Unit 1

Introduction to Networking

Layered Architecture

In layered network architecture there are a set of layers and protocols. The layers are organized as a stack, with each one built upon the one below it. A layered architecture with four layers is shown in following figure.

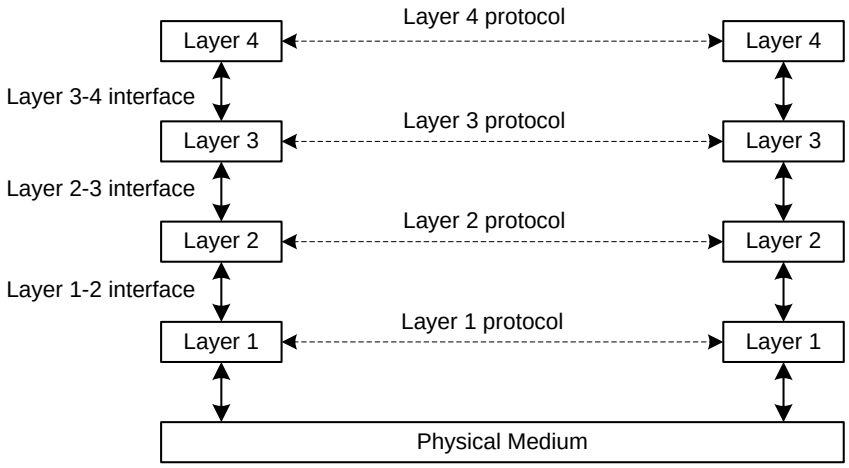


Figure: layer, protocol and interfaces

Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible.

Interfaces, Services and Protocols

Each interface defines the information, operation and services a layer must provide for the layer above it. Well-defined interface and layer functions provide greater modularity to a network.

Within a host, each layer calls upon the services of the layer just below it. For example, Layer 3 uses the service provided by layer 2 and provides its own services for layer 4.

Between machines, layer x on one communicates with the corresponding layer x on another machine. This communication is governed by agreed rules of services called protocols. Below layer 1 is the physical medium through which actual communication occurs.

Importance of layered architecture

- Layering reduces the design complexity.

- Provision of localized services strengthens modularity.
- They allow complete interoperability between incompatible systems
- Hardware and software vendor independence.

