Multimedia and Future Network

Compiled By: Hiranya Prasad Bastakoti

What is Multimedia ?

- Multimedia is an integration of text, graphics, still and moving images, animation, sounds, and any other medium where every type of information can be represented, stored, transmitted and processed digitally.
- Media may be Text, Graphics, image, video, animation, sound, etc
- Characteristics of multimedia
  - ✓ Digital – key concept
  - ✓ Integration of multiple media type, usually including video or/and audio
  - ✓ May be interactive or non-interactive

Multimedia Networking

- The four most critical components involved in a multimedia networking system – data compression, quality of service (QoS), communication protocols, and effective digital rights management – are intensively addressed.

Some Example of Multimedia application:

Streaming stored audio and video

One to many streaming of real-time audio and video

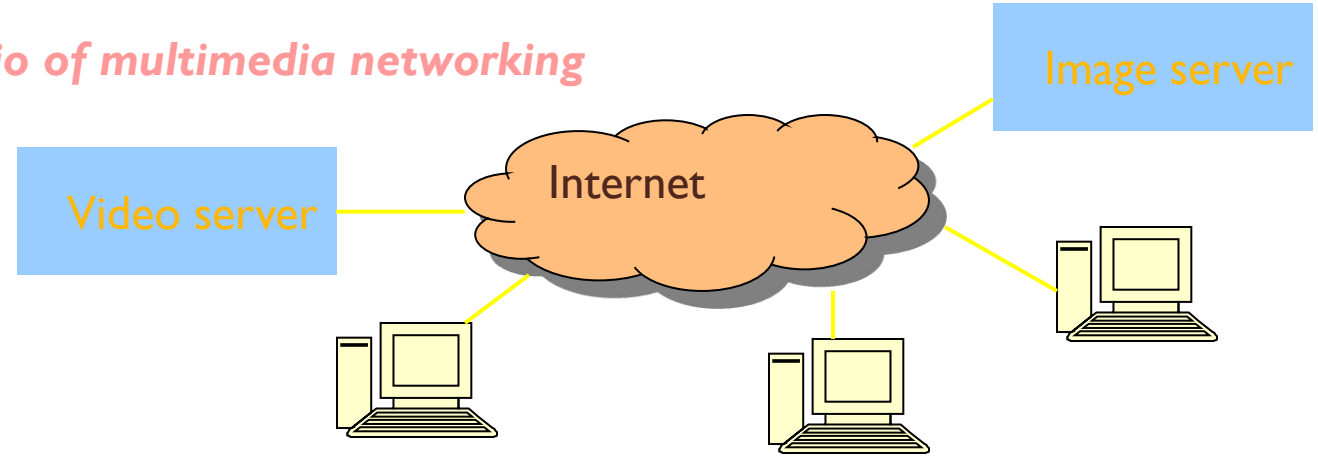
Real-time interactive audio and video

- Multimedia Extended Email
- World Wide Web
- Video Distribution Services
- Video Conferencing
- Interactive Distributed Games
- Virtual Reality
- Distant Learning
- Instant Messaging

Networked Multimedia

- Local vs. networked multimedia
  - Local: storage and presentation of multimedia information in standalone computers
    - Sample applications: DVD
  - Networked: involve transmission and distribution of multimedia information on the network
    - Sample applications: videoconferencing, web video broadcasting, multimedia Email, etc.

A scenario of multimedia networking



Stream Control Transmission Protocol (SCTP)

- Stream Control Transmission Protocol (SCTP) is an IP Transport Layer protocol.
- SCTP exists at an equivalent level with User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), which provides transport layer functions to many Internet applications.
- SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP and supports data transfer across the network in single IP or multi-IP cases.
- SCTP provides multihoming support where one or both endpoints of a connection can consist of more than one IP address.
- This enables transparent failover between redundant network paths.

