FINAL REPORT

ITU-D STUDY GROUP 2

QUESTION 26/2

MIGRATION FROM EXISTING NETWORKS TO NEXT-GENERATION NETWORKS FOR DEVELOPING COUNTRIES: TECHNICAL, REGULATORY AND POLICY ASPECTS

5TH STUDY PERIOD 2010-2014

Telecommunication Development Sector

CONTACT US

Website: www.itu.int/ITU-D/study_groups
ITU Electronic Bookshop: www.itu.int/pub/D-STG/
e-mail: devsg@itu.int
Telephone: +41 22 730 5999

QUESTION 26/2:

Migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspects

ITU-D Study Groups

In support of the knowledge sharing and capacity building agenda of the Telecommunication Development Bureau, ITU-D Study Groups support countries in achieving their development goals. By acting as a catalyst by creating, sharing and applying knowledge in ICTs to poverty reduction and economic and social development, ITU-D Study Groups contribute to stimulating the conditions for Member States to utilize knowledge for better achieving their development goals.

Knowledge Platform

Outputs agreed on in the ITU-D Study Groups and related reference material are used as input for the implementation of policies, strategies, projects and special initiatives in the 193 ITU Member States. These activities also serve to strengthen the shared knowledge base of the membership.

Information Exchange & Knowledge Sharing Hub

Sharing of topics of common interest is carried out through face-to-face meetings, e-Forum and remote participation in an atmosphere that encourages open debate and exchange of information.

Information Repository

Reports, Guidelines, Best Practices and Recommendations are developed based on input received for review by members of the Groups. Information is gathered through surveys, contributions and case studies and is made available for easy access by the membership using content management and web publication tools.

Study Group 2

Study Group 2 was entrusted by WTDC-10 with the study of nine Questions in the areas of information and communication infrastructure and technology development, emergency telecommunications and climate-change adaptation. The work focused on studying methods and approaches that are the most suitable and successful for service provision in planning, developing, implementing, operating, maintaining and sustaining telecommunication services which optimize their value to users. This work included specific emphasis on broadband networks, mobile radiocommunication and telecommunications/ICTs for rural and remote areas, the needs of developing countries in spectrum management, the use of ICTs in mitigating the impact of climate change on developing countries, telecommunications/ICTs for natural disaster mitigation and relief, conformance and interoperability testing and e-applications, with particular focus and emphasis on applications supported by telecommunications/ICTs. The work also looked at the implementation of information and communication technology, taking into account the results of the studies carried out by ITU-T and ITU-R, and the priorities of developing countries.

Study Group 2, together with ITU-R Study Group 1, also deals with Resolution 9 (Rev. WTDC-10) on the “Participation of countries, particularly developing countries, in spectrum management”.

This report has been prepared by many experts from different administrations and companies. The mention of specific companies or products does not imply any endorsement or recommendation by ITU.

Table of Contents

Figures and Tables

Page

Page

QUESTION 26/2
Migration from existing networks to next-generation networks for developing countries: technical, regulatory and policy aspects

1 Migration to NGN

1.1 Why is There a Need for Migration?

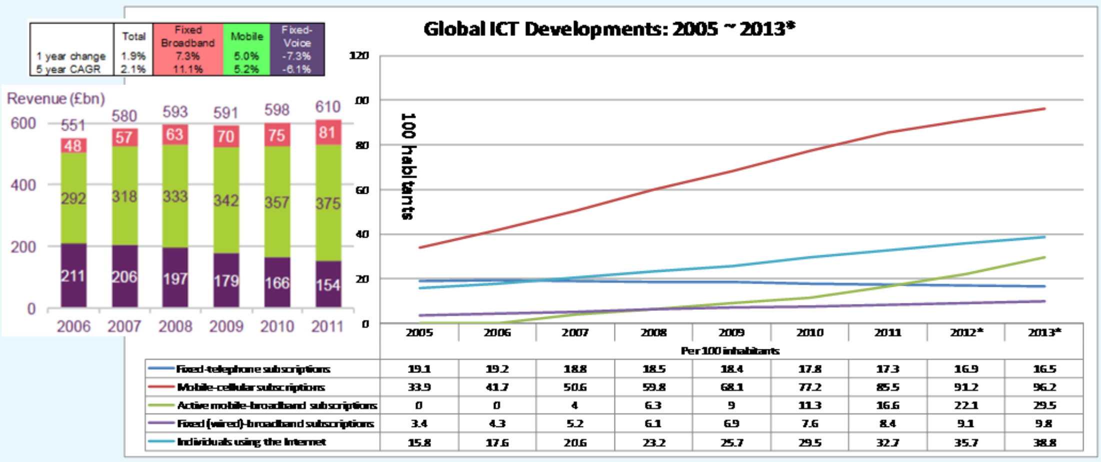
This section describes motivations to migrate from legacy network infrastructure to the new network infrastructure. There are several reasons according to the different viewpoints such as business aspects, technical aspects and etc.

1.1.1 General Motivation for Migration

One of the important factors to consider migration to the new network infrastructure such as NGN is that following the trend caused by the business flows.

One of the critical point of the business flows is the movement of voice services from legacy fixed based (e.g. PSTN and ISDN) to mobile and IP based. As shown in Figure 1-1 below, this trend has been triggered since the year 2003 and is being continued. This trend caused two directions: one is for reducing revenue of fixed voice services (e.g. falling down of fixed voice revenue around -6% during the 2006 and 2011 period and the other is requesting more mobile oriented services and IP based capabilities over fixed and/or mobile broadband on their networks which requests additional investment in addition to the legacy network infrastructure (e.g., increasing revenue of mobile 5.2% and broadband around 11% during the period 2006 to 2011).

Figure 1-1: Status of ICT developments



Source: IDATE/industry data/Ofcom 2012

There are several ways to meet these trends and it could be classified two ways: Compensate reduction of revenue and finding new revenue sources.

For the compensation of revenue reduction, cost reductions by sharing network infrastructure and systems should be the most important point in addition to the reduction of network and service infrastructure deployment cost. Followings are requirements in this sense and are caused to consider migration to NGN:

- Reduced OPEX and enhancing streamline operations.
- Integrated platforms for provisioning of various types services and applications.
- Integrated operation platforms including integrated maintenance and training.
- Centralized Management and Control.

In general, providing commercial multimedia services in economic ways should be the one of strong candidate in the viewpoints of finding new revenue sources. In this regard, followings should be considered as high level requirements when provide multimedia services and will be leaded reasons of migration to NGN:

- Compensate voice revenue reduction and increase Broadband related businesses.
- Providing Service innovation (e.g. VPN).
- Decreased time to market to introduce any new types of services and applications.

1.1.2 Operator's View on Migration

Meeting the business trend is also very serious subject to the operators, because they position in the center of these trends. That is, operators should be prepared, as soon as possible, that their service provisioning and operation will be enough to compensate falling down of their revenue stream. And their new systems and any elements will be enough to provide new revenue timely manner when they introduce those into their infrastructure.

Followings are taking into account when operators are willing to introduce new infrastructures:

- Support of business continuity required to maintain ongoing dominant services and customers that require carrier-grade service.
- Flexibility to incorporate existing new services and react quickly to the ones that appear on real time (well utilize main advantage of IP mode).
- Profitability to allow feasible return on investments and in the best practices market values.
- Survivability to allow service assurance in case of failures and external unexpected events.
- Quality of Service to guarantee the Service Level Agreements for different traffic mixes, conditions and overload.
- Interoperability across networks to allow the carrying of end to end services for flows in different network domains.

It is generally recognized that NGN should one of the dominant candidate to fulfill those requirements. Therefore, many operators start migration of their legacy infrastructure to NGN and even some of them already migrate to NGN.

1.1.3 Technical View on Migration

There are many of technical issues on the today's internet even use of IP technology which is used also in NGN. These technical issues caused certain difficulties to resolve requirements of network operators and service providers. In addition, more technical issues are coming from handling the media effectively such as IPTV. Therefore it is required to develop completely new technology or additional capabilities on top of current IP when IP use.

Key summary of technical issues are shown in Table 1.

NGN according to its definition given by the ITU-T Recommendation Y.2001 announced as one of the strongest candidate to solve many of these technical issues even not all of them. So most of industries are being developed NGN systems and operators are being migrated of their legacy telecom infrastructure based on NGN.

Table 1-1: Technical issues for migration

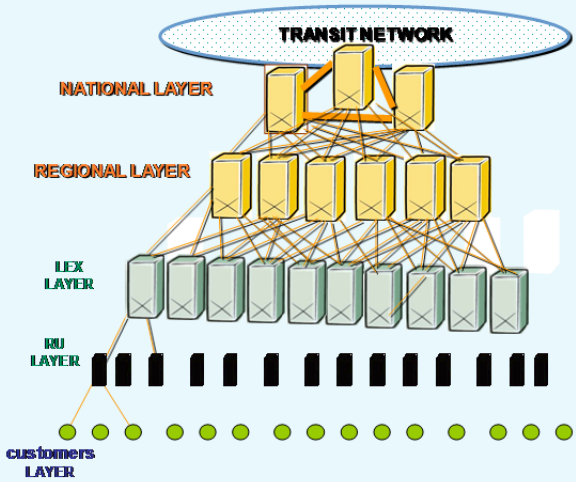
Technical Area	Issue
Management	Scalability Billing
QoS & security	Higher reliability Higher resiliency Secure systems Robustness Performance Application performance Authentication, Authorization and Accounting
Ubiquity	A ubiquitous network enabling user to be connected – always on, anytime, anywhere, anyhow Presence awareness
Content	Digital Rights Management (DRM) Conditional access Secure and efficient delivery
Network optimization	Common services infrastructure Fewer number of network nodes Fewer switching operations Simplified service deployment Higher capacity
Interoperability	Interoperable equipments from all vendors
Multitude of access networks	Fixed, mobile, copper, fibre, wireless… Support of multiple connections Transparent mobility across wireline & wireless
Shared resources	Shared transport resources for both voice & data Shared service platforms as much as possible
Mixing of traditional and internet service	Ability to combine traditional legacy communication services and IP-based services
Interactivity	End-to-end interactivity (e.g., Personalized interactive multimedia communication, etc.) Client-Server interactivity (e.g., Gaming: High performance and low latency) User controlled interactivity (e.g., anycasting, m-to-n interactivity, etc.)
Storage	Business continuity Sharing storage in public (e.g., NPVR and Cloud computing) and in private (e.g., PVR) Data retention
Standards compliant	Implementing standards compliant devices Standardized protocols and interfaces

1.1.4 Architectural Considerations

One of tradition in the legacy telecommunication has been constructed with several hierarchies. There are two aspects: one is for technology bases such as physical network, transport network and service network etc., and the other is geometric distribution basis such as Remote access network, access network, regional network and national network etc. These hierarchies are generally very helpful not only for installation and operation but also system developments. And these hierarchies are quite well fitted with traditional telephone based service provision and network operation, in terms of identification, that is, E.164 number based.

However these hierarchies are becoming bottleneck, especially properly providing end to end connectivity and handling routing effectively taking consideration of various IP features such as using flat address and dynamic routing. Therefore legacy hierarchies are subject for the preparation of IP based infrastructure. Following Figure 1-2 shows an architecture model of traditional telecommunication networks.

Figure 1-2: General architecture model of traditional telecommunication networks



Followings are summary of key features which traditional architecture model comprised.

- Hierarchical topology with 4 to 5 layers, connectivity to the upper next layer and within each layer as a function of economical optimization.
- Number of nodes as a function of output data traffic and nodes capacity.
- Service handling for media, signalling, control and management at all exchange nodes.
- Carrier grade quality with well-defined QoS criteria and standardized engineering rules.

While try to keep good features of existing infrastructure, it is required to improve certain features to meet the moving trend. Following aspects should be taken into account in this regard:

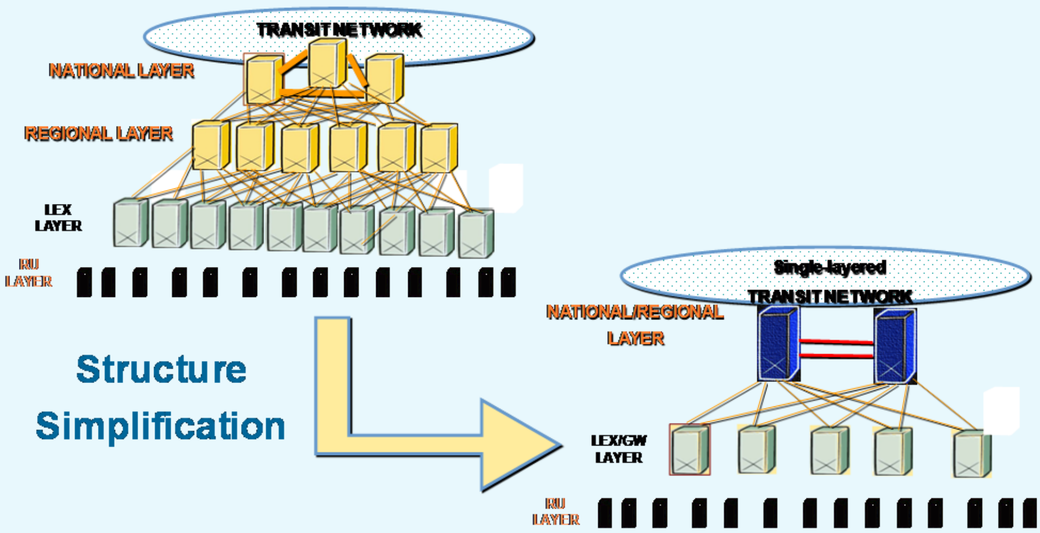
- Less network nodes and links due to the higher capacity of systems (one order of magnitude).
- Same capillarity at access level due to identical customer location.
- Topological connectivity higher for high capacity nodes and paths due to security.
- High protection level and diversity paths/sources in all high capacity systems, both at functional and physical levels.

Taking consideration of above rationale, it is anticipated that new infrastructure should be built with simple architecture than existing one. Following Figure 1-3 would be one of example for this anticipation.

Such simpler architecture will give many of benefits in addition to resolve issues which are resided in legacy telecommunication infrastructure. One of important benefits should be addressed in the access networks which are dominated by physical infrastructure cost and deployment time. This benefit is obtained through shorter local loop length than classical networks and paves the way for high bandwidth Multimedia services.

This simpler architecture will allow quick deployment of broadband capabilities by using xDSL and/or Fiber optic closer to customer when implementing new outside plant or renovating existing one. In addition, this will also give flexibility to introduce new Wireless technologies for low density customer. All these enhancement of access networks equipped with fixed and mobile broadband capabilities will provide very flexible ways to provide various multimedia services covering fixed and mobile convergence situation.

Figure 1-3: Way of improving the architectural aspect



1.2 NGN as a Migration Path

1.2.1 Features of NGN

The full name of NGN is "Next Generation Network" so the name itself does not give enough information to understand the overall pictures. Thanks to ITU-T developed clear definition and various key features to identify NGN in more details including service and functional aspects. ITU-T Recommendations Y.2001 and Y.2011 provide us the definition of NGN and its features in the sense of agreed in global consensus.

The ITU-T Recommendation Y.2001 identified the global definition of NGN such as "A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users."

In addition, Recommendation Y.2001 identified fundamental characteristics of NGN as following:

- packet-based transfer;
- separation of control functions among bearer capabilities, call/session, and application/ service;
- decoupling of service provision from transport, and provision of open interfaces;
- support for a wide range of services, applications and mechanisms based on service building blocks (including real time/ streaming/ non-real time and multimedia services);
- broadband capabilities with end-to-end QoS (Quality of Service);
- interworking with legacy networks via open interfaces;
- generalized mobility ;
- unfettered access by users to different service providers;
- a variety of identification schemes;
- unified service characteristics for the same service as perceived by the user;
- converged services between fixed/mobile;
- independence of service-related functions from underlying transport technologies;
- support of multiple last mile technologies;
- compliant with all regulatory requirements, for example concerning emergency communications, security, privacy, lawful interception, etc.

Looking at the definition and characteristics of NGN, following key features of NGN are derived and these should be a framework to understand and use 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.

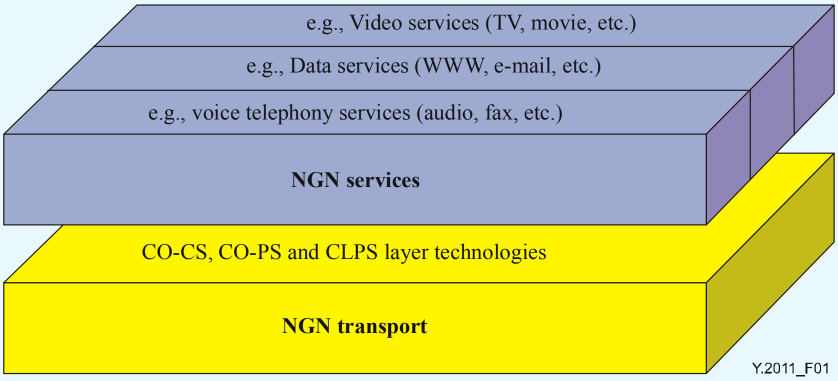
Comparing these key features which derived from the definition and characteristics of the NGN defined by ITU-T, it is recognized those features will provide certain conditions to resolve difficulties which coming from meeting the business trend described in Chapter 1.

1.2.2 Basic Reference Model for NGN Architecture

One of the beauties and the biggest challenge of the NGN is the separation between services from underline transport technologies. The basic reference model for NGN is shown in Figure 1-4 (ITU-T Recommendation Y.2011). This diagram shows the figure when services are separated from the underlying transport.

In general, any and all types of network technologies may be deployed in the transport stratum indicated as "NGN transport", including connection-oriented circuit-switched (CO-CS), connection-oriented packet-switched (CO-PS) and connectionless packet-switched (CLPS) layer technologies according to ITU-T Recommendations G.805 and G.809. Until today it is considered that IP is the preferred transport protocol used to support NGN services as well as supporting legacy services. The "NGN services" provide the user services, such as a telephone service, a Web service, etc. Therefore "NGN service" may involve a complex set of geographically distributed services platforms or in the simple case just the service functions in two end-user sites.

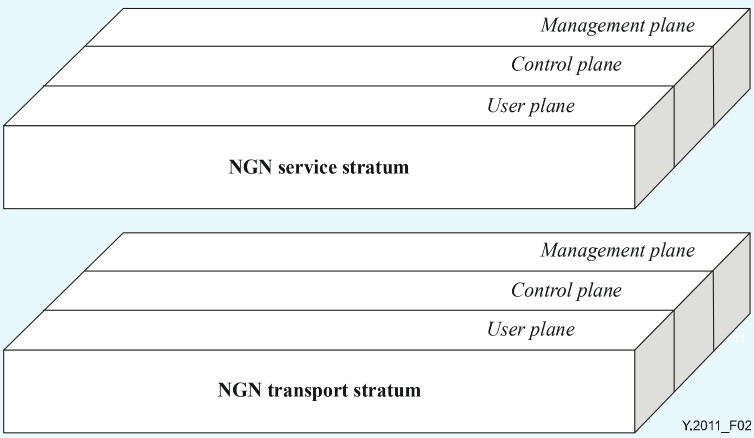
Figure 1-4: Separation of services from transport in NGN



ITU-T Recommendation Y.2011 uses a language to identify these two important aspects with the name of "NGN Service Stratum" and "NGN Transport Stratum" shown in Figure 1-5 and provides overall views to understand both two as following:

- **NGN service stratum**: That part of the NGN which provides the user functions that transfer service-related data and the functions that control and manage service resources and network services to enable user services and applications. User services may be implemented by a recursion of multiple service layers within the service stratum. The NGN service stratum is concerned with the application and its services to be operated between peer entities. For example, services may be related to voice, data or video applications, arranged separately or in some combination in the case of multimedia applications. From an architectural perspective, each layer in the service stratum is considered to have its own user, control and management planes.

Figure 1-5: NGN Basic Reference Model (NGN BRM)



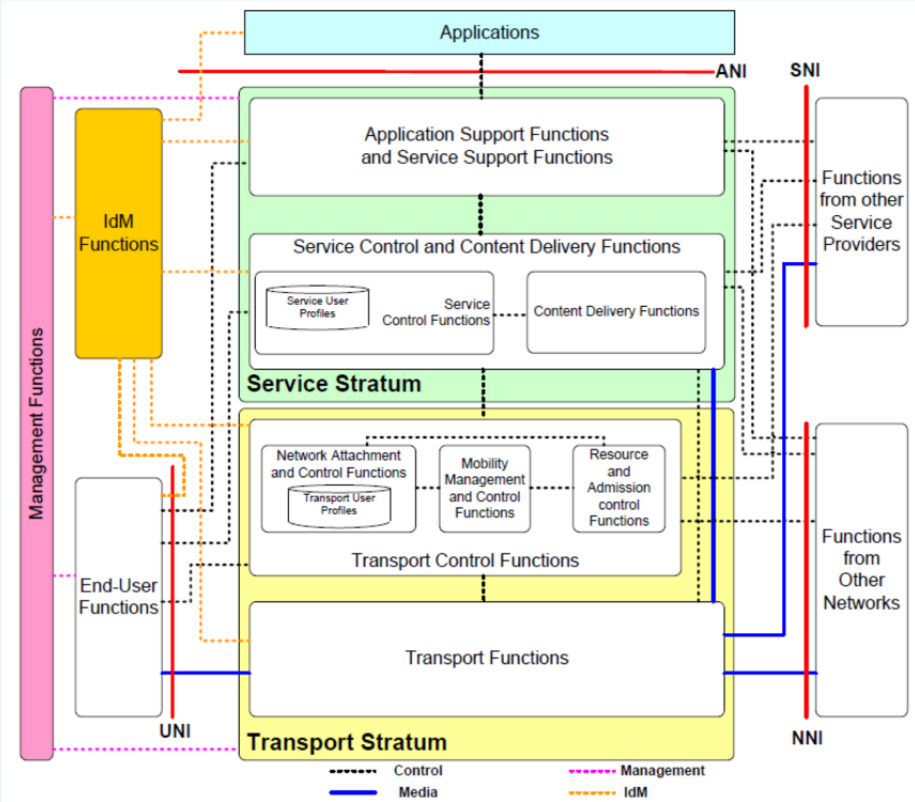
- **NGN transport stratum**: That part of the NGN which provides the user functions that transfer data and the functions that control and manage transport resources to carry such data between terminating entities. The data so carried may itself be user, control and/or management information. Dynamic or static associations may be established to control and/or manage the information transfer between such entities. An NGN transport stratum is implemented by a recursion of multiple layer networks as described in ITU-T Recommendations G.805 and G.809. From an architectural perspective, each layer in the transport stratum is considered to have its own user, control and management planes.

Based on the above basics of NGN architecture, ITU-T developed NGN architecture model with detailed functions and published by ITU-T Recommendation Y.2012 as shown in Figure 1-6.

NGN Architecture in ITU-T Recommendation Y.2012 has been developed to incorporate the following principles:

- Support for multiple access technologies: The NGN functional architecture shall offer the configuration flexibility needed to support multiple access technologies.
- Distributed control: This will enable adaptation to the distributed processing nature of packet-based networks and support location transparency for distributed computing.
- Open control: The network control interface should be open to support service creation, service updating, and incorporation of service logic provision by third parties.
- Independent service provisioning: The service provisioning process should be separated from transport network operation by using the above-mentioned distributed, open control mechanism. This is intended to promote a competitive environment for NGN development in order to speed up the provision of diversified NGN services.
- Support for services in a converged network: This is needed to generate flexible, easy-to-use multimedia services, by tapping the technical potential of the converged, fixed-mobile functional architecture of the NGN.
- Enhanced security and protection: This is the basic principle of an open architecture. It is imperative to protect the network infrastructure by providing mechanisms for security and survivability in the relevant layers.
- Functional entity characteristics: Functional entities should incorporate the following principles:
  - Functional entities may not be distributed over multiple physical units but may have multiple instances.
  - Functional entities have no direct relationship with the layered architecture. However, similar entities may be located in different logical layers.

