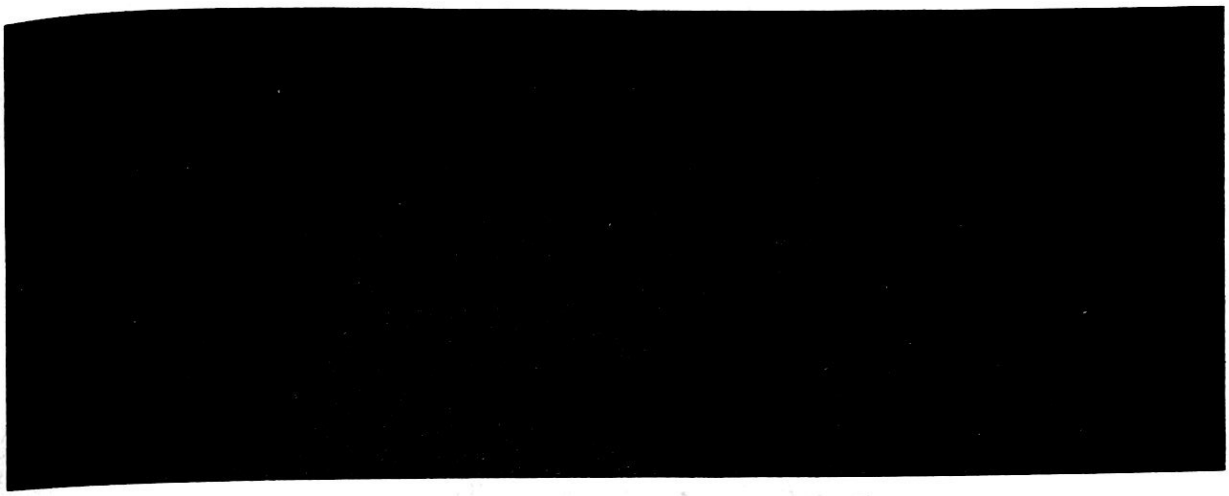

Overview Multimedia Streaming Protocols

We use the term multimedia to refer to data that contains audio or video, and may include text. The phrase real-time multimedia refers to multimedia data that must be reproduced at exactly the same rate that it was captured (e.g., a television news program that includes audio and video of an actual event).

Instead of requiring the underlying networks to handle real-time transmission, the Internet uses additional protocol support. Interestingly, the most significant problem to be handled is jitter, not packet loss. To see why, consider a live webcast. If a protocol uses timeout-and-retransmission to resend the packet, the retransmitted packet will arrive too late to be useful – the receiver will have played the video and audio from successive packets and it makes no sense to insert a snippet of the webcast that was missed earlier.

Stream Control Transmission Protocol (SCTP)

The Stream Control Transmission Protocol (SCTP) is a computer networking communications protocol which operates at the transport layer and serves a role similar to the popular protocols TCP and UDP. It is standardized by IETF in RFC 4960. SCTP provides some of the features of both UDP and TCP: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP. It differs from those protocols by providing multi-homing and redundant paths to increase resilience and reliability. SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users:

- Acknowledged error-free non-duplicated transfer of user data.
- Data fragmentation to conform to discovered path MTU size.
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages.
- Optional bundling of multiple user messages into a single SCTP packet.

- Network-level fault tolerance through supporting of multi-homing at either or both ends of an association.

