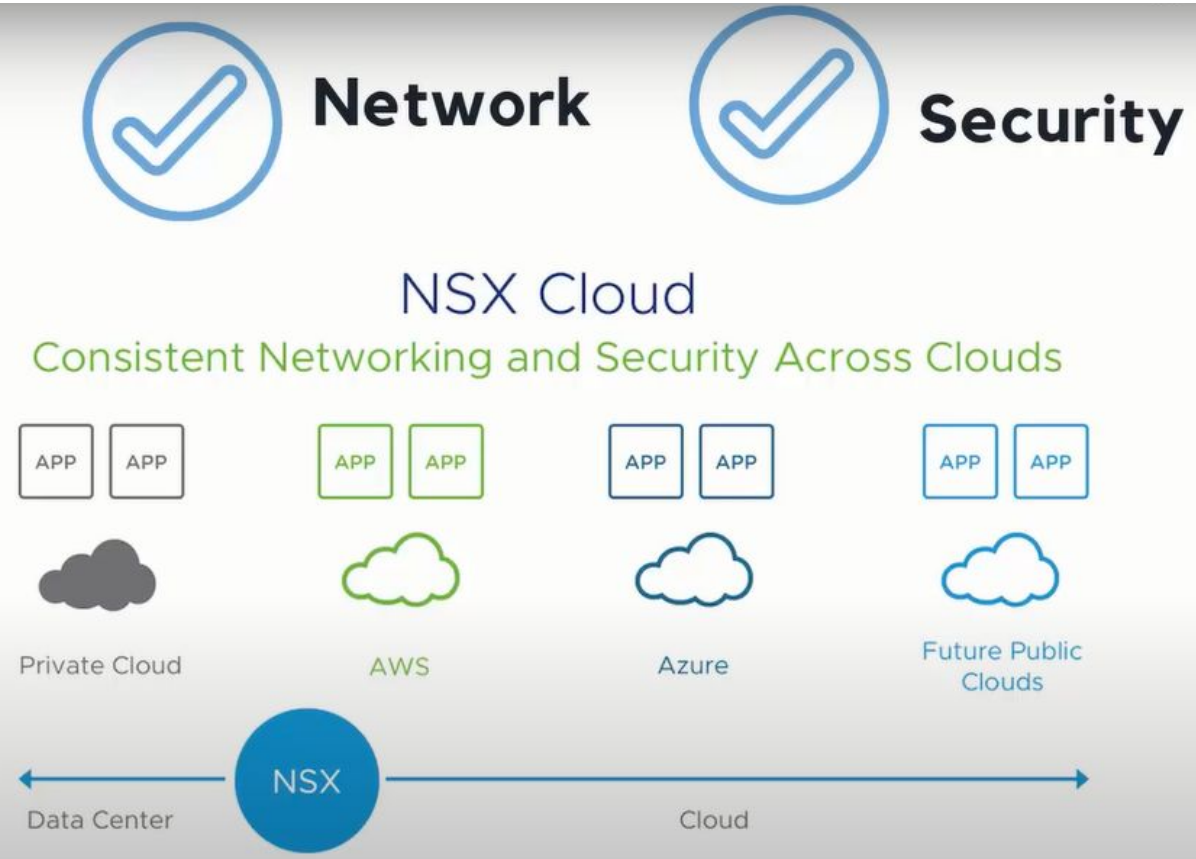
- **Public cloud environments** offer great **agility, flexibility, and operational efficiency**
- Traditional based networking and security solutions are complex to design, deploy and manage. They are also expensive and only partially automated.
- VMware NSX takes a **software centric approach** implementing network functions including **switching, firewalling, routing, IDS/IPS, and load balancing** in a distributed architecture.



VMware Product Evolution

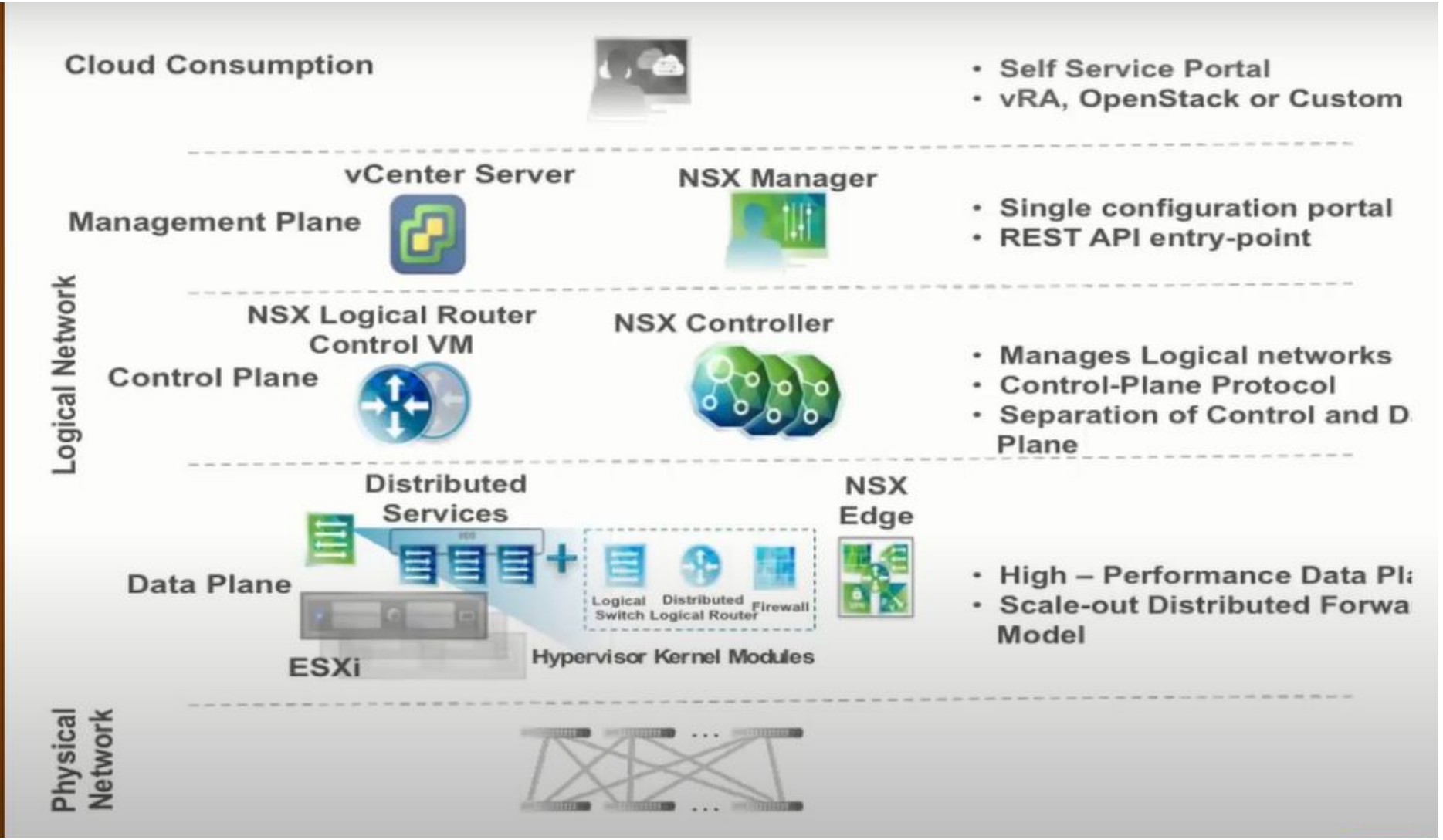


What really Matters in a cloud enviornment

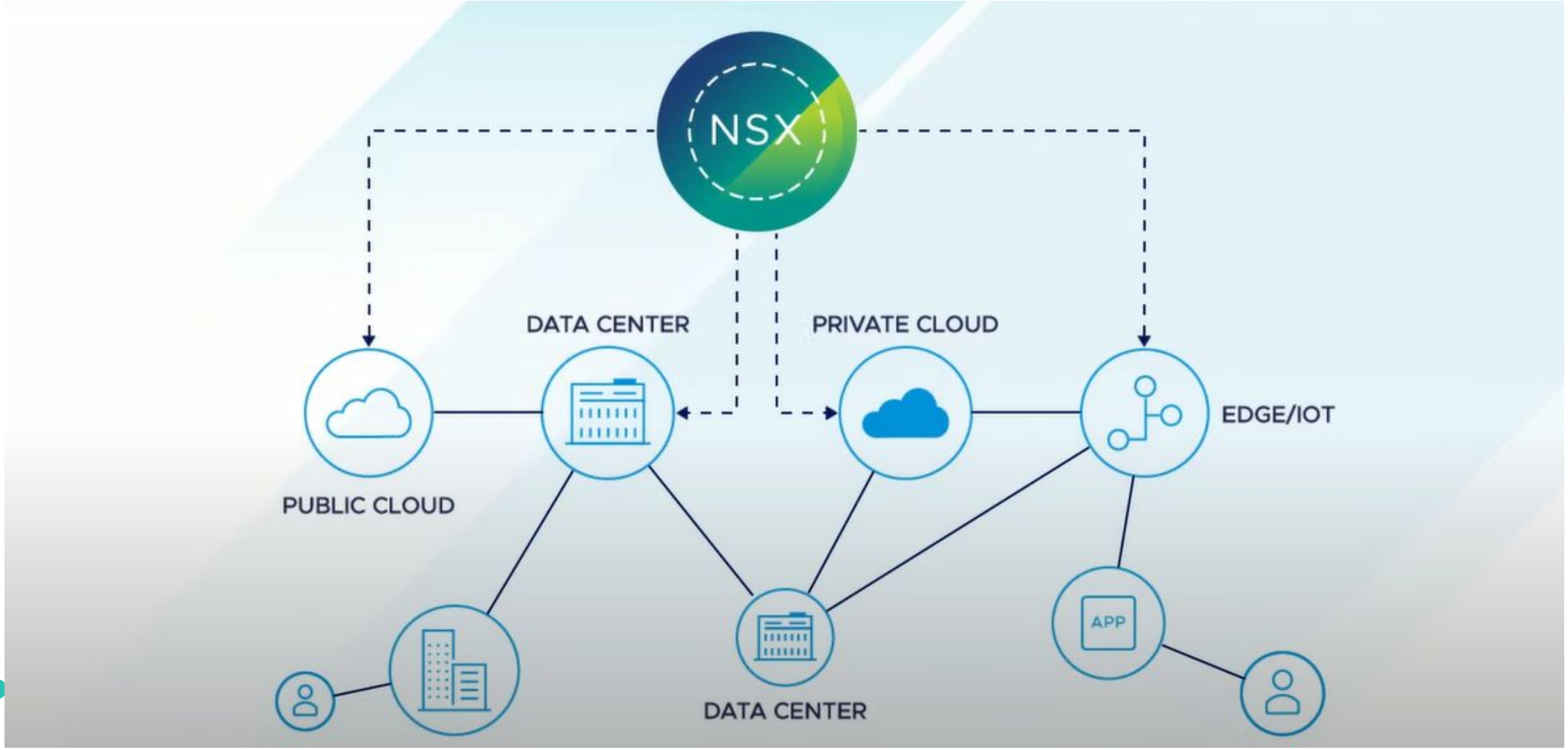


NSX Network Model

NSX Network Model



Virtual Cloud Network



NSX BENEFITS

ADVANCED COMPUTER NETWORKS

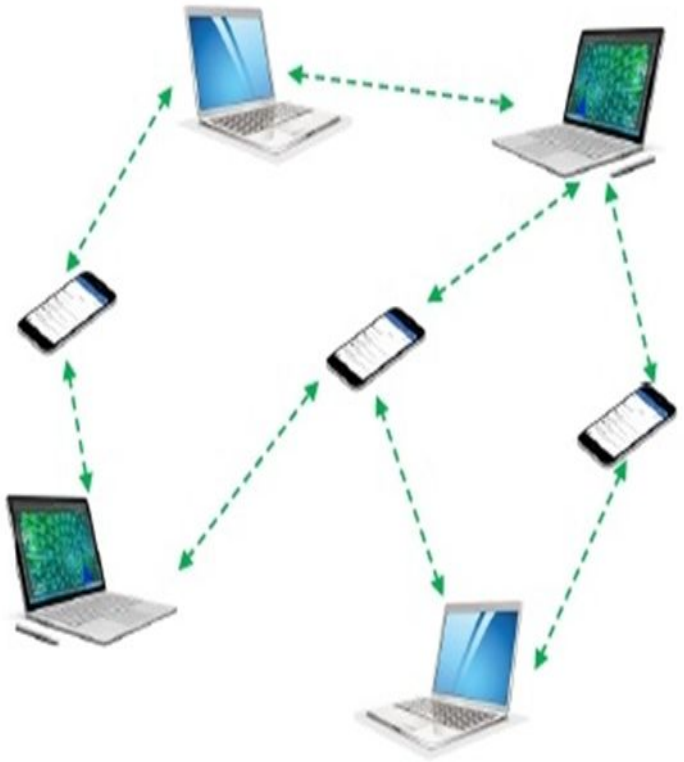
By: Mrs. Nidhi Divecha (ME CMPN)