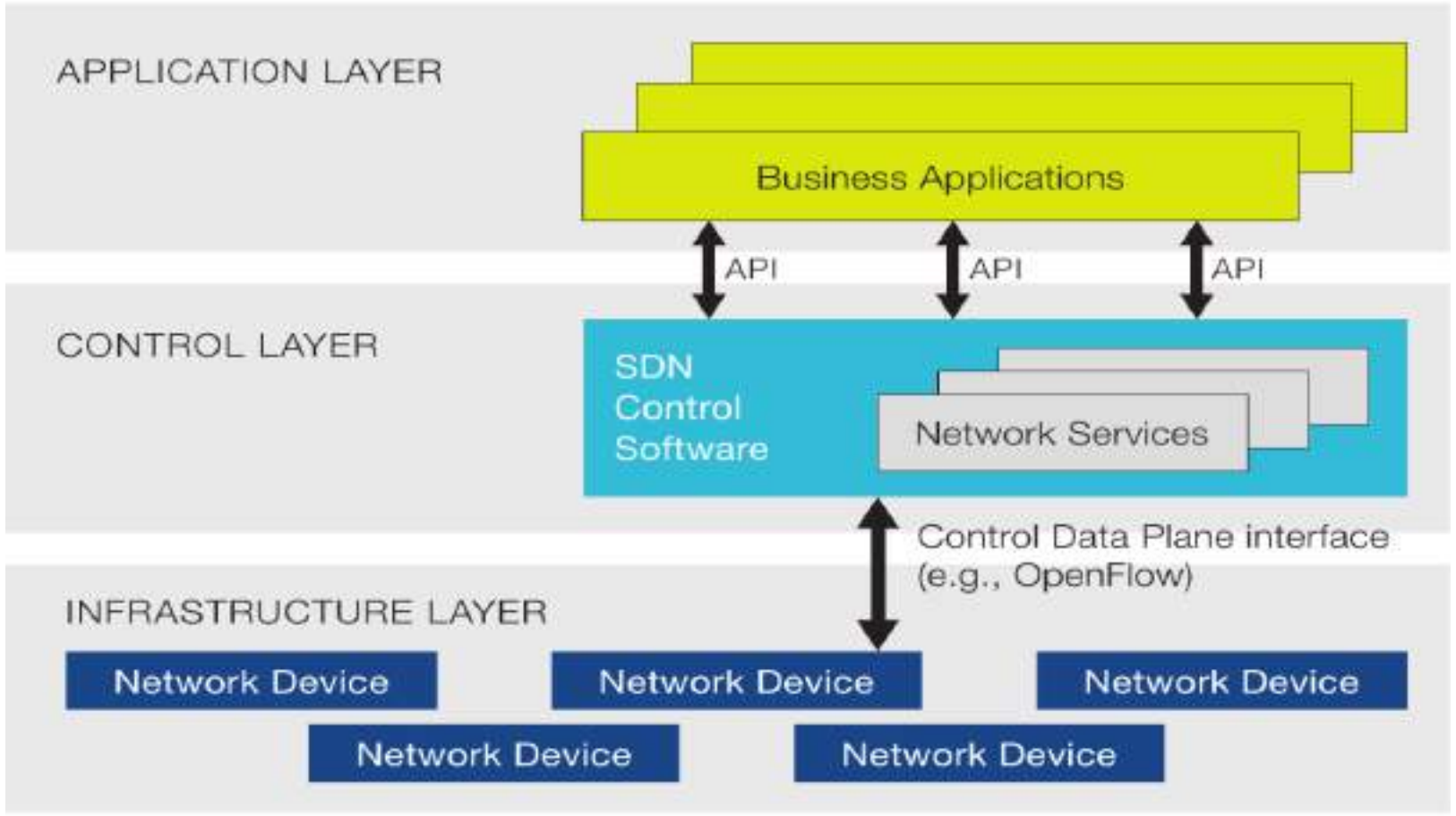
Features of SCTP

- **Confirmed transmission** of user data (error-free and without duplicates)
- **Data fragmentation** to maintain the maximum packet size of each network path
- **Sequenced delivery** of user messages within multiple data streams (multi-streaming) – including the option to specify the order of these messages
- **Bundling** (optional) of several users' messages in a single SCTP package (chunk bundling)
- **Fault tolerance at network level** thanks to multi-homing (host with several valid network addresses) of one of both communication partner(s)

SDN

- A software-defined networking (SDN) architecture (or SDN architecture) defines how a networking and computing system can be built using a combination of open, software-based technologies and commodity networking hardware that separate the SDN control plane and the SDN data plane of the networking stack.
- 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.