OSI MODEL

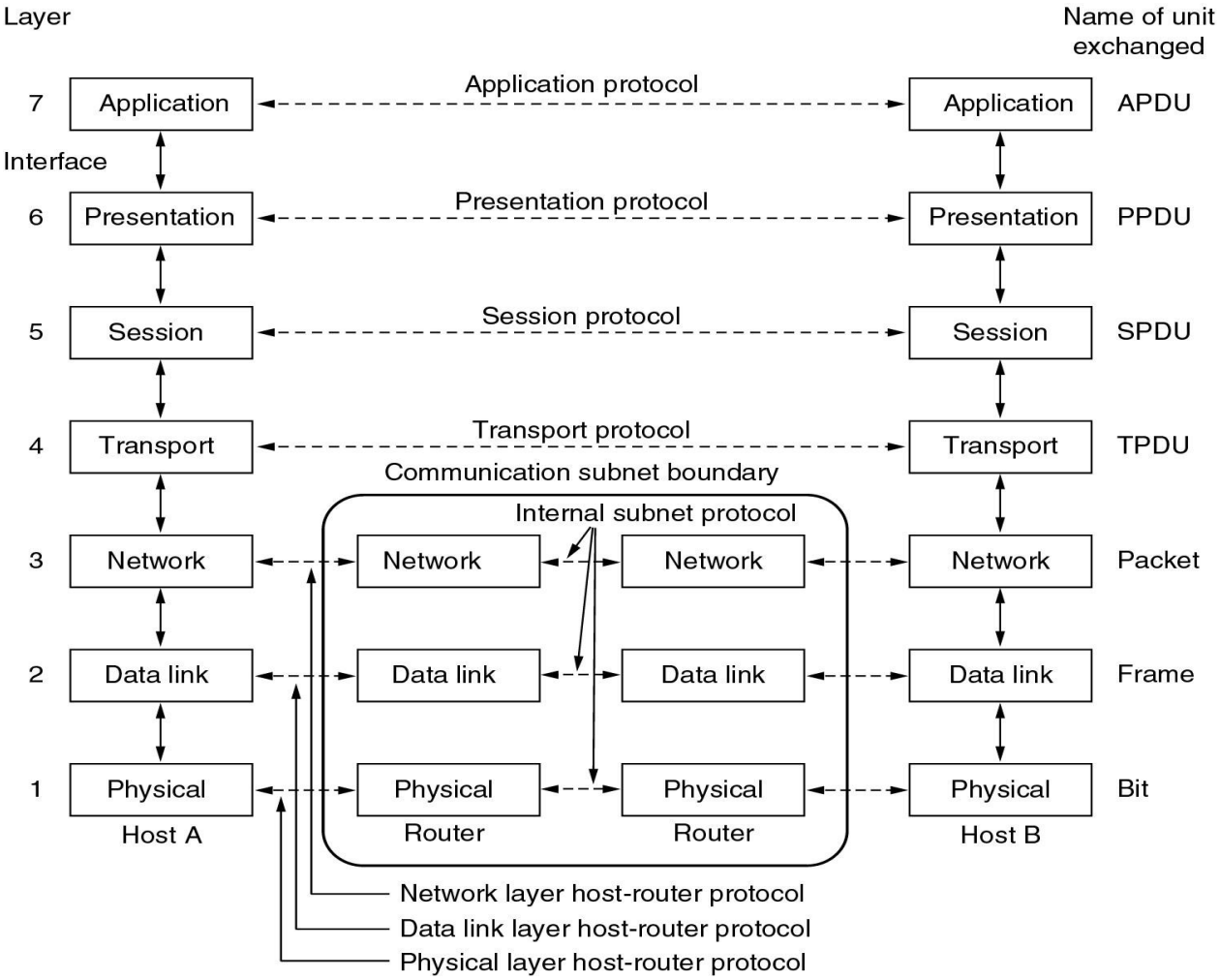


Figure: OSI model

The OSI model has seven layers. Open System Interconnection (OSI) is a reference model for all the digital communication system. OSI was developed by ISO (International Standard Organization)

The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. The design issues largely deal with mechanical, electrical, and timing interfaces, as well as the physical transmission medium.

The Data Link Layer

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors. It breaks up the input data into data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially. Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data (i.e., flow control).

The Network Layer

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are ‘‘wired into’’ the network and rarely changed, or more often they can be updated automatically to avoid failed components. If too many packets are present in the subnet at the same time, they will get in one another’s way, forming bottlenecks. Handling congestion is also a responsibility of the network layer, in conjunction with higher layers.

The Transport Layer

The basic function of the transport layer is to accept data from above it, split it up into smaller units, if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network.

The Session Layer

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation simultaneously), and synchronization (check pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

The Presentation Layer

Unlike the lower layers, which are mostly concerned with moving bits around, the presentation layer is concerned with the syntax and semantics of the information transmitted.

The Application Layer

The application layer contains a variety of protocols that are commonly needed by users. One widely used application protocol is HTTP (Hyper Text Transfer Protocol), which is the basis for the World Wide Web.

Internet Protocol (IP)

Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the internet. Each computer on the internet has at least one IP address that uniquely identifies it from all other computers on the internet. IP is the defining set of protocols that enable the modern internet.

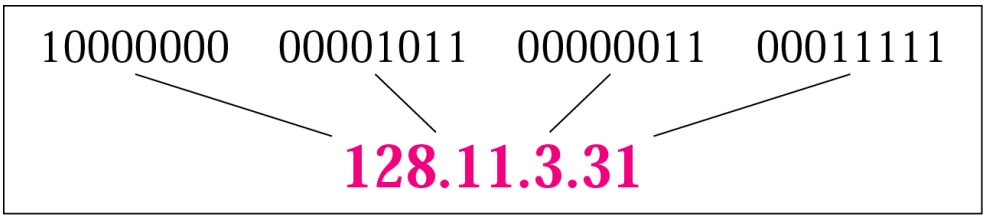
While IP defines the protocol by which data moves around the internet, the unit that does the actual moving is the IP packet. An IP packet is like a physical parcel or a letter with an envelope indicating address information and the data contained within.

An IP packet's envelope is called the header. The packet header provides the information needed to route the packet to its destination.