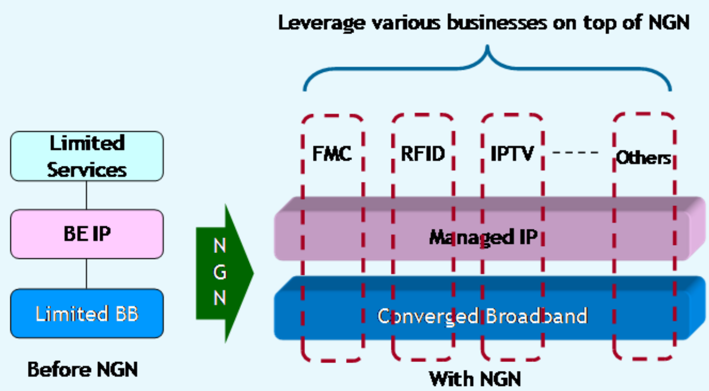
Figure 1-6: NGN architecture overview



1.2.3 Benefits from NGN Architecture

One of the greatest benefits of NGN architecture is support a way to provide various services over common transport platform. And various broadband technologies over fixed and mobile access network domains will give more opportunity to leverage this benefit such as providing various broadband and convergence services over fixed and mobile converged transport networks. Following Figure 1-7 shows how NGN architecture will support various services.

Figure 1-7: Benefits of NGN architecture



One of the advantages of using IP is providing the simple linkage between Layer 3 and Layer 4 which is the critical point of separation, in general, between service and transport. Before the NGN (shown in the left side of the figure), IP only provide one type of capability called "Best Effort" which could not support enough quality and security considerations. In addition, underlying transport has been relying on the very limited broadband capabilities provided by xDSL causing certain limitation to meet such business trend. This situation could not provide enough platforms to leverage convergence services and businesses.

After the NGN, enlarged capabilities in IP (called "Managed IP") and underline transport with converged broadband capabilities will provide a way to support various services (e.g. IPTV, RFIDs, FMC etc) over the common transport while keeping the simple linkage between Layer 3 and Layer 4. Consequently this will lead diverse business models and players to encourage diverse and flexible business relationships.

1.2.4 Enhancements to IMS for NGN Applications

The IMS specifications were developed for use with cellular access networks and were based on certain assumptions regarding the access network such as bandwidth available. Inherent differences between the different types of access networks will have concrete consequences on the IMS specifications. Examples of such consequences are:

- To Support xDSL based access networks the IMS may also need to interface to the Network Attachment functions of the IP-CAN, for the purpose of accessing location information. No equivalent interface exists in the base IMS specifications.
- Support of IPv4 has to be taken into account and this leads to a requirement to support NAPT functionalities. There are at least two reasons leading to this:
  - Some operators have (or will have) to face IPv4 addresses shortage.
  - Privacy of IP addresses for media streams cannot rely on RFC 3041 (Privacy Extensions for Stateless Address Auto-configuration in IPv6), as would have been the case for IPv6. NAPT provides an alternative for hiding terminal addresses.

Support of NAPT functionality is covered in the NGN Functional Architecture. Extensions to IMS for working with configurations containing NAPT need to be provided in the IMS specifications.

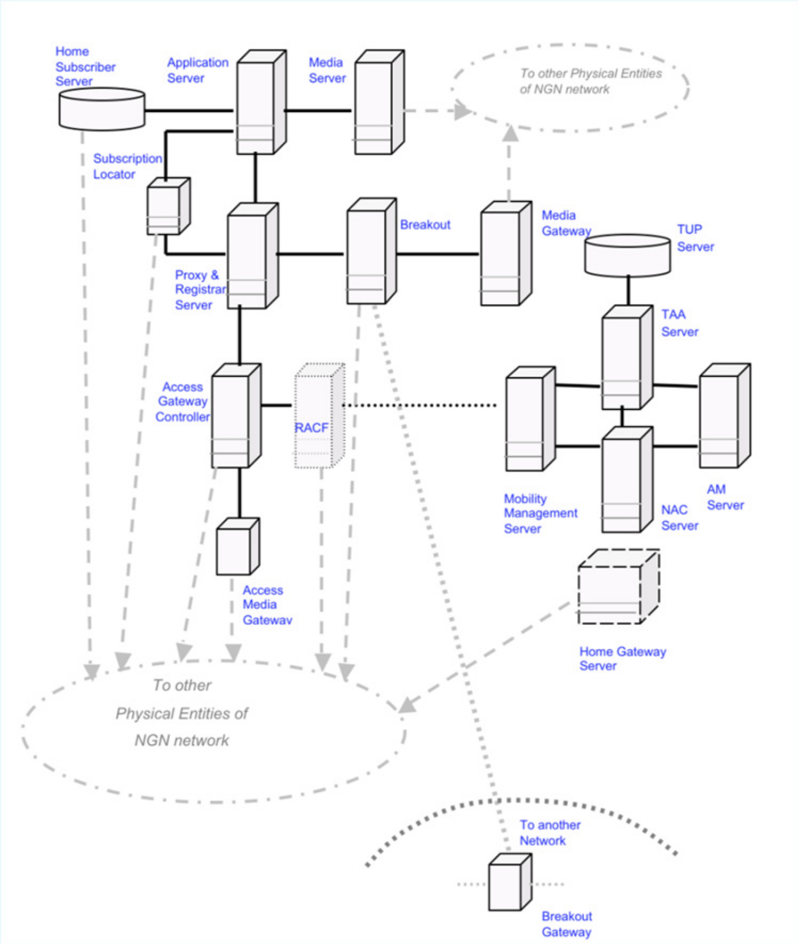
- Relaxing the constraints on bandwidth scarcity may lead to considerations for the optional support of some features that are currently considered mandatory (e.g.; SIP compression).
- Differences in location management will impact various protocols that convey this information, both on signalling interfaces and charging interfaces.
- Differences in resource reservation procedures in the access network will require changes to the IMS resource authorisation and reservation procedures, as the resource reservation procedures for xDSL access networks will have to be initiated by a network entity (i.e.; the P-CSCF in case of SIP-based services), on behalf of end-user terminals.

The above mentioned extensions are being examined by various standards bodies to support the use of IMS in NGN.

1.2.5 NGN Physical Architecture

A physical architecture of NGN identifies physical entities corresponding to the functional entity or a group of functional entities specified in the generalised functional architecture of NGN. Through a physical architecture, the interoperability points between the physical entities are possibly identified for enabling interoperability between different physical entities within an NGN network. One of the possible physical architectural realizations of NGN, as an example, is shown in Figure 1-7:

Figure 1-8: Possible physical architecture for NGN



1.3 Ways for Migration to NGN

1.3.1 Considerations for Migration to NGN

Many of views and consideration would be carefully examined during the set up of migration plan for the new infrastructure because this will impact so many aspects to the related entities as well as communities. Migration of legacy network infrastructure such as PSTN/ISDN to NGN also will have huge impacts to whole of communication infrastructure.

In order to keep pace with technological developments and market expectations, it is necessary that either the systems are regularly upgraded or the systems are replaced by new technology without hampering the service. Replacement and upgrading of existing equipment to newer and advanced technologies is not only the requirement for providing newer services, but often time is spent for getting hardware and software support from the manufacturers. Manufacturers usually opt for such modifications to cope with technological evolution where the older versions of the equipments have to be replaced by more efficient, compact and dependable equipment that is also expected to provide better quality of service to the users.

Especially for service expansion in rural remote areas, it is preferable that migration to NGN should not be abrupt, and both the older and the newer technologies should co-exist for a reasonable period of time.

From the consumers' perspectives, they shall not be forced to replace their terminal equipments for the reason that their service provider has "upgraded" their system to NGN.

Taking consideration of this, ITU-T recommendation Y.2261 gives guidance when operator will build up a migration plan.

For migration of PSTN/ISDN to NGN, aspects identified in the followings are to be considered.

1.3.1.1 Signaling and Control

PSTN/ISDN uses signalling systems such as analogue line signalling, channel associated signalling (CAS) like signalling systems R1 [Q.310-Q.332], R2 [Q.400-Q.490], and common channel signalling (CCS), like SS7 or DSS1 [Q.931]. All these signalling systems are for the circuit switched networks. Since NGN transport is packet-based (and call and bearer are decoupled), other suitable types of signalling (e.g., BICC, SIP-I [Q.1912.5], etc.) may be required. Also, the signalling function and call control function may reside in more than one NGN element.

Since the NGN has to work with the PSTN/ISDN and other networks, interworking between NGN signalling systems and the legacy network signalling systems is required. Signaling aspects within the next generation corporate network shall remain independent from NGN access or core network signalling.

It is further anticipated that signalling aspects for access and core networks be independent in order to provide the possibility for a step-wise approach for migration to NGN.

1.3.1.2 Management

An NGN management system is comprised of three planes, namely the network management plane, the network control plane and the service management plane. Each of the three planes implements corresponding management functions to each layer in the NGN layered model.

Migration of PSTN/ISDN management (i.e., operations, administration and management) systems requires the ability to support the transition of PSTN/ISDN through intermediate stages towards NGN.

1.3.1.3 Services

PSTN/ISDN services which are traditionally provided by PSTN/ISDN exchanges may be provided by application servers (ASs) in NGN. It is expected that some or all of the legacy services will be provided by NGN. As the voice quality of PSTN service is regarded as the “best”, any migration from this “best” service to IP-based NGN would require assurance of services that are comparable to those offered by the legacy Class 5 (or, TDM) infrastructure.

However, there is no guarantee that all services will be provided when PSTN/ISDN is simulated.

Use of legacy terminals via adaptation to the NGN is expected in order to support existing services.

- Bearer services: While evolving from PSTN/ISDN to NGN, continuity of bearer services should be provided. Use of NGN to connect PSTNs/ISDNs shall be transparent for all bearer services. NGN should provide same or better QoS for PSTN/ISDN bearer services.
  - PSTN/ISDN simulation provides functionality that is similar but not identical to existing PSTN/ISDN bearer services.
  - PSTN/ISDN emulation shall be capable of providing all bearer services offered by PSTN/ISDN. However, there is no requirement for NGN to support all N-ISDN bearer services identified in the ITU-T I.230-series Recommendations.

- Supplementary services: While evolving from PSTN/ISDN to NGN, continuity of supplementary services should be provided to the extent practical. PSTN/ISDN emulation shall provide support for all supplementary services offered by PSTN/ISDN while PSTN/ISDN simulation provides functionality that is similar but not identical to existing PSTN/ISDN services. The NGN need not support all ISDN supplementary services identified in I.250 series of ITU-T Recommendations. NGN shall appear transparent when used to connect supplementary services between PSTNs/ISDNs.
- Operation, administration and maintenance (OAM): OAM functionality is used to verify network performance, and to reduce operational expenses by minimizing service interruptions, service degradation and operational downtimes. As a minimum, when performing PSTN/ISDN migration to NGN, the ability to detect faults, defects and failures such as lost, errored or mis-inserted packets, should be provided. Additionally, there should be mechanisms to indicate connectivity status and provide support for performance monitoring.
- Naming, numbering and addressing: The NGN naming, numbering and addressing schemes, in accordance with ITU-T Recommendation Y.2001 shall be able to interwork with the existing E.164 numbering scheme. During PSTN/ISDN migration to NGN process, it should be ensured that the sovereignty of ITU Member States, with regard to country code numbering, naming, addressing and identification plans, is fully maintained. Also, as a minimum, support should exist for Internet IP addressing schemes including E.164 Telephone uniform resource identifiers (TEL URIs), e.g., tel: +98 765 4321 and/or SIP Uniform Resource Identifiers (SIP URIs), e.g., sip:my.name@company.org.
- Accounting, charging and billing: During the transition period, maintaining the existing accounting, charging and billing procedures, to the extent practical, may be required. Migration from existing networks to NGN will also imply replacement of the existing sources of the accounting data generation. The NGN shall support both offline and online charging.
- Interworking: Interworking is used to express interactions between networks, between end-systems, or between parts thereof, with the aim of providing a functional entity capable of supporting an end-to-end telecommunication. PSTN/ISDN migration to NGN should take the following into consideration:
  - Ability to interwork with legacy networks such as PSTN/ISDN and internet
  - Ability to interwork with IMS-based or call server based networks;
  - Ability for inter-domain, inter-area or internetwork interworking;
  - Support for authentication and authorization;
  - Ability to perform call admission control;
  - Capability to support network performance parameters as defined in [Y.1541];
  - Support for accounting, charging and billing.
- Call routing: When an NGN coexists with PSTN/ISDN, the routing scheme should allow the carriers to control where their traffic enters and leaves the NGN. This will make it possible for the carrier to optimize use of their network resources and to avoid multiple points of interworking between NGN and PSTN/ISDN along the media path.
- Service requirements by national regulatory bodies: Following requirements are required by national/regional regulation or law, an NGN service provider shall provide which means in the case of interworking:
  - the basic telephone service with the same or better quality and availability as the existing PSTN/ISDN;
  - the capability for accurate charging and accounting;

– capabilities to support number portability;
– the availability of a directory inquiry service for PSTN/ISDN and the NGN users;
– support of emergency telecommunications;
– support for all users, including the disabled. Support should provide at least the same capabilities as the existing PSTN/ISDN. NGN offers the opportunity for more advanced support, e.g., network capabilities for text to speech;
– mechanisms to support lawful interception and monitoring of various media types of telecommunications such as voice, data, video, e-mail, messaging, etc. Such a mechanism may be required of a network provider for providing access to content of telecommunication (CT) and intercept-related information (IRI) by law enforcement agencies (LEA), to satisfy the requirements of administrations and international treaties;
– interoperability between an NGN and other networks e.g., PSTN/ISDN and PLMN.

1.3.2 Generic Migration Procedure

Migration from one to other is not an easy or simple task because many of things are involved with various perspectives. Especially migration of network infrastructure need very careful plan and examine various aspects. As a conclusion, there is no single way or the best way for the migration to NGN, because migration should be based on each country situation as well as each operator given condition.

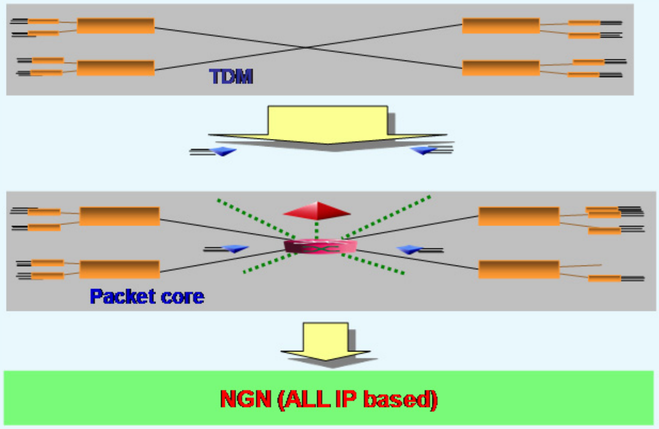
It is recommended to consider following procedure for building migration plan of legacy network infrastructure to NGN:

1. Provision of new communication services to broadband users in addition to existing network.
2. A significant portion of users switches to those services. Reduction of true PSTN/ISDN usage visible.
3. Cost of maintaining both systems in parallel becomes a factor. **Decision to begin replacement of infrastructure**.
4. Replacement of part of the infrastructure (e.g. local switch) by new infrastructure, **without forcing all users to migrate**.
5. Full change to new infrastructure.
6. Migrate remaining users to NGN.

1.3.3 Generic Way for Migration

Result of migration should be became "All IP environment" which is a key technology of the NGN, so from the technical viewpoints migration should be explained as change from "TDM based" to "IP based." Taking consideration of possession portions between "Access Network domain" and "Core Network domain" of each country, migration procedure should be applied to one of such domains first. It is general understanding that it is easier to set up migration plan for "Core Network domain" to. Core migration will have less impact on the service provision rather than "Access Network domain" migration. Figure 1-9 shows generic view of Core Network migration to NGN.

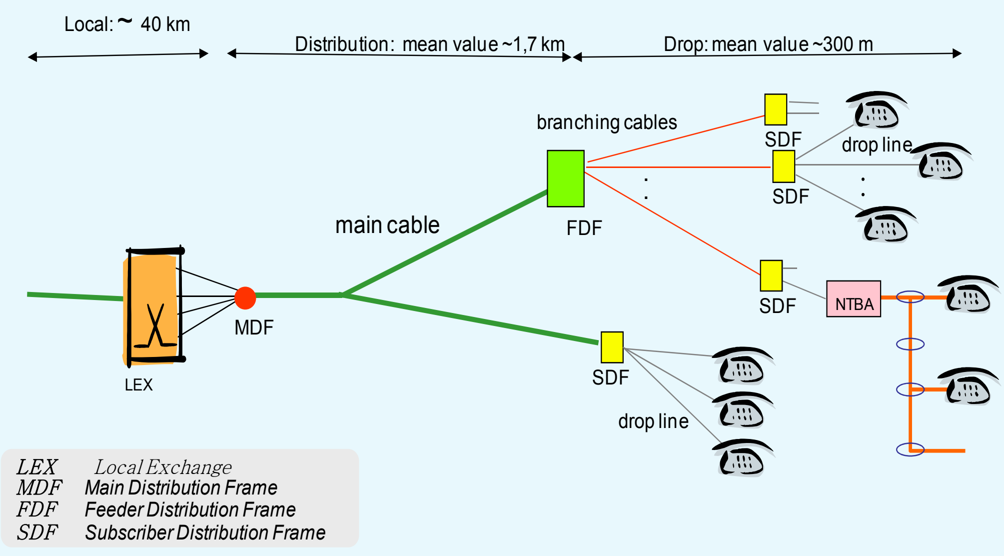
Figure 1-9: Generic view of core network migration to NGN



In the case of Access Network Domain which has quite complicated situations not only for technical aspects but also geographical differences, it is not recommended to choose one specific technology to replace any legacy access network systems. It is rather recommended to consider harmonization among different technologies to cover customer requests in more flexible and economical way. Many of different access technologies are developed using fixed and mobile with supporting broadband connectivity. And most of technology also provides IP connectivity which is the critical technical feature to meet NGN requirements (e.g. Packet based transfer).

In case of fixed based access networks, xDSL technology is mainly used to provide broadband today. The final goal in the fixed network will be to deploy fibre based infrastructure. xDSL gives the possibility to utilize existing copper based access infrastructure as much as possible for deploying broadband infrastructure in economic way, but with limited capacity (maximum few 10s Mbps). Fiber optics is a kind of target technology in the area of fixed networks with its unlimited capacity not only for core networks but also access networks including home network as well. Only concerns are related to the cost and construction difficulties. Both concerns will be faced by the quick development of the technology. Therefore it is recommended to use both xDSL and Fiber together in the access network as a preparation of migration to NGN including preparation of enough broadband capability. Following Figure 1-10 shows an example how access networks constructed taking consideration of geographical distances.

Figure 1-10: Generic view of access network (fixed) migration to NGN



Another important area should be utilize mobile (including wireless such as WiFi and WiMAX) to provide broadband connectivity. This aspect is also very important because many of people, especially in developing regions, uses mobile phone for their life communication and mobile will provide mobility to the people. There are many technologies to provide broadband capability in mobile access networks including IP connectivity but still has certain limits on the providing bandwidth (around 10 Mbps). Standard organizations are working hard to develop technologies for better bandwidth but will take a time. Following Figure 1-11 shows an example diagram how different mobile technologies are used in the access networks and Figure 1-12 shows a diagram mixed between mobile and fixed.

Figure 1-11: Application of different mobile access technologies

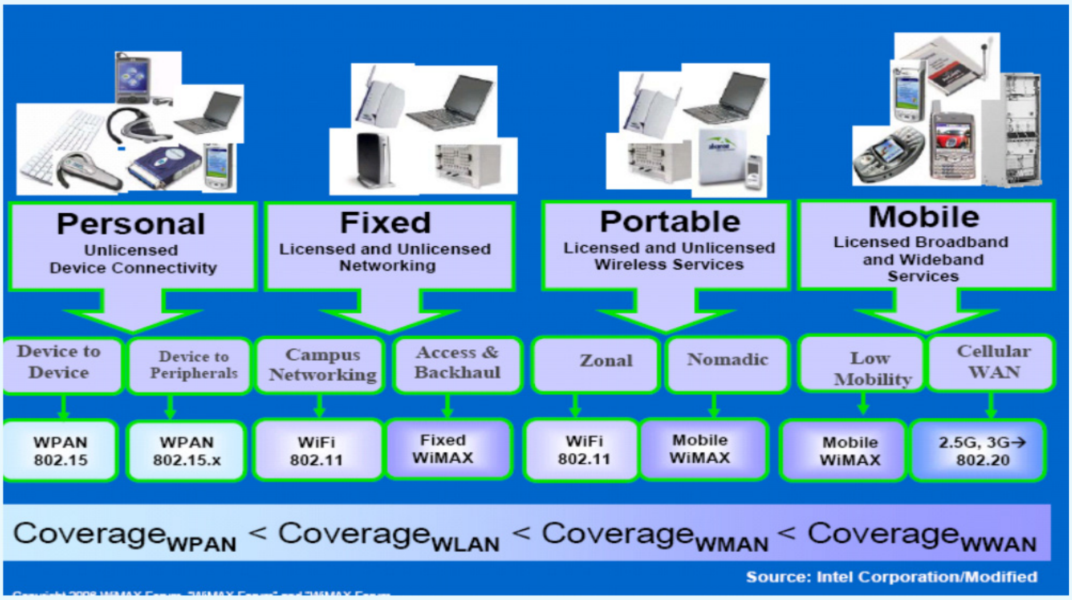
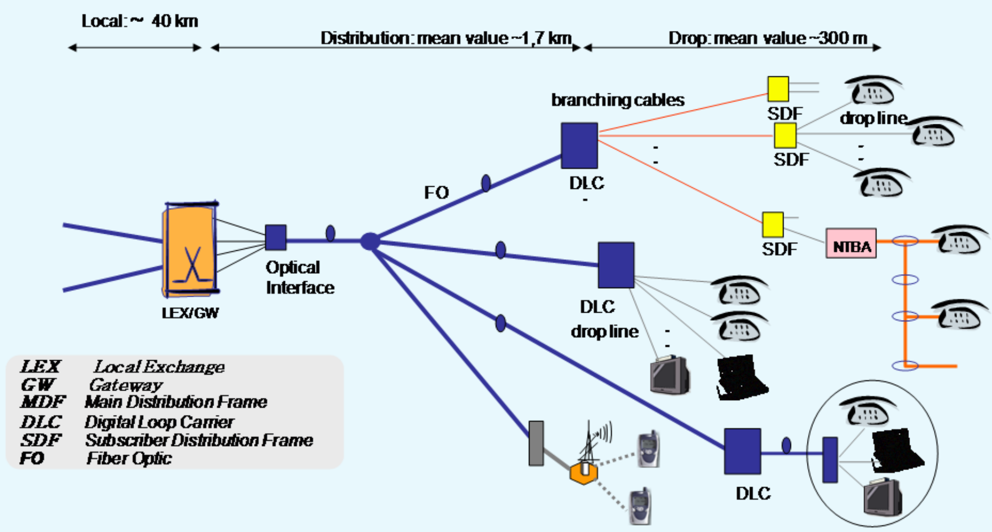


Figure 1-12: Generic view of access network (mixed) migration to NGN



1.3.4 NGN Technology for Support Migration

To help migration of legacy networks to NGN at least voice based services, NGN provides two capabilities. One of this is "Emulation" which supports provision of PSTN/ISDN service capabilities and interfaces using adaptation to an NGN infrastructure using IP. The other is "Simulation" which supports provision of PSTN/ISDN-like service capabilities using session control over IP interfaces and infrastructure.

1.3.4.1 Emulation Scenario

Following Figure 1-13 shows a high level view of emulation scenario. Using NGN Emulation capability which provides "Adaptation Function (ADF)" legacy terminal devices such as black phone connects to the NGN and uses their services with following aspects:

- An encapsulation process.
- All services available to PSTN/ISDN users.
- User experience not changed by the network transformation.