SDN


APPLICATION LAYER
Business Applications
API
API
API
CONTROL LAYER
SDN
Control
Software
Network Services
Control Data Plane interface
(e.g., OpenFlow)
INFRASTRUCTURE LAYER
Network Device
Network Device
Network Device
Network Device
Network Device

Architecture of SDN

- SDN Applications:

SDN Applications are programs that communicate behaviors and needed resources with the SDN Controller via application programming interfaces (APIs).

In addition, the applications can build an abstracted view of the network by collecting information from the controller for decision-making purposes.

These applications could include networking management, analytics, or business applications used to run large data centers.

For example, an analytics application might be built to recognize suspicious network activity for security purposes.

- SDN Controller:

The SDN Controller is a logical entity that receives instructions or requirements from the SDN Application layer and relays them to the networking components.

The controller also extracts information about the network from the hardware devices and communicates back to the SDN Applications with an abstract view of the network, including statistics and events about what is happening.

- SDN Networking Devices: The SDN networking devices control the forwarding and data processing capabilities for the network.
- This includes forwarding and processing of the data path.
- *The SDN architecture APIs are often referred to as northbound and southbound interfaces, defining the communication between the applications, controllers, and networking systems.*
- *A Northbound interface is defined as the connection between the controller and applications, whereas the Southbound interface is the connection between the controller and the physical networking hardware.*
- *Because SDN is a virtualized architecture, these elements do not have to be physically located in the same place*.

- With SDN, an administrator can change any network switch's rules when necessary -- prioritizing, deprioritizing or even blocking specific types of packets with a granular level of control and security. This is especially helpful in a cloud computing multi-tenant architecture, because it enables the administrator to manage traffic loads in a flexible and more efficient manner. Essentially, this enables the administrator to use less expensive commodity switches and have more control over network traffic flow than ever before.
- Other benefits of SDN are network management and end-to-end visibility. A network administrator need only deal with one centralized controller to distribute policies to the connected switches, instead of configuring multiple individual devices. This capability is also a security advantage because the controller can monitor traffic and deploy security policies. If the controller deems traffic suspicious, for example, it can reroute or drop the packets.
- SDN also virtualizes hardware and services that were previously carried out by dedicated hardware, resulting in the touted benefits of a reduced hardware footprint and lower operational costs.
- Additionally, software-defined networking contributed to the emergence of software-defined wide area network (SD-WAN) technology. SD-WAN employs the virtual overlay aspect of SDN technology, abstracting an organization's connectivity links throughout its WAN and creating a virtual network that can use whichever connection the controller deems fit to send traffic.

Benefits of SDN and SDN planes

- Security is both a benefit and a concern with SDN technology.
- The centralized SDN controller presents a single point of failure and, if targeted by an attacker, can prove detrimental to the network.
- SDN Planes:
- Data plane refers to all the functions and processes that forward packets/frames from one interface to another.
- Control plane refers to all the functions and processes that determine which path to use. Routing protocols, spanning tree, ldp, etc are examples.
- Management plane is all the functions you use to control and monitor devices.
- These are mostly logical concepts but things like SDN separate them into actual devices.
- Finally, all manufacturers use these concepts.