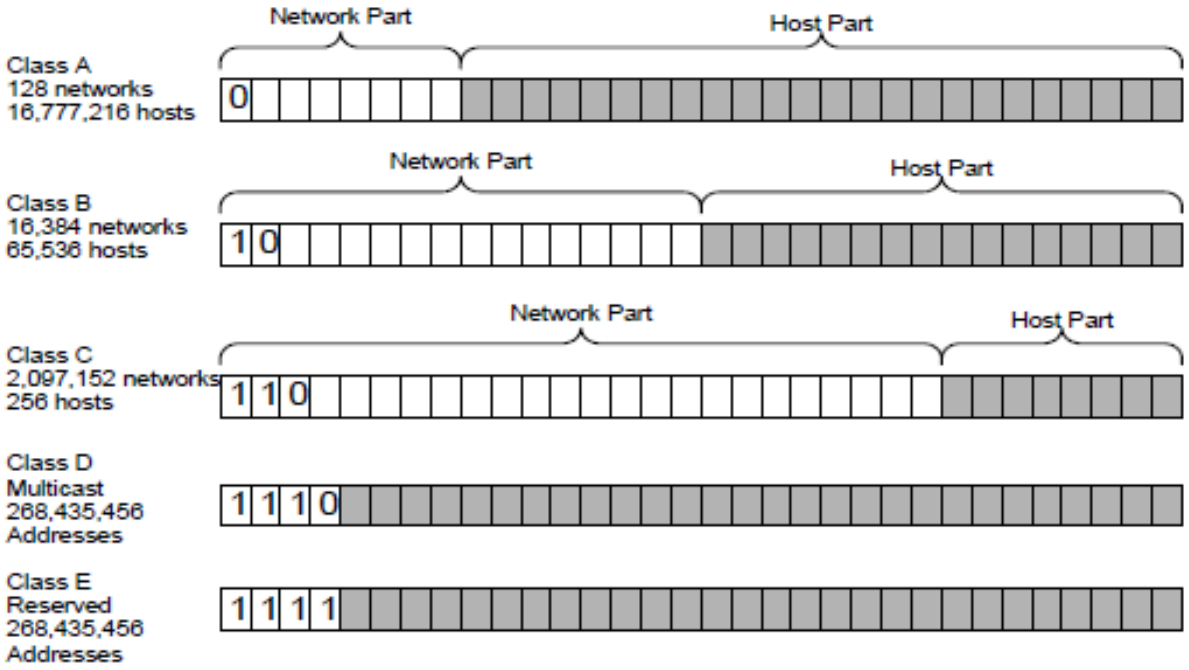
IPV4 Address Overview

- It is 32 bit unique address
- Total unique address equals to 2^32 that gives around 4.2 billion addresses
- It is represented in Dotted Decimal Format

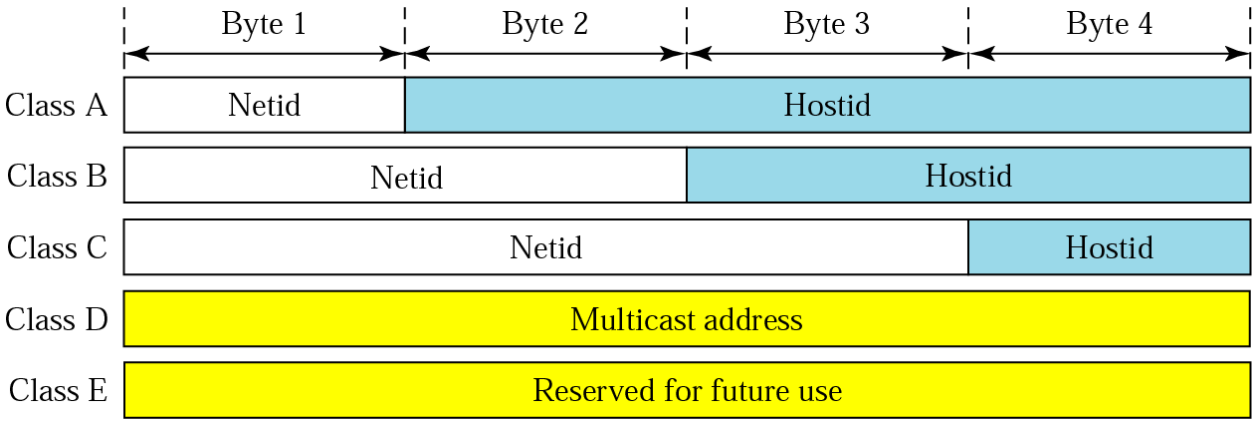
For Example,



Classful Address



Network and Host ID in classful address



Default Subnet Mask for Classful Address

Class	*In Binary*	*In Dotted-Decimal*	*Using Slash*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 111111111 11111111 00000000	255.255.255.0	/24

Classless Address

To overcome address depletion, classless concept is used. With classful addressing, the size of networks is fixed. According to class, each address range has a default subnet mask. Classless addressing decouples IP address ranges from a default subnet mask, allowing for variable-length subnet masking (VLSM). Classless addressing works by allowing IP addresses to be assigned random network masks without respect to class.

