Unit 7: Multimedia & Future Networking

Introduction to Multimedia:

Multimedia is a form of communication that combines different content forms such as text, audio, images, animations, or video. By definition, Multimedia is a representation of information in an attractive and interactive manner with the use of a combination of text, audio, video, graphics and animation.

The major multimedia network applications use audio video communications, which can be classified into three categories: streaming stored audio/video, streaming live audio/video, and interactive audio/video.

In streaming stored audio/video, the files are compressed and stored on a server. A client downloads the files through the Internet. This is sometimes referred to as on-demand audio/video. Examples of stored audio video files are songs, movies, TV shows, and music video clips etc.

In streaming live audio/video, a user listens to broadcast audio and video through the Internet. A good example of this type of application is the live streaming of football matches.

In interactive audio/video, people use the Internet to interactively communicate with one another. A good example of this application is VoIP e.g., audio and video chats in social media platforms.

Streaming Protocol:

Each time we watch a live stream or video on demand, streaming protocols are used to deliver data over the internet. Streaming protocols like Real-Time Messaging Protocol (RTMP) enable speedy video delivery using dedicated streaming servers, whereas HTTP-based protocols rely on regular web servers to optimize the viewing experience and quickly scale.

Streaming media is multimedia that is constantly received by and presented to an end user while being delivered by a provider over the Internet. Real-time Transport Protocol (RTP) is the protocol designed to handle real-time traffic on the Internet. RTP does not have a delivery mechanism (multicasting, port numbers, and so on); it must be used with UDP. Sometimes RTP is sometimes referred to as RTSP (Real Time Streaming Protocol). These are network control protocol designed for use in entertainment and communications systems to control streaming media servers.

Multimedia Streaming Protocol: SCTP

Stream Control Transmission Protocol (SCTP) is a transport-layer protocol that ensures reliable, in-sequence transport of data. It is a protocol for transmitting multiple streams of data at the same time between two end points that have established a connection in a network (multi streaming). SCTP provides multihoming support where one or both endpoints of a connection can consist of more than one IP address. It also provides congestion control facilities to maintain the smooth flow of data between media server and end devices.

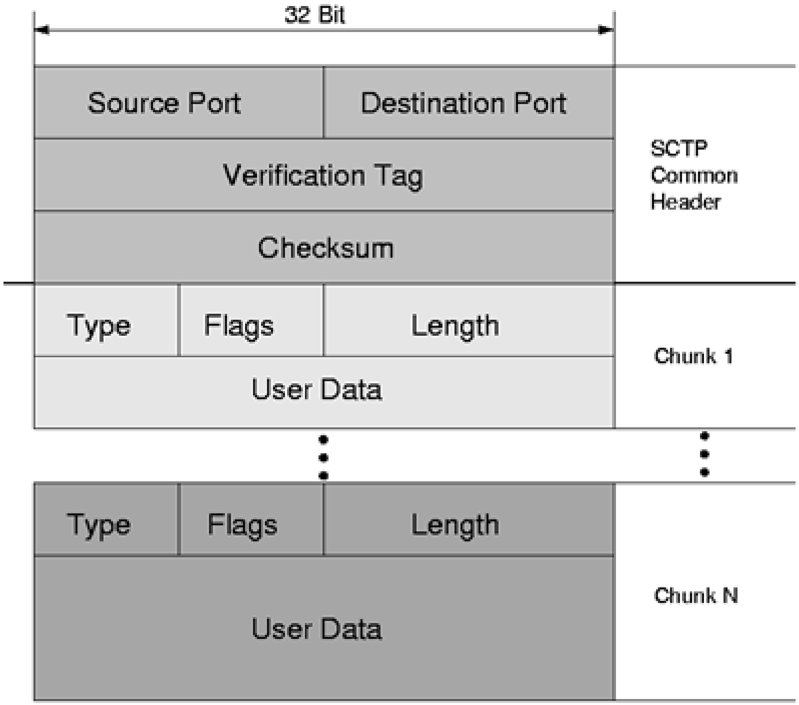
Features of SCTP:

- Supports full-duplex associations
- Supports multihoming
- Provides reliability
- Provides Flow Control

- Avoids Congestion
- Supports Multiple Streams

SCTP Packet:

- A SCTP packet forms the payload of an IP packet.
- It is composed of a common header and chunks.
- A chunk may contain either control information or user data.
- Multiple chunks may be multiplexed into one SCTP packet up to the MTU Size.
- Control chunks are bundled before data chunks.