S No	Control Plane	Data Plane
1	The control plane process is responsible for building and maintaining the IP routing table.	The data plane process is responsible for actual forwarding of IP packet.
2	Makes decisions about where traffic will be sent. Control Plane = Learning what we will do.	Forwards traffic to the next hop along the path to the selected destination network according to control plane logic. Data Plane = Actually moving the packets based on what we learned.
3	Control plane packets are destined to or locally originated by the router itself.	Data plane packets go through the router.
4	Control plane packets are processed by the router to update the routing table information.	The routers/switches use what the control plane built to dispose incoming and outgoing frames and packets
5	Control plane is the process of learning what we will do before sending the packet or frame.	Data plane is moving the actual packets based on what we learned from control plane.
6	Routing (exchange of routing information) is performed in the control plane.	Switching (packet forwarding) is performed in the data (forwarding) plane
7	Includes STP, ARP, DHCP, RIP, OSPF etc.	Includes decrementing TTL, recomputing IP header checksum etc.
8	Router inserts the results of the control-plane protocols into Routing Information Base (RIB) and Forwarding Information Base (FIB).	Data plane software or ASICs uses FIB structures to forward the transit traffic.

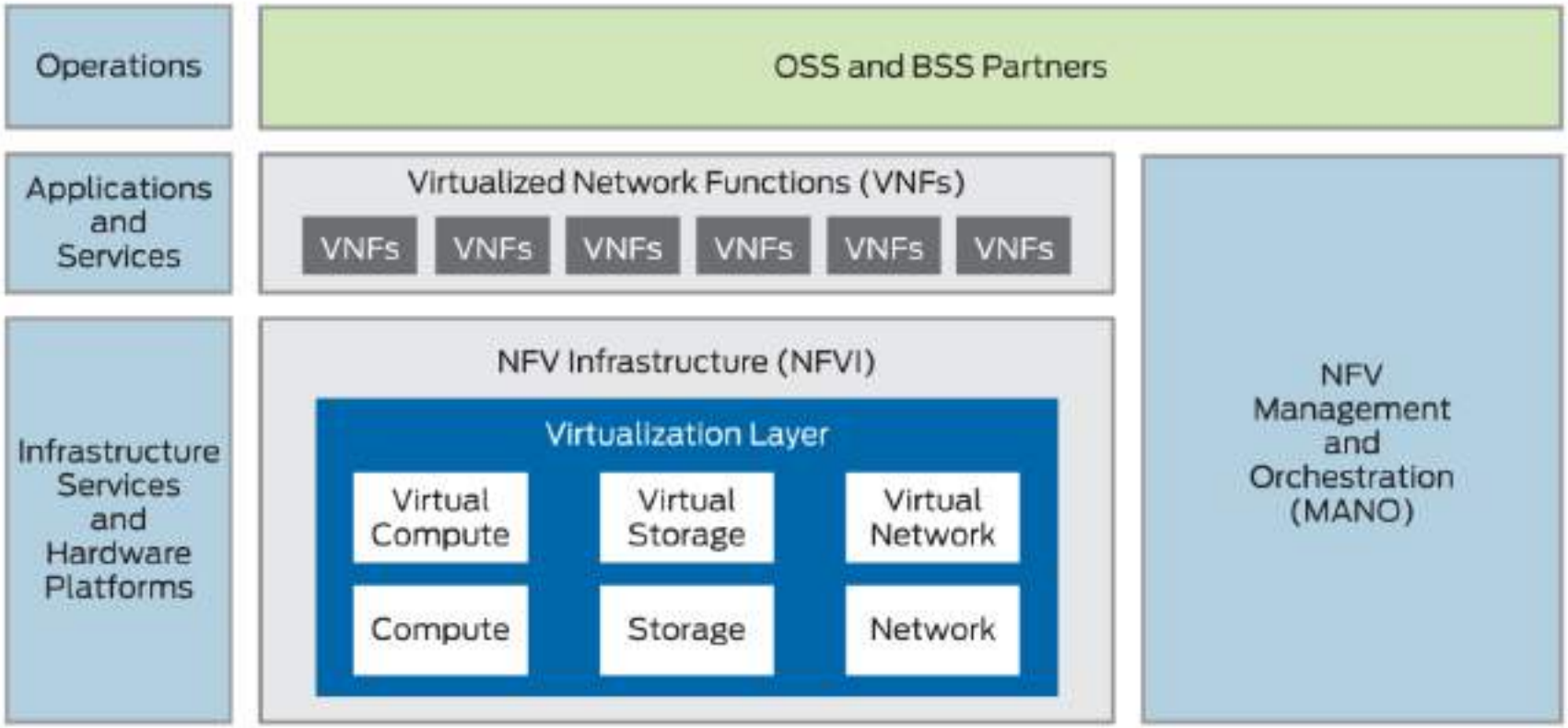
NFV