Figure 1-13: NGN emulation of PSTN/ISDN

1.3.4.2 Simulation Scenario

Simulation is for providing PSTN/ISDN like service to the NGN users. So NGN users will communicate with PSTN/ISDN users using this simulation capability. Key features of NGN Simulation summarizes following:

- PSTN/ISDN-like services available.
- Availability of possible new services.

- User experience is changed by the network transformation.

Figure 1-14: NGN Simulation Scenario-1 of PSTN/ISDN

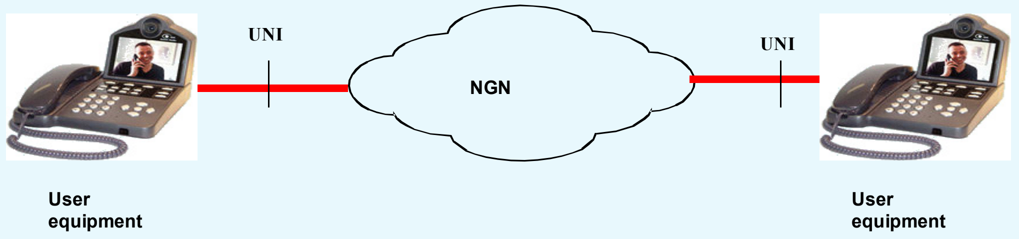
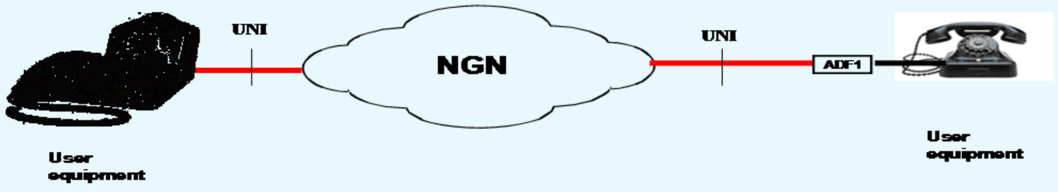


Figure 1-15: NGN Simulation Scenario-2 of PSTN/ISDN



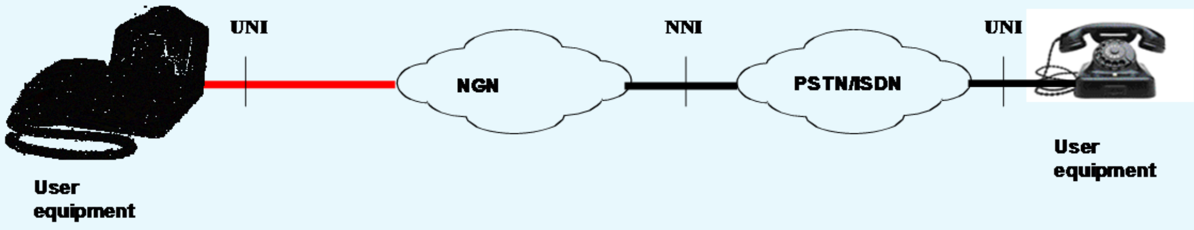
1.3.4.3 Interworking using Emulation and Simulation

Taking into consideration the importance of voice services, NGN voice oriented services should be linked with voice services in PSTN/ISDN environment. To support of this requirement, emulation and simulation jointly are used for interworking between NGN and legacy networks such as PSTN/ISDN. It will be decided according to the interworking situation which technology would be used in which area.

Figure 1-16 shows an example of interworking between NGN and legacy PSTN/ISDN. Simulation is used in NGN side while interworking with legacy side is using emulation. Service features in this case are characterized as following:

- Service interworking between NGN and PSTN/ISDN is required
- Only PSTN/ISDN-like services available
- Legacy terminal user experience cannot be fulfilled for end-to-end connection

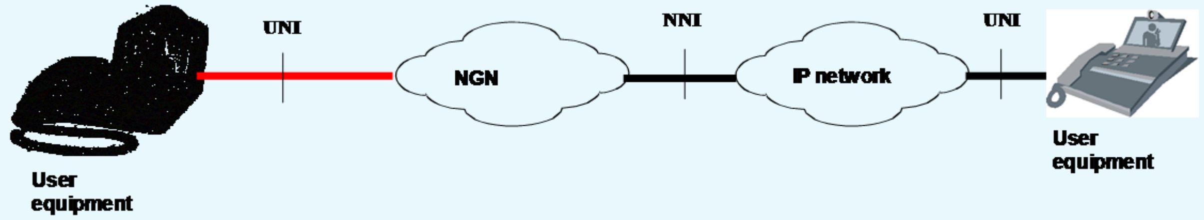
Figure 1-16: Interworking-1 between NGN emulation and simulation



Following Figure 1-17 shows another example of interworking between NGN and legacy IP based network which support voice service (e.g. VoIP). Simulation is used in NGN side while interworking with legacy side is using emulation. Service features in this case are characterized as following:

- Service interworking between NGN and IP network is required.
- Both the NGN and IP network user experiences may not be fulfilled for end-to-end connection.

Figure 1-17: Interworking-2 between NGN emulation and simulation

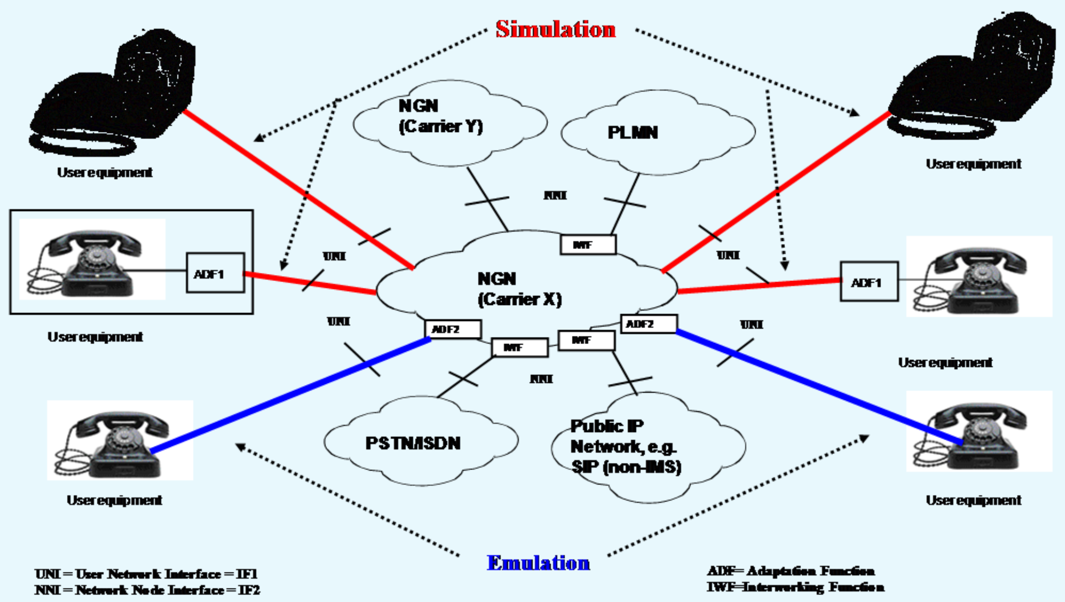


1.3.4.4 Overall Configuration using Emulation and Simulation

Key requirement of Emulation and Simulation technology is supporting voice oriented services. PSTN/ISDN is a major network infrastructure today to support voice services including various supplement services especially in case of ISDN. In addition, there are continuously increasing end users of using voice services over legacy IP environment.

Therefore NGN should support its voice related capabilities such as emulation and simulation to cover PSTN/ISDN and legacy IP based networks. So combination of these capabilities with proper interworking scenarios will help to support end user voice service requirements in the cases of end user device connected to fixed, mobile and legacy IP based to cover voice services wherever end user places. Following Figure 1-18 shows overall configuration model of using emulation and simulation with indicating interworking situation combined.

Figure 1-18: Overall view of using NGN emulation and simulation



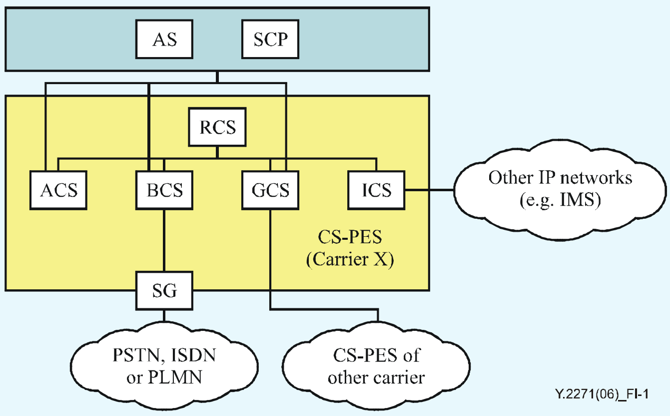
1.3.4.5 Call Server Supporting Migration to NGN

The Call Server is the core element for PSTN/ISDN emulation which is responsible for call control, gateway control, media resource control, routing, user profile and subscriber authentication, authorization and accounting. The call server may provide PSTN/ISDN basic service and supplementary services, and may provide value-added services through service interaction with an external service control point (SCP) and/or Application Server in the service/application layer.

A call server may function in one or more of the following roles as identified in ITU-T Recommendation Y.2271 and Figure 1-19 shows an example of the deployment:

- Access call server (ACS) – to implement access gateway control and media resource control functions, thus providing PSTN/ISDN basic service and supplementary services;
- Breakout call server (BCS) – to implement interworking functions to enable interconnection with PSTN/ISDN networks;
- IMS call server (ICS) – to provide interoperability between PSTN/ISDN emulation components and IP multimedia components within a single NGN domain;
- Gateway call server (GCS) – to provide interoperability between different NGN domains from different service providers;
- Routing call server (RCS) – to provide the routing function between call servers.

Figure 1-19: Call server deployment example

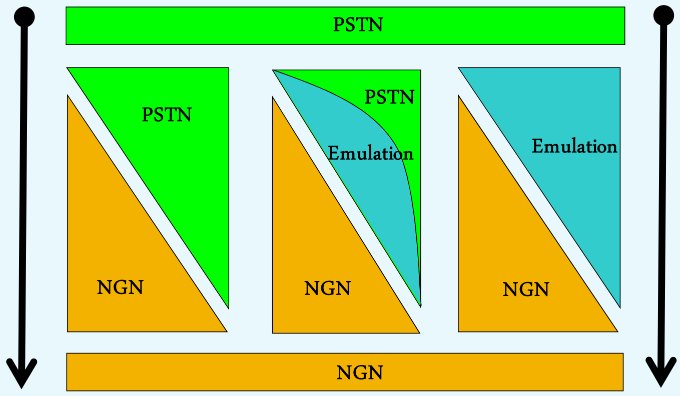


AS: Application Server, SCP: Service Control Point, SG: Signaling Gateway, PES: PSTN Emulation Service Component.

1.4 Migration Scenarios

Using emulation and/or simulation of NGN, there are various ways of migration from legacy network to NGN. This should be decided according to the each country or provider situation. In this report, three different types of migration scenarios are introduced as a framework consideration but other possibility should not be limited. Following Figure 1-20 shows a pictorial explanation of these three types of migration from PSTN/ISDN to NGN.

Figure 1-20: Overall migration scenarios



The three scenarios are the following:

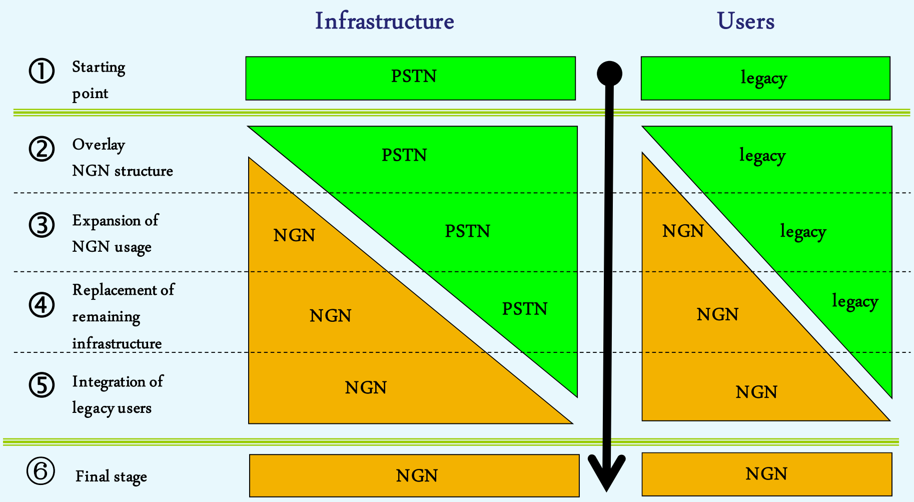
- Overlay Scenario (Left Side of Figure 1-20): NGN will be deployed and operate jointly with PSTN/ISDN. NGN will occupy more portions while PSTN/ISDN will continuously decrease and finally migration to NGN.
- Replace Scenario (Right Side of Figure 1-20): NGN emulation will widely use to support voice oriented services but keeping the legacy terminal such as black phone. So end user could not recognize the change of technology behind their terminal.
- Mixed Scenario (Middle of Figure 1-20): This is a scenario to use both overlay and emulation, so at the beginning some of PSTN user connection will replace by NGN emulation while other PSTB users will keep their PSTN connections. And according to the increase of NGN deployment, Emulation and PSTN users will replaced by NGN users.

1.4.1 Overlay Scenario

This Overlay Scenario will be useful in the case of country or operator who have well stable or new PSTN/ISDN infrastructure. In this case, it is hard to justify replace all PSTN/ISDN equipments to NGN because this legacy infrastructure could not yet return value to compensate all their investment. And the status of infrastructure is quite good stage and will use next several years without any serious amount of operation, administration and maintenance including fault management.

Through this scenario, operator will be gradually preparing enough resources for the next investment while keeping their customers in a good situation. In addition to this, operator will also meet users' requirements which use advanced capabilities through newly deployed NGN. According to the increasing of users who wish to use advanced capabilities, then operator will expand the coverage of NGN and consequently will decrease customers in legacy networks. Finally someday will fully deployed of NGN and cover all users. In this case, NGN users will communicate with PSTN/ISDN users using their simulation but through interworking between NGN and PSTN/ISDN networks. Following Figure 1-21 shows the steps of this scenario.

Figure 1-21: An overlay migration scenario

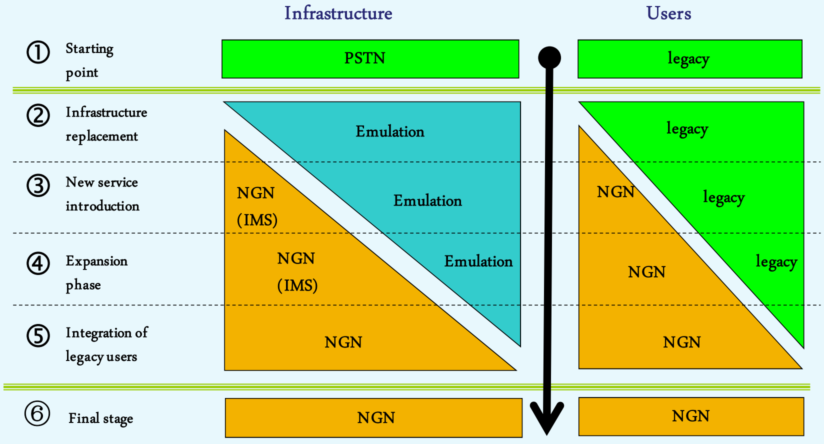


1.4.2 Infrastructure Replacement Scenario

This scenario will be useful in the case of country or operator who does not have enough PSTN/ISDN infrastructures, where there is already lack of connectivity to support voice services. In this case, it is hard to continue the deployment of PSTN/ISDN equipments because this will also need new investment while investment for NGN will be also necessary. But in this case, current users even using PSTN/ISDN will be continuously supported without any change of their terminal if possible.

Through this scenario, operator will stop their deployment of PSTN/ISDN but replaced investment to NGN. Then operator will provide ADF (Adaptation Function) to the current PSTN/ISDN users to provide continuous usage of voice services which means expansion of NGN emulation capabilities as shown in Figure 1-22. And according to the increasing of users who wish to use advanced capabilities, then operator will expand the coverage of NGN and consequently will decrease customers who using emulation services. Finally someday all users will be fully covered by NGN capabilities. Following Figure 1-20 shows the steps of this scenario.

Figure 1-22: An infrastructure replacement migration scenario

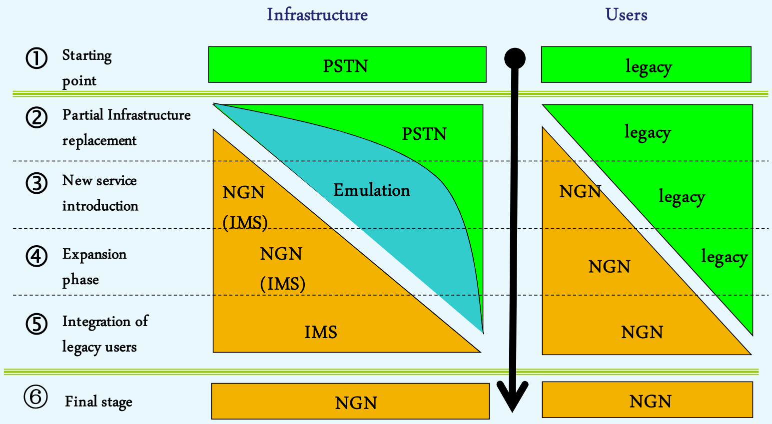


1.4.3 Mixed Scenario

This scenario will be useful in the case of country or operator who is placed in the middle stage, i.e. some parts of PSTN/ISDN need to be replaced but other parts of PSTN/ISDN are still in good and stable status using new PSTN/ISDN infrastructure. In this case, considerations from both overlay and replacement scenarios should be taken into account. That is, operator should keep PSTN/ISDN networks with relevant customers until the time of returning their investment or the status of PSTN/ISDN will request serious amount of operation, administration and maintenance including fault management which means time to replacement. In other direction, operator will start to deploy NGN infrastructure replacing other parts of PSTN/ISDN which reach to time to replacement. Figure 1-23 shows the steps of this scenario.

Through this scenario, operator will be gradually preparing enough resources for the next new investment while keeping their customers in PSTN/ISDN situation. In addition to this, operator will also meet users' requirements which use advanced capabilities through newly deployed NGN. According to the increasing number of users who wish to use advanced capabilities, operator will expand the coverage of NGN and consequently will decrease the number of customers in legacy networks. The final solution will be to fully deploy of NGN for covering all users.

Figure 1-23: Mixed migration scenario



2 Technology Developments for NGN Migration

The last 10 years or more have seen an increasingly fast integration of information and communication, both equipment and networks. Traditional public network operators have seen a decrease in telephony traffic on their Public Switched Telecommunications Networks, due in part to the increasing popularity of Mobile Telephones and the movement of services from Telephone Networks to the Public Internet.

The concept of a new, integrated broadband network has developed over the last several years and has been labelled "Next Generation Network: NGN".

The basic characteristics of an NGN can be determined from the problems faced by the network operators: the need to provide services over broadband accesses (to increase revenue); the need to merge diverse network services – data (web browsing), audio, telephony, multimedia and emerging "popular" internet services such as Instant Messaging and Presence and broadcast type services; and the desire of customers to be able to access their services from anywhere (inherent mobility). Rather than a network to provide a specific solution (such as the PSTN), what was needed for the next generation was a series of networks that could support a flexible platform for service delivery.

2.1 Service Aspects

Understanding the service requirements should be the 1st step for all telecommunication developments and in this regard, identify the media characteristics should be the initial phase to identify the services. According to the development of processors enhancing processing powers and semi-conductor technology producing small enough to mount on board lead the requirements to use diverse multimedia in various ways which need broadband connectivity an any cases of fixed or mobile.

Table 2-1 shows high level abstract view of media requirements in terms of bandwidth and QoS aspects. Many of services except normal voice required broadband at least 2 Mb/s with high priority treatment for ensuring QoS requirement. To support these trend of services, it is highly requested networks be equipped with enough capabilities to manage traffics (e.g. sessions, flows etc.) whatever broadband connectivity provided with over provisioning or well managed. NGN provides one of way to meet these requirements in carrier class level but in managed way.

Table 2-1: Media service requirements

Service	Bandwidth (downstream)	QoS Requirement
Broadcast TV (MPEG-2)	2 to 6 Mb/s	Parameterized
HDTV (MPEG-4)	6 to 12 Mb/s	Parameterized
PPV or NVoD	2 to 6 Mb/s	Prioritized
VoD	2 to 6 Mb/s	Prioritized
Picture in Picture (MPEG-2)	up to 12 Mb/s	Parameterized
PVR	2 to 6 Mb/s	Prioritized
Interactive TV	up to 3 Mb/s	Best effort
High speed Internet	3 to 10 Mb/s	Best effort
Video Conferencing	300 to 750 Kb/s	Prioritized
Voice/Video Telephony	64 to 750 Kb/s	Prioritized

2.2 Access Transport Technology

As explained above, supporting various types of multimedia is required that networks are equipped with enough bandwidth and traffic management capabilities. Ensuring required bandwidth is the initial point to support these service (and media) requirements. There are two perspectives to provide bandwidth: over fixed and over mobile.

Mobile networks are still on-going of their development. Benefiting the mobility, mobile access is a crucial access for the nomadic users such as business people and students etc., using connectivity wherever they stay or move.

In recent years, the interest in frequency ranges between 57and134 GHz for wireless communication applications has increased significantly, because of the potential for wide bandwidth implementations, which meet the growing requirement for high data rate applications in the range of hundreds of Mbit/s, including last-mile connectivity. Various short distance link configurations may be expected in these bands, including high-density applications.

Wireless solutions in the 60/70/80/95 GHz bands are presently available but the system cost is not yet competitive with lower frequency technologies. Design challenges at these frequencies still exist. For 60/70/80/95/120 GHz band range systems to be competitive with those at lower frequencies, the volume of deployed systems needs to be very high.

The very high operating frequencies in the 60/70/80/95/120 GHz bands permit the design of small size high gain antennas with directive beams. Therefore, for communication devices in close proximity, practical antennas could be designed to form small mesh radio networks with minimum interference.

Examples of outdoor/indoor applications that could benefit from the 60/70/80/95/120 GHz bands:

- wireless local area networks (WLANs) and wireless personal area networks (WPANs);
- microcellular and frequency reuse architecture, e.g. fixed links for mobile;
- high-resolution nomadic multimedia services;
- wireless video distribution systems;
- wireless communications serving underground tunnels and large convention halls;
- wireless links with data rates up to and greater10 Gbit/s.

The advantages of using the 60/70/80/95/120 GHz bands include:

- frequency reuse in dense areas with reduced potential for undesired interference;
- use of smaller size antennas (antenna gains are proportional to the antenna dimension and the wavelength);
- small size radio equipment as to provide nomadic applications;
- narrow antenna beam-widths (antenna beam-width is inversely proportional to the operating frequency) which reduce interference and increase frequency reuse;
- potential frequency sharing feasibility with other radio services;
- support for high capacity transmission due to their wider usable bandwidth (Shannon's Law).

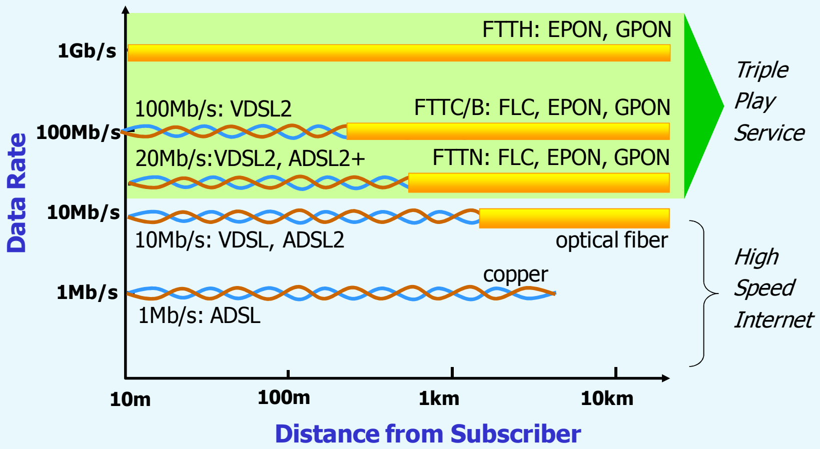
The disadvantages of these bands include:

- signal obstruction by an object or persons;
- oxygen absorption in the 60 GHz range;
- susceptibility to outage in heavy rain and snow-fall regions;
- unsuitable for long-haul transmission.