(UNIT 3)

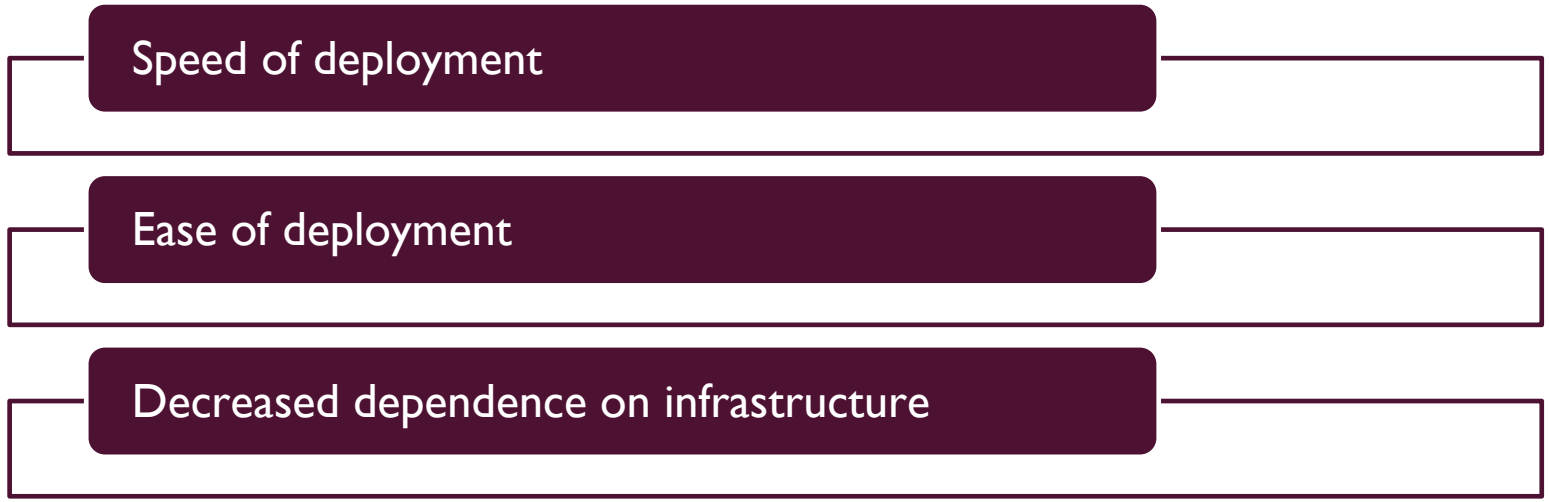
WIRELESS & ADHOC NETWORKING

AD-HOC NETWORKS

- Adhoc networks are mostly **wireless local area networks (LANs).**
- An ad-hoc network is a **temporary network** used for sharing files, presentations , or an Internet connection among multiple computers and devices.
- Computers and devices in ad-hoc networks must be **within 30 feet** of each other.
- If you set up an **adhoc network permanently, it becomes a LAN.**
- The devices communicate with each other directly in an adhoc network
- The two devices communicate through an **ethernet cable or wireless cards.**
- However, this **connection is only temporary.**
- The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination.
- Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.



WHY AD-HOC NETWORK?



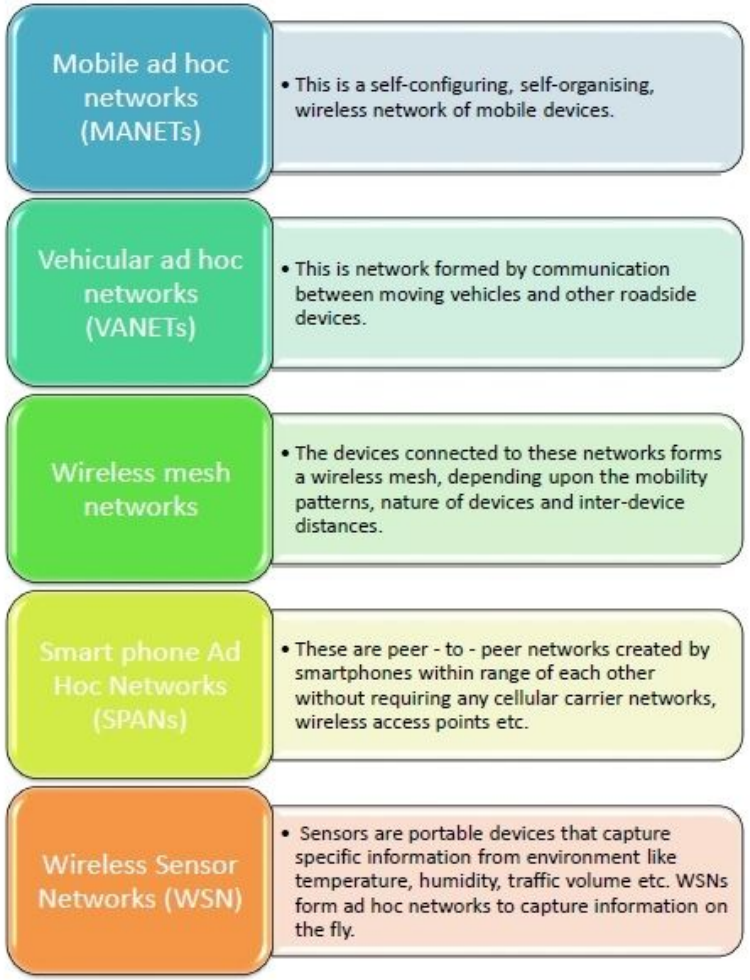
- Generally the networks developed are of the type having some fixed infrastructure.
- If the network is required to be made for some short period of time, then we go for Ad-hoc networks.

ADVANTAGES OF AD-HOC NETWORKS

Ad-hoc networks have several advantages over the traditional networks, like:

- **Infrastructure less networks**
- Ad-hoc networks can have **more flexibility.**
- It is better in **mobility**
- It can be **turn up and turn down** in a very short time
- It can be **more economical**
- **Less setup time**
- **Cost-effective**

CLASSIFICATIONS OF AD-HOC NETWORKS



TWO TYPES OF WIRELESS NETWORKS

- **Infrastructured Network**

A network with fixed and wired gateways. When a mobile unit goes out of range of one base station, it connects with new base station.

Single hop : E.g. – Wi-Fi

Multihop: E.g. – GSM

- **Infrastructure less (Ad-hoc) Network**

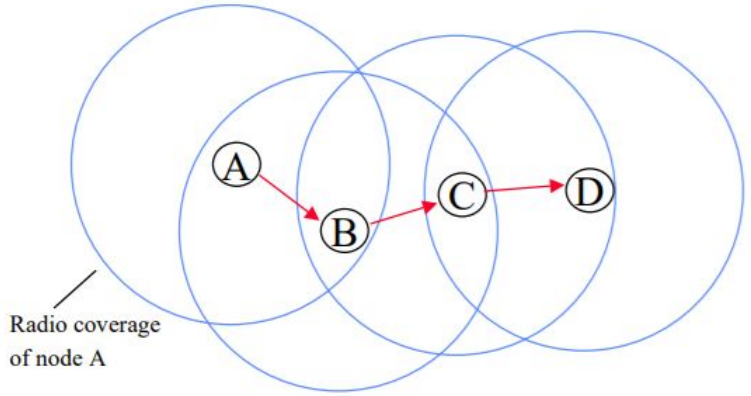
All nodes of these networks behave as routers and take part in discovery and maintenance of routes to other nodes.

Single hop : E.g. – Bluetooth

Multihop: E.g. – Adhoc

MOBILE AD-HOC NETWORK (MANET)

- MANET stands for Mobile ad-hoc Network also called a wireless ad-hoc network or ad-hoc wireless network.
- It is purely a wireless network.
- There is **no fixed infrastructure.**
- **Dynamic topologies**
- **Nodes** in MANET can act as **HOST or ROUTER.**
- MANET nodes are free to move randomly as the network topology changes frequently.
- Each node behaves as a router as they forward traffic to other specified nodes in the network.
- MANET is an **autonomous** collection of mobile users that communicate over wireless links.
- This can be used in road safety, ranging from sensors for the environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.



Traffic from A → D is
relayed by nodes B and C

CHARACTERISTICS & PROPERTIES

Characteristics

- Dynamic Topology (nodes can join or leave the network anytime)
- Energy Constrained nodes
- Limited Security (because there is no fixed infrastructure)
- Autonomous (Each node can play both the roles i.e.. of router and host showing autonomous nature)
- Distributed (no central node)

Properties

- Peer-to-peer connectivity
- Independent computation
- No requirement of access point
- Less wireless connectivity range (multi-hop routing possible)

CHALLENGES OF MANET

- **Topology** (Dynamic since nodes keep on moving)
- **Security** – (Limited - More prone to attacks due to limited physical security)
- **Bandwidth** – Limited
- **Energy** (constrained –Resources are limited due to various constraints like noise, interference conditions, etc.)
- **Routing** – Difficult (because nodes are mobile in nature & changes the links frequently so maintaining the routing table is difficult)

APPLICATIONS OF MANET

Military applications.

- Ad-hoc networking would allow the military to take advantage of technology to maintain an information network between the soldiers, vehicles and military information head quarter.

Rescue Operation

- Ad-hoc can be used in emergency/rescue operations for disaster relief efforts. E.g. in fire, flood or earthquake.

Business work

- Whenever any emergency meeting is planned outside the office exchange of information on a given project is made possible by means of MANET.