- **Network functions virtualization** (also **network function virtualization** or **NFV**) is a network architecture concept that uses the technologies of IT virtualization to virtualize entire classes of network node functions into building blocks that may connect, or chain together, to create communication services.
- VNF 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.

- NFV infrastructure (NFVI) building block—Provides the virtualization layer (hypervisors or container management systems such as Docker), and the physical compute, storage, and networking components that host the VNFs. NFVI is managed through the NFVI infrastructure manager (VIM), which controls the allocation of resources for the VNFs. OpenStack is an example of an open source VIM, controlling the physical and virtual resources. VMWare is an example of a commercial VIM.
- VNFs—Software-based applications that provide one or more network services. VNFs use the virtualized infrastructure provided by the NFVI to connect into the network and provide programmable, scalable network services. VNF Managers support the lifecycle of VNF instances and management of a VNF software.

- Management and orchestration (MANO)—Provides the overarching management and orchestration of the VNFs in the NFV architecture. MANO instantiates the network services through the automation, provisioning, and coordination of workflows to the VIM and VNF Managers that instantiate the VNFs and overlay networking service chains. MANO connects the NFV architecture with the existing OSS/BSS.

Architecture of VNF



Benefits

- 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

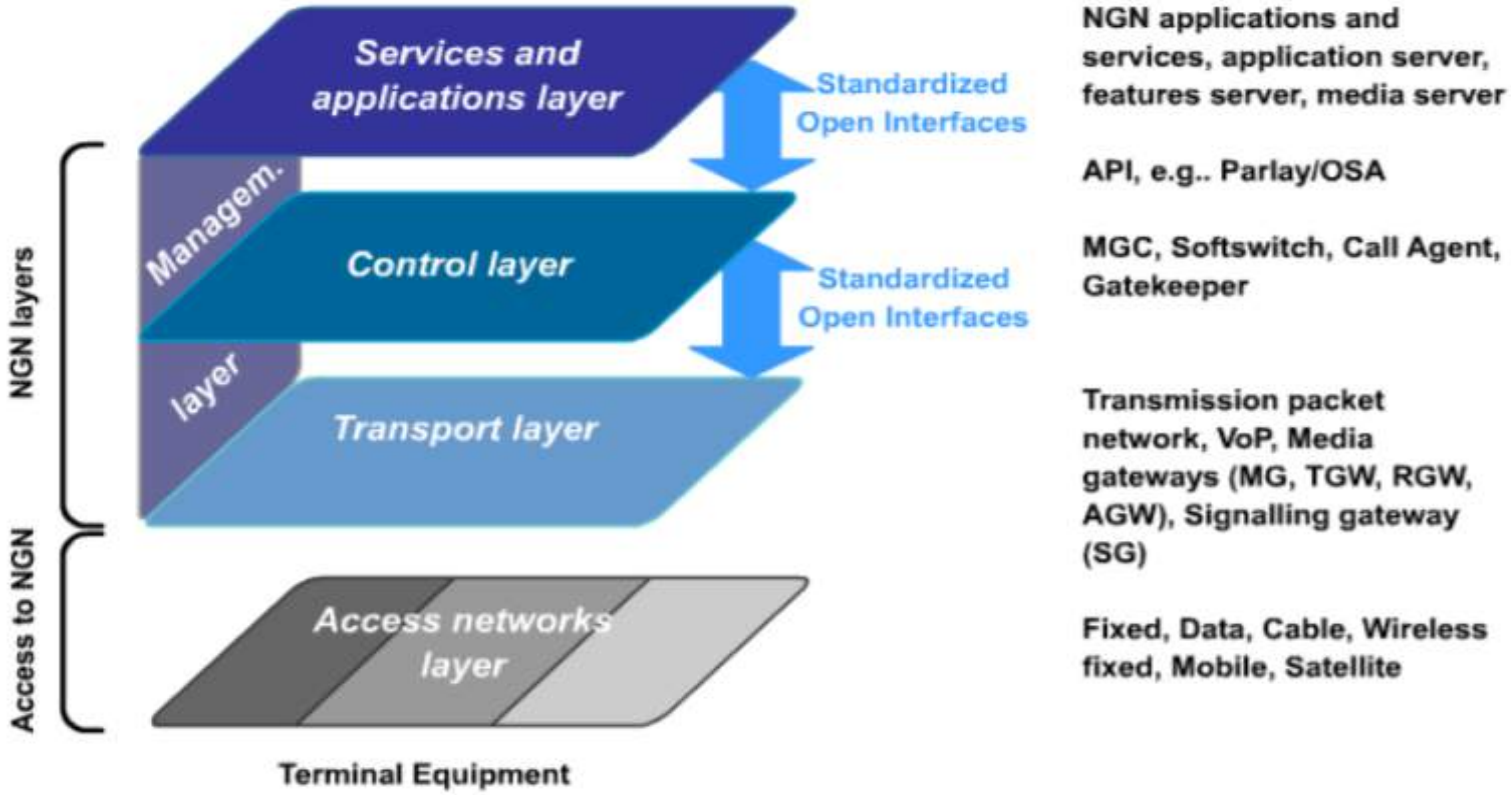
NGN(Next Generation Network)