In fixed networks, since provide the xDSL which is very popular broadband access in the world (actually the best technology to build up broadband today) fibre based broadband is becoming deploy now in various countries with FTTC (Fiber to the Curb) and FTTH (Fiber to the Home). With the development of PON (Passive Optical Network) 100 Mb/s is now available to everyone in economic way. Therefore many of developed country cases, business users are being cover by the fibre and some of home also.

As shown Figure 2-1, fibre based technology provide much longer distance than legacy accesses with enough bandwidth. This feature contributes greatly to enlarge providing broadband connectivity including rural areas. Especially combination of fibre with xDSL support economical provision of broadband extending distance to reach end users but keeping broadband capabilities e.g. FTTC with VDSL provide 30 Mb/s to the household.

Figure 2-1: Transmission technology developments

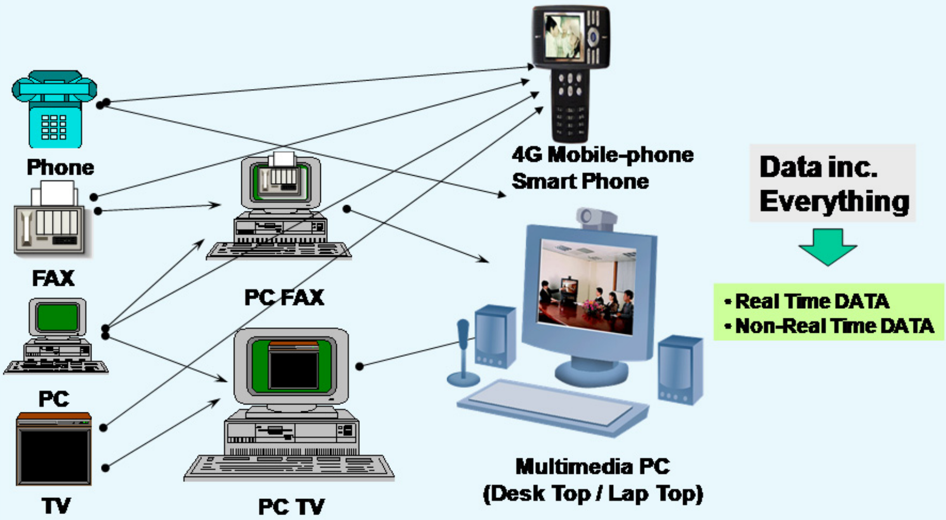


2.3 Terminal Device Development

Thanks to the processing technology developments, terminal devices have been remarkably developed and are continuing now. During the last decade, terminal devices especially with Lap Top computer and mobile phones including smart phone (e.g. PDA) have been kept the leading role of most of telecommunication services developments. Portable and smart are major key themes in this developments.

As shown in Figure 2-2, legacy terminal functions for graphic, text and video are integrated into one physical device such as PC based or mobile based. Voice service function also very well developed and integrated into small piece called mobile phone and this function also incorporated into PC consisting integrated multimedia terminal device. With this integration, all traffic types are change to "Data" including voice, so output signal of terminal device should be "Data but with real time or non real time differences." This integration of various functions into Lap Top PC is resulting nomadic life such as moving personal office etc.

Figure 2-2: Terminal device development

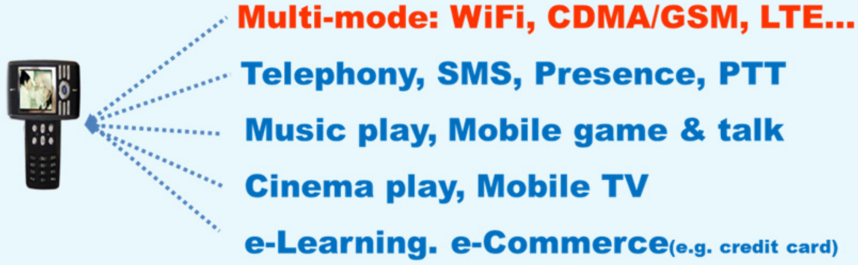


Out of this development, mobile terminal device should be one of the remarkable one to enhancing our ICT life. Mobile phone is not anymore only phone, this becomes smart handheld device allowing people to communicate anywhere and anytime including personal entertainments (Figure 2-3)

Figure 2-3: Mobile terminal device development

As a result of his development, end user terminal device, even single device such as a smart mobile phone, is now ready to support most multimedia services as shown in Figure 2-4.

Figure 2-4: Various services over multi-function terminal device



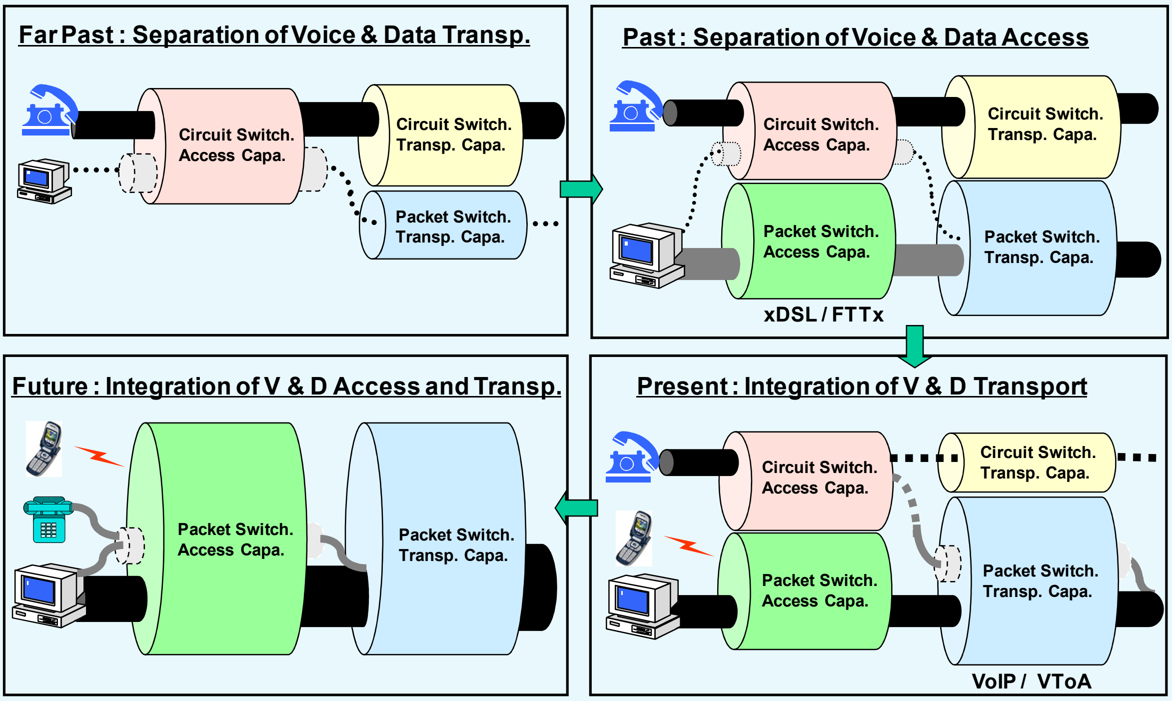
2.4 Telecom Network Development

Many technologies are developed and used in networks not only for mobile but also fixed networks. It is quite hard to analyze such developments in detail like in this short report. Therefore this report tries to analyze big stream to evolve the telecommunication networks today and future.

One of important changes or direction to lead the evolution of telecom networks should be the change from "Circuit" to "Packet." Until the end of 1980s, change to analog to digital was the biggest theme for the telecom network development such as the initiation of ISDN etc. But since the introduction of IP technology in the middle of 1990s, circuit based networks migration to packet based is the most crucial point for the development. Figure 2-5 shows an abstract view of the efforts technology developments did and future direction.

- Far Past: Telecommunication networks were quite clearly separated based on the services such as voice and data. So PSTN has been developed for voice services including voice-band data such as for facsimile, and PSDN has been developed for data communications. But both networks used circuit technology for access to the networks.
- Past: Packet technologies widely deployed in most of networks not only for core networks similar as far past but also access networks. This has been mainly derived by the IP technology supporting the xDSL and remarkable contribution to build up connected world. There were several data services still used circuit access such as using modem.
- Present: Packet capability is the major capability which provided by the telecom networks whatever voice and data including mobile communications. Benefiting broadband accesses, this packet based infrastructure covers many of multimedia services including voice. But still circuit based networks position as a major network for voice services while some of voice service using circuit access start to transport by the packet core.
- Future: It is expected that packet capabilities to cover all areas of networks such as access and core networks. And this will support not only for multimedia but also voice services over fixed and mobile together with broadband capability.

Figure 2-5: Trends in telecom network development



Note: V: Voice, D: Data.

2.5 Numbering and Routing Aspects

2.5.1 Numbering and Naming

Individual users will be identified by names or numbers and a name/number resolution system will be used to translate a given name/number into a routable address in the network. Since NGN and traditional networks will exist in parallel for some time to come, NGN must be able to support the existing Naming, Numbering and Addressing plans for fixed and mobile networks. The international numbering plan for telephony is defined in ITU-T recommendation E.164, while ITU Recommendation Y.2001 "general overview of NGN" addresses the topic of numbering, naming and addressing in a NGN. An address is an identifier for a specific termination point and used for routing to this termination point. Routing is the process of distributing and collecting topology-related information, calculating the routes, establishing and maintaining the routing table in the network (Y.2612). In traditional analogue networks numbers were used to address network elements. In digital switches addressing is decoupled from numbering. Numbering schemes are, however, rather long lived, since customers know and use numbers and CPE integrate them.

But in case of NGN, another URI i.e. SIP URI can also be thought of. In case of VoIP calls the TEL URI or SIP URI will be converted to IP address via DNS (Domain Name System). SIP URI can be in service provider domain or self-provided domain. Some of the examples of SIP URIs are as follows:

SIP: 911125368781@<dummy> > E.164 format only

SIP: 911125368781@opr1.in > E.164 + service provider domain

SIP: abc@opr2.in > Name + service provider domain

Therefore existing numbering scheme may be used in NGN as well. For the network and end user, it does not make any difference in the numbering scheme. The soft-switch and SIP server will be responsible for the routing of calls based on the E.164 number. All the SIP subscribers will be assigned by an E.164

number. The SIP server functionality of soft-switch will create a database for all such SIP subscribers in which the IP address allocation vis-à-vis E.164 number be stored. The routing of call from PSTN to SIP subscriber will be done based on this database table. The biggest advantage of this approach is to keep the same numbering scheme as the existing one. The end users will not be confused with the introduction of new technology for carrying voice in the network.

Number/name resolution is traditionally done by routing tables in individual digital exchanges. In the Internet the domain name system (DNS) is used for number/name resolution. Since NGN are packet switched networks and are using the IP protocol, DNS will probably be the logical choice for number/name resolution mechanism within an NGN.

E.164 **NUM**bering (ENUM) is the mapping of telephone numbers to Uniform Resource Identifiers (URIs) using the Domain Name System (DNS). ENUM enable convergence between the PSTN and IP and is using the DNS thus saving the capital expenditure.

Each service provider would need internal ENUM DNS which support numbering and routing and it sits in common backbone of that operator. Using this type of concept the operator can use their existing numbering scheme along with the existing Carrier Identification Code which is as follows:

(Area Code: 2to 4 Digits) + (Carrier Identification Code: 1 Digit) + (Subscriber Number: 5 to 7 Digits)

All the PSTN and IP switch should terminate on common IP backbone of that operator where the DNS is connected. The DNS derive the routable address of the destination and terminate the call. Also by using the Global DNS the Routing and switching is possible in multi-operator, multi-service network scenario.

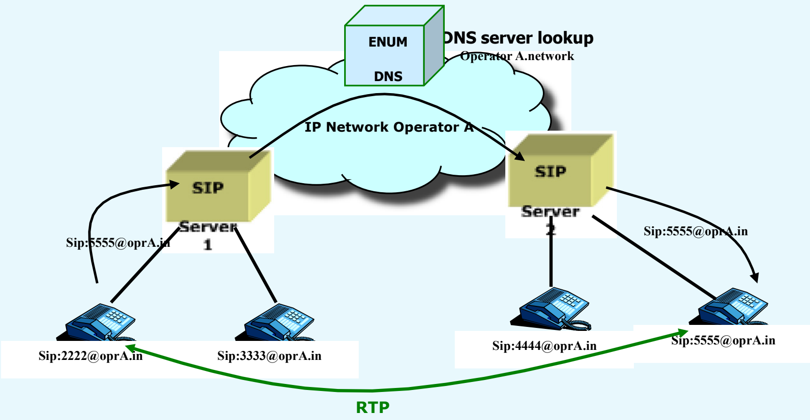
For calls from IP to PSTN, the destination's telephone number can be represented as a SIP URI. For these calls, the gateway strips out the telephone number and uses it to initiate the call using ISUP signalling.

This allows to present an E.164 number as a URI that can be resolved into an IP address by the DNS. The main political discussion is focusing on the tree to be used for telephone numbers. It was envisaged to agree on a world-wide tree (called "golden tree"), however, the e164.arpa tree is only one of the options implemented today. In context with the discussion of the golden tree is the search for a business model for ENUM. The original vision of ENUM was a global, public directory-like database, with subscriber opt-in capabilities and delegation at the country code level in the e164.arpa domain. This is also referred to as *user ENUM*. However, no viable business case for the User ENUM concept has emerged yet.

The technical concept of ENUM is viable and today mainly *Carrier ENUM* is implemented. Groups of carriers or communication service providers agree to share subscriber information via ENUM in private peering relationships, whereas the carriers themselves control subscriber information. Carrier ENUM is also referred to as *infrastructure ENUM.*

ENUM is also used for resolving numbers into addresses in the IMS specifications and in the IPX specifications by GSMA. Hence, the implementation of IMS requires the implementation of carrier ENUM.

Figure 2-6: Inter-operability and ENUM



2.5.2 Routing

Routing is the process of distributing and collecting topology-related information, calculating the routes, establishing and maintaining the routing table in the network (Y.2612).Routing in IP based networks is determined by information in the individual routers. Between networks routing information is advertised with the border gateway protocol (BGP). In traditional networks routing is performed within a network. If it is determined, that a specific address is not within the network the connection is routed to an appropriate point of interconnection. Routing might also involve overflow or traffic management mechanisms that take care of outages or congestion in the network.

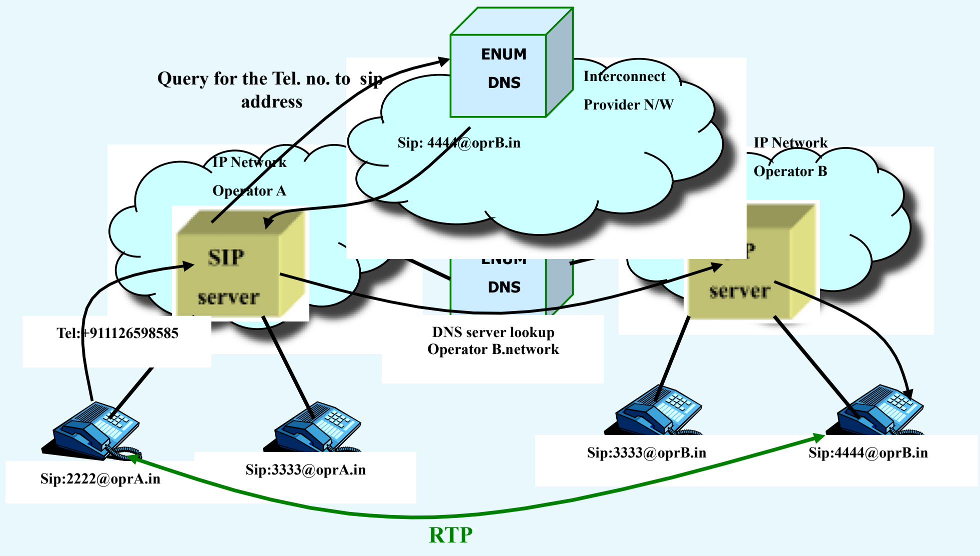
The Core architecture will use well known IP protocols like OSPF, BGP etc. for routing updates and MPLS for traffic engineering. The Routing procedures and configuration for handing over the IP traffic from one operator to another operator will depend upon how the two operators are interconnected. Besides IP connectivity and routing protocols between two operators, NGN will require special provisioning to enable voice and video to pass smoothly from one network to another. There will be issues related to Firewall traversal, Security, SLAs, translation of protocols in two networks (interoperability), and lawful interception of calls. To handle these issues devices like Session Border Controllers (SBC) will be required at borders, between two NGN operators. The network devices like routers and switches in the core and border networks shall support IPV4 as well as IPV6 protocols for easy migration to IPV6 in future.

Mobile networks have implemented the concept of roaming. It means that subscribers can make and receive calls in visited networks and receive the bill from their home network. According to GSM specifications calls towards a roaming subscriber are routed via the home network, which determines the charge for the roaming leg. Active calls by a roaming subscriber are routed directly to the destination without a detour through the home network. The visited operator records the call detail records and sends them to the home network via the so called transferred account procedure (TAP), which is specified by the GSMA. Mobile internet usage by roaming subscribers is routed to the home network in all cases and the home network controls the access to the internet.

Routing and roaming in next generation networks will use IP mechanisms. It is expected that operators will maintain their influence on roaming traffic and will be included in the call path to roaming subscribers. From a technical point of view this would not be required provided HLR-information can be accessed from other networks as well. The solution for the routing and exchange of this information is included in the IMS specifications.

In IP based network the SIP session establishment with the help of GLOBAL ENUM DNS is as follows:

Figure 2-7: SIP session establishment with the help of GLOBAL ENUM DNS



3 Regulatory Challenges Raised by NGN Migration

NGN raises regulatory challenges that can be linked, in one way or another, to the convergence process at the service provision and network access levels. This section discusses a number of NGN-related regulatory challenges from a regulatory perspective. These challenges include open access, market definition, QoS and interconnection.

In this discussion, it is important to remember that NGN will inherit some of the same regulatory obligations imposed on the PSTN like lawful interception and access to emergency services. The need for access to emergency services has been taken into account by both 3GPP and TISPAN. However, the first introduction of emergency services within 3GPP IMS architecture is only planned for Release 7 onwards, while the first two IMS releases, R5 and R6, only allows access to emergency services through the circuit-switched domain, the legacy GSM core infrastructure used for voice calls.

Lawful interception for packet mode services is already enabled by GPRS in 2G mobile networks. GPRS has the capability to send a duplicate of all packets exchanged by a user over a PDP context as well as the address of the entity accessed through this context. Lawful interception was introduced from the first 3GPP IMS R5 specification.

3.1 High Level Regulatory Considerations

Although NGNs and their services appear to offer numerous advantages, it is anticipated to get better understanding of all the options available and all the advantages and disadvantages related to NGNs. The followings are issues to be helpful for identifying these considerations:

- What networks for what services?
- What actions can the regulator envisage to facilitate migration to NGNs to the benefit of the consumer?
- How is the regulation of dominant operators modified by migration to NGN?
- What is the impact of the introduction of NGN networks on interconnection, tariff-setting for services, numbering, frequency spectrum management, etc.?

With a view to preparing transition of the existing telecommunication environment towards NGNs, possible problems raised by NGNs, such as interconnection, consumer protection, redefinition of universal access, technological neutrality, quality of service, numbering and licensing should be carefully considered. Technical, economic and regulatory study on arrangements for migration to NGN networks is very important with the purpose of determining the right time for migration. It is important to note that the regulator ensures the market emerging from the transition is fair, open and competitive and, on the other, to elucidate for the regulator all the technical, economic and regulatory issues raised by transition to NGN networks, allowing it to identify as early on as possible the areas of interest related to its activity.

The following study issues have been considered for these objectives:

- review the legal and regulatory telecommunication regime and identify those elements that may require adaptation in order to accommodate convergence;
- gather the expectations of operators and service providers vis-à-vis NGN networks;
- examine the migration strategy of the major fixed and mobile telephone operators regarding the core network and access network segments;
- identify what elements hamper or boost migration to NGN (at the technological, economic and regulatory levels);
- identify the new economic models that will be associated with NGN and their suitability and durability;
- draw up the strategy for migration of fixed and mobile telephone networks to NGN;
- propose for that migration an ambitious roadmap that is adaptable to new technological changes, along with a budget, realistic realization deadlines and indicators/mechanisms to monitor its implementation.

The study should be conducted according to the following proposed phases:

1. gathering and analysis of information on the legal and regulatory framework for telecommunications;
2. organization of a seminar/workshop on NGNs open to all players in the telecommunication and ICT sector;
3. collections of data from fixed and mobile telephone operators and Internet access and service providers;
4. analysis and exploitation of the data on the situation in each country and comparison with the experiences of other countries;
5. preparation of a roadmap, production of the final study report and the strategy document for transition to NGN.

One of the ways to have regulatory perspective could be focused on the necessity of examining the NGN regulatory issues within the framework of a methodological approach. In this sense, a question about whether the NGNs are public goods or not is a good subject to examine many of aspects such as non-excludability in supply, non-rivalry in consumption and externalities. Study on these aspects may provide valuable inputs to direct very high level regulatory regime for NGN, possibly adopting new regulatory approach which will have different regulatory frameworks than legacy telecommunication.

Followings are summary of key features about aforementioned aspects:

- Non-excludability in supply: This determinant means that the supply of the related product should cover everybody without a manner of excludability. The product that has been supplied in the market in a country or a society is within the reach of all individuals there. A supply on the level of market operation cannot be made by market players. One of the fundamental elements here is that the supplied product has not been supplied upon request. A product which has been provided for a person, at the same time, has been provided for each person or player in the society. The supply of the related product is provided homogenously. The supply is itself should be a homogenous product.

- Non- rivalry in consumption: This determinant means that the consumption of the related product by a person does not pose a hindrance to another person's consumption of the product. Consumption preferences of individuals are not homogenous but heterogeneous. On the other hand, this heterogeneous nature of preferences about consumption does not generate a competition or rivalry in consumption.
- Externalities: This is the ratio relationship between benefit and cost for other units concerned with the product. A product which has been provided as a public good does not operate as efficiently within the framework of benefit-cost-balance unlike the functionality of free market. Public goods form a negative externality, so cannot be regarded as efficient situation in term of open market.

ITU-D has developed a series of papers and seminars related to regulation, costing and policy approaches to help countries develop their telecoms services, a major focus in recent years has been on Next Generation Networks, specially related to what are the challenges and benefits from the new telecommunications/ICT technologies. To assist ITU Members on this issue, a report on "Strategies for the deployment of NGN in a broadband environment - Regulatory and economic aspects"[1] has been prepared. It looks at the higher levels strategic issues as well as the economics and fundamental aspects related to the migration to NGN. The purpose of the report is to provide insights to help develop national strategies and regulatory approaches towards broadband that will benefit the telecoms industry, consumers and all businesses that make use of telecoms services.

3.2 Next Generation Access Networks

According to the above clause 3.1, Next Generation Networks have started to change the fundamental elements in the telecommunication sector such as services, network structure and the functioning model of the network structure. Thus, there needs to be a new regulatory approach other than the conventional regulatory approach that was used in the previous telecommunication networks. One of the main reason lies under this concession arises from the implications of the specific technological changes in the NGN structure. Therefore, National Regulatory Authorities should consider how the existing regulations can be adapted to this new environment aligned with the current market structure.