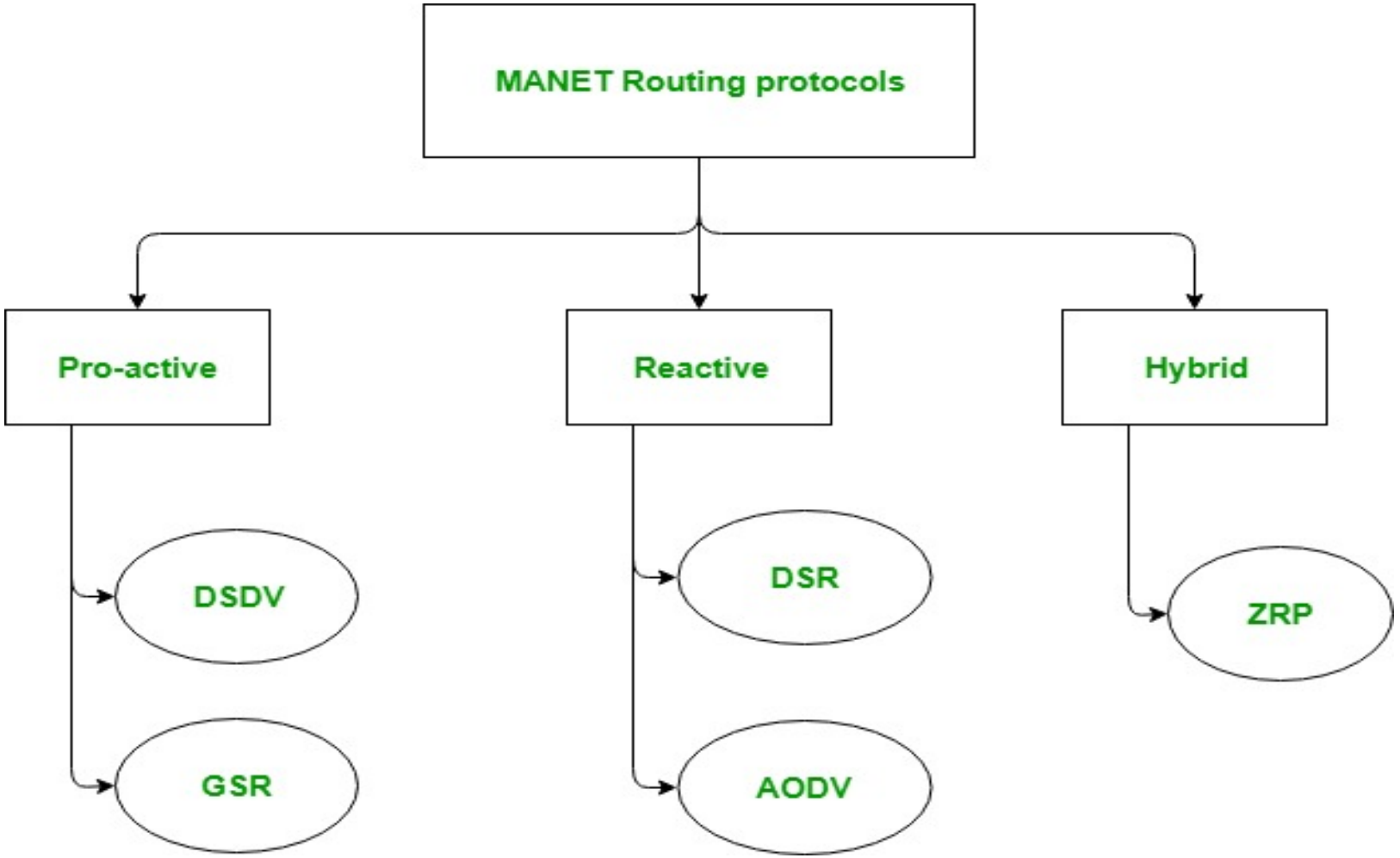
Classroom and conference

- Ad-hoc networks can automatically link an instant and temporary multimedia network using notebook computers to spread and share information among participants. E.g. **conference or classroom**

VANET (Vehicular Adhoc n/w)

- It is used for communication between vehicles and roadside equipment

ROUTING IN ADHOC NETWORKS



ROUTING PROTOCOLS

- Routing in MANET is difficult than normal n/w due to non-fixed infrastructure and rapid change in topology.

Routing Protocol should follow the following:

- Reliability
- Least cost in routing traffic in network.
- Maximum – throughput

MANET ROUTING PROTOCOLS

Proactive Routing	Reactive Routing	Hybrid Routing
- Route is determined in advance. - Also called Table Driven Routing. → Low Route Latency → State info^n → QOS Gurantee → More overhead → Periodic update is	- Route is determined only when needed. - Less overhead - Scalability is good. - Route Latency is high - Route Caching can be reduced.	Proactive + Reactive Near by Node Far away Nodes

Proactive Routing (table – driven)

- Proactive, or table – driven routing protocols.
- Maintains routing information in the Routing table.
- Routing information is flooded in the whole network.
- Any changes in network topology needs to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

Reactive Routing (on-demand)

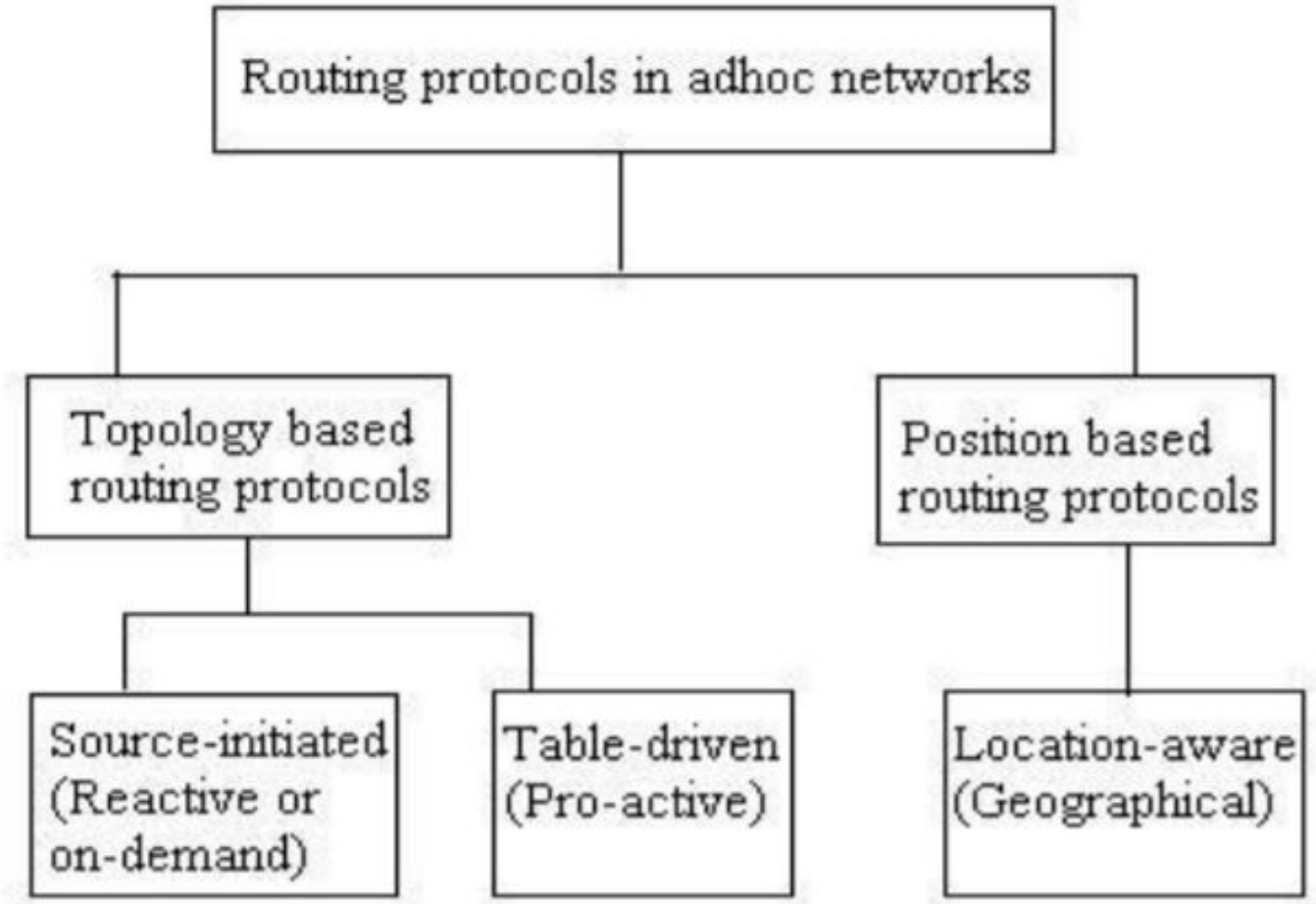
- **Reactive Routing** is also known as **on-demand routing protocol** since they do not maintain routing information or routing activity at the network nodes if there is no communication.
- If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmits and receive the packet.
- The route discovery occurs by flooding the route request packets throughout the network.

Hybrid Routing

- Hybrid Routing **combines reactive and proactive routing protocols.**
- The **zone protocol (ZRP)** is a hybrid routing protocol that divide the **networks into zones.**

Location-aware (Geographical or Position based)

ROUTING PROTOCOLS IN AD-HOC NETWORKS



TOPOLOGY BASED ROUTING PROTOCOL

A. REACTIVE ROUTING PROTOCOL

- The examples of reactive or on-demand routing protocols are: **AODV** (Ad-hoc On-demand Distance Vector routing), **DSR** (Dynamic Source Routing).

Ad hoc On-demand Distance Vector (AODV)

- This protocol will perform **route request (RREQ) and route reply (RREP)** through the route discovery which a node will send packets to the destination.
- Operates on two phases: Route discovery & Route maintenance
- **Source node will not carry the complete path i.e., each node maintains route cache**
- Each node only knows its previous and next hop information.
- It aims to reduce the number of broadcast messages forward throughout the network by discovering routes on-demand instead of keeping of up-to-date information of the route.