- A multi-service network able to support voice, data and video
- A network with a control plane (signaling, control) separated from the transport/switching plane
- A network with open interfaces between transport, control and applications
- A network using packet mode technology to transport of all kind of information
- A network with guaranteed QoS for different traffic types and SLAs (SLA refers to service-level agreement)
- NGN is a network based on packet transfer, enabling to provide services, including telecommunication services, and is capable of using several broadband transmission technologies allowing guaranteeing QoS. The functions related to services are at the same time independent of the basic transmission technologies. NGN provides unlimited user access to different service providers. It supports general mobility providing the users with consistency and availability of services.[ITU)

Characteristics

- Packet-based transfer
- Separation of control functions among bearer capabilities, call/session, and application/ service
- Decoupling of service provision from network, and provision of open interfaces
- Support for a wide range of services and applications
- Broadband capabilities with end-to-end QoS
- Interworking with legacy networks via open interfaces
- Generalized mobility
- Unrestricted access by users to different service providers
- Converged services between Fixed/Mobile
- Compliant with all Regulatory requirements, for example concerning emergency communications and security/privacy, etc

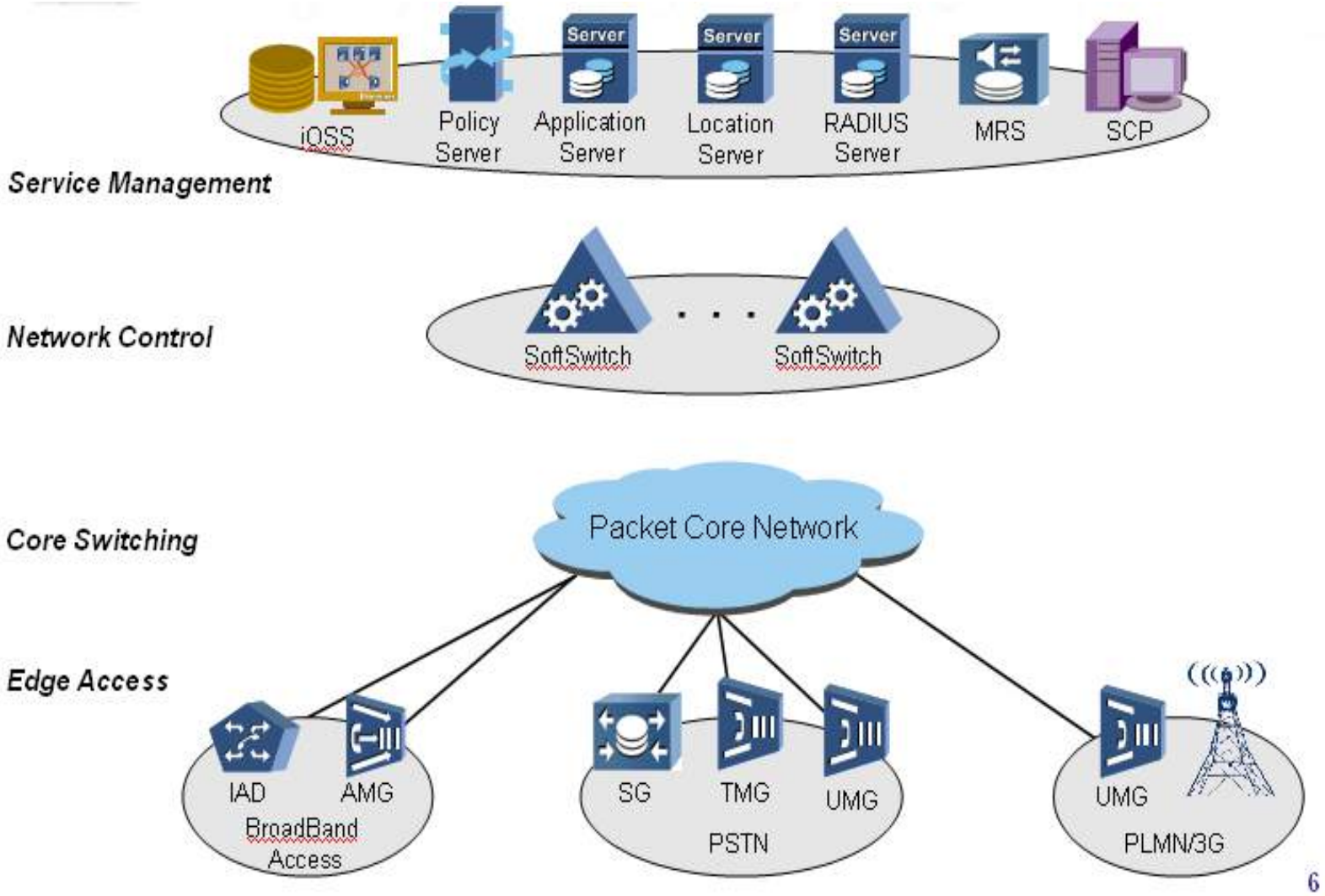
NGN Layers


Services and applications layer