Example:

In an organization, if we need 500 IP addresses, we can use a /23 block which is much more efficient than using a Class B allocation. /23 give us 510 usable host addresses. By switching to classless addressing, we have avoided wasting over 65,000 addresses.

Private IP Address

Range of IP address, which is not routable to internet commonly, used for home, office, and enterprise local area networks (LANs). If such a private network needs to connect to the Internet, it must use either a network address translator (NAT) gateway, or a proxy server.

	Range
Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0 - 192.168.255.255

VLSM

VLSM is an abbreviation for "Variable Length Subnet Mask". It is a mechanism for allocating host space of different sizes between networks by dividing a network into numerous subnetworks. It was primarily created to provide greater flexibility for creating a network using several masks.

With VLSM, an IP address space can be divided into a well-defined hierarchy of subnets with different sizes. This helps enhance the usability of subnets because subnets can include masks of varying sizes without wasting large numbers of addresses.

In VLSM, each subnet chooses the block size based on its requirement. So, if requirements change, subnetting will be required multiple times.

CIDR (Classless Inter Domain Routing)

Classless Inter-Domain Routing (CIDR) is a method of IP address allocation and IP routing that allows for more efficient use of IP addresses. CIDR is based on the idea that IP addresses can be allocated and routed based on their network prefix rather than their class, which was the traditional way of IP address allocation.

For example, an IP address of 192.168.1.0 with a prefix length of 24 would be represented as 192.168.1.0/24. This notation indicates that the first 24 bits of the IP address are the network prefix and the remaining 8 bits are the host identifier. Similarly an IP address 10.10.0.0/25 will represent 25 bit as network bit and remaining 7 bit as host bit.

Features	**CIDR**	**VLSM**
Full Form	CIDR is an abbreviation for "Classless Inter-Domain Routing".	VLSM is an abbreviation for "Variable Length Subnet Mask".
Basic	It allows routers to combine routes together.	It helps in the optimization of available address space.
Concept Utilization	It utilizes the concept of supernetting.	It utilizes the concept of subnetting.
Supported Protocol	BGP and OSPF are two protocols that help CIDR.	IGRP, RIPv2, OSPF, and BGP protocols that support VLSM.

Operational and Management Issues of Legacy of IPV4 Network

The operational and management issues associated with the legacy IPv4 network refer to the challenges and limitations that arise due to the continued use of IPv4 (Internet Protocol version 4) in the face of increasing demands for IP addresses and the transition to IPv6 (Internet Protocol version 6). Here are some key points regarding these issues:

IPv4 Address Exhaustion: The primary concern is the depletion of available IPv4 addresses. The 32-bit addressing scheme of IPv4 allows for approximately 4.3 billion unique addresses, which is no longer sufficient to accommodate the growing number of devices connecting to the internet.

Network Address Translation (NAT): NAT has been widely adopted to mitigate the address shortage. It allows multiple devices to share a single public IP address by translating private IP addresses to public ones. While NAT provides a temporary solution, it introduces complexities, such as issues with peer-to-peer applications, increased administrative overhead, and potential performance degradation.

Address Management: The distribution and management of IPv4 addresses have become increasingly complex. Regional Internet Registries (RIRs) allocate IP address blocks to Internet Service Providers (ISPs) and other organizations, but as the available address space decreases, obtaining additional addresses becomes more challenging.

Dual Stack Deployment: With the ongoing transition to IPv6, network operators face the challenge of managing and maintaining both IPv4 and IPv6 protocols simultaneously. This requires the deployment of dual-stack networks, where devices and infrastructure support both protocols. Managing the coexistence and interoperability of IPv4 and IPv6 introduces additional complexity and potential security vulnerabilities.

Security and Compatibility: IPv4 networks are more susceptible to certain security risks due to the limited address space, lack of built-in security features, and the widespread use of NAT. As more devices transition to IPv6, maintaining compatibility and ensuring consistent security measures between the two protocols becomes essential.