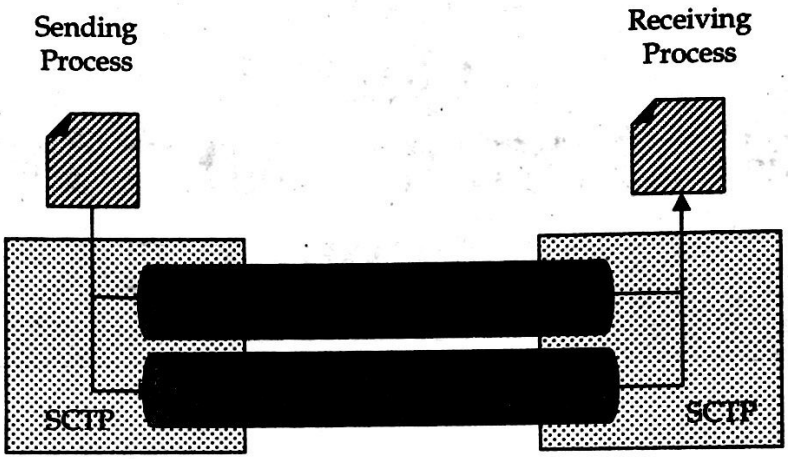

Figure 7.1: SCTP

Features of SCTP

- Multi homing support in which one or both endpoints of a connection can consist of more than one IP address, enabling transparent failover between redundant network paths.
- Delivery of chunks within independent streams eliminates unnecessary head-of-line blocking, as opposed to TCP byte-stream delivery.
- Path selection and monitoring to select a primary data transmission path and test the connectivity of the transmission path.
- Validation and acknowledgment mechanisms protect against flooding attacks and provide notification of duplicated or missing data chunks

Overview of Software-defined networking (SDN)

Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. The Open Flow protocol is a foundational element for building SDN solutions.

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. The centralized SDN controller directs the switches to deliver network services wherever they're needed, regardless of the specific connections between a server and devices. This process is a move away from traditional network architecture, in which individual network devices make traffic decisions based on their configured routing tables.

SDN architecture

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

The application layer, not surprisingly, contains the typical network applications or functions organizations use, which 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 the controller to manage data plane behavior.

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.

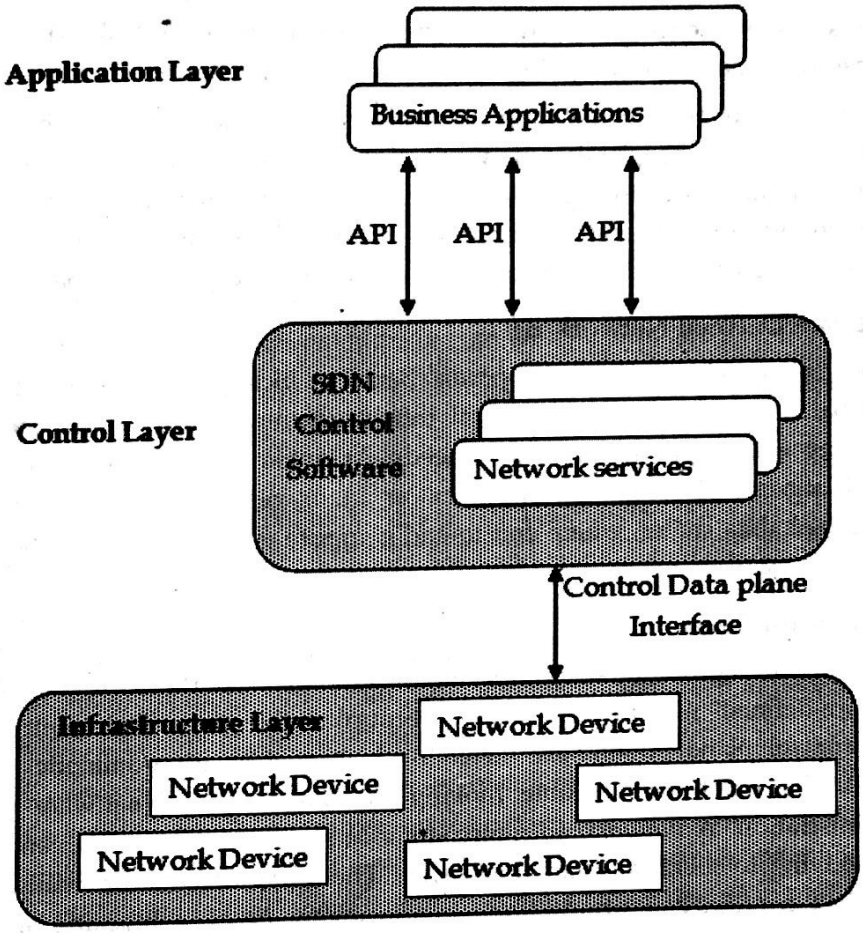

Figure 7.2: SDN architecture

These three layers communicate using respective northbound and southbound application programming interfaces (APIs). For example, applications talk to the controller through its northbound interface, while the controller and switches communicate using southbound interfaces, such as OpenFlow -- although other protocols exist.