1) Route Discovery

RREQ - Source Node ID

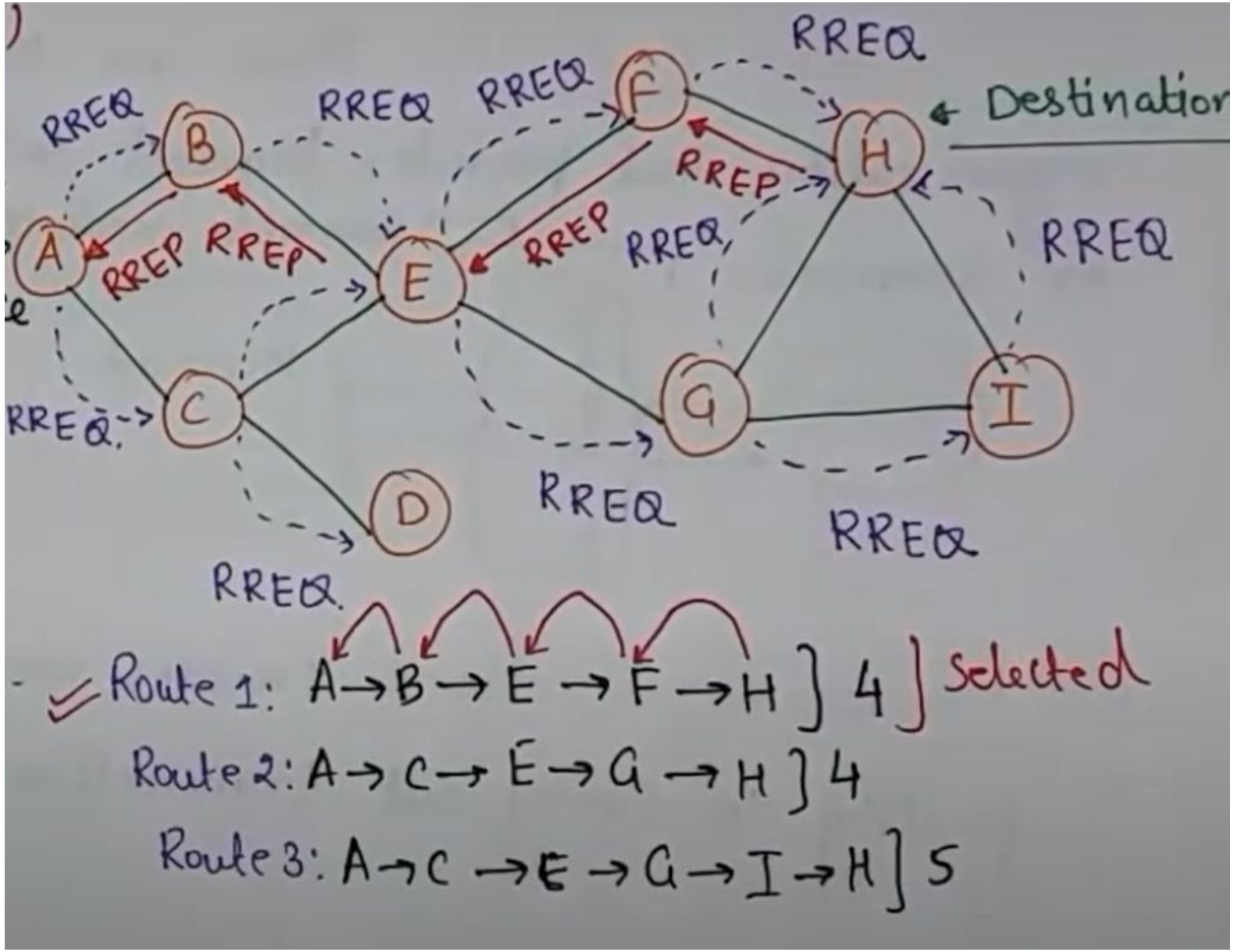
Destination node ID

Recent Sequence no

Broadcast ID

Hop count

Example of AODV



Dynamic Source Routing (DSR)

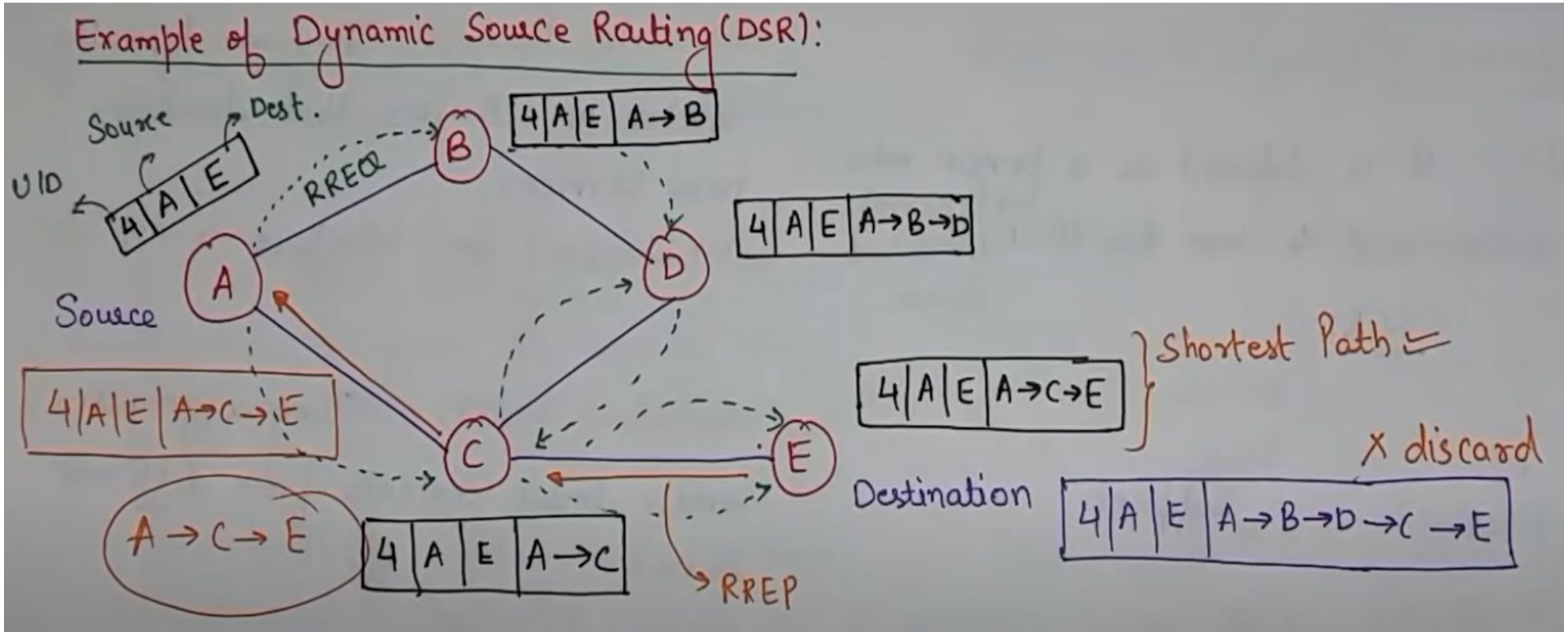
- Discovers the route between source and destination when required.
- Operation is based **on Source Routing i.e. sender knows the complete path.**
- Intermediate nodes do not maintain routing information to route the packets to the destination.
- Less network overhead as the no of message exchanges between nodes is very low.

Phases of DSR Protocol

- **Route Discovery** - Each RREQ packet is defined by the route discovery of the source and destination. The source node will provide a unique id request number to its route request packet. When no route is found, the destination node will discover the route mechanism in order to reach the source node.

- **Route Maintenance** - The route maintenance is used when the source node is unable (Route error) to use its current route the destination due to changes in the topology of network. In that case, the source node will need to select another route to the destination node.

- The **advantages** of this protocol to provide the multiple routes and to avoid the loop formation and **disadvantages** are large end to- end delay, scalability problems caused by flooding and source routing mechanisms.


Example of Dynamic Source Routing (DSR):
Source
Dest.
UID
4 A E
RREQ
B
4 A E A→B
4 A E A→B→D
A
D
Source
4 A E A→C→E
4 A E A→C→E
Shortest Path
C
E
A→C→E
4 A E A→C
RREP
Destination
X discard
4 A E A→B→D→C→E

B. PROACTIVE ROUTING PROTOCOL

- The examples of proactive routing protocols are: **Optimized Link State Routing (OLSR) and DSDV (Destination-Sequenced Distance Vector).**

Optimized Link State Routing (OLSR)

- **OLSR** stands for **Optimized Link State Routing Protocol.**
- This protocol is a **proactive routing protocol** where route is available immediately when needed.
- In this, each node periodically floods status of its links.
- Each node re-broadcasts link state information received from its neighbors.
- Each node keeps track of link state information received from other nodes.
- Each node uses above information to determine next hop to each destination.
- It utilizes a technique to reduce message flooding – **MultiPoint Relaying (MPR).**

Advantages of OLSR :

- OLSR has less average end-to-end delay therefore it is used for applications which needs minimum delay.
- The OLSR implementation is more user friendly and worked with fewer headaches than other protocols.
- It is also a flat routing protocol.
- It does not need a central administrative system to handle its routing process.
- It increases protocol's suitability for an ad hoc network with the rapid changes of the source and destination pairs.
- It does not require the link which is reliable in controlling messages, since the messages are sent periodically, and the delivery does not have to be sequential.

Destination-Sequenced Distance Vector (DSDV) Routing

- In this protocol, each node keeps record of route information in the form of routing table.

The routing table contains entries such as:

- Destination ID
- Next node
- Distance (no of hops)
- Sequence no

Route Broadcast msg:

- Destination node
- Next hop
- Recent sequence no

- Each node exchanges its updated routing table with each other

POSITION BASED ROUTING PROTOCOL

- Since mobile ad-hoc networks change their topology frequently and without prior notice, routing in such networks is a challenging task.
- Position-based routing algorithms eliminate some of the limitations of topology-based routing by using additional information.
- They require information about the physical position of the participating nodes in the network their availability.
- The best and easiest technique is the use of the **Global Positioning System (GPS)** to determine exact coordinates of these nodes in any geographical location.
- This location information is then utilized by the routing protocol to determine the routes.

LOCATION-AIDED ROUTING PROTOCOL (LAR)

- LAR is a mobile ad-hoc routing protocol.
- LAR uses location information using **Global Positioning System (GPS)**, through which every node can know its current physical location.
- LAR essentially describes how location information such as GPS can be used to reduce the routing overhead in an ad hoc network and ensure maximum connectivity.

Two Phases:

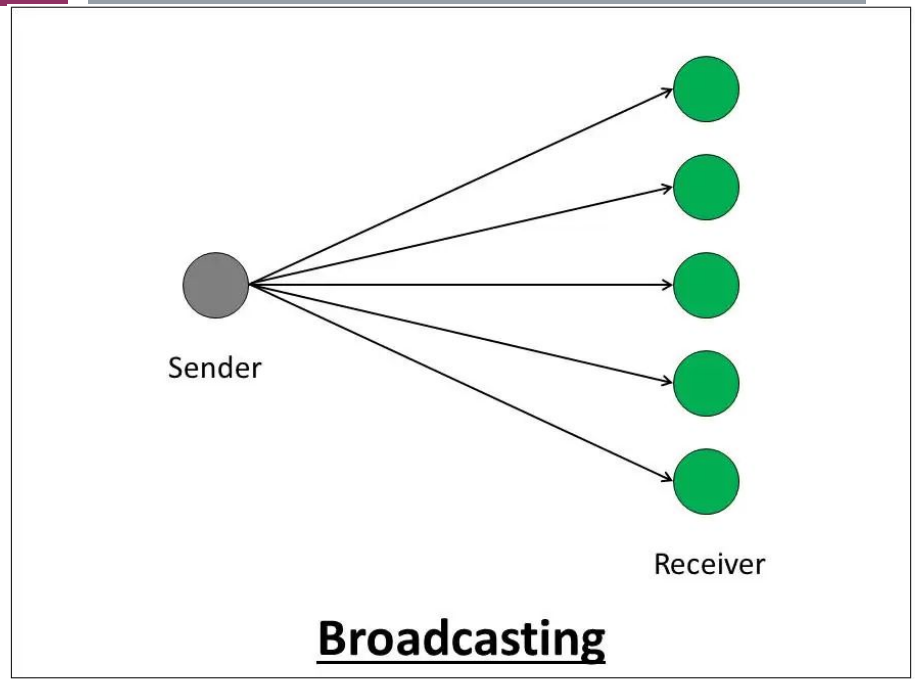
1) Route Discovery

2) Route Error

- LAR divides the network into **two zones**: i.e. **Request zone and Expected zone.**
- Request zone is the area in which the node forwards the route request only when the node is inside the zone.
- When the nodes does not belong to request zone then it simply discards the message.
- Expected zone is the area in which there is the maximum probability of finding the destination nodes.

Broadcasting in Networking

- Broadcasting is the transmission type in which the traffic flows from a single source to all the receivers on the network.
- The advantage of broadcasting is that it is easy to notify with messages to all the nodes in the broadcast domain at the same time.
- Also, broadcasting is easy to implement and efficient.
- The disadvantage of broadcasting is that it cannot be implemented in IPv6 addressing.
- Also, in most cases, it creates unnecessary traffic in the communication channel.