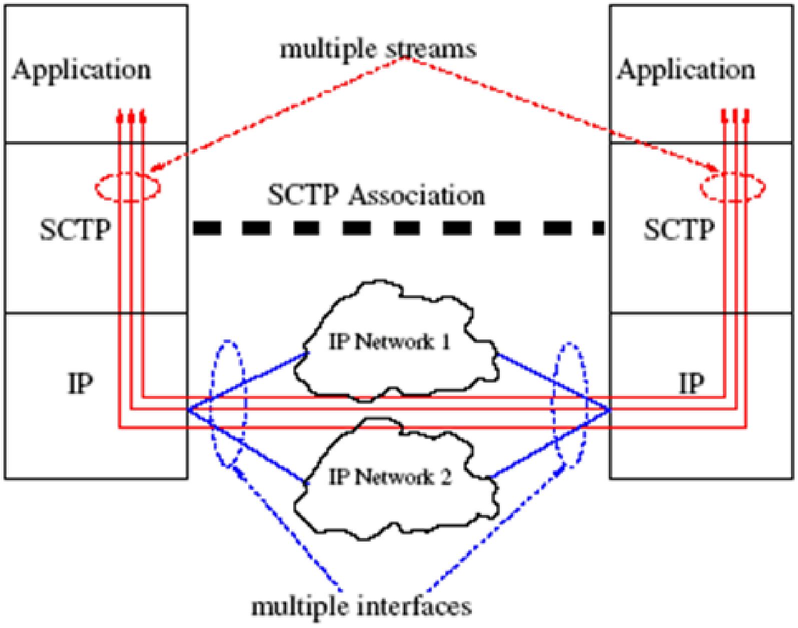


Source and Destination port is same as TCP and UDP. The verification tag is used to validate the sender of the SCTP packet at the receiver side. Checksum is used for error detection but is of 32 bits unlike 16-bit checksum of TCP and UDP.

SCTP Association:

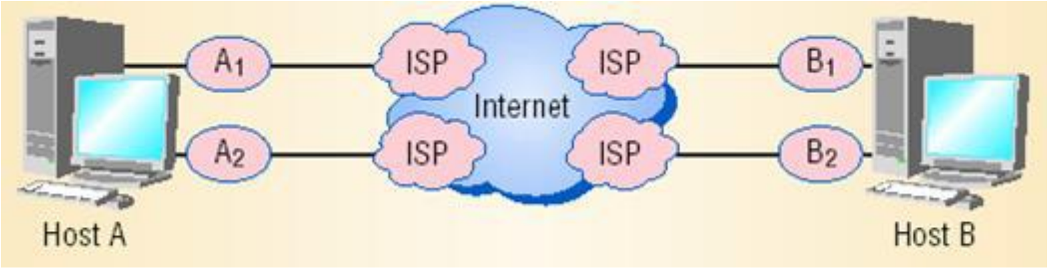
SCTP Association is the relationship between SCTP endpoints. It is composed of the two SCTP end points and protocol state information including verification tags and the currently active set of transmission sequence numbers.

An association can be uniquely identified by the transport addresses used by the endpoints in the association. Two SCTP endpoints must not have more than one SCTP association between them at any given time.



SCTP and Multihoming:

An essential property of SCTP is its support of multihomed nodes, i.e., nodes which can be reached using several IP addresses.



If IP networks are configured on physically different paths (Different ISPs), associations become tolerant against physical network failures and other network problems.

Overview of SDN:

Software-defined networking (SDN) is a network architectural model that enables dynamic, programmatically efficient network configuration, control and optimization of network resources in order to improve network performance and monitoring. It enables the network to be intelligently and centrally controlled, or ‘programmed,’ using software applications. SDN is an architecture designed to make a network more flexible and easier to manage. The goal of SDN is to improve network control by enabling enterprises and service providers to respond quickly to changing business requirements.