Lack of Native IPv4 Support: As the adoption of IPv6 increases, new services and technologies are being developed that operate solely on IPv6. This may result in certain

legacy IPv4 systems becoming incompatible with these newer advancements, potentially limiting their functionality and interoperability.

Addressing these operational and management issues requires a gradual transition from IPv4 to IPv6. IPv6 offers a significantly larger address space, improved security features, and simplified address management. However, due to the widespread deployment of IPv4 and the need for a coordinated effort across the internet ecosystem, the transition process is ongoing and poses its own set of challenges

Introduction to Smart Networking

Smart networking refers to the use of intelligent technologies and strategies to establish and cultivate professional relationships for personal and business purposes. It leverages the power of digital tools and platforms to expand one's network and build connections.

Smart networking involves adopting a strategic approach to networking, utilizing technology to optimize the process. Here are some key elements of smart networking:

Digital Platforms: Smart networking takes advantage of social media platforms like LinkedIn, Twitter, and Facebook to connect with professionals, industry experts, and potential collaborators.

Personal Branding: Establishing a strong personal brand is crucial for smart networking. It involves defining and showcasing your expertise, skills, and unique value proposition online. By consistently curating and sharing relevant content, you can position yourself as an authority in your field, attracting like-minded professionals.

Relationship Management Tools: Smart networking relies on using relationship management tools, such as customer relationship management (CRM) systems, to organize and track connections, interactions, and follow-ups. These tools enable you to stay organized, manage your network effectively, and nurture relationships over time.

Online Communities: Participating in online communities and forums related to your industry or areas of interest allow you to connect with like-minded individuals, share knowledge, and contribute to discussions.

Virtual Events and Webinars: With the rise of remote work and virtual meetings, attending webinars, conferences, and online events has become an integral part of smart networking.

These platforms offer opportunities to connect with industry leaders, experts, and peers, fostering meaningful connections even from a distance.

Mutual Value Exchange: Smart networking emphasizes creating mutually beneficial relationships. It involves actively seeking opportunities to provide value to others, such as sharing insights, making introductions, or offering assistance. By nurturing a mindset of reciprocity, you can build trust and strengthen your network.

SDN (Software Defined Network)

SDN is a new modularized network architecture that separates the control plane from the data plane. SDN is changing the way networks are designed and handled. SDN is an evolutionary approach to network design and functionality based on the ability to programmatically modify the behavior of network devices. SDN is the future of network technology that will change the way that network engineers and designers build and operate their networks to achieve business requirements.

SDN enables networks to become open standards, nonproprietary, and easy to program and manage. SDN will give enterprises and carriers more control of their networks, allow them to tailor and to optimize their networks to reduce the overall cost of keeping the network. OpenFlow is the first and most dominant standard communication interface for SDN. OpenFlow protocol is a standardized interface that enables flow tables in switches and routers to be programmed. OpenFlow protocol allows separation of the control plane and the forwarding plane.

SDN Architecture

In traditional network, the application layer contains network applications or functions like IDS, load balancer or firewalls whereas in SDN it consist of application that uses controller to manage data plane behavior. The Control layer is the brain of SDN. It resides on server and manages policies and the flow of traffic. The infrastructure layer is made of the physical switches in the network. The three layers communicate using respective northbound and southbound API. Eg., Applications talk to controller through northbound interfaces while controller and switch communicate using southbound interface such as openflow