Standardized Open Interfaces
Managem.
Control layer
Standardized Open Interfaces
layer
Transport layer
NGN layers
Access networks layer
Access to NGN
Terminal Equipment
NGN applications and services, application server, features server, media server
API, e.g.. Parlay/OSA
MGC, Softswitch, Call Agent, Gatekeeper
Transmission packet network, VoP, Media gateways (MG, TGW, RGW, AGW), Signalling gateway (SG)
Fixed, Data, Cable, Wireless fixed, Mobile, Satellite

NGN Layers

- The access layer provides the infrastructure, for example an access network between the end user and the transport network. The access network can be both wireless and fixed and it can be based on various transport media.
- The transport layer ensures the transport between the individual nodes (points) of the network, to which are connected access networks. It connects physical elements deployed in the individual layers It also enables the transport of different types of traffic, media (signalling, interactive data, real-time video, voice communication, etc.)
- The control layer includes the control of services and network elements. This layer is responsible for set-up/establishing, control and cancelling of the multimedia session. It ensures the control of sources as well, depending on the service requirements. One of the fundamental NGN principles is the separation of control logic from the switching hardware.
- The service layer offers the basic service functions, which can be used to create more complex and sophisticated services and applications. It controls the progress of the service based on its logic.

NGN Network Architecture



NGN Applications