To begin with, it is worthwhile to focus on whether NGA (Next Generation Access) networks are essential facilities or not. There was only a single access network infrastructure in legacy networks, thus it requires an obligation to reach access of local loop. However, in the scope of NGN which has no dependency on specific access networks, even fibre access is not an essential facility for NGN services. Because of in order to ensure fibre as an essential facility, there must not be any other access of network. During migration to IP networks, legacy telephone based networks can be considered as an alternative to NGA networks. Consequently, NGN can be considered as a technologic device to give more IP based new services (visual call, broadband, IPTV and intelligent services, etc.) with respect to legacy telephone based network structure. Moreover, as NGN is a new approach in the telecommunication sector, the market structure and the demand preferences are not mature yet. Since NGN and NGA are diversified from the legacy telecommunication network structures in terms of features and functionality, the market structure through these new networks are not definite yet.

Therefore, as mentioned above, during the process of migration to NGN, there needs to be a new regulatory approach. One of key issues for promoting competition, while encouraging investment in NGN

[1] This report is freely available on the website at: http://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Studies.aspx

access networks, is the question of local loop unbundling (LLU) in a fibre environment. Today's local loop unbundling regulations focuses on the last mile. But the move to FTTH, FTTB and FTTC means the focus is on the last quarter mile or less. Given the costs and other resources involved, the LLU model appropriate for legacy copper may have to be adapted for fibre or different remedies identified. Where regulators mandate LLU one option could be a bit-stream offer at the Central Office level, where the nature of the access network is totally transparent. Other options could include requiring collocation at the street cabinet level and backhaul from the cabinet to the operator's node. In addition, there will be a new approach to LLU, throughout the NGN migration, different from the conventional perspective of LLU in legacy networks. Not having a regulation for LLU of NGA during the process of migration to NGN can be considered as a new approach. Because exposing LLU to the regulation in the migration process will aggravate the formation of distributive efficiency and fair competition. Companies deployed on the NGA networks should not be exposed to LLU, until sunk costs will have been recovered and the competitive environment will be emerged in the service market. The duration of the return of investment depends on the company business models, the market structure and the welfare of the society but it is generally understood that should be at least 4 or 5 years long. Obligation to LLU to NGA networks may cause the emergence of free-rider problem in the market. The free-rider issue must not be considered only for the return of the investments but also fairness and service differences of the various providers participated into the NGN.

After a competitive market structure is formed and the migration phase is completed, there exist other devices apart from LLU to benefit from fibre cable deployment such as bit-stream access, exchange and virtual unbundling. Beyond this, it should be also decided whether the competitive market is desired for retail service market or wholesale access market. However, backhaul could be difficult for competitive operators to provide for themselves unless duct-sharing is available.

There are a number of difficulties associated with new fibre deployments. Long-term civil engineering costs that involve passive infrastructure renovation in the public domain, such as trench digging and duct installation, and drop-cable connectivity in the private domain, such as indoor and residential cabling, are significant. They also involve significant negotiating complexity that would be prohibitive for any individual service provider to assume alone. For these reasons, requiring passive infrastructure sharing is one solution regulators are exploring.

Another issue raised by FTTx is related with the removal of Main Distribution Frames (MDF) by the incumbent operator thereby making obsolete the "old" scheme of LLU for copper at least in its full unbundling and line sharing options, since LLU takes place at the MDF under traditional LLU scenarios. Where points of interconnection are withdrawn, it will be important for competitive operators both that they not face additional costs as part of the NGN migration process, and that they remain able to continue their current service offerings, and not face the problem of "stranded investments". The Netherlands's incumbent operator, KPN, for instance[2] announced that it would remove all of its MDFs as part of its NGN migration, to consolidate its network into a reduced number of switching nodes and shift DSLAMs only within street cabinets. KPN hopes, by selling the buildings that house its MDFs, to raise EUR 1 billion which it can then use to finance its FTTx rollout. KPN and the Dutch national regulatory authority, OPTA, are discussing KPN's plans for MDF removal, which could include phase-out conditions for the withdrawal of MDF access, as well as KPN's proposal to provide "sub loop unbundling (SLU)" for street cabinets and a "Wholesale Broadband Access (WBA)" offer at local, regional or national switching levels. Regulators in other countries may wish to follow the regulatory developments in Europe and elsewhere as operators continue to roll out their NGN access networks.

As a matter of fact, the milestone for economy is not to form competition in infrastructure market in the process of migration to NGN but to establish competition in the market of services. This type of

---

2 See http://erg.eu.int/doc/whatsnew/kpn_van_den_beukel_erg_17_apr_07.pdf

competitive market might have more tendencies to bring innovation into economy. So, the market competition desire to be built on NGN based services is not completely free from fibre cable distribution within the scope of NGA. The distribution of fibre is a significant device for the competition based on NGN services.

3.3 Market Definition

The identification and definition of relevant markets are the basis of competition analysis used for the establishment of *ex ante* regulation in many countries, particularly in the EU. With NGN this task will become much more complex due to the blurring of the boundaries between technologies and services. This complexity could be at the source of disputes between regulatory authorities and market players.

The case of Deutsche Telekom's NGN deployment and its dispute with the regulator regarding its obligation to provide access to its network to competitors is a good example of the new regulatory challenges raised by NGN. Enabling Environment for NGN, it is worthwhile highlighting its technical aspects. At the heart of the dispute between Deutsche Telekom and the regulator lies a difference of interpretation as to the qualitative differences between fibre access and DSL access. In Deutsche Telekom's view, the extra bandwidth provided by fibre will qualitatively change the service, through for instance the provision of High-Definition TV, making it a different market from the DSL one in which it is currently designated as having SMP. However, the regulator views the project mainly as an upgrade of Deutsche Telekom's DSL service with the intention of retaining its current DSL subscribers.

The results of such disputes could be dramatic if incumbents threaten to freeze their investment. However, given the potential returns, European regulators seemed confident that operators would continue to invest in similar projects.

3.4 Quality of Service

NGN's unified transport of services raises issues related to the connection-less nature of IP transport, especially for real-time interactive voice or multimedia communication streams that are sensitive to packet loss, delay or jitter. However, many technologies that ensure QoS over an IP network already exist. These can be broadly split into technological approaches based on over-provisioning that is associated with relative priorities or on explicit end-to-end resource reservation.

It must be noted that the bulk of the Internet uses the "best-effort" model with no QoS guarantees. Many applications on the Internet use the Transmission Control Protocol (TCP) that reduces user traffic in the case of congestion. TCP, however, is not suitable for real-time applications like video streaming, voice or multimedia communications that cannot limit the rate of packet sending in case of congestion. Recently, more real-time applications such as voice telephony or video streaming are being represented, not only from fixed but also from mobile network environments, a significant amount of Internet core traffic. Today over-provisioned core network, as is the case of many Internet backbones, has serious challenges to handle this traffic including the problems about fair usage of network resources and data explosions.

A next-generation network, however, is different from the Internet even though they share the same IP transport technology. NGN relies on explicit guarantees provided by the network to its end-user for quality sensitive applications, such as IPTV and guaranteed VoIP. Such applications are expected to constitute a large portion of NGN traffic.

A next-generation network, however, is a managed and closed network. As such, many of the QoS techniques involving differentiated priorities and resource reservations that are not widely applied in the Internet because of scalability and cost issues can be applied within next-generation networks. Furthermore, in NGN architecture the transport domain is under the control of a service domain which guarantees that proper resources are allocated by the transport domain for the duration of a given service provision by the network. This is something that does not exist in the Internet since the "control" is end-to-end and not within the network.

The critical issue that remains is the need to ensure the coordination between different next-generation networks in order to provide end-to-end QoS. There is a general misconception that in the PSTN end-to-end QoS is associated with the reservation of a TDM circuit of 64 Kbit/s all along the traversed networks. While this is true, end-to-end PSTN QoS also depends on proper end-to-end signalling through ITU Signaling System N°7 (SS7). The same principle of end-to-end signalling could be applied over any packet transport bearer, the possibility of which was demonstrated by ITU's specification of the Bearer Independent Call Control (BICC) protocol which is an adaptation of SS7.

By definition and design, IMS architecture uses the SIP protocol for call (session) signalling. SIP is essentially an Internet end-to-end protocol; however 3GPP and ETSI TISPAN have extended it to make it usable for network control functions in NGN voice and multimedia calls. This occurs in a manner similar to call and service control functions in legacy SS7-based intelligent network architecture. ITU is developing NGN signalling protocols for resource reservation on a call-by-call basis that will be applicable within networks, especially at network interconnection points. This work is being advanced in close cooperation with 3GPP and ETSI TISPAN. ITU has already produced some Recommendations on NGN signalling protocols for resource reservation while further work is being undertaken by ITU-T SG11.

It is, of course, not the regulator's duty to enter into the detailed technicalities of QoS provision within NGN. However, to support essential services, such as interactive voice, regulators could contribute to the definition of the basic requirements needed at interconnection points, in a similar way to what occurs today between telephony networks.

3.5 Interconnection

The need for interconnection between telecommunication networks stems generally from the over-arching necessity of service completion. NGN is no exception; in fact it introduces even more interconnection requirements than legacy telephony networks as a consequence of the ubiquity of access to services it introduces.

In addition to the legacy interconnection requirements for service completion among different next-generation networks and between a next-generation network and other voice networks, it must allow subscribers the ability to:

- Connect from any other network and get their service profile from their home network in order to be served according to it, which is similar to the concept of mobile roaming, but applied to all types of broadband packet access;
- Access the services of their own network in preference to those of the visited network, which is a feature currently present in mobile networks through the Customized Application for Mobile network Enhanced Logic (CAMEL) IN interface that allows roaming subscribers to receive, for instance, network information messages and access value-added service in their own language; and
- Access value-added services from a third-party service provider, which is a concept that is currently available for some 2.5 and 3G content services such as access to alternative Wireless Application Protocol (WAP) portals, or I-mode services.

NGN interconnection requirements necessitate a common definition of what constitutes a multimedia call. Such an issue may be critical in the selection of either a calling party pays (CPP) or a bill-and-keep regime. Interconnection in an IP-based NGN Environment, it is important to clarify a misconception that links the CPP regime with circuit-switched transport. A CPP regime owes more to a service completion agreement for a given call between two network domains rather than on actual resource reservation for a given call. The fact that in legacy voice telephony this implies a reservation of a dedicated circuit is only a technical detail that will evolve as networks move towards packet transport. In NGN, such a service completion guarantee would be meaningful for individual multimedia calls only if a signalling interaction exists, or is deemed necessary, between respective control entities at network domain boundaries. For this signalling to exist, a common definition of the requirements of these multimedia calls must exist, similar to what already exists for voice calls.

It is likely that the roaming issue will be even more complex with NGN. Today, the mobile industry has agreed on mutual roaming agreements without the necessity of regulatory intervention. Regulators have only intervened on the topic of roaming tariffs. With NGN, regulators will have to consider whether it will be necessary to mandate roaming. For example, should an NGN mobile access operator be required to allow clients of any NGN fibre access operator to roam on its access network and vice-versa?

The issue of access to third-party services is also important. In the past, mobile operators have attempted to lock-in their customers to their own service provision platform. Fortunately, such practices are no longer in place even if, in practice, most third-party service provision is done though operator portals. In a similar way, regulators should closely monitor third-party access to services in a NGN environment. Even if, on paper, IMS architecture and NGN by using NGN-OSE and NGN-SIDE enshrines third party access to service provider platforms, its actual implementation will be quite complex, perhaps allowing room for uncompetitive behavior veiled behind technical arguments.

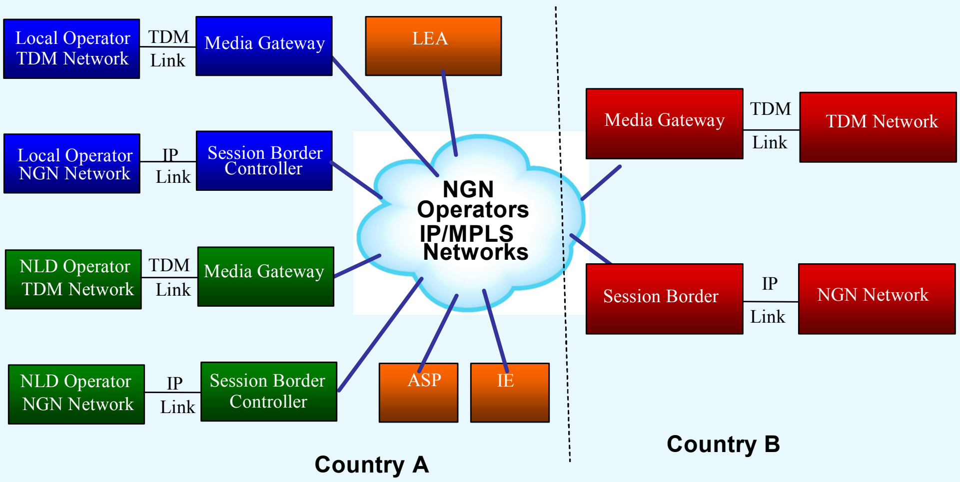
3.5.1 Interconnection Architecture

Many of the networks created over the last few years contain most of the elements of the NGN. Advances approaches to interconnection have been slow to deploy, even where the technology has been mature or within the hailing distance of maturity. Due to efficiency and flexibility of IP technology, most new networks being established are IP based.

The inter-operator scenario in the NGN environment is shown in Figure 3-1.

Peering with traditional PSTN and mobile networks based on the ISDN User Protocol (ISUP) may be interconnected via the Media Gateway for IP to TDM or TDM to IP conversion and the Signaling Gateway for SS7 transport over IP.

Figure 3-1: Interconnection architecture of inter-operator environment in NGN scenario



Note: LEA: Law Enforcement Agency
ASP: Application Service Providers

As shown in Figure 3-1, NGN networks are interconnected by Session Border Controllers (SBCs), which are located at the administrative boundary of a network for enforcing policy on multimedia sessions. A session policy may be defined to manage security, service level agreements, network device resources, network bandwidth, inter-working and protocol interoperability between networks.

SBCs can perform a number of functions such as:

- Network Security
- Denial of Service attacks and overload control
- Network Address Translation and Firewall Traversal
- Lawful Interception
- Quality of Service (QoS) management
- Protocol Translation
- Call accounting

The MGW (Media Gateway) shown in Figure 3-1 will be controlled by a soft switch deployed by the PSTN/mobile operators in NGN. A SGW (Signalling Gateway) can be integrated into the MGW or can also be a stand-alone device.

3.5.2 Interfaces

3.5.2.1 Physical interfaces

The Session Border Controller SBC provides IP interface(s) towards other NGN networks. The physical interfaces consist of:

- Gigabit Ethernet interfaces.
- 10/100 Base-T Fast Ethernet interface(s).

SBC provides redundant signalling and media control sub-systems, each with redundant network interfaces. Sub-systems of the SBC communicate to one another over any of the available IP interfaces.

3.5.2.2 Signaling interfaces

The network model for which the signalling interfaces have been defined is assumed to be an all IP next-generation network (NGN) where the control point in the network could be the:

- Soft switch or
- IMS (IP Multi-media Service) core

Standardization of signalling is mainly the role of ITU-T and therefore does not fall within the scope of this question. However, regulatory issues arising from the adoption of particular types of interfaces are important. While ITU-T standardizes protocols and signalling, this question should address whether regulators should mandate a given standard to ensure interoperability or leave this to operators, risking lack of interoperability.

ITU-T study group 13 has already forwarded two recommendations in response to the liaison statement for this question. ITU-T recommendations Y.2701 and Y.2201 provide security requirements for interfaces and high level requirements for services and capabilities for next-generation networks. In addition to these recommendations there are a series of NGN release recommendations.

ITU-T has also approved a signalling recommendation Q.3401, NGN Signaling profile, which regulators may wish to use.

3.5.3 Points of Interconnection

During the transition phase, dominant operator may be obliged to maintain traditional PSTN interconnection capabilities. Assuming that it is possible for competitors to reach dominant's NGN-based end-user customers through traditional interconnection, there may not necessarily be a regulatory obligation to provide new NGN-based interconnection capabilities. Dominant operator will offer IP-based interconnection at some point during the transition phase. As the transition phase draws to a close, they may like to withdraw traditional interconnection. To the extent that they still possess market power, they should almost certainly be under regulatory obligations to provide interconnection to the NGN at cost-based prices. In the world of the Internet, the great majority of interconnection takes the form either of peering or of transit. In case of NGN market participants may prefer peering, transit, or some other model of interconnection. In fact, peering offers exchange of traffic only between dominant customers and those of its peer, but does not provide either with access to third parties. In a typical transit relationship, by contrast, the transit customer can use the transit provider's network to reach destinations anywhere on the Internet. Dominant service provider is unlikely to be motivated to offer peering arrangements to tiny competitive operators. It might offer peering arrangements to just a few of its largest domestic competitors. At that point, small domestic competitors have limited options either they might stick with PSTN interconnect or they may purchase transit service from one of the dominant operator. A plethora of problems stand in the way of implementing a robust interconnection framework for IP based NGN and of successfully operating such a frame work to emerge. Establishing and maintaining an interconnecting arrangement with another firm takes work. The technical effort sometimes is essential, depending upon circumstances. What are often overlooked are administrative and contractual costs of establishing IP interconnection arrangements. One of the possibilities may be explored to set up an IP based Interconnect exchange which may transit all IP traffic of all operators in default if there is no peering arrangement between the operators.

3.5.3.1 Interconnect Exchange (IE)

The basic concept of the Interconnect Exchange is to enable different operators to interconnect to a common point, to exchange mutual traffic efficiently. Internet Exchanges may be one option regulators may wish to consider as a model appropriate for NGN interconnection.

The role of Interconnect Exchanges

- Inter-Carrier Billing

Presently inter-carrier billing is a major issue of dispute between various service providers and is likely to escalate unless corrective steps are put in place. Using an interconnect exchange also as an inter-carrier billing clearing house may provide a solution to this major challenge. Inter-operator charging could be a function of a) grade of service, b) content, and c) network elements used while carrying traffic to the Interconnect exchange.

- Intelligent Network Services

Intelligent Network Services in a multi-operator multi-service scenario could be provided through the combination of the Interconnect Exchange/Inter-Carrier Billing Clearing House.

- Number Portability

Number Portability could also be addressed for a multi-operator multi-service scenario through a centralised database available to the Interconnect Exchange/Inter-Carrier Billing Clearing House

- Simplification

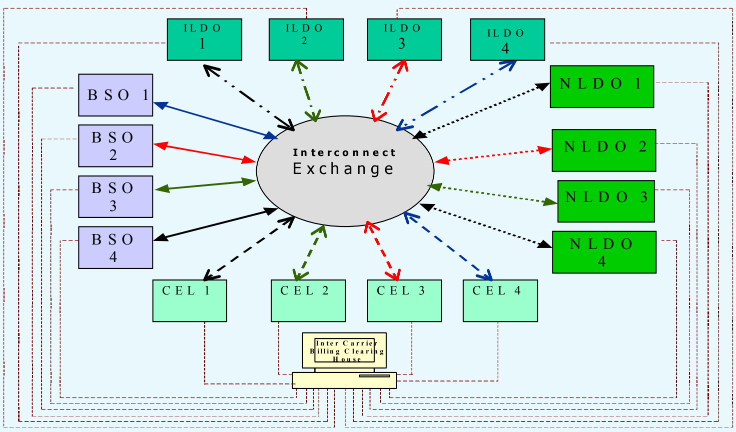
Use of an Interconnect Exchange/Inter-Carrier Billing Clearing House could also lead to simplified network architecture, a reduction in the number of Points of Interconnection (POI), simplification in settlement of interconnect usage charges as well as shorter waiting periods for interconnection capacity.

Challenges posed by current interconnection regimes

Current bilateral interconnection arrangements in a multi-operator, multi-service environment can lead to:

- High interconnection cost and port charges
- Asymmetric interconnection agreements and litigation due to ambiguities and a non-level playing field.
- Delays in provisioning of interconnection due to capacity constraints
- Sub-optimal utilization of resources
- Inefficient handling of calls
- High operational costs for managing inter-operator settlements
- Inter carrier billing
- Complexity in settlement of interconnect usage charges
- Sharing of Intelligent Network Platform
- Implementation of Number Portability
- Increase of CAPEX and OPEX making operation unviable

Figure 3-2: Interconnect Exchange



Note: BSO means basic service providers/fixed line service provider
CEL means mobile network

3.5.3.2 Location of Points of Interconnection

Currently operators peer among themselves at mutually agreed POIs. At areas where the operators are unable to peer among themselves, the network of other operators is used for transit.

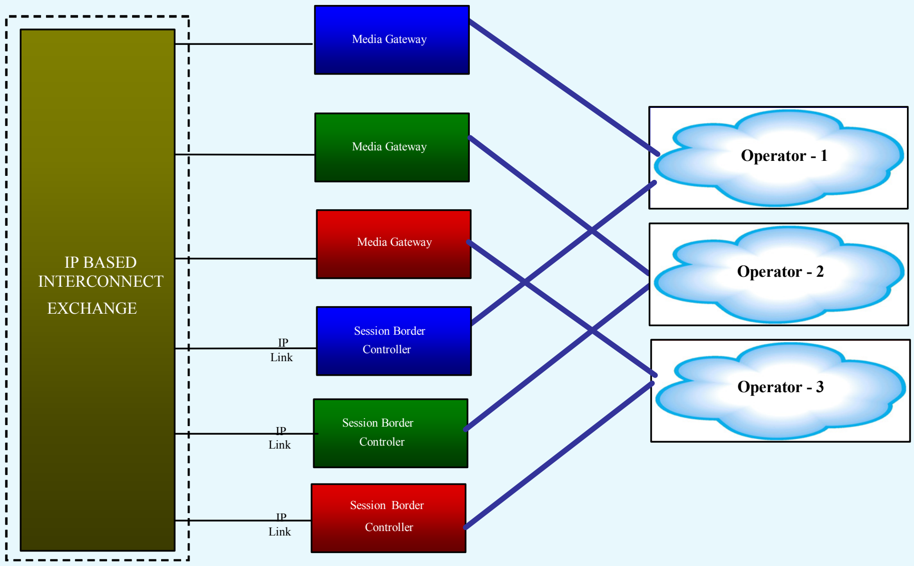
At present, both peering partners must have TDM based switches at the POI locations. With implementation of MPLS networks, the concept of cost of carriage with respect to distance loses its relevance. NGN with its separation of control and media functions and distributed architecture eliminates this restriction. The following methodology is proposed for the NGN environment.

i) The operators may be allowed to have the option of either a centralized control point in its network controlling the distributed media gateways or SBCs within the service area.

ii) The operator should be allowed to place media gateways and/or SBCs anywhere in the country, wherever POIs are desired.

iii) An Interconnect Exchange is proposed for interconnection between different operators in the NGN environment as shown in Figure 3-3.

Figure 3-3: Interconnect Exchange Model



One or more Interconnect Exchanges can be established at service area level depending on the traffic requirements, at the locations where most of the operators have a presence.

The advantage of this model is that it makes network planning more efficient. Every operator is aware of the physical location at which it would have to provide the POI enabling transmission network roll-out in a more planned way.

The architecture for interconnection in NGN should be comparable or more rugged than the current PSTN/ISDN/mobile network service since NGN is expected to replace these networks over time. Consequently, one of the key objectives of the architecture would be to have service restored with minimum downtime in case of failure of interconnection. It implies that a resilient multiple node architecture has to be used along with IP protocols and networking technologies specially configured to meet the stringent requirement.

The interconnection in an NGN environment should operate at two logical layers – the signalling layer and the Media layer. In order to minimize the cost and complexity in the interconnection, L2 connectivity may be preferred over L3 interconnects with Logical VLANs/VPNs (virtual local area networks/virtual private networks).

Interconnection in an NGN environment would provide a secure, low latency environment in which the quality of wholesale interconnects is guaranteed between all operators.