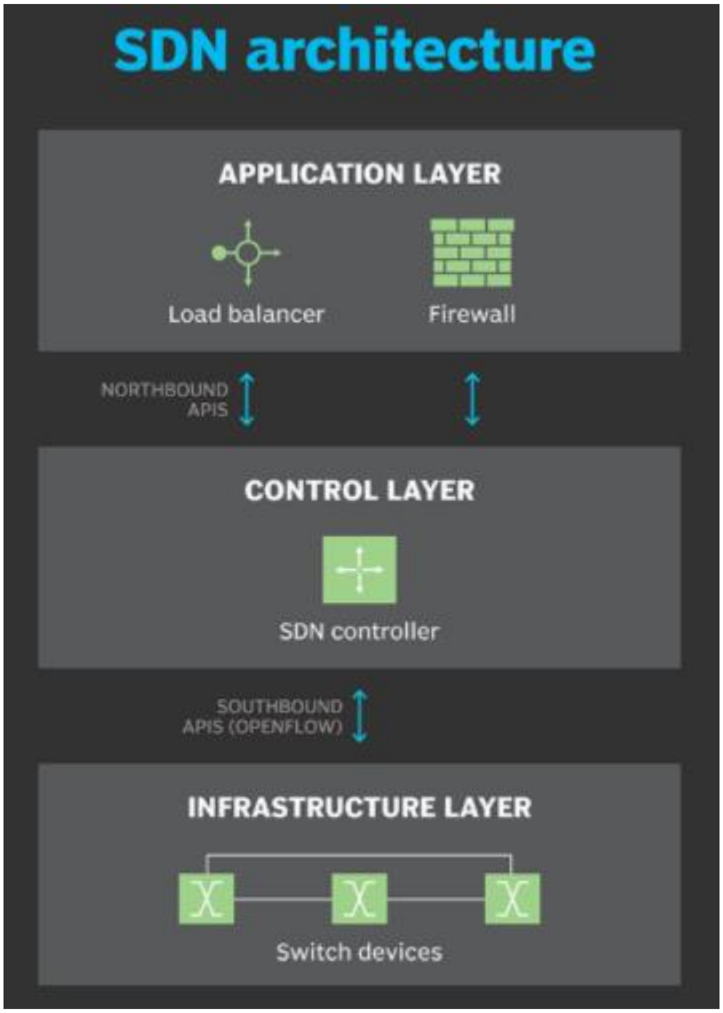
In a software-defined network, a network engineer or administrator can shape traffic from a centralized control console without having to touch individual switches in the network. A centralized SDN controller will direct the switches to deliver network services wherever they're needed, regardless of the specific connections between a server and devices.

Features of SDN:

- **Agile:** As business and application needs change, administrators can adjust network configuration dynamically.
- **Centrally managed:** Network is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policies as a single, logical switch.
- **Programmable:** SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.
- **Open Connectivity:** SDN is based on and implemented via open standards. As a result, SDN streamlines network design and provides consistent networking in a vendor -neutral architecture

SDN Architecture:

A typical representation of SDN architecture comprises three layers: the application layer, the control layer and the infrastructure layer.



An SDN architecture delivers a centralized, programmable network and consists of the following:

- A controller, the core element of an SDN architecture, that enables centralized management and control, automation, and policy enforcement across physical and virtual network environments
- Southbound APIs that relay information between the controller and the individual network devices (such as switches, access points, routers, and firewalls)
- Northbound APIs that relay information between the controller and the applications and policy engines, to which an SDN looks like a single logical network device.

The application layer, not surprisingly, contains the typical network applications or functions organizations use. This can include intrusion detection systems, load balancing or firewalls. Where a traditional network would use a specialized appliance, such as a firewall or load balancer, a software-defined network replaces the appliance with an application that uses a controller to manage data plane behavior.

SDN architecture separates the network into three distinguishable layers, connected through northbound and southbound APIs.

The control layer represents the centralized SDN controller software that acts as the brain of the software-defined network. This controller resides on a server and manages policies and the flow of traffic throughout the network.

The infrastructure layer is made up of the physical switches in the network.

Components of SDN:

Data Plane
Control Plane
Management Plane

The **Control Plane** refers to the network architecture component that defines the traffic routing and network topology.

The **Data Plane** is the network architecture layer that physically handles the traffic based on the configurations supplied from the Control Plane.