How SDN works

SDN encompasses several types of technologies, including functional separation, network virtualization and automation through programmability. Originally, SDN technology focused solely on separation of the network control plane from the data plane. While the control plane makes

decisions about how packets should flow through the network, the data plane actually moves packets from place to place.

In a classic SDN scenario, a packet arrives at a network switch, and rules built into the switch's proprietary firmware tell the switch where to forward the packet. These packet-handling rules are sent to the switch from the centralized controller.

The switch -- also known as a data plane device -- queries the controller for guidance as needed, and it provides the controller with information about traffic it handles. The switch sends every packet going to the same destination along the same path and treats all the packets the exact same way.

Software-defined networking uses an operation mode that is sometimes called adaptive or dynamic, in which a switch issues a route request to a controller for a packet that does not have a specific route. This process is separate from adaptive routing, which issues route requests through routers and algorithms based on the network topology, not through a controller.

The virtualization aspect of SDN comes into play through a virtual overlay, which is a logically separate network on top of the physical network. Users can implement end-to-end overlays to abstract the underlying network and segment network traffic. This micro-segmentation is especially useful for service providers and operators with multi-tenant cloud environments and cloud services, as they can provision a separate virtual network with specific policies for each tenant.

Benefits of Software Defined Networking

Software defined networking offers numerous benefits including on-demand provisioning, automated load balancing, streamlined physical infrastructure and the ability to scale network resources in lockstep with application and data needs. As noted on Enterprise Networking Planet, coupled with the ongoing virtualization of servers and storage, SDN ushers in no less than the completely virtualized data center, where end-to-end compute environments will be deployed and decommissioned on a whim.

SDN Data and Control Plane

In conventional networking, all three planes are implemented in the firmware of routers and switches. Software-defined networking (SDN) decouples the data and control planes and implements the control plane in software instead, which enables programmatic access to make network administration much more flexible. Moving the control plane to software allows dynamic access and administration. A network administrator can shape traffic from a centralized control console without having to touch individual switches. The administrator can change any network switch's rules when necessary -- prioritizing, de-prioritizing or even blocking specific types of packets with a very granular level of control.

Conceptually, data plane is the part where all the packet processing and forwarding logic is there. Data plane decides what to do with the packet, where to transfer, whether to encapsulate or encapsulate the packet. It is also known as forwarding plane. Control plane provides the management interface through which network can be configured.

Generally, these control plane and data plane are tightly coupled. For example, network admin can assign VLANs or he can fill the forwarding entries in the in the forwarding tables. But he can configure particular classification rules or cannot control how packets are handled. So we need to decouple the vendor's control plane with customized version and we should be able to control the packet processing and forwarding from this control system.

Difference between control plane & data plane

Control Plane

- Makes decisions about where traffic is sent
- Control plane packets are destined to or locally originated by the router itself
- The control plane functions include the system configuration, management, and exchange of routing table information
- The route controller exchanges the topology information with other routers and constructs a routing table based on a routing protocol, for example, RIP, OSPF or BGP
- Control plane packets are processed by the router to update the routing table information.
- It is the Signaling of the network
- Since the control functions are not performed on each arriving individual packet, they do not have a strict speed constraint and are less time-critical

Data Plane

- Also known as Forwarding Plane
- Forwards traffic to the next hop along the path to the selected destination network 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

Overview of Network function virtualization (NFV)

NFV allows network operators to manage and expand their network capabilities on demand using virtual, software based applications where physical boxes once stood in the network architecture. This makes it easier to load-balance, scale up and down, and move functions across distributed hardware resources. With continual updates, operators can keep things running on the latest software without interruption to their customers.

Network functions virtualization (NFV) provides a new way to create, distribute, and operate networking services. It is the process of decoupling the network functions from proprietary hardware appliances so they can run in software on standardized hardware. These functions (such as firewall, deep packet inspection, and intrusion prevention) become virtual network functions (VNF).

NFV is designed to consolidate and deliver the networking components needed to support an infrastructure totally independent from hardware. These components include virtual compute, storage and network functions. NFV utilizes standard IT virtualization technologies that run on off-the-shelf hardware like commodity x86 servers. It is applicable to any data plane processing or control plane function in both wired and wireless network infrastructures.