3.5.4 Interconnection Charges

The current concept of interconnection charges in the PSTN/mobile network environment is based on distance and the time/duration of a call. In the world of the IP-based NGN, the network provider will still in most cases still be a service provider, but it will not necessarily be the only service provider Vonage, Skype and SIPgate are examples of competitive firms that provide services without operating a network of their own. For the foreseeable future, integrated and independent service providers are likely to coexist, and to compete for the same end-users customers. This separation of function has profound implications for both the network provider and the service provider. In theory, the network provider in an IP-based world does not know or care about the nature of the application traffic that it is carrying – and in this context, voice is just another application.

In the NGN scenario interconnection charges could adopt a variety of models, including the Bill & Keep model, or, where charges are used, they could be based on bandwidth and application usage, quality of service provided, the number of network elements used, the volume of data exchanged during a session, time-of-day, etc.

Next generation networks may require many more features for charging as given below:

- Charging based on call duration, bearer capability, time and type of day etc.
- Charging based on QoS, bandwidth, application etc.
- Chargeable party (calling, called or third party).
- Charging of supplementary and value added services.

Generation of CDR (Call Data Records), subscriber billing, trunk billing and automatic backup and format conversion functions should be possible.

Standard interfaces and protocols will be required for sending relevant information to billing centers.

In an NGN environment, it will be important to develop an Interconnection Charge regime that provides certainty to inter-operator settlements and facilitates interconnection agreements. India, for example, currently has adopted cost-based Interconnection Usage Charges (IUCs) which include origination, carriage and termination charges. However, there are at least four possible models for interconnection charges on NGN-based networks. These are: 1. Calling Party Network Pays, 2. Bill and Keep, 3. Charges based on Quality of Service, and 4. Bulk Billing. The exercise to determine interconnection charges could involve an assessment of the various cost items attributable to different network elements involved in setting up of a call in the NGN environment, or conducted on a barter basis, or by measuring traffic sent (volume, level of QoS provided, etc). Even where the Bill & Keep model is used, some countries may continue the use of carrier charges paid by the originating operator to the access provider. Where interconnection charges are based on network elements, every effort would need to be made to accurately assess relevant network element costs based on the inputs to be provided by various operators. The important issue is to identify the network elements involved in completion of the carriage of a long distance call from its origin to destination in a multi-operator environment.

Migration to NGN would substantially affect the network costs and the relationship between the cost of carrying traffic and distance over which traffic is carried. The similarities between NGNs and the Internet have raised the question of whether the move to NGN will bring the "death of distance" in interconnection charges. Where Internet charges are typically independent of the distance over which data is conveyed, under NGNs the distance related network costs may become much smaller. Therefore, cost based interconnection charges would help in bringing the correct regulatory framework in facilitating faster deployment of NGNs in the market.

Four main bases for interconnection charges in the NGN regime

In the Internet, some things are known at the level of the application or service, while very different things are known at the level of the network. For VoIP, a server that implements a protocol like SIP will know the time at which a session is initiated, and may know that time at which it ends, but will know next to nothing about the network resources consumed in the interim. The topological location (the logical location within the network) of the originating and terminating end points will be known, but not necessarily the geographical location. Beyond this, an IP-based network will be dealing with a far broader array of applications than just traditional voice. The notion that the call originator should be viewed as the cost causer breaks down in the general case. In the general case, there is no obvious "right answer" to the question of how to allocate costs among end-users. The underlying network knows very different things. In an IP-based environment, each IP datagram is independently addressed, and could in principle be independently routed (although routing in practice is much more stable than this implies). Relatively simple applications can generate a very large number of IP datagrams. For accounting purposes, it is necessary to summarize this data – otherwise, the accounting systems will be deluged with unmanageable data volumes. For analogous reasons, it is trivial to measure the traffic over a given point-to-point data transmission link, but expensive and cumbersome to develop an overall traffic matrix based on end-to-end traffic destinations.

3.5.4.1 Calling Party's Network Pays (CPNP)

CPNP- the network that initiates the call pays for the call, usually based on the duration of the call; generally, the party that receives (terminates) the call pays nothing. In IP based networks, instead of duration of the call, the charging can be based on the number of packets transferred. This can either take the form of Element Based Charging (EBC) or Capacity Based Charging (CBC). Both systems constitute cost-based systems.

Limitations:

- Under EBC the interconnection rates depend on the number of network elements. Implementation of EBC (or CBC) for IP networks would cause transaction costs (e.g. for determining IP points of interconnection).
- Termination Monopoly.

3.5.4.2 Bill and Keep

With this regime there are no charges for termination. Basically, Bill & Keep is a kind of barter exchange where network operator *A* terminates traffic from network *B* on its network and vice versa. As traffic flows may balance out in both directions so that there are no payment flows, the price for *A* of getting its traffic terminated on *B's* network consists of *providing network capacities* for terminating traffic coming from *B*. In that sense, interconnection services are not provided for free.

With Bill & Keep, transaction costs can be reduced and there is no termination monopoly problem under Bill & Keep. Without payments for termination services the problem of arbitrage is avoided.

Limitations:

- With Bill and Keep, service providers have an incentive to hand over their traffic to another network for termination as early as possible, giving rise to the "hot potato" phenomenon. To counter this problem, it may be reasonable to make requirements with regard to the minimum number and location of interconnection points for Bill & Keep to be applicable for a specific network operator.

3.5.4.3 Based on Quality of Service

If two providers want to compensate one another for carrying their respective delay-sensitive traffic at a preferred Quality of Service, each will want to verify that the other has in fact done what it committed to do.

In the case of QoS, this would seem to imply measurements of (1) the amount of traffic of each class of service exchanged in each direction between the providers; and (2) metrics of the quality of service actually provided. Measuring the QoS is much more complex, both at a technical level and at a business level.

Limitations:

- Commitments between providers would be primarily in terms of the mean and variance of delay. First, it is important to remember that this measurement activity implies a degree of cooperation between network operators which are direct competitors for the same end-user customers. Each operator will be sensitive about revealing the internal performance characteristics of its networks to a competitor. Neither would want the other to reveal any limitations in its network to prospective customers.
- Second, there might be concerns that the measurement servers – operated within one's own network, for the benefit of a competitor – might turn into an operational nightmare, or perhaps a security exposure, within the perimeter of one's own network.

3.5.4.4 Bulk Basis (can also be termed as "Interconnect Hotel")

The legacy interconnection charge regime, i.e. per-minute basis, would certainly complicate the smooth settlement of claims. The reason being, NGN products will be based on capacity, quality of service and class of service. Since the aggregation of traffic would take place at the common node, it is necessary to mandate charging of applicable interconnection charges for NGNs on a bulk-usage basis rather than a per-minute basis prevalent currently. Under NGN, total network costs and carriage would become much smaller relative to traffic volumes and thus average network costs associated with each traffic unit decreases. Charging of interconnect charges on a bulk basis would establish a clear level playing field among the operators and facilitate saving legal costs and time from unwanted litigation and dispute settlement.

In this regard, it is also necessary to identify what should be regulated and what can be left for mutual negotiation.

3.5.5 Economic Impact of Interconnection Arrangement

NGN promises simpler network architectures, higher bandwidths, fewer network elements, lower costs and more functionality. Furthermore the distinction between transport and services will allow independent evolution of business models, network elements and applications. Hence, next generation networks imply technological changes, changes to products and service offerings and eventually the market structures resulting from the introduction of next generation (access) networks. Further (NGN and NGA) also affects the way costs are calculated because of new cost drivers and cost/volume relationships (CVR). The regulatory costing and charging regime should reflect these developments. Clearly, the voice-centric view on costs in telecom networks established in the past has to consider the growing role of data and the fact that voice becomes "another form of data communication". This implies substantial changes in the view and analysis of costs in an NGN environment.

When looking at the development in the markets new retails tariff structures (especially due to the increase in bundled tariffs and flat-rate tariffs) and new forms of usage, especially growth in mobile broadband and IPTV, change the desired network architecture and impact the level of costs and the cost structures of the operators. With increased data traffic in All-IP networks with multiple services sharing one network, the fixed costs are distributed to a lesser extent to voice services. This means that the economies of scales, driven by data traffic, reduce the costs for voice services.

The implementation of IP and NGN networks implies that the networks are becoming more centralized than today. This will likely motivate the implementation of a smaller number of PoI. It is important that the regulatory framework, e.g. with regard to the tariff structures and levels is considering this development.

A further outcome of the networks economics due to NGN is the decoupling of the network and the service levels in IP networks, which implies new Cost-Volume-Relationships (CVRs) as the costs for transmission is reduced (due to All-IP networks, reaping the benefits of economies of scales and scope) while the costs for the control layer and the service platforms are increased (due to additional investments in softswitches and IMS platforms). As the control layer and the service level have the overall network load, the number of active end-users, number of call set-ups and signalling as cost driver, the decoupling could motivate the implementation of new charging regimes.

The migration towards IP interconnection could possibly be accelerated by abandoning the principle of technology neutrality, and compelling operators to interconnect on an IP basis. This could be implemented as part of a seeker/provider regime, by requiring that, when the seeker requests IP interconnection, the other operator is obliged to provide same. The advantage of this arrangement is that IP interconnection would be driven by the requirements of the most advanced operators. Otherwise, the migration to IP interconnection will not take place on a large scale until the major operators identify an interest. Enforcing IP interconnection raises a number of issues, however, including how to establish a reference offer, and how to regulate interconnection usage charges and charges for interconnection links.

According to the currently high number of PoIs, some of the operators would like to see a reduction of PoIs in NGN because it will positively influence the existing operator landscape and future management of QoS, but according to some concerns this should not be done by fast changes on the number and architecture of PoIs.

Currently, most service providers are migrating towards IP based networks. While voice traffic is internally carried over IP, interconnection is though still based on TDM and CS#7 technology. This exhibits elements of inefficiency as it leads to multiple conversions between packet and circuit based networks for traffic handles by two or more networks. As long as the current structure for interconnection with the several layers of points of interconnections remains, the call routing is inefficient. Another negative outcome is that the full benefits of NGN, including new service creation and the establishment of new business models are foreclosed.

In order to increase the efficiency in the future, interconnection based on IP instead of TDM technologies will have to be implemented. As of today, the existing service providers have implemented TDM based interconnection. If these networks should migrate to IP interconnection, additional investments are required. Therefore, a balance has to be struck between one-time investments in the migration from TDM to IP interconnection on the one hand, and the potential static and dynamic efficiency gains to be realized from such a migration. As the costs are mainly to be borne by the legacy service providers, the incentives to migrate to IP interconnection are limited.

3.6 Legislative Framework for NGN

The deployment of NGN would require high upfront cost. The investor would require stable regulatory and legislative environment before putting such huge investments. The regulatory challenges and obstacles related to migration to NGN, emergence of new category of service providers, changing business models, network security risks, competition and level-playing field etc. need to be addressed on priority basis. Unless license conditions and regulations are properly redefined, it would be difficult to encourage smooth migration to NGN. Considering all the above issues and given the stage of fast network and infrastructure development in various countries, the time is appropriate to address regulatory and licensing issues related to NGN. This will not only help to have a closer look at licensing and regulatory framework, but will also help in reducing investment risk for operators. Initially the regulatory framework in various countries envisaged access service providers' (viz. Basic Service Operators and Cellular Mobile Telecom Service Operators), Long Distance Service and Internet Service Providers (ISPs. The services under each license were rigidly defined and likelihood of overlapping of any particular service under other telecom license was very remote. Later, Unified Access License under which a licensee can provide different access services i.e. Fixed Mobile & Internet. The licensing framework so evolved effectively brought huge investments in telecom sector resulting in enormous growth, better quality of service, competition, choice to the customer and above all availability of telecom services covering wide geographical area and population. The fast telecom growth in the sector has witnessed equally fast technological advancements. The advanced network architecture and hierarchy has facilitated provision of new services and applications with ease which was not possible earlier when services were rigidly bind with type of switches (Exchange) installed. These new developments are facilitating large number of value added services and applications which can be provided using different platforms blurring the boundaries between different licenses. As an example, Broadband is permitted to Internet Service Providers but same platform supports Internet telephony also. IPTV and many more triple play services, which are conventionally under access service provider's license, can technically be provided by ISPs over broadband services. The challenge before the Regulators is how to maintain balance between existing regulatory framework and fast technological developments taking place in telecom sector. Sticking to the existing regulatory framework may restrict fruits of technological advancement to reach to the common masses; whereas permitting new technologies and applications and encouraging use of IP networks contradict existing legislative provisions and may affect level playing field. While one school of thought advocates support to encourage migration to NGN as it is user friendly and enables customers to access advanced services and applications at cheaper cost, others feel that NGN is nothing but technological advancement and therefore, they feel that there is no legislative concern. The decision to either migrates to NGN platform or otherwise is commercial and therefore they feel that it may be left to service providers. According to them, existing time tested licensing framework should not be tampered with.

The migration to NGN implies that the borders between different business models, services and markets are dissolving. To cope with this, the licensing regime must contain universal licenses for network operators enabling these to offer any IP based service and application of one single All-IP network.

A major issue to be regarded when licenses are amended is the issue of mandated IP interconnection. In addition there are some minor issues with regard to licensing which might have negative outcomes on the service providers, but these are no major obstacles for the migration to NGN.

The changes to the completely technology neutral licensing regime are important for the migration to NGN and these are technology neutral, there is no need to wait for further technological or market developments to occur.

It is an interesting question to discuss the role of the regulatory framework to enable and foster NGN. NGN is a significant change to the market triggered by technical and economic processes. In a competitive environment, NGN needs a certain framework, however, the question is whether such framework can and should be predefined or whether market forces should prevail and regulation should step in case competition is hampered.

The role of regulation is to step in case of market failure, e.g. the abuse of market power or foreclosure of market entry. This seemed to be a "natural" development in times of market opening when there was the danger that legal monopolies became factual monopolies despite formal market opening. The situation today is different. Regulation needs to be justified by market failures. The migration to NGN does not display market failures, the distortion of competition or foreclosure of entry right away. These results are possible, depending on the local situation but there is no inherent connection between the migration to NGN and e.g. market power. Therefore, any approach to "plan" the migration to NGN from a regulatory perspective must be taken with great care. The alternative is to let market forces work first and then to intervene only in case where the market does not fulfil its functions. This would also imply that the migration to NGN follows a technology and market defined "roadmap" but not a regulatory roadmap.

4 Reviews from NGN Deployment

4.1 Objectives for NGN Deployment

Scenarios and plan for migration should be decided according to each country or operator situation. In general there are two high level views to be considered when migration is requested.

First one is the considering migration to NGN as a way to improve infrastructure. In this case, migration plan should be focused on replacement of legacy telecommunications by so called "All IP" including expansion of deployment of "Broadband."

The other is the considering migration to NGN as an enabler of their society such as encouraging e-Society. In this case, migration plan should be focused to support convergences such as Fixed Mobile convergence as well as supporting various applications (e.g. e-health, USN etc).

It is recommended that both views should be combined with balance which will be different according to each country or operator situation.

4.2 Learning from Prior Experiences

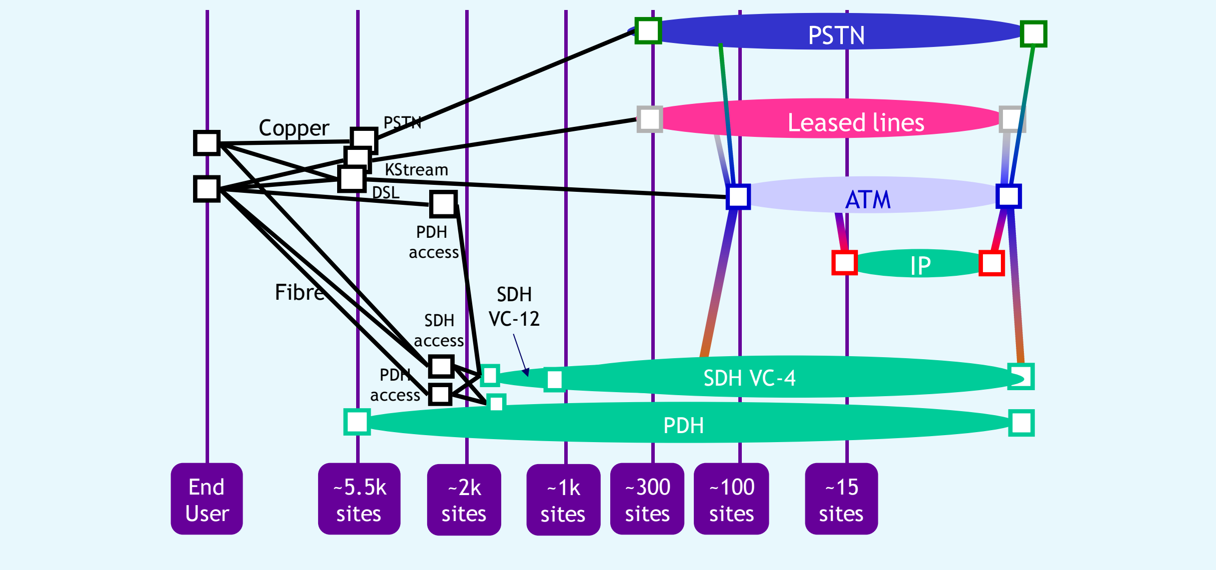
4.2.1 Improve Infrastructure

One of the advanced experiences on migration to NGN has been announced by the BT with the name of "21C Network" which will take a key role of BT networks for 21C businesses. One of interesting things to find from BT's 21C network plan is that comparing their current network structure and 21C network's. This gives us very important message what are benefits of implementing NGN especially for the network operators.

Following Figure 4-1 shows network structures of current BT's network comprising with various transmission networks and various different nodes which have different roles according to their responsible services and geographical position. In the case of core network, there are also different networks supporting different routings according to the service specific features.

This service oriented structure and network configuration cause duplication of infrastructural elements such as transmission nodes or routing nodes. In addition it also requests complicated operation of services and networks because different systems involved for specific services. These aspects need more investments which might cause duplication of provisioning and might require additional resources for operation and maintenance causing more expense of human and financial resources.

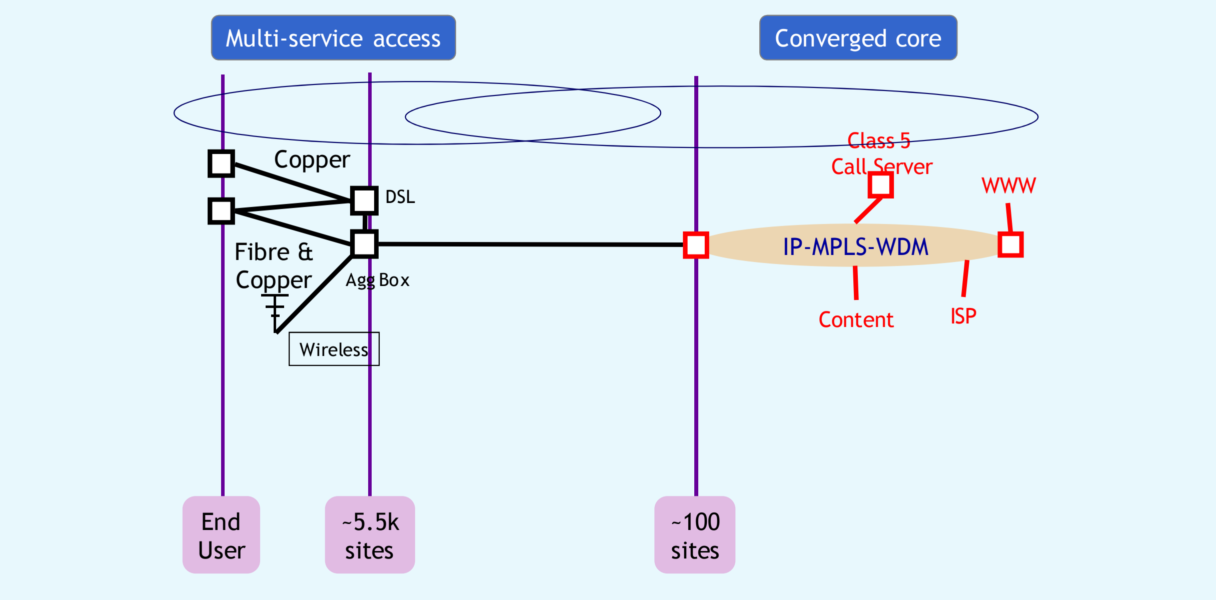
Figure 4-1: Legacy Network structures of BT with number of nodes



In contrast of the current BT's network configuration, 21C network shows a rather simple structure but more powerful capabilities not only for voice services but also broadband services as well. Figure 4-2 is a simple configuration model of 21C network. Figure 4-1 is showing simplicity of structure and especially remarkable reduction of number of nodes while keeping full coverage of customers. This structure has been advantaged from "All IP" features to make simple configuration in core networks, so all services should be routed by the IP core networks with different flows which have different treatment from the traffic management and service provisioning aspects but using same systems.

One more advantage of this structure is to shorten and to extend the contacting points of the customers allowing the network to cover customers more closely. This is the reason this structure keeps most number of the nodes located in the customer sides while removing other nodes from the previous structure.

Figure 4-2: 21C Network structures of BT with number of nodes



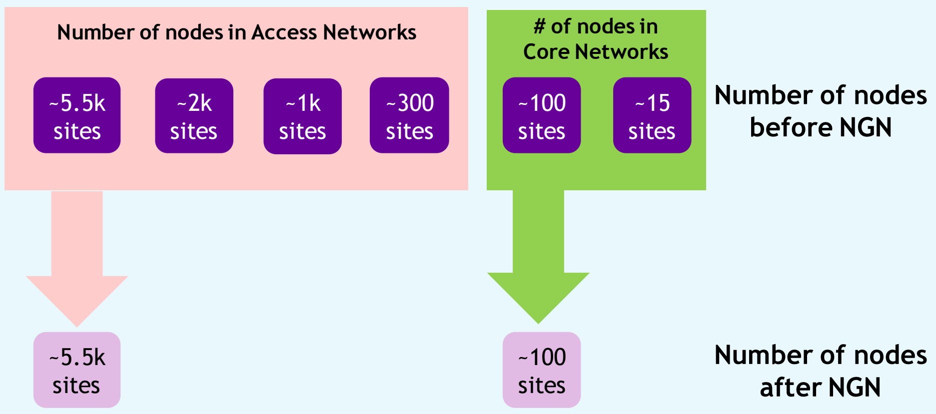
Adoption of NGN in BT's network by the name of "21C Network" shows how infrastructure be improved to meet future business trends and users/operators' requirements. It is required to look at carefully BT's implementation of NGN and will get more learning from improvement of infrastructure aspects.

One of report tells us this new structure will give benefit to reduce 30~40% reduction of Green House Gas emission which is now becomes serious subject for the world. Simple calculations are support this report as following:

- Reduction of Access Nodes: from 8.8 K sites to 5.5 sites (37.5 % reduction).
- Reduction of Core Nodes: from 115 sites to 100 sites (14 % reduction).

This report does not try to evaluate this result from cost aspects, but this is generally assumes huge amount of cost savings if including costs of operating each site.

Figure 4-3: BT benefits from 21C networks



4.2.2 Enhancing Society

The other types of migration to NGN is providing infrastructure for building up new society such as e-Society. This approach has been announced from the Rep. of Korea by their name of "BcN: Broadband Convergence Networks" and is being deploy now in Rep. of Korea.

One difference of Korean case is that they initiate this project at the almost end stage of their broadband deployment. Therefore their vision on the BcN has been quite different from BT's case study. The main points are the following:

- Build a state of the art information infrastructure in the world.
- Create an environment to use high-quality multimedia services.
- Prepare the core plan according to the IT Industry market growth.

As shown these vision statements, Korea rather focuses to build up their new social infrastructure while BT focuses to improve their infrastructure. So Korea uses kind of role sharing model which each sector took different roles. According to this, government took a role to encourage development of new services and application which will use for building up e-Society such as e-learning, e-health, USN etc. Network operators, are rather focusing to upgrade their infrastructure for supporting convergence services such as FMC and IPTV while continuing improving access network capabilities to provide more bandwidth to the customer.