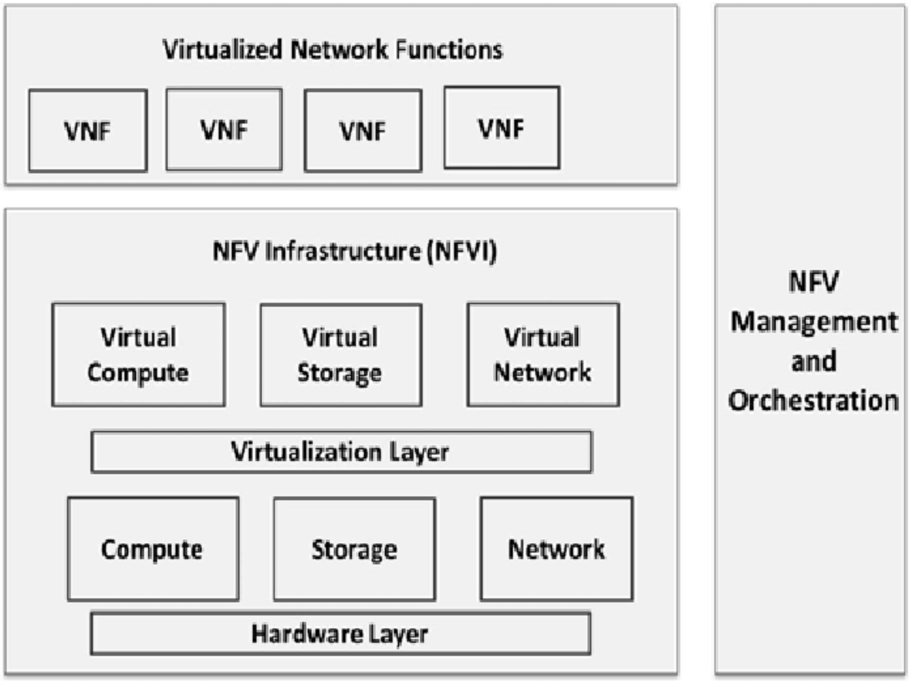
The **Management Plane** takes care of the wider network configuration, monitoring and management processes across all layers of the network stack

Overview of NFV:

Network functions virtualization (NFV) is a way to virtualize network services, such as routers, firewalls, and load balancers, that have traditionally been run on proprietary hardware. These services are packaged as virtual machines (VMs) on commodity hardware, which allows service providers to run their network on standard servers instead of proprietary ones.

With NFV, we don't need to have dedicated hardware for each network function. NFV improves scalability and quick service by allowing service providers to deliver new network services and applications on demand, without requiring additional hardware resources.

Architecture:



NFV architecture consists of:

- Virtualized network functions (VNFs) are software applications that deliver network functions such as file sharing, directory services, and IP configuration.
- Network functions virtualization infrastructure (NFVI) consists of the infrastructure components—compute, storage, networking—on a platform to support software needed to run network apps.
- Management, automation and network orchestration (MANO) is the collection of all functional blocks, data repositories used by these blocks, and reference points and interfaces through which these functional blocks exchange information for the purpose of managing and orchestrating NFVI and VNFs.

Relation between SDN and NFV:

- NFV and SDN are not dependent on each other, but they do have similarities. Both rely on virtualization and use network abstraction, but how they separate functions and abstract resources is different.
- SDN separates network forwarding functions from network control functions with the goal of creating a network that is centrally manageable and programmable. NFV abstracts network functions from hardware. NFV supports SDN by providing the infrastructure on which SDN software can run.
- NFV and SDN can be used together, depending on what you want to accomplish, and both use commodity hardware. With NFV and SDN, you can create a network architecture that is more flexible, programmable, and uses resources efficiently.

Benefits of NFV:

With NFV, service providers can run network functions on standard hardware instead of dedicated hardware. Also, because network functions are virtualized, multiple functions can be run on a single server. This means that less physical hardware is needed, which allows for resource consolidation that results in physical space, power, and overall cost reductions.

NFV gives providers the flexibility to run VNFs across different servers or move them around as needed when demand changes. This flexibility lets service providers deliver services and apps faster.

For example, if a customer requests a new network function, they can spin up a new VM to handle that request. If the function is no longer needed, the VM can be decommissioned.

Overview of NGN:

A next-generation network (NGN) is a packet-based network which can provide services including Telecommunication Services and is able to make use of multiple broadbands, quality of service-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers with generalized mobility.