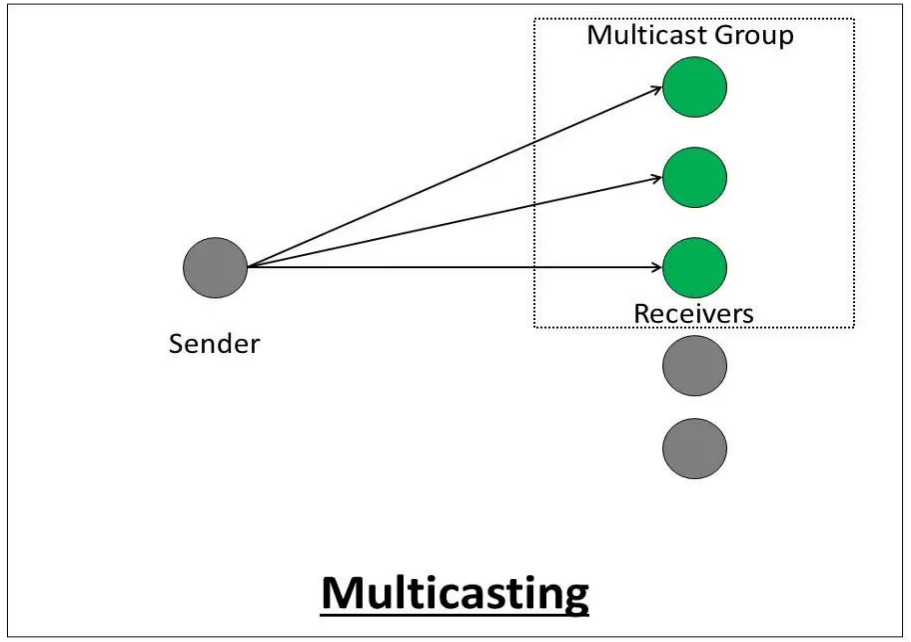


Multicasting in Networking

- Multicasting is a type of transmission where a single source or multiple sources can communicate with multiple receivers or nodes in the network simultaneously.
- Also, Multicasting communication can be one-to-many and many-to-many between sender or senders and receivers.

Multicasting is used in so many areas like

- Internet Protocol (IP)
- Streaming Media
- Video conferencing
- Webcasts



Geocasting

- It is a technique of delivering data packets to a group of nodes located in a specified geographical area.

Parameter	Broadcasting	Multicasting	Geocasting
Transmission	One to all	One to many or many to many	One to many (Location based)
Processing time required	More	less	Moderate
Traffic	Unnecessary traffic	Traffic is less	Moderate traffic
Management	No management required	Management required	Management required
Protocols	Simple flooding	Multicast AODV	LBM scheme 1

Sr no.	Broadcast	Multicast
1.	It has **one sender and multiple receivers.**	It has **one or more senders and multiple receivers.**
2.	It sent data from one device to all the other devices in a network.	It sent data from one device to multiple devices.
3.	It works on **star and bus topology**.	It works on **star, mesh, tree and hybrid** topology.
4.	It **scale well** across large networks.	It **does not scale well** across large networks.
5.	Its **bandwidth is wasted.**	It utilizes **bandwidth efficiently.**
6.	It has **one-to-all** mapping.	It has **one-to-many** mapping.
7.	**Hub** is an example of a broadcast device.	**Switch** is an example of a multicast device.

WIRELESS PERSONAL AREA NETWORKS (PAN)

- WPAN is also known as a **short wireless distance network.**
- A **Wireless Personal Area Network (WPAN)** is a type of personal network that uses **wireless communication technologies** to communicate and transfer data between the user's connected devices.
- This sort of network is generally used for linking peripheral devices (like printers, cellphones, and home appliances), a PDA to a computer or just two nearby computers, without using a hard-wired connection.
- Typically, a wireless personal area network uses some technology that permits communication within about **10 meters** - in other words, a very short range.
- One such technology is **Bluetooth**, which was used as the basis for a new standard, **IEEE 802.15.**
- A WPAN's range depends on the wireless router's capabilities, access point or the device itself, but it is usually restricted to a house or small office.
- WPAN can be created **using Wi-Fi, Bluetooth, infrared**, or any similar wireless technologies as well.

TYPES OF WPAN NETWORKS

- **Bluetooth:** Bluetooth technology is based on Ad-hoc technology, which is a local area network with a very limited coverage.
- **ZigBee (also known as IEEE 802.15.4):** it can be used to connect devices wirelessly at a very low cost and with little energy consumption, which makes it particularly well-suited for being directly integrated into small electronic appliances (like home appliances, stereos, and toys). It operates on the frequency band of 2.4 GHz and on 16 channels, can reach transfer speeds of up to 250 Kbps with a maximum range of about 100 meters.
- **Infrared:** the transmission is done in a direct way, whereby the devices must remain close together and in the same position during data transmission. Nowadays, it is rarely used. IrDA(Infrared Data Association) was formed in 1995.
- **Wireless USB:** short-range, high-bandwidth wireless radio communication protocol created by the Wireless USB Promoter Group. This method uses radio wave technology at 2.4 GHz or 5 GHz frequencies. Wireless USB adapter enables data communication between computers and the wireless local area network (WLAN). The adapter is connected to the USB port of the computer, and in most cases works in plug&play mode, as no additional drivers are required for operation.

THE BLUETOOTH TECHNOLOGY

- Bluetooth wireless technology is a short-range communications technology intended to replace the cables connecting portable unit and maintaining high levels of security.
- Bluetooth technology is based on Ad-hoc technology, which is a local area network with a very limited coverage.
- The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of **Personal Area Networks (PANs).**
- Bluetooth technology was invented by Ericson in 1994.
- Bluetooth employs Radio Frequency (RF) for communication.
- Maximum devices that can be connected at the same time are 7.
- Bluetooth ranges upto 10 meters.
- It provides data rates upto 1 Mbps or 3 Mbps depending upon the version.
- A Bluetooth network is called **piconet** and a collection of interconnected piconets is called **scatternet.**

Symbol of Bluetooth

HOW BLUETOOTH WORKS ?

Piconets

- Piconet is a type of Bluetooth network that contains one primary node called **master node** and **seven active** secondary nodes called **slave nodes.**
- Thus, we can say that there are total of **8 active nodes** which are present at a distance of **10 meters.**
- The communication between the primary and secondary node can be **one-to-one or one-to-many.**
- **Possible communication** is only between the **master and slave**; **Slave-slave communication is not possible.**
- It also have **255 parked nodes,** these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

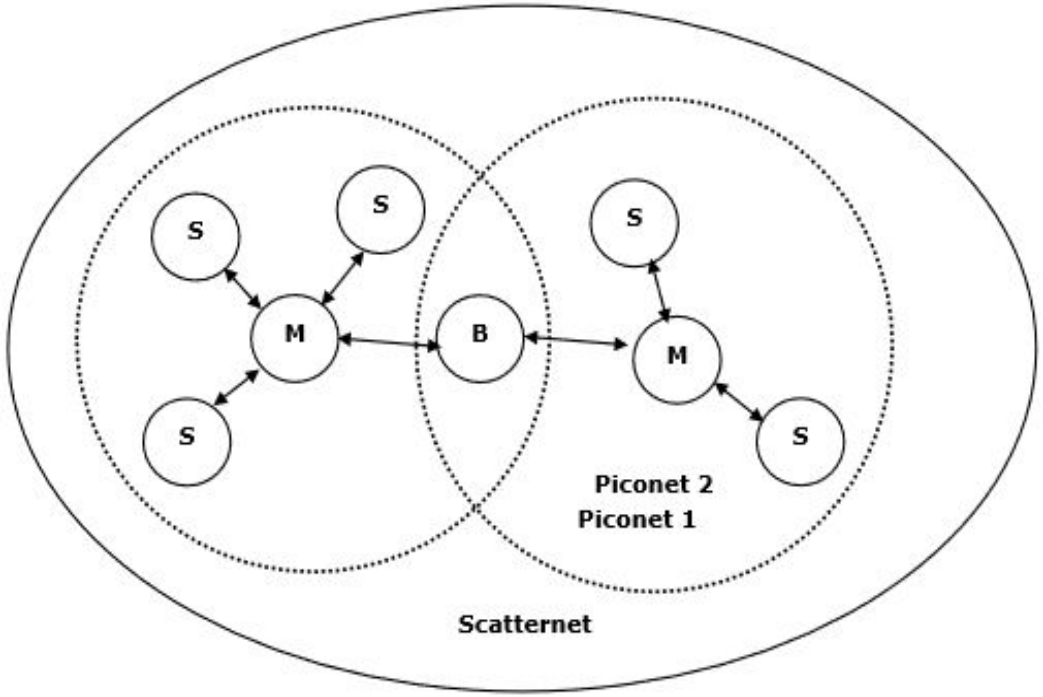


Figure: Piconets and Scatternets

Scatternet:

- It is formed by combination of various piconets.
- A slave in one piconet can be act as master or we can say primary in other piconet.
- This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave.
- This type of node is referred as bridge node.
- A station cannot be master in two piconets.

TYPES OF BLUETOOTH

- This technology eliminates the necessity of wires and cables.

Headsets

- The most known device is the Bluetooth headset. Generally, a headset allows a person to make as well as receive calls through a cell phone without using your hands otherwise wires. These headsets are prepared with voice recognition; thus one can dial & talk without utilizing a mobile handset.

Bluetooth System In-Car

- An in-car Bluetooth system connects the cell phone to the sound system in your vehicle. So, you can make & receive phone calls through the speaker system without using a mobile device.

Printer

- A printer with Bluetooth enabled can get files like pictures and text documents from any device that is equipped with a blue tooth like a PDA or laptop & print the data without using wires. This device must be connected to the printer for the purpose of printing to work properly.