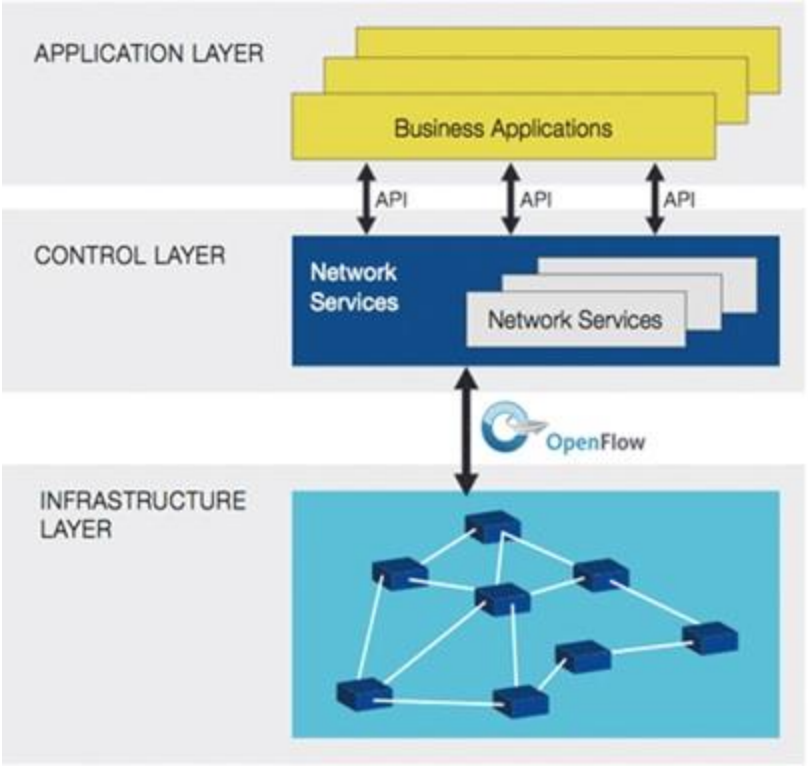


Figure: SDN Architecture

Control Plane

- Makes decision about where to send data traffic
- Its functions include system configuration, management and exchange of routing table information
- Control plane packets are destined to or locally originated by router itself
- The route controller exchanges the topology information with other routers and construct a routing table based on routing protocols
- Control plane packets are processed by the router to update the routing table information

Data Plane

- Also known as forwarding plane
- Forwards traffic to the next hop according to control plane logic
- Data plane packets go through the router
- The routers/switches use what the control plane built to dispose of incoming and outgoing frames and packets

Benefits of SDN

- Network management Simplicity
- Fast service deployment
- Automated configuration
- Network Virtualization
- Reducing the operational expense

NFV (Network Function Virtualization)

Network Function Virtualization (NFV) is a technology that aims to transform traditional networking by virtualizing network functions, such as firewalls, routers, load balancers, and intrusion detection systems. It allows these network functions to be implemented in software and run on standard servers, rather than relying on dedicated hardware appliances. The key idea behind NFV is to decouple network functions from specific hardware devices and instead run them as software instances on generic servers. This brings several benefits, including increased flexibility, scalability, and cost-efficiency. NFV enables network operators to deploy and manage network functions more dynamically, allowing them to adapt and scale their networks more easily to meet changing demands.

By virtualizing network functions, NFV enables the consolidation of multiple network functions onto a shared hardware platform, reducing the need for specialized hardware and simplifying network management. It also enables the rapid deployment of new services and applications by spinning up virtual instances of network functions as needed, rather than relying on lengthy and costly hardware procurement and deployment processes.

Overall, NFV aims to bring the benefits of virtualization and cloud computing to the networking domain, revolutionizing the way networks are designed, deployed, and managed. It offers greater flexibility, scalability, and cost-efficiency, allowing network operators to adapt and innovate more rapidly in response to evolving user needs and market demands.

Differences between SDN and NFV

The basic Concepts of SDN separates control and data plane while NFV transfers network functions from dedicated appliances to generic servers. The area of operation for SDN is in campus, data centers and cloud environment while NFV targets the service provider network.

Initial Application Target for SDN is cloud while NFV targets routers, firewall, gateways, WAN,CDN

IPV6 Network Migration Status

There are plenty of challenges related to the full adoption of IPV6. It includes:

- Hardware limitations
- Huge Infrastructure Cost
- Lack of training and skills

Many countries have been migrating to the latest version of the Internet Protocol in recent years. Some regions and countries are making significant progress in IPv6 deployment, while others are lagging behind. The progress varied across different sectors, such as Internet service providers (ISPs), content providers, and enterprises.

Google, Facebook, and YouTube are just a few of the well-known websites and online businesses that have already made IPv6 connectivity available. Additionally, IPv6 capability is incorporated into a lot of operating systems and networking hardware.

However, moving to IPv6 requires upgrading network infrastructure, modernizing software and processes, and making sure that IPv4 networks can still communicate with IPv6 networks. This complexity, along with the expense and work required, has played a big role in IPv6's slow but steady acceptance.

The high rate of IPv6 implementation in India is increasing rapidly. For example, Reliance JIO – India's biggest telecom – had 358 million users in 2021. Germany follows India with a steady increase in IPv6 deployment. IPv6 deployment fluctuated because more people worked from home at the beginning of the pandemic than in 2021.

It is estimated that all US mobile carriers combined support 87% of IPv6 deployment. This shows that mobile networks drive the deployment of IPv6 to simplify operations and network scalability.