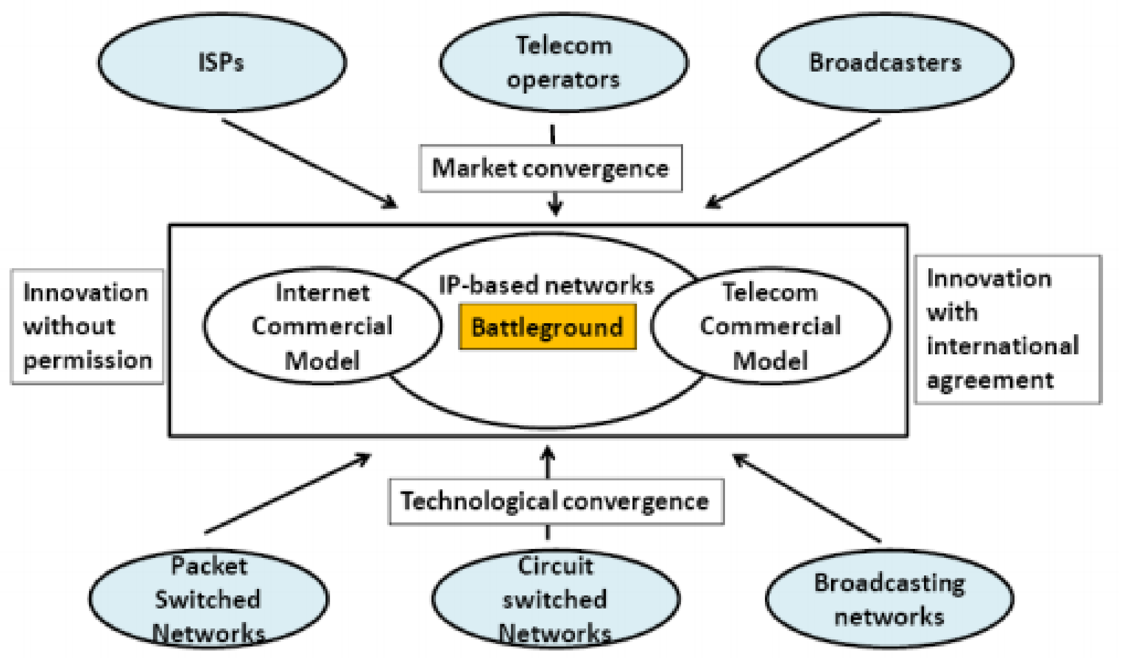
Next Generation Network (NGN) completely redefines our traditional telecommunication system. Using NGN, a key innovation which is expected to bring further significant changes in the communications market is the transformation from circuit-based public switched telecommunication networks to packet-based networks using the Internet Protocol. The general idea behind the NGN is convergence in which one network transports all information and services (voice, data and all sorts of media) by encapsulating these into packets.

Key Principles of NGN:

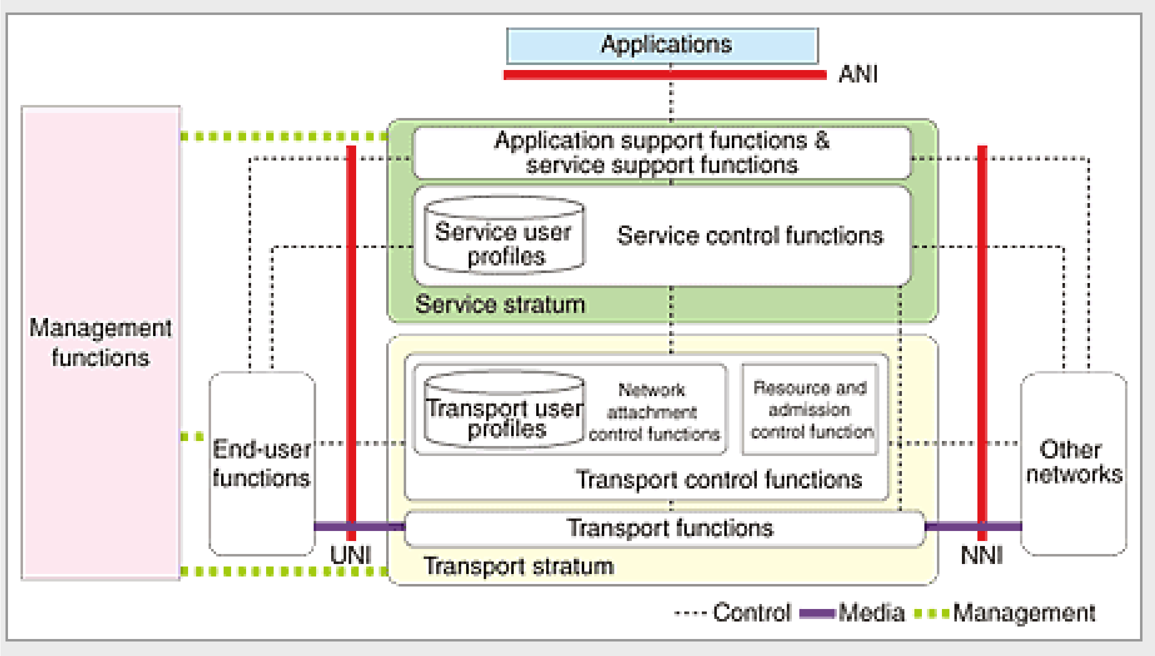
- **Open Architecture**: open to support service creation, service updating, and incorporation of service logic provision by third parties and also support “Distributed control” as well as enhanced security and protection.
- **Independent Provisioning:** service provision process should be separated from network operation by using distributed, open control mechanism to promote competition.