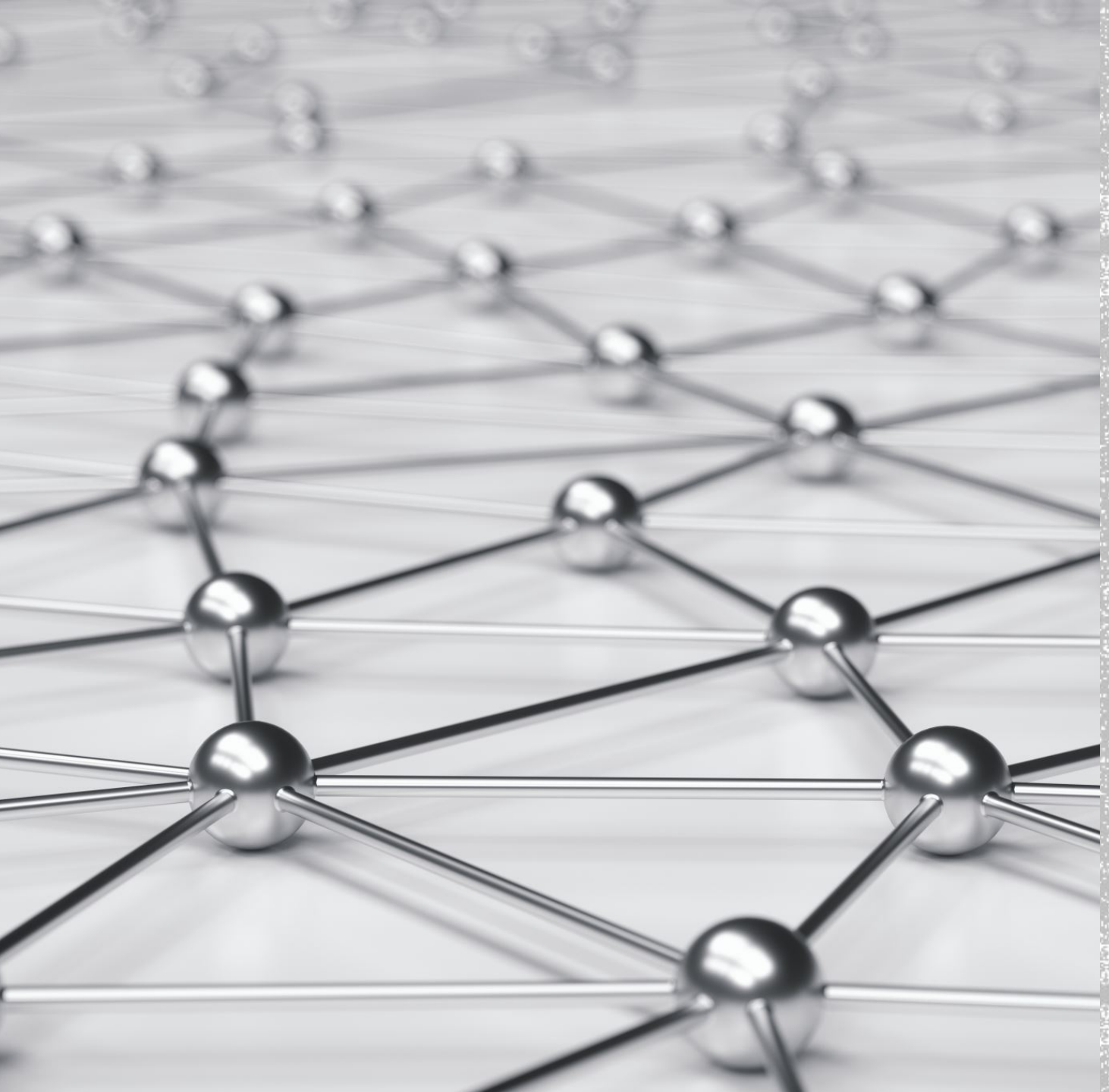
Webcam

- A webcam enabled by Bluetooth mainly works as a usual webcam without the requirement of wires. The wireless capabilities add mobility to the device, unlike traditional webcams, which remain docked onto or near the computer.

ADVANCED COMPUTER NETWORKS

By: Mrs. Nidhi Divecha (ME CMPN)

(UNIT 4)



ENTERPRISE NETWORKING

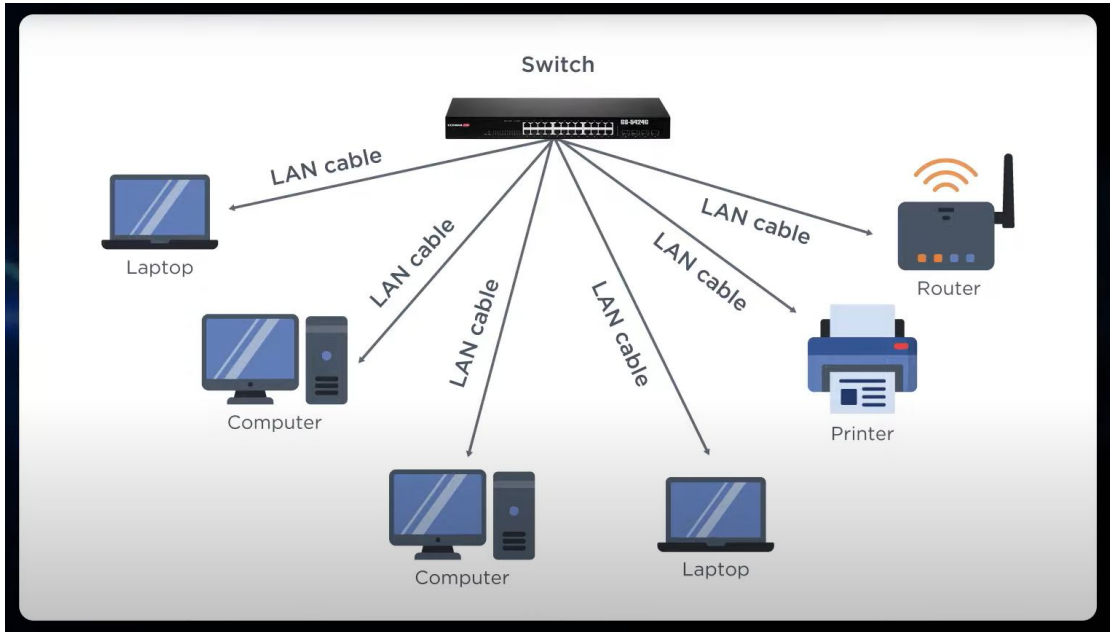
WHAT IS ENTERPRISE NETWORKING?

- An enterprise network is also known as a **corporate network.**
- It facilitates file and resource sharing between different departments and teams in an organization.
- The term **‘enterprise network’** refers to the physical, virtual, or logical connectivity infrastructure that enables systems and apps to:
- Communicate
- Share information
- Run services and programs
- Analyze system performance
- An enterprise network may include local and wide area networks (LAN/WAN), depending on operational and departmental requirements.
- To establish an enterprise network at geographically disparate locations, use Virtual Private Networks (VPNs) to connect these regions.

TYPES OF ENTERPRISE NETWORKS

Some of the common types of enterprise networks include:

- **Local Area Networks**
- **Wide Area Networks**
- **Cloud networks**

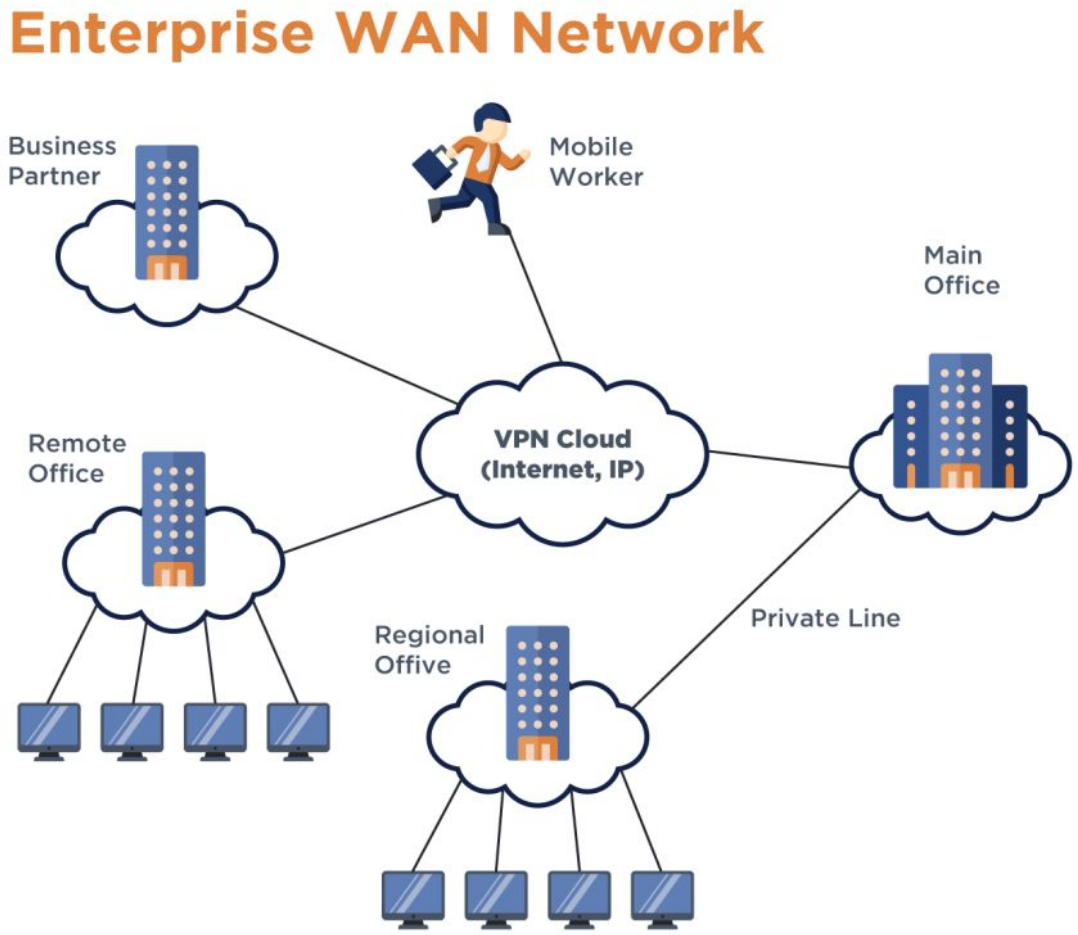


Local Area Network (LAN)

- A LAN is a computer network that interconnects systems within a small building or room. Typically used for personal, non-commercial use cases
- For example, each department within the enterprise network can operate a small LAN where multiple computers are connected to the same switch but decoupled from other departmental LANs.

Wide Area Network (WAN)

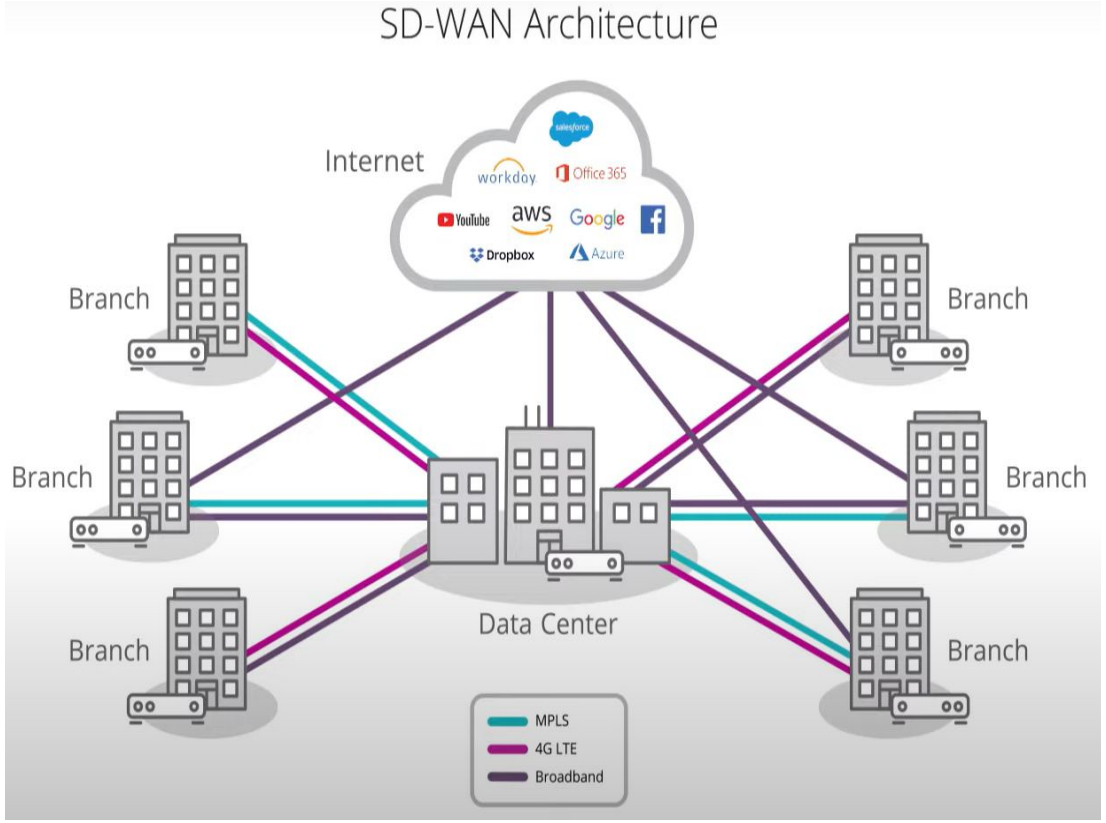
- A WAN (wide area network) connection provides a much larger coverage than local area networks.
- Wide area networks are not restricted to any particular location or geographic area; they can stretch across countries, continents, and the entire world.
- WAN connections are the most sophisticated and expensive computer networks; they are usually owned by service providers who lease their network to the public.
- Other examples of wide-area networks are virtual private networks (VPN) and mobile broadband connections, including 3G network, 4G network, and the most recent 5G network.