5 Case Studies

5.1 Case studies on LLU and Fiber Investment

Turkey, National Regulatory Authority (NRA) ICTA, took a decision for the fibre investments. According to the 03.10.2011 dated decision of ICTA, fibre investments of operators will not be subjected to any obligation for a 5 year period or until the rate of retail internet subscribers come to the level of %25 within the total broadband subscribers. It means that fibre services will not be assessed in any market definition within this time period. Turkey is still in a process of the migration from existing networks to NGN. In the beginning of the migration process, upon the application of Turk Telekom which is the incumbent operator in fixed line services, ICTA analyzed the situation very deeply. Within the assessment period, ICTA also considered how the fibre infrastructure deployment can be fostered in a best way and spread in the shortest time by promoting the operators to invest.

During this 5 years period Turk Telekom will also provide wholesale services via fibre infrastructure by re-sale and bit-stream access customers under equal terms and without discrimination. On the other hand, the regulations in the fibre deployment area should not contradict with the right of way applications. Laws taken as a right of way must support fibre exemption.

Fiber exemption decision of Turkish NRA can be envisaged as an alternative method in order to stimulate the operators for making fibre investments and taking the return of investment in a shortest and rational time period. However, outcomes and results of this exemption decision should be monitored for sure. We should keep in mind that all the approaches needed for the new situation comprise some risks and may result negatively. However, we believe that Turkish NRA's above mentioned exemption decision can be accepted as a role model for some countries having similar market structure compared with Turkey.

This regulation aims to protect the investment not to obstruct the fibre division. In conclusion, countries should analyse their own market structure and infrastructure during the fibre deployment. Countries' own national regulatory authorities should decide for a way to protect the investments according to their own market structure, infrastructure properties and welfare of the country.

5.2 Case Studies on NGN Deployments

ITU recently took up the project for the developing countries in Asia-Pacific region to have assessment on technical and regulatory aspects of NGN Migration with specific country experiences with the objective that it would also help to build capacities in the migration to NGN environment through workshops and trainings on related NGN issues in the Asia-Pacific region as well as disseminate NGN related case studies by promoting cooperation mechanism. The report on Best Practices for Implementing NGN in Asia Pacific Region – Case Studies on India, Philippines, Sri Lanka and Bangladesh can be found online at: http://www.itu.int/ITU-D/tech/NGN/CaseStudies/CaseStudies.html

6 Methods for the Promising Technologies and Status of NGN Deployments

6.1 Methods for Determining Most Promising Technologies for NGN Construction

The technique is based on the principle of simulation of construction or reorganization of the infocommunication network in order to evaluate the cost and duration of the transition to the use of certain sets of technologies that meet all the requirements of the network owner.

In Figure 6-1 generalized algorithm of method is shown. The algorithm involves a parallel (independent) four preparatory procedures, the results of which further are used in determining the most promising in terms of cost and construction period (reorganization) variant of construction of infocommunication network.

The first of the four procedures (indicated by number 1 in Figure 6-1) consists of two basic steps: entering of the information about the structure of an existing or projected network and allocating independent network segments to be built. The first of these two steps involves the gradual introduction of information about each network element (hardware or communication channel) to those levels which upgrading or building regard to. Besides the types and specifications of each element at this step the information about elements interconnection between each other through special interfaces (both within the same level and with equipment from other levels) should be entered.

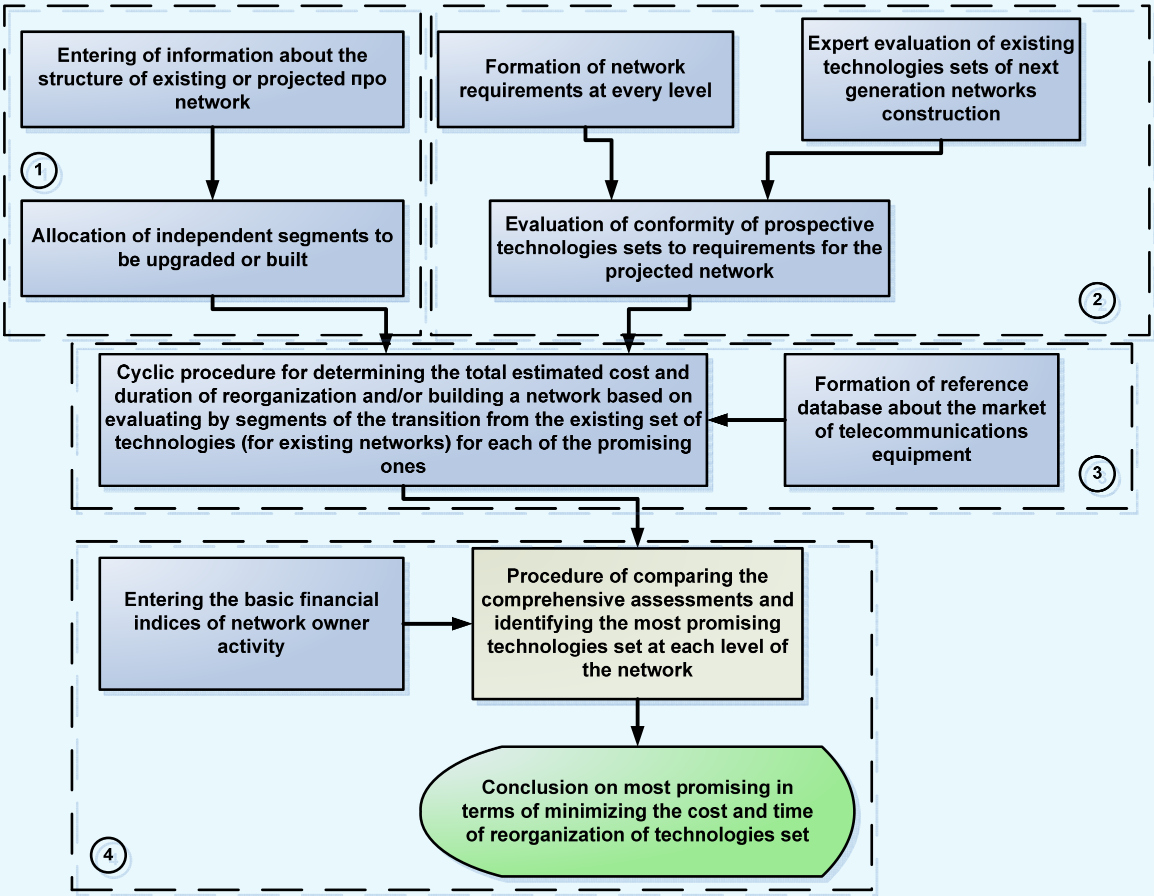
The second procedure (indicated by number 2 in Figure 6-1) is intended for allocation from the totality of sets of technologies that today can be seen as promising for upgrading or construction of infocommunication network, only those sets that meet the requirements of the network owner. The procedure consists of three main steps: the formation of network requirements at all levels, expert evaluation of existing sets of technologies of infocommunication networks building and evaluation of conformity of prospective technologies sets to requirements for the projected network. As a result of the procedure it should be obtained the list of those sets of technologies (for each of the levels of the network) that fully meet the requirements of this network by its owner. The transition to these technologies sets will be matched in subsequent steps of the method in terms of cost and duration of reorganization for each of them.

The third procedure (indicated by number 3 in Figure 6-1) is the most complex in terms of number of operations. This procedure involves cyclical bust of all selected independent segments (that are upgrading or building) for consistent evaluation of their transfer to new promising technology sets (or building using these sets of technologies). This difference between upgrading the existing network and building the new one is primarily in the fact that when upgrading the existing one the additional time and costs of dismantling of existing equipment and / or existing communication channels are taken into account. The basis for the procedure is specially formed informational database about the market of telecommunications equipment, which includes information about the possible interchangeability of models against each other. The result of this procedure is a vector of cost and duration of modernization (or construction) of network (by its levels) on the use of a set of promising technologies.

The last procedure of algorithm (indicated by number 4 in Figure 6-1) involves identifying the most promising set of technologies at each level of the network based on the comparison of cost and duration of modernization (or construction) taking into account the basic financial indices of the network owner activity in the direction of its operation (e.g. by defining payback period of telecommunications network operator)

It should also be noted algorithm that shown in Figure 6-1 shows only the general principle of determining the set of promising technologies, and its specification for specific conditions (building a new network or reorganization of existing, construction of networks on various levels, etc.) involves the use of detailed algorithms.

Figure 6-1: Generalizes algorithm of method



6.2 Status of NGN Deployments

ITU Databases, especially Tariff Policies databases shown various useful statistics. The objective of this database is to track and show trends in the application of Tariff Policies related to pricing, cost/tariff models, analytical accounting, interconnection charges, management of universal service and price control in different countries. Data is provided annually by Telecommunication Regulatory Authorities and Network Operators. This reflects the situation of the Regions at the date the questionnaire is completed. Followings from Figure 6-2 to Figure 6-4 are statistics, especially related on Next Generation Networks which come from ITU World Tariff Policies Database.[3]

[3] See ITU's ICT eye for further information, http://www.itu.int/icteye

Figure 6-2: Stage of introduction of NGN system by operators, 2012

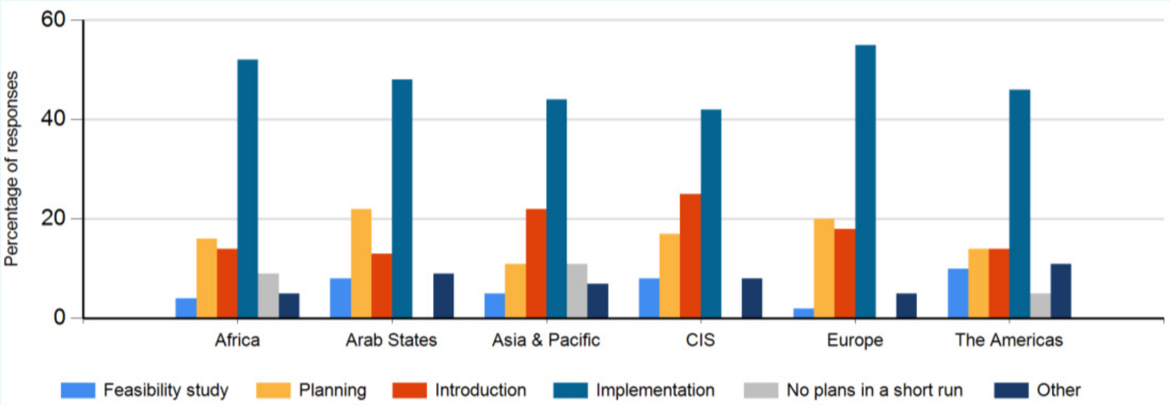


Figure 6-3: NGNs: Regulations that govern the use of IP networks for voice services, 2012

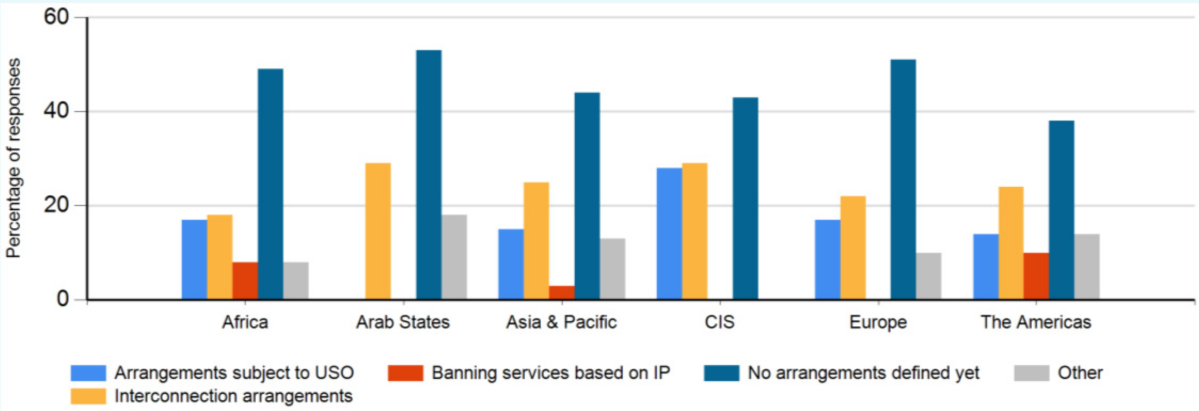
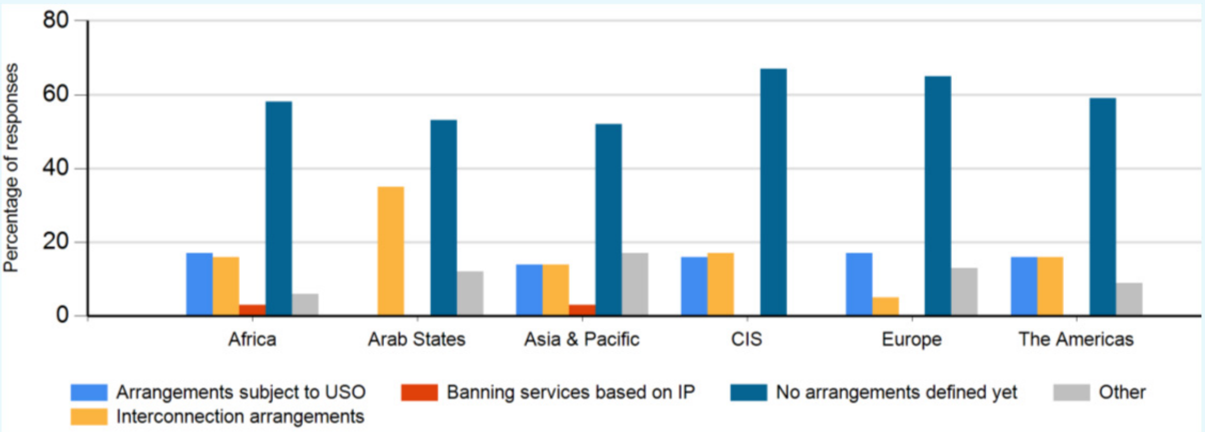


Figure 6-4: NGNs: Regulations that govern the use of IP networks for data services, 2012



Annexes

Annex 1: Trends in Telecommunications

Annex 2: Tariff Considerations for Data Services including NGN

Annex 3: NGN Functional Architecture/Security

Annex 4: Quality of Service in NGN

Annex 5: NGN Management

Annex 6: NGN Testing

Annex 7: Examples of Migration Scenarios

Annex 8: NGN Issues

Annex 9: ITU NGN Standards

Annex 1: Trends in Telecommunications

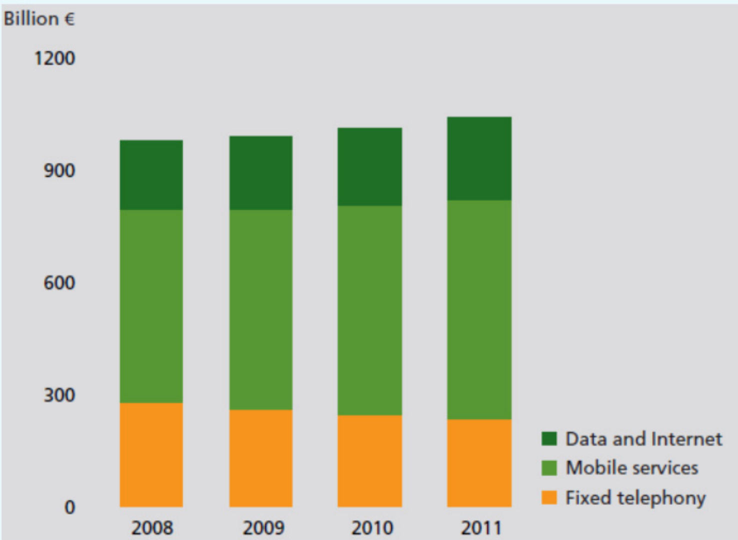
1 Market Trends

1.1 Overall Telecom Market Trends

General analysis of telecom market trend is rather positive in many of countries. Many of reports informed their last year analysis results. This report makes references to various reports: the analysis from Ofcom, United Kingdom published as “The International Communications Market 2012”, ITU reports on “Measuring the information society: 2012” and “ICT Facts and Figures: 2011 and 2013” . These reports do not cover all areas on the world but give certain information to look at overall trend of telecom businesses.

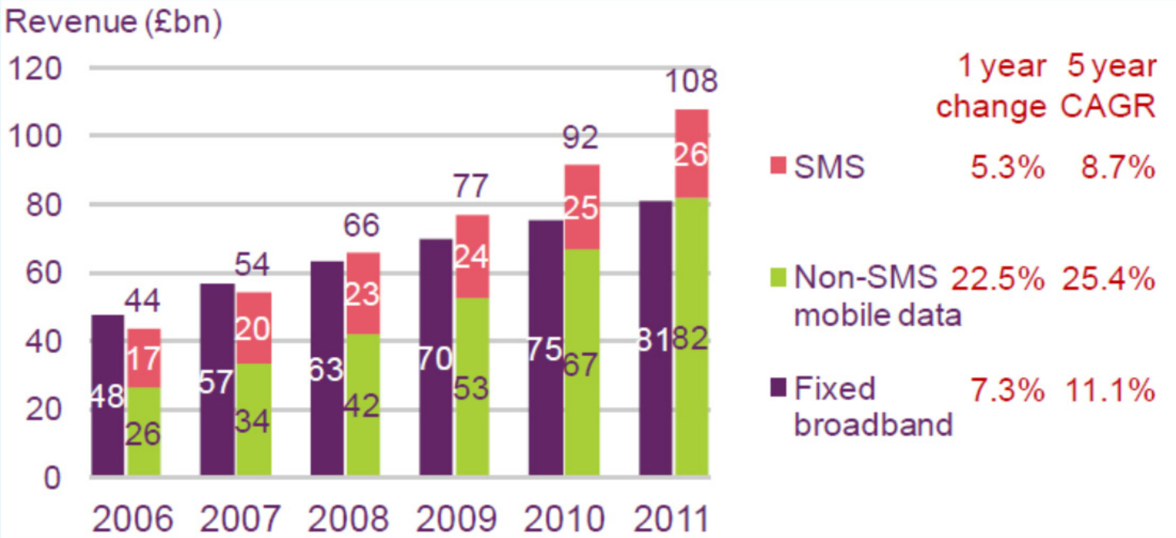
Figures from the ITU show that by the end of 2011 2.3 billion people (around a third of the world’s population) accessed the internet globally, almost double the 1.2 billion figures recorded in 2006. Over this period growth in internet use was fastest among developing countries, and by 2011 62% of internet users were located in developing countries, an increase from 44% in 2006. This trend is lead by expansion in mobile and broadband services for data and internet as the key telecommunication market while fixed voice oriented services are continuously diminishing as shown in Figure 1-1.

Figure 1-1: Global telecom services market growth by segment (IDATE)



The report by Ofcom, United Kingdom indicated that there was rapid growth in the take-up of fixed broadband services across the 17 countries in the five years to 2011, during which time fixed broadband take-up almost doubled to reach 42 connections per 100 homes. Increasing take-up of fixed broadband and mobile voice and data services have contributed to an accelerating decline in the use of traditional fixed telephony services in most of the countries. Despite significant growth in fixed broadband take-up, revenues from mobile data services exceeded those from fixed broadband connections for the first time among surveyed 17 countries in 2011 as shown in Figure 1-2.

Figure 1-2: Fixed broadband and mobile data revenues (2006 ~ 2011) (IDATE)



As a total in the survey of Ofcom, mobile data has seen the fastest growth rate (CAGR) of 25.4% between 2006 and 2011 meaning that, for the first time in 2011, mobile data revenues (£82bn) exceeded fixed broadband revenues (£81bn, CAGR of 11.1%). The report analyzed that this growth in mobile data revenue has been driven by a rapid increase in the adoption of smartphones, from which it is much easier and quicker to access the internet. SMS revenues increased at a slower CAGR of 8.7% between 2006 and 2011. Although SMS volumes are still growing but revenues have failed to keep pace as operators have started to offer large bundles of SMS messages as part of subscription packages; this has stimulated use but caused revenue pressure for SMS in many markets. However, much of the revenue growth in fixed broadband in developed countries was realised towards the start of the five-year period when take-up was growing rapidly. Fixed broadband may now be approaching market saturation in many European countries, as the majority of households subscribe to fixed broadband services – limiting revenue growth for the year 2011.The Ofcome report identified three of the key developments which are transforming the global telecoms market, both in terms of industry structures and consumer behaviour:

- The mobile data explosion: the growth in mobile data, with key volume, subscriber and revenue statistics, and sheds some light on the transition from large-screen PCs to small screen smartphone mobile data use.
- Continued growth in superfast broadband networks: the deployment of superfast technologies across countries, and the extent to which consumers are migrating to these services.
- Increased use of text messaging: the contrasting levels of use and expenditure related to texting, and examine attitudes towards texting.

1.2 Trends in the Voice Service Market

The Ofcom report indicated that the fixed voice call volumes continuously fell in most of countries for which figures were available in 2011 except France, where they increased by 0.6% to 113 billion minutes during the year (Figure 1-3). The resilience of the fixed voice market in France is largely as result of high take-up of managed VoIP services, often provided as part of a triple-play bundle of fixed broadband and IPTV services over naked DSL. Naked-DSL-based broadband services do not require a standard fixed line, so VoIP over naked-DSL provides a low-cost alternative to voice calls made over traditional fixed networks, as no line rental is paid. It is this which is the primary driver of the 13.1% fall in fixed voice revenues in France in 2011, despite call volumes increasing during the year. In the UK, fixed voice call volumes fell by 10.0% to 116 billion minutes in 2011, this rate of decline being the fourth highest among 15 countries.

It is noted that the major drivers behind declining fixed call volumes are the low cost of mobile voice and text services and high smartphone take-up, which has contributed to the increasing use of alternative forms of communication such as email and instant messaging. France and the Netherlands (where VoIP use is widespread) were the only countries compared where fixed call volumes increased in the five years to 2011 (up by 1.8% and 0.4% a year on average, respectively). Conversely, the highest average annual rate of decline over the period (13.0%) was in Australia, where fixed call volumes halved over the period, largely due to the increasing use of mobile voice services. As a consequence, fixed voice revenues continuously fell in 2011, the fastest rates of decline, with revenues falling by 17.8% in China and 15.3% in India during the year.