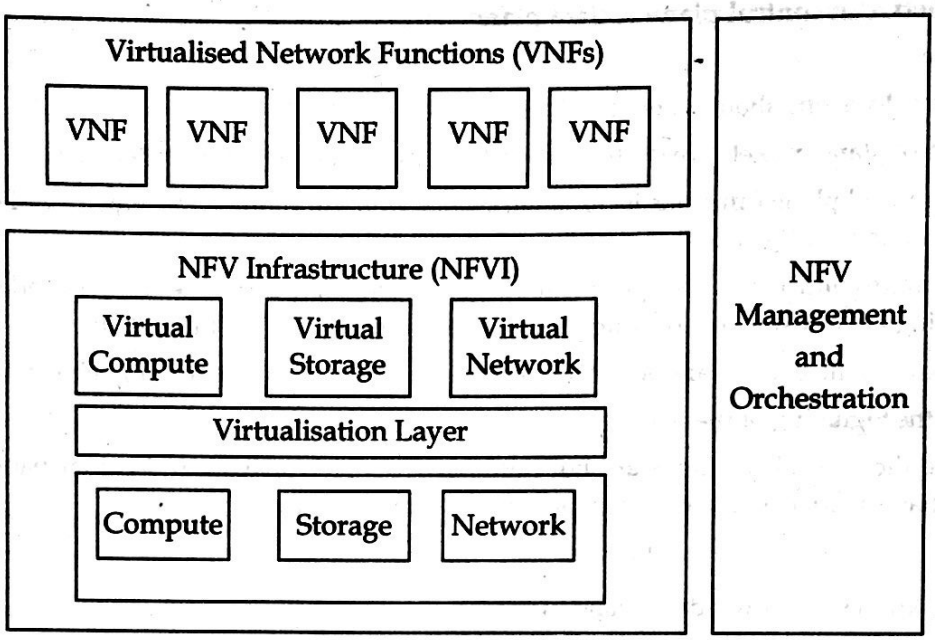

Figure 7.3: Components of NFV

The Benefits of NFV

NFV virtualizes network services via software to enable operators to:

- Reduce CapEx by reducing the need to purchase purpose-built hardware and using pay-as-you-grow models to eliminate wasteful over-provisioning.
- Reduce OpEX by reducing space, power and cooling requirements of equipment and simplifying the rollout and management of network services.
- Accelerate time-to-market by reducing the time required to deploy new networking services to support changing business requirements, new market opportunities, and return on investment of new services. NFV lowers the risks associated with rolling out new services, allowing providers to easily trial and evolve services to determine what best meets the needs of customers.
- Deliver agility and flexibility to quickly scale services up or down to address changing demands; services can be delivered via software on any industry-standard server hardware.

Differences between SDN and Network Functions Virtualization

Network functions virtualization and software defined networking are very closely linked, but they are not the same. Often the terms are incorrectly used synonymously. The main points of each are summarized below so that both SDN and NFV can be evaluated with their similarities and differences.

1. **The Basic Idea**

   SDN separates control and data and centralizes control and programmability of the network.

   NFV transfers network functions from dedicated appliances to generic servers.

2. **Areas of Operation**

   SDN operates in a campus, data center and/or cloud environment

   NFV targets the service provider network

3. **Initial Application Target**
   SDN software targets cloud orchestration and networking
   NFV software targets routers, firewalls, gateways, WAN, CDN, accelerators and SLA assurance
4. **Protocols**
   SDN - OpenFlow
   NFV - None
5. **Supporting organization**
   SDN: Open Networking Foundation (ONF)
   NFV: ETSI NFV Working Group

Overview of Next-Generation Network (NGN)

The **next-generation network** (NGN) is a body of key architectural changes in telecommunication core and access networks. The general idea behind the NGN is that one network transports all information and services (voice, data, and all sorts of media such as video) by encapsulating these into IP packets, similar to those used on the Internet. NGNs are commonly built around the Internet Protocol, and therefore the term all IP is also sometimes used to describe the transformation of formerly telephone-centric networks toward NGN.