Cloud Networks

SD-WAN

- SD-WAN, a software-defined wide area network, is a virtual or cloud-based WAN configured and managed using software programs.
- A software-defined wide area network is a virtual WAN architecture that is software-driven and basically achieved by applying software-defined networking (SDN) technologies to traditional WAN connections.
- SD-WAN offers more flexibility than traditional WAN, with improved bandwidth efficiency, business productivity, and lower IT costs.
- It delivers better network connectivity at significantly lower costs without compromising security and data privacy.



WHY ENTERPRISE NETWORKING?

Driving Efficiency and productivity

- Contributes employees efficiency & ensures better customer relationships.

Enhancing Security

- Detects cyberattacks and security threats & data tampering.

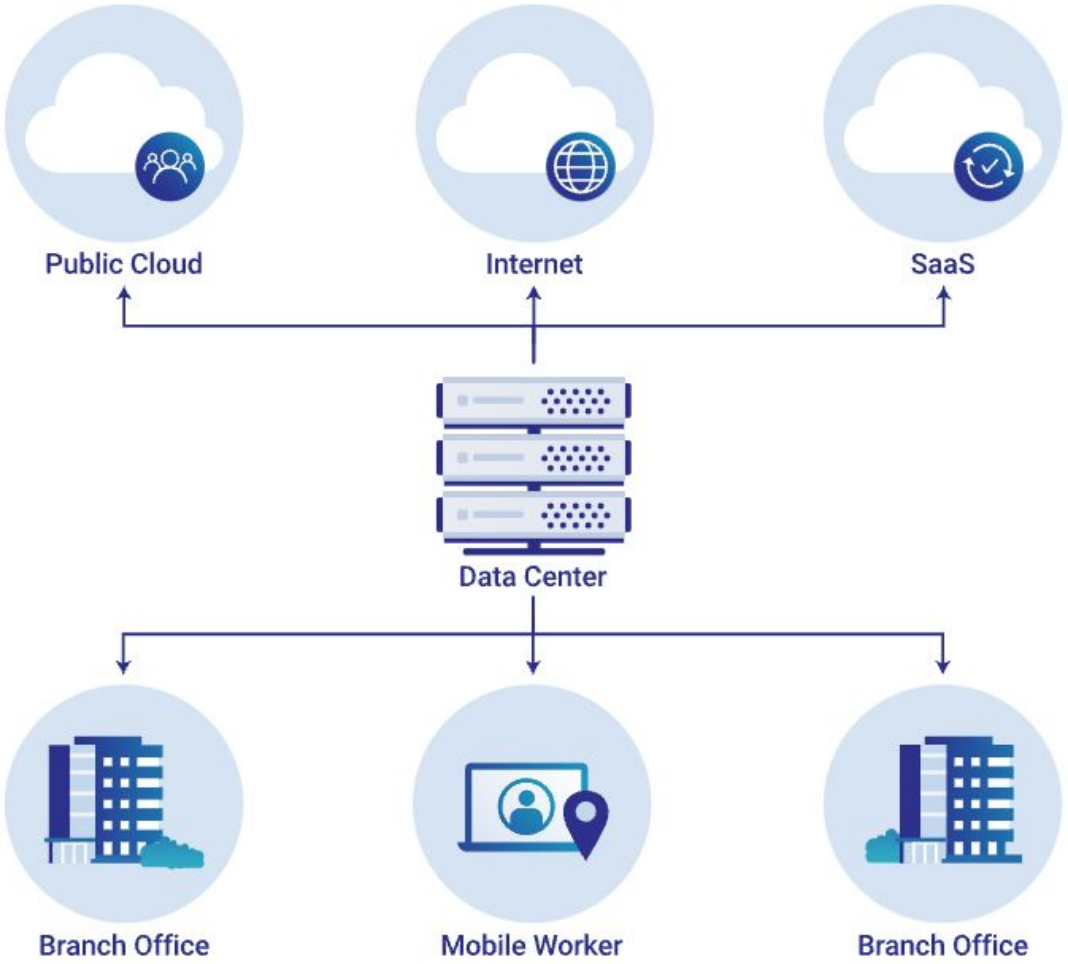
Reducing IT Downtime

- Faster speed & high level of network availability

Minimizes cost

- Reduces costs for software, hardware, operations, services and maintenance.

HOW DOES ENTERPRISE NETWORKING WORK?



- For many years, the main focus for enterprise networks was connecting everyone and everything to the on-premise, self-hosted centralized data centers where data was saved and applications ran.
- This access was provided by connecting users and devices to the LAN in the corporate office.
- Each office's LAN was connected to the other offices via a large enterprise WAN.
- Enterprise networking infrastructure was comprised of physical appliances, connected to each other and to personal computers, printers, and IoT devices through a combination of Ethernet cables and Wi-Fi signals.

The networking appliances used included:

- **Routers** send data from one network to another, enabling network-to-network connections and Internet access.
- **Switches** forward data within a network to individual devices.
- **Gateways** provide connections between different networks using multiple protocols and at multiple layers of the OSI model.
- **Firewalls** process all traffic coming into and out of a network to block potential attacks.
- **Load balancers** distribute network traffic among multiple servers in a data center to ensure no server becomes overloaded (load balancers can do the same for web applications).
- **VPN servers** establish and terminate VPN connections to provide secure access to the internal network.

ENTERPRISE CAMPUS ARCHITECTURE

- Enterprise campus: Hierarchical design models

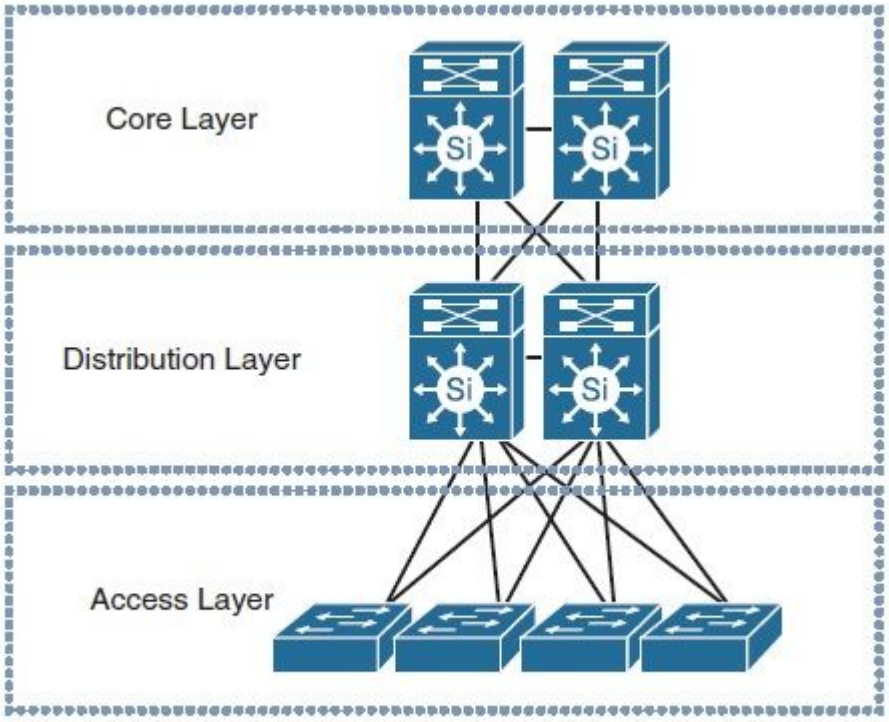


Figure 3-1 *Three-Tier Network Design Model*

- The hierarchical network design model breaks the complex flat network into multiple smaller and more manageable networks.

A typical hierarchical enterprise campus network design includes the following three layers:

- **Core layer:** Provides optimal transport between sites and high-performance routing. Due the criticality of the core layer, the design principles of the core should provide an appropriate level of resilience that offers the ability to recover quickly and smoothly after any network failure event with the core block.

- **Distribution layer:** Provides policy-based connectivity and boundary control between the access and core layers.

- **Access layer:** Provides workgroup/user access to the network.

The two primary and common hierarchical design architectures of enterprise campus networks are the **three-tier and two-tier layers models.**

THREE-TIER MODEL

- This design model is typically used in large enterprise campus networks, which are constructed of multiple functional distribution layer blocks.

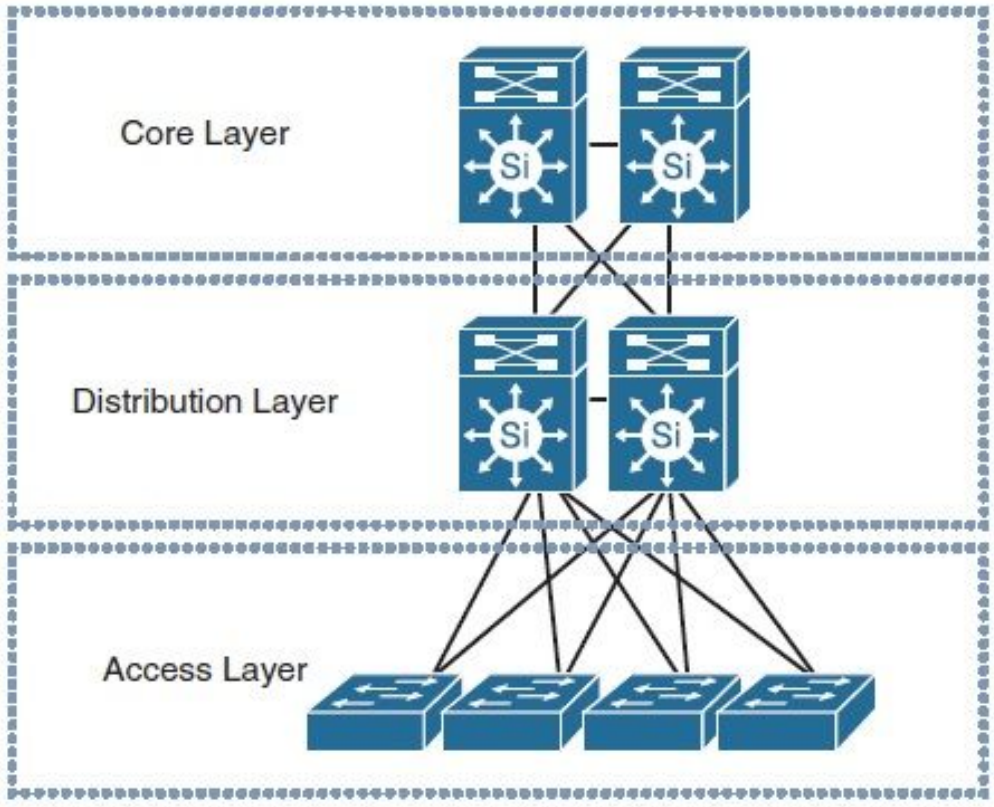


Figure 3-1 *Three-Tier Network Design Model*

TWO-TIER MODEL

- This design model is more suitable for small to medium-size campus networks, where the core and distribution functions can be combined into one layer, also known as collapsed core-distribution architecture .