- **Multiplicity:** The NGN functional architecture shall offer the configuration flexibility needed to support multiple access technologies.

Convergence through NGN:



Architecture:



The NGN consists of four function groups and two types of user profiles. Transport functions transfer multimedia streams over the IP network. Transport control functions allocate IP addresses, perform authentication tasks, and enable control functions such as resource admission for guaranteeing IP-layer QoS to be used from service components. Service control functions and application support functions & service support functions provide support functions such as presence management.

Two types of user profiles are specified based on how user information used by the service control function group and transport control function group is applied and how it relates to the functions. One of these is the transport user profile, which is referred to by the transport control function group. This profile includes information such as user authentication data and the bandwidth that the user may obtain when connecting to the access network. The other is the service user profile used by the service control function group. This profile includes information such as what services the user is allowed to use and how many simultaneous connections may be made.

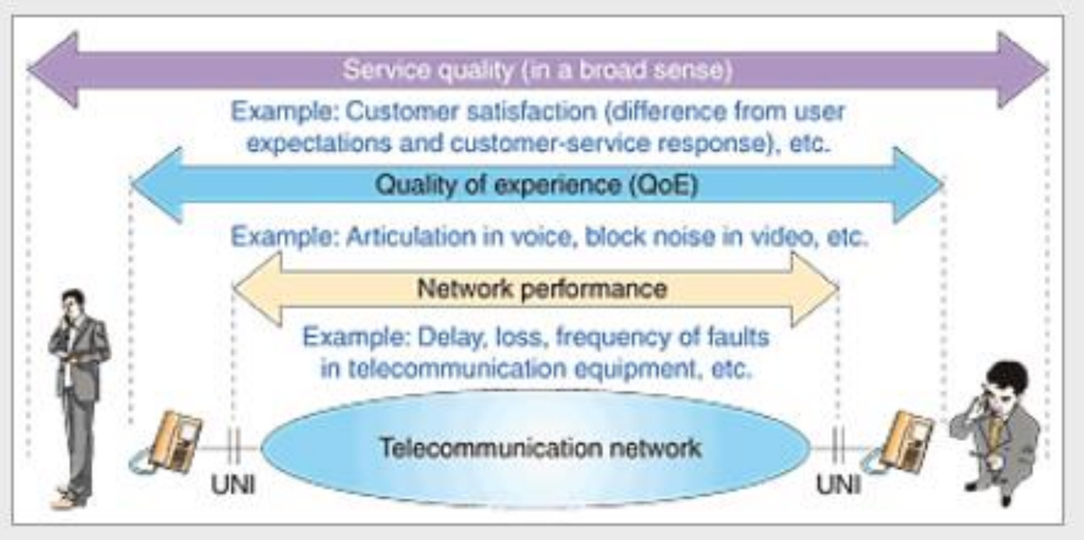
There are three types of interfaces:

(i) the user-network interface (UNI), which is the connection point with end-user functions;
(ii) the network-network interface (NNI), which is the connection point with other networks; and
(iii) the application-network interface (ANI), which is the connection point with application functions.

QoS Specification in NGN:

Quality is an important concept in NGN construction. However, the word "quality" can have various meanings. For example, quality can be used in relation to speech quality in telephone calls or picture quality in video delivery services. It may also be used in connection with communication services to describe, for example, the degree to which telecommunication equipment operates correctly without faults and the response that a customer receives from a service provider when applying for a service. But the focus is on quality of service (QoS) on the IP layer in the NGN.

The overall quality in telecommunication services with respect to QoS defined in NGN can be understood as:


Service quality (in a broad sense)
Example: Customer satisfaction (difference from user expectations and customer-service response), etc.
Quality of experience (QoE)
Example: Articulation in voice, block noise in video, etc.
Network performance
Example: Delay, loss, frequency of faults in telecommunication equipment, etc.
Telecommunication network
UNI
UNI