Next Generation Network (NGN) is a term that describes the evolution and migration of fixed and mobile network infrastructures from distinct proprietary networks to converged networks based on IP. It is conceived to be an interworking environment of heterogeneous networks of wired and wireless access networks, PSTN, satellites, broadcasting, etc. The concept of this network will not only bring wide range of possibilities to introduce new and existing technologies in field of information transmission and processing, but also many possibilities especially in the branch of network services.

Architecture of NGN

The complete Next Generation Networks are divided into two typical constituents those are Access and Core networks. The Fig below shows the two network components. The end users have direct access to the Access network that is shown by an external circle in the figure and it provides a common service to both the wire line and wireless service users. The core networks take care to carry the data across the network. They include legacy technologies such as Asynchronous Transport Mode (ATM) and the modern family of IP based core. IP based technologies such as Multi-Protocol Label Switching (MPLS) possess two QoS models standardized by IETF, the Differentiated Services and the Integrated Services models. NGN provides end-to-end communication and employs multiple services at a time.

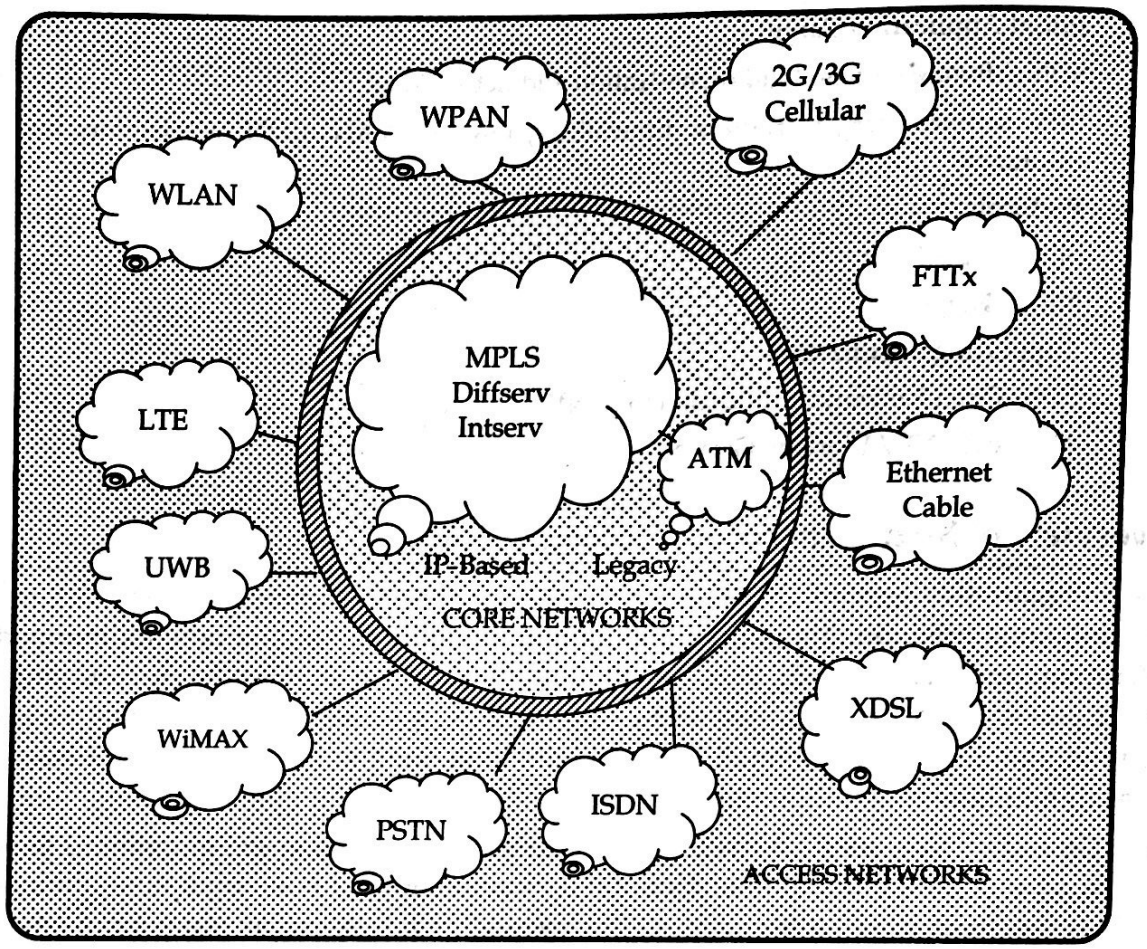

Figure 7.4: Access and Core Networks of NGN

But, this multi-tasking feature of NGN makes it somewhat complex network with the requirement to provide proper internetworking and interconnection between the different users and telecommunication operators. With the aim to create a logical framework for NGN, the functional model is mainly organized in three layers: the Transport layer, the Service Control layer and the Application layer are described below:

Transport Layer: Transport Layer of NGN is based on IP and can utilize the advantage of MPLS. Transport Layer forms the core of the Network. It basically consists of an assembly of Routers with optical network, which are responsible for carrying traffic originated by access layer. As the same core network is going to be used for all kinds of subscribers enjoying different kind of real time and non real time services, it should be able to make use of bandwidth policies and QoS policies. Operator has to think of managed Network for its subscribers. The underlying packet transport and media infrastructure are grouped under Transport layer which also interworks with circuit-switched (PSTN) network through Media Gateways so that existing networks can co-exist and need not be scrapped.

Service Control Layer: It consists of call servers where all information of the network resides and these servers are responsible for call setting up and routing, modifying, charging, tear down of the calls and controls some other activities within NGN environment. The Service Control layer consisting of Soft Switches, Media Gateway Controllers and IMS performs the functions of

authentication, accounting, maintaining QoS, security and network management. NGN may work on soft switch principle. It consists of MGC (Media Gateway Controller) as an overall controller and MGs (Media Gateway) for termination of traffic. MGC is basically a server and it is having all the necessary information of network. MGC instructs MGs for establishing the call. Under the control of MGC, MG performs different call related tasks such as connection, modification and termination of media streams, packetization of media etc.

Application Layer: The Application layer makes use of the capabilities provided by other functional layers to provide multimedia services and applications based on Open Architecture of Application Programming Interfaces (APIs). The enhanced services to the subscribers will be provided with the help of application servers. It may include prepaid servers, Announcement servers, Service servers etc. Hence NGN is making service separation from Network. Any service can be introduced with the help of server at any time without any modifications in the control, transport or access layers.

Features of NGN

- NGN works on Packet based transferring.
- There is an automatic separation of control functions among bearer capabilities, call/session and application/service.
- Decoupling of service provision from network and provision of open interface is also available under NGN.
- It supports a wide range of services, applications and mechanisms based on service building blocks.
- The network has Broadband capabilities with end to-end QoS and transparency.
- This network also has a feature of interworking with legacy networks via open interfaces.
- It provides the advantage of general mobility.
- It provides unrestricted access by users to different service providers.
- It also provides variety of identification schemes which can be resolved to IP addresses for the purpose of routing in IP network.
- It is composed of Unified service characteristics for the same services as perceived by the user.

Applications of NGN

The various applications of NGN are explained below:

- Voice Telephone services
- Multimedia services
- Data services
- Push to talk over NGN (PoN)
- Content delivery services
- Global mobility services
- Virtual Private Services (VPNs)
- Broadcasting/Multicast services
- E- commerce and M- commerce

- Session Controller based Internet services
- Third party/OSA based services
- 3D Imaging
- Machine to Machine communication
- Data Augmentation

Advantages of NGN

NGN makes use of the best of both the worlds i.e. flexibility, efficiency & innovativeness of IP and QoS, Security, Reliability, Customer-friendly features of proven PSTN. Besides this it has following advantages:

- It generates additional revenue streams for new IP/Ethernet services.
- It fulfils customer's demand for high bandwidth, Ethernet/ IP solutions.
- It diminishes expertise in legacy.
- It gives End of Life/ End of Service vendor notification.
- Users can choose multiple service providers to take maximum advantage of competitive offers but may get single bill.

Disadvantage of Next Generation Network

Though having huge advantages and applications, NGN is having some major loopholes which are stated as follows:

- Migration complexities
- Not all legacy services can be replaced with new alternatives
- Not all existing infrastructure can be shut down
- Regulatory restrictions for critical services
- NGN technology is still under research and development.
- Lack of Standardization and governing body.
- Difficult to make it work with existing technology and convert the whole system as well