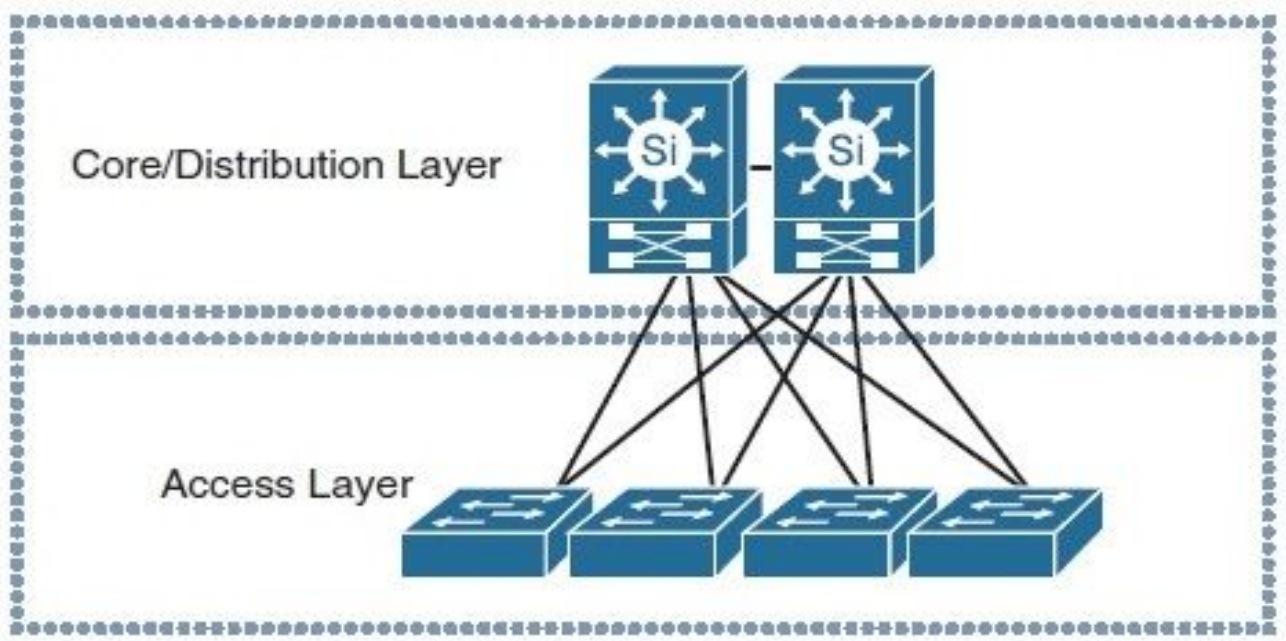


Figure 3-2 *Two-Tier Network Design Model*

DESIGN PRINCIPLES

- **Hierarchy:** Any large complex system must be built using a set of modularized components that can be assembled in a hierarchical and structured manner.
- **Modular:** Campus network designs that are modular easily support growth and change. By using building blocks, also referred to as pods or modules, scaling the network is eased by adding new modules instead of complete redesigns.
- **Resilient:** Campus network designs deploying best practices and proper high-availability (HA) characteristics have uptime of near 100 percent. Campus networks deployed by financial services might lose millions of dollars in revenue from a simple 1-second network outage.
- **Flexibility:** Change in business is a guarantee for any enterprise. As such, these business changes drive campus network requirements to adapt quickly. Following campus network designs yields faster and easier changes.

ENTERPRISE CAMPUS: MODULARITY

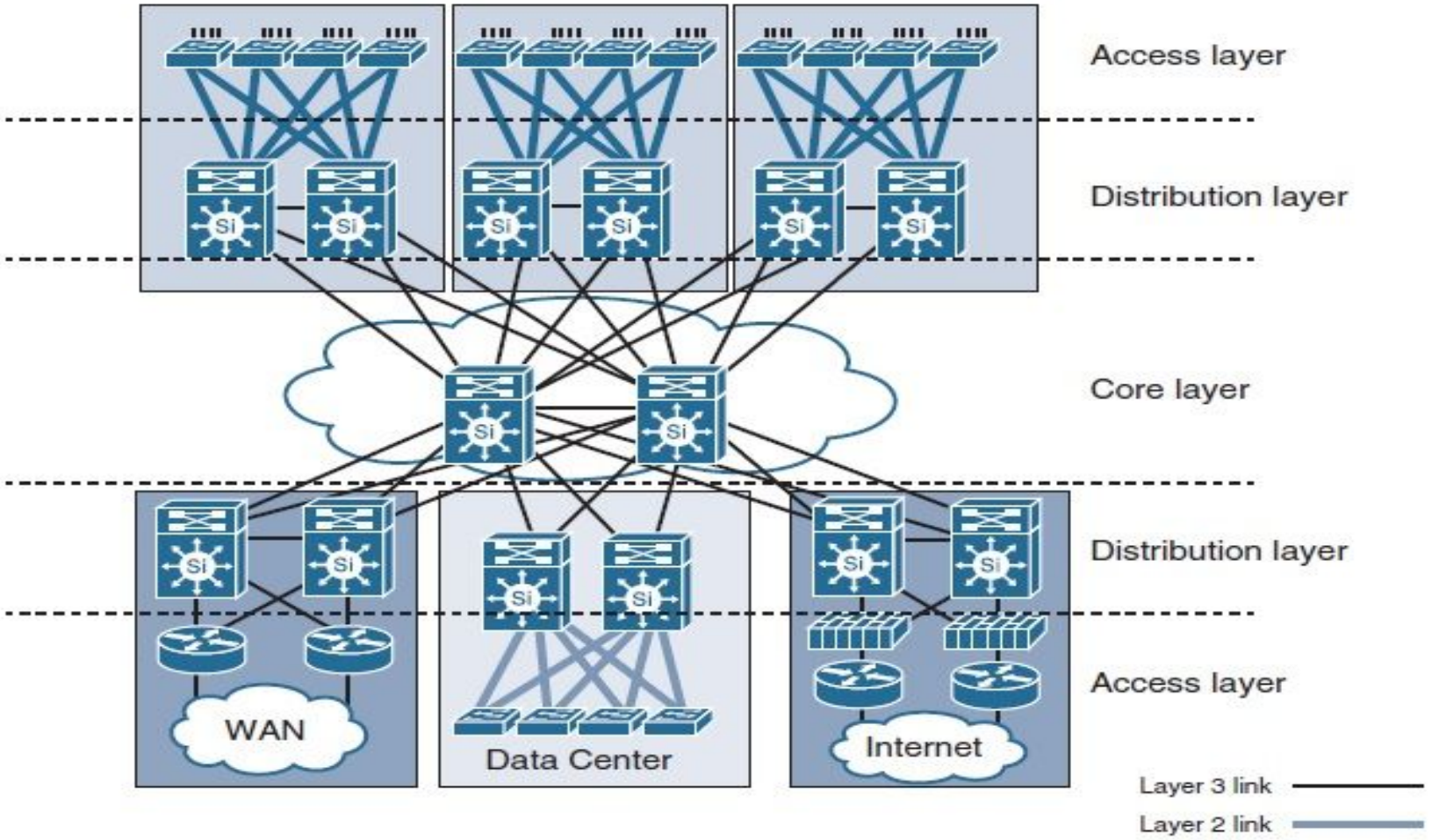


Figure 3-3 *Typical Modular Enterprise Campus Architecture*

- The second of the four principles of structured design is modularity.
- The modules of the system are the building blocks that are assembled into the larger campus.
- The advantage of the modular approach is largely due to the isolation that it can provide.
- Failures that occur within a module can be isolated from the remainder of the network, providing for both simpler problem detection and higher overall system availability.
- Network changes, upgrades, or the introduction of new services can be made in a controlled and staged fashion, allowing greater flexibility in the maintenance and operation of the campus network.
- When a specific module no longer has sufficient capacity or is missing a new function or service, it can be updated or replaced by another module that has the same structural role in the overall hierarchical design.

ENTERPRISE CAMPUS SERVICES

Non-Stop High Availability

- In many cases, the principle service requirement from the campus network is the availability of the network.
- The ability for devices to connect and for applications to function is dependent on the availability of the campus.
- Availability is not a new requirement and historically has been the primary service requirement for most campus designs.
- The calculation of availability is based on a function of the mean time between failures (MTBF) of the components in the network and the mean time to repair (MTTR)—or how long it takes to recover from a failure.

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

MTBF = Mean Time Between Failure
MTTR = Mean Time To Repair

VIRTUALIZATION SERVICES

- Virtualization—the ability to allocate physical resources in a logical fashion (one physical device shared between multiple groups or multiple devices operated as a single logical device)—provides the ability to design in a high degree of flexibility into the campus architecture.
- Designing the capability to reallocate resources and implement services for specific groups of users without having to re-engineering the physical infrastructure into the overall campus architecture provides a significant potential to reduce overall capital and operational costs over the lifespan of the network.
- The introduction of Virtual LANs (VLANs) provided the first virtualization capabilities in the campus.

Network Virtualization

- Network Virtualization is best described as the ability to leverage a single physical infrastructure and provide multiple virtual networks each with a distinct set of access policies and yet support all of the security, QoS, Unified Communication services available in a dedicated physical network.

SECURITY SERVICES

All of these various security attacks fall within six fundamental classes of security threats that the campus design must consider:

- Reconnaissance attacks
- Denial of service/distributed denial of service attacks
- Eavesdropping attacks
- Collateral damage
- Unauthorized access attacks
- Unauthorized use of assets, resources, or information

Infrastructure Security

- There are two general security considerations when designing a campus network infrastructure.
- First, the infrastructure must be protected from intentional or accidental attack—ensuring the availability of the network and network services.
- Secondly, the infrastructure must provide information about the state of the network in order to aid in detection of an ongoing attack.
- Infrastructure Protection
- Protecting the Network Devices
- Protect the Links

Endpoint Security

- The campus security architecture should be extended to include the client itself.
- Endpoints, such as laptops, are the most vulnerable and most desirable targets for attack.
- The installation of client applications, such as **Cisco Security Agent (CSA),** is an important step towards completing the end-to-end security architecture

Operational and Management Services

Fault Management

- One of the primary objectives of the overall campus design is to minimize the impact of any fault on the network applications and services. The redundancy and resiliency built into the design are intended to prevent failures (faults) from impacting the availability of the campus.
- Fault management process can be broken down into three stages or aspects, proactive, reactive and postmortem analysis.

Proactive Fault Management

- Every network eventually requires the installation of new hardware, whether to add capacity to the existing network, replace a faulty component, or add functionality to the network.
- The ability to proactively test this new hardware and ensure that it is functioning correctly prior to installation can help avoid any further service interruptions once equipment is installed in the network.
- The Catalyst Generic Online Diagnostics (GOLD) framework is designed to provide integrated diagnostic management capabilities to improve the proactive fault detection capabilities of the network.

Reactive Fault Management

- One of the central objectives for any campus design is to ensure that the network recovers intelligently from any failure event.
- Capabilities, such as **Enhanced Object Tracking (EOT)**, also provide an additional level of configurable intelligence to the network recovery mechanisms.
- The capability for each switch in the network to be programmable in the way it reacts to failures—and have that programming customized and changed over time—can improve the reactive capabilities of the network to fault conditions.

Postmortem Analysis Capabilities

- Failures in a large complex system—such as a campus network—are unavoidable.
- Having the capabilities designed into the network to support a postmortem problem analysis process is highly valuable to any enterprise aiming for a high number of nines of availability.