Figure 1-3: Fixed line call volumes and revenue, 2006 and 2011

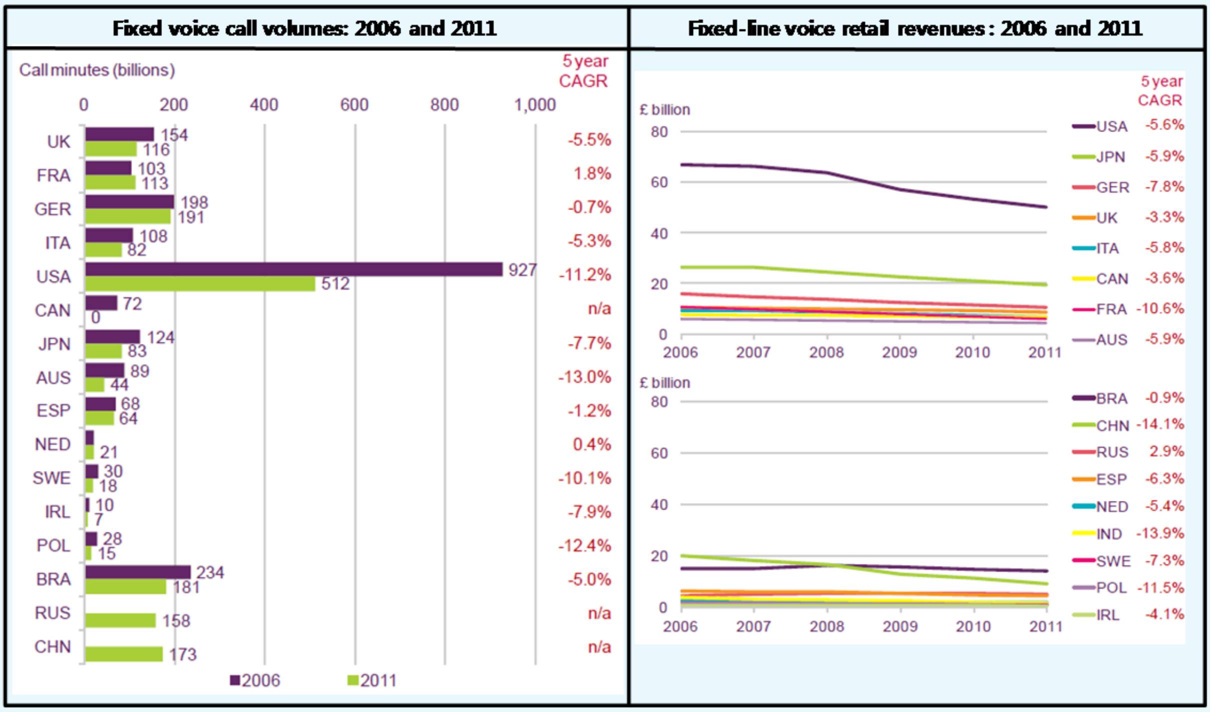
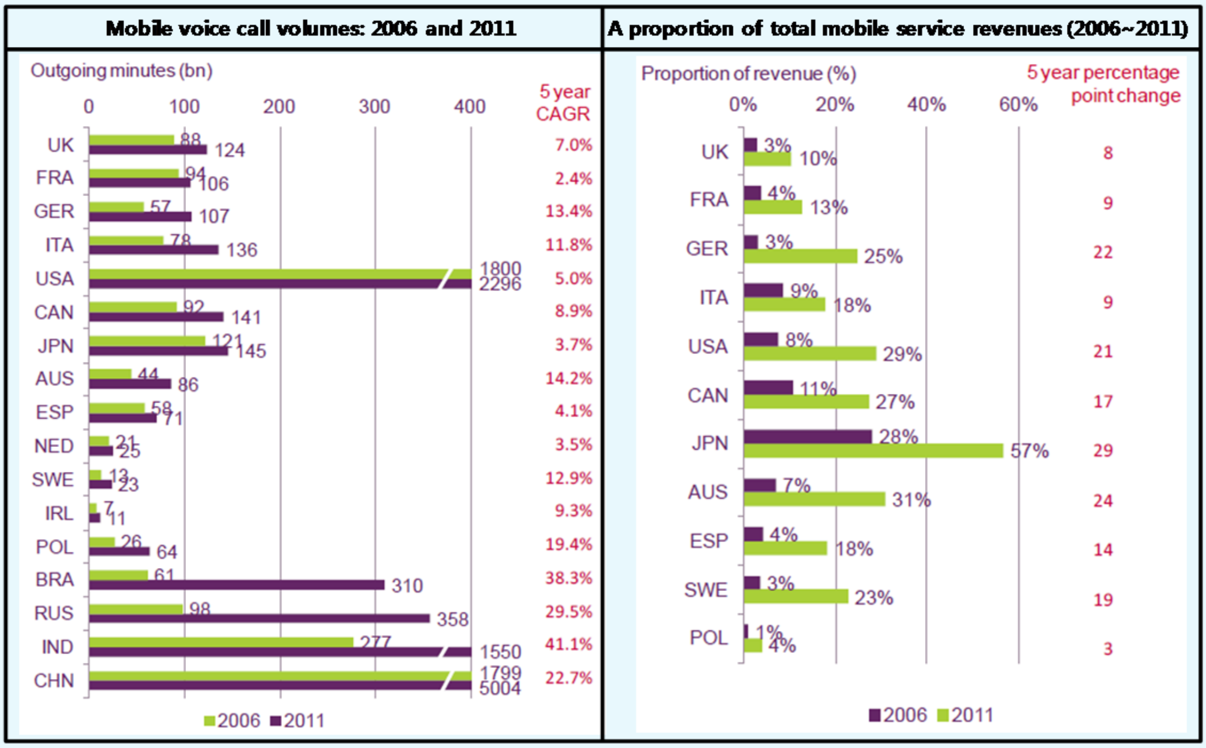


Figure 1-4 shows the status of mobile voice call minutes and revenues by Ofcom report. The countries where the highest proportion of calls originated on mobiles in 2011 were China (97%), the United States (82%) and Poland (81%). In China and Poland this is partly due to the limited availability of fixed telephony networks, while the proportion of calls that are mobile-originated will be overstated in China, the US and Canada as the mobile call volumes used in the calculation include incoming call minutes. Germany and France were the only comparator countries where less than half of voice call minutes originated on mobile networks in 2011 (36% of voice call minutes were mobile-originated in Germany in 2011, while the figure was 49% in France).

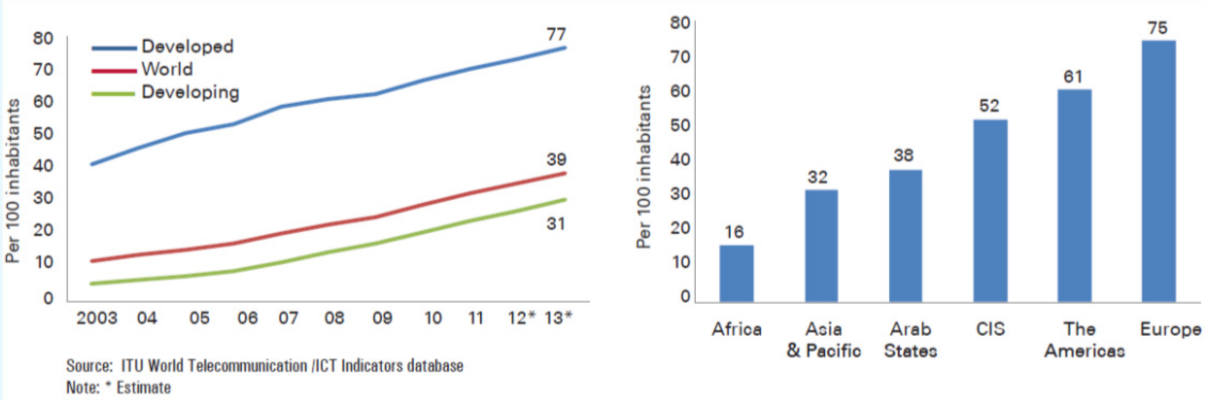
Figure 1-4: Mobile call volumes and revenue, 2006 and 2011



1.3 Broadband Market Trends

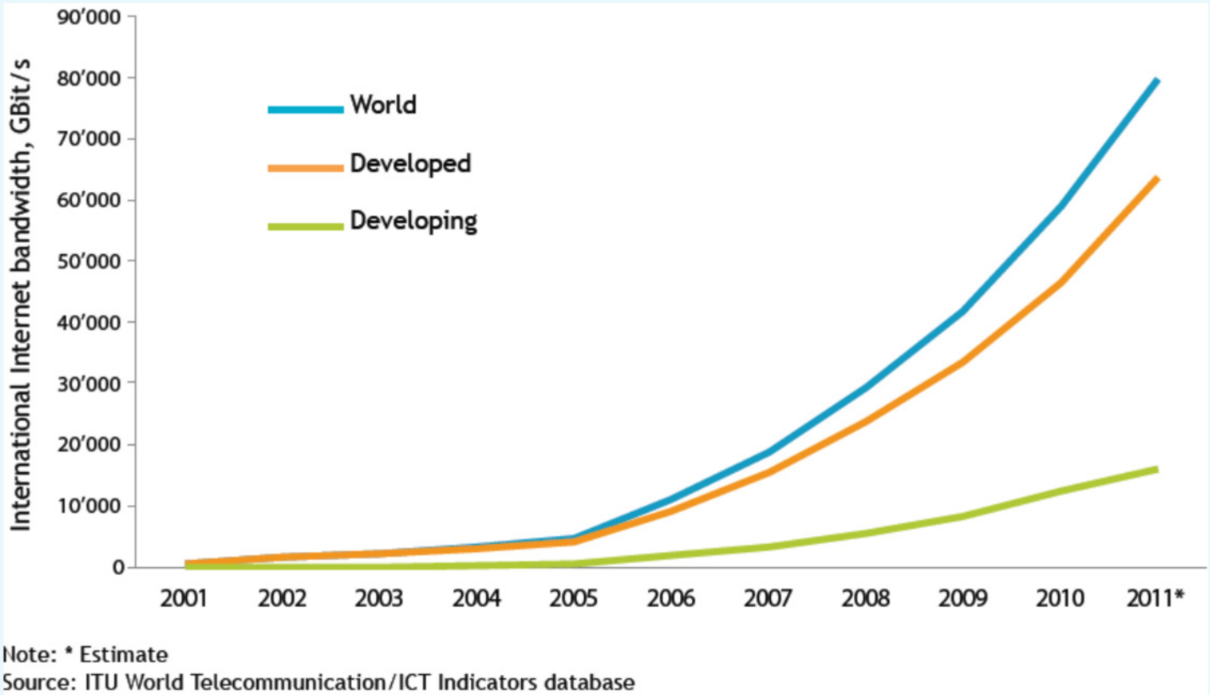
Benefitting fixed broadband and mobile, especially smartphones, internet users (use of more data including information) is increasing as shown in Figure 1-5 (by ITU, ICT facts and figures 2013).

Figure 1-5: Internet users by development level and region



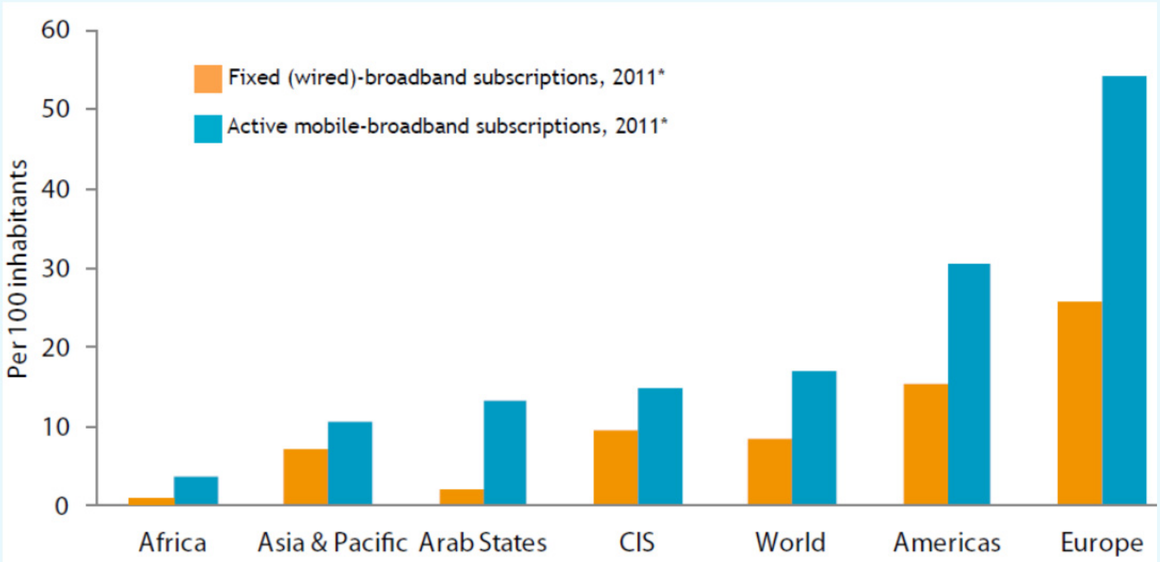
As a consequence, bandwidth consumption of the world continuously increased as shown in the Figure 1-6 below (by ITU, ICT facts and figures 2011).

Figure 1-6: Growth of bandwidth



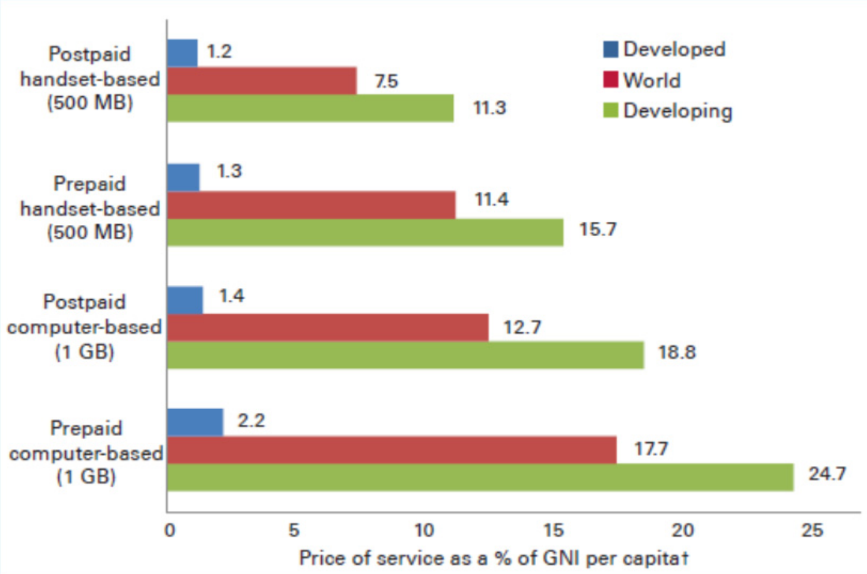
One interesting phenomena is that mobile broadband users are exceed fixed broadband users as shown in Figure 1-7 (ITU, ICT facts and figures 2013). This phenomena is apparent in all of the regions, in both developed or developing countries, which in turn means users enjoyed connectivity over mobile environments.

Figure 1-7: Status of broadband in 2011



Following the analysis by ITU as shown in Figure 1-8, it is noted that mobile broadband is more expensive in developing countries but considerably cheaper than fixed broadband services. By early 2013, the price of an entry-level mobile-broadband plan represents between 1.2-2.2% of monthly GNI p.c. in developed countries and between 11.3-24.7% in developing countries, depending on the type of service. However, in developing countries, mobile broadband services costs are considerably lower than fixed-broadband services costs: 18.8% of monthly GNI p.c. for a 1 GB postpaid computer-based mobile-broadband plan compared to 30.1% of monthly GNI p.c. for a postpaid fixed-broadband plan with 1 GB of data volume. Among the four typical mobile-broadband plans offered in the market, postpaid handset-based services are the cheapest and prepaid computer-based services are the most expensive, across all regions.

Figure 1-8: Price of mobile-broadband services, early 2013



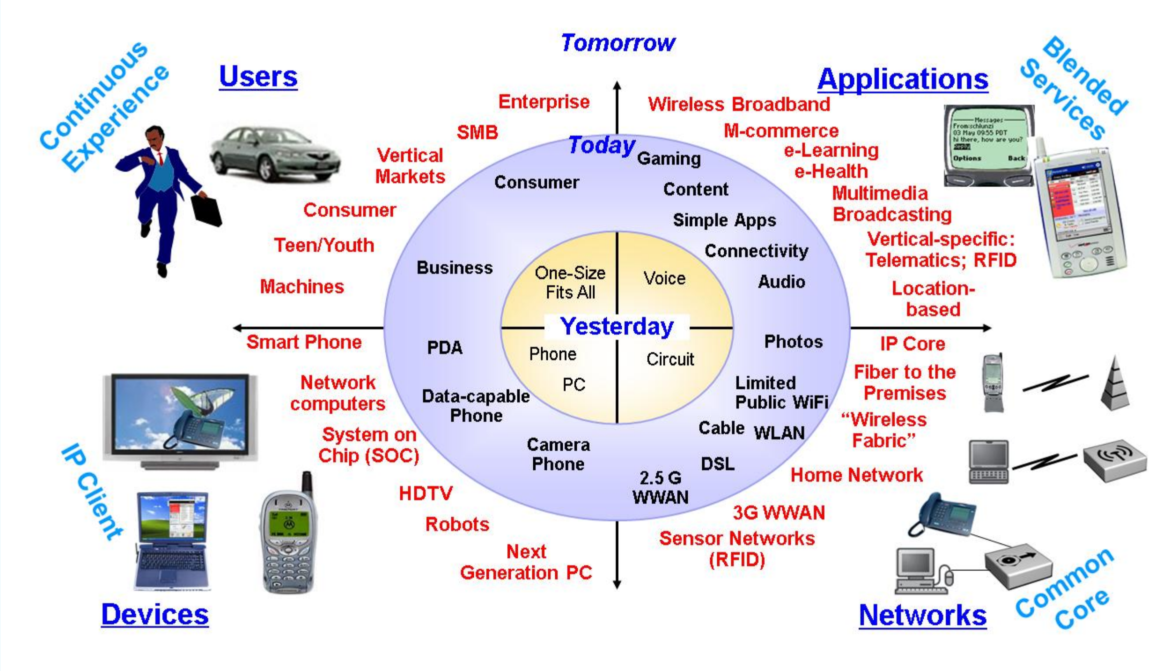
2 Overall Trends in Telecommunications

2.1 Overall Development Trends

There are various angles to look at trends of development in telecommunication such as users' aspects, services/applications' aspects, devices' aspects and networks' aspects etc. Because of the recent developments in telecommunication (should be included with the concept of ICT), this is not an easy task with short sentences like in this report. Therefore this report broadly looks at the development trend from these four different aspects.

In this regard, following Figure 2-1 provided an overview of technology development, taking into account the evolving trends related to users and services/applications.

Figure 2-1: Abstraction of development trends



- **User perspective:** Previous users were quite well-fitted with fixed types of services e.g. a black phone for voice service and a facsimile terminal for graphic service. So it featured as one size service fits all kinds of users. However, users today request more dynamic types of services depending on their lifestyle, and whether they are using the service as a consumer or for their business, etc. This is likely to continue developing in the future and as a result their usage of telecommunication services and applications with require services at anytime, anywhere and on any device.
- **Service/Application perspective:** Voice services have been the key service for telecommunication providers during more than 100 years. This has is now expanding to cover more other services than just voice, including multimedia services with broadband connectivity which are available today. It is further anticipated to expand to cover various services/applications mixed together, which sometimes is called convergence and other the provision of blending services.
- **Network perspective:** Previous circuit oriented networks have evolved to the packet networks of today (mainly using internet protocol (IP)), including continuously increasing bandwidth using xDSL and fibre optics and wireless technologies such as WiFi and WiMAX. This will be leveraged by common core networks in the near future, which will be IP-based but enhanced by other elements such as Quality of Service (QoS) and security.
- **Device perspective:** The area which has seen the most remarkable development is the device area. The key themes in the development of devices include the need for them to be portable, multi-functional and smart. Moreover, as the use and growth of IP is expected also for the near future, devices should be IP-enabled.

2.2 Convergences

During the past several years, the ICT domain has continuously developed to support various types of convergences with a vision of "Any Time, Any Where, Any Services and Any Devices." This trend has been led by the development of the associated technology and the notion of "any information/service over any transport infrastructure." One traditional example of this is VoDSL (Voice over DSL). DSL was developed to provide broadband connectivity but today this is used for voice services such as VoIP. Another example is TVoMobile (TV service over Mobile). Mobile was developed to provide voice services while users move around, but today mobile is also used for watching TV.

Especially with development of NGN, fixed mobile convergence (FMC) is now becoming the first instance of converged fixed and mobile services, and IPTV is also following with the convergence between telecom and broadcasting. Moreover, convergences using ICT are rapidly expanding to cover many of the industrial areas.

Figure 2-2: High level view of the converged environment

Convergence can be classified into two main groups:

- **Internal Convergence** (within the same industry): This means the convergence between different services and/or networks but within the same industries, such as FMC and IPTV. FMC is the convergence between fixed and mobile, but both two belong to the same industry, the telecom industry. IPTV is the convergence between telecom and broadcasting but they also belong to telecom industry in their wider interpretation.
- **External Convergence** (between different industries): This means the convergence between/amongst different industries, e.g., Telematics/ITS, USN, e-Health, Networked Robotics and others. This type of convergence requires more complicated processing not only from the technical aspect but also from regulatory and political aspects.

Whether internal or external convergences, the high level view of how services are used in a converged environment can be show as in Figure 2-2 above. Networks will then look like a cloud which allows for the provision of connectivity to the devices anywhere, anytime and where any service can be delivered to any device. Consequently, end users can make use of the services they wish to use in close relation to their real life using handy smart terminal devices and sensors (e.g. USN), even while driving a vehicle.

2.3 Trend of User Willingness

As technology develops further (or maybe even the other way round), end user willingness to pay for specific telecommunication services are also continuously changing. Actually it is better to say “expanding” or “increasing.”

Figure 2-3 shows some interesting results of users’ willingness to pay for services. All types of services shown in the figure (such as online shopping, accessing news online, etc.) have been identified as important activities for end users, which they are not willing to pay for, especially when they are using their mobile phones. However, there is a certain amount of willingness to use the services, even using the mobile phone, when advertisements cover the associated costs. Both these two cases show that there are potential customers who are willing to use such services if they are made available in an economically beneficial way, such as using flat-rates for the fixed-mobile convergence access.

Figure 2-3: Customers’ willingness to pay for services

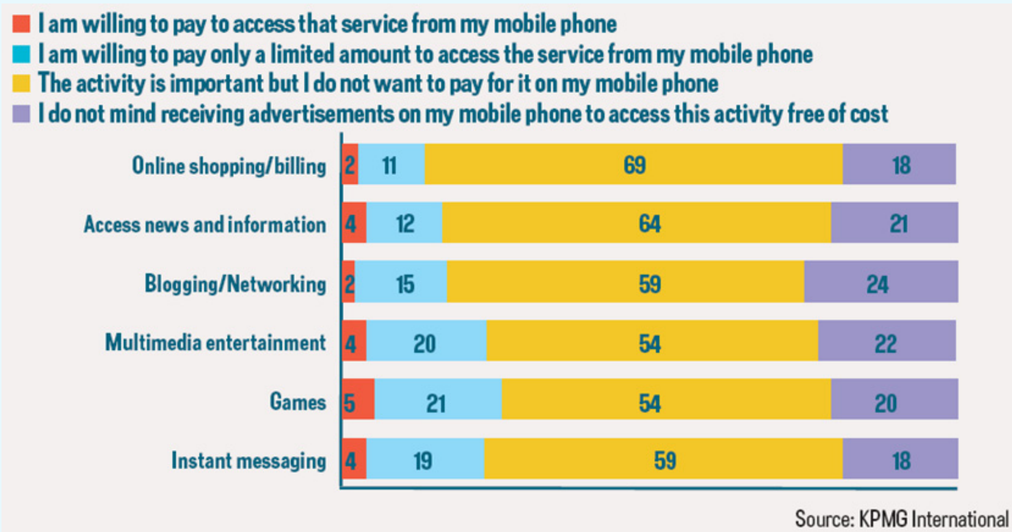
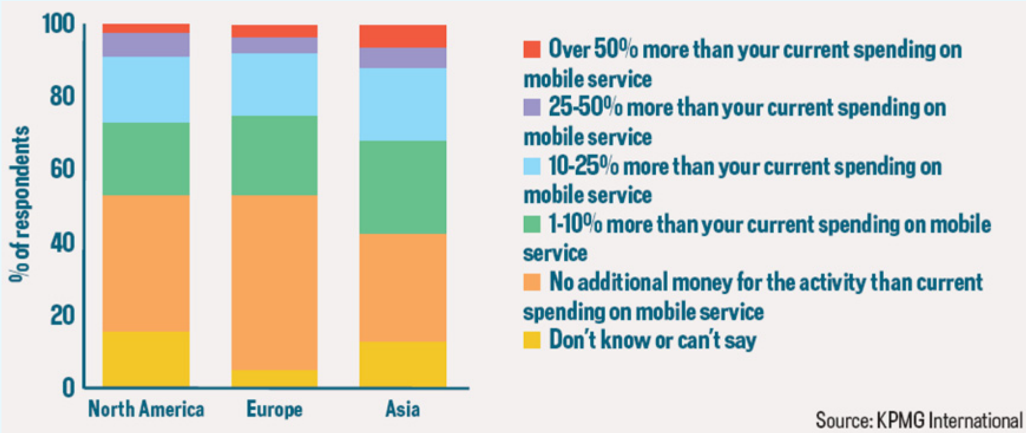


Figure 2-4 shows the results of research done on end user willingness to pay for convergence services. One can see that people in Asia show more interest in converged services than those living in other regions.

Figure 2-4: Customers' willingness to increase spending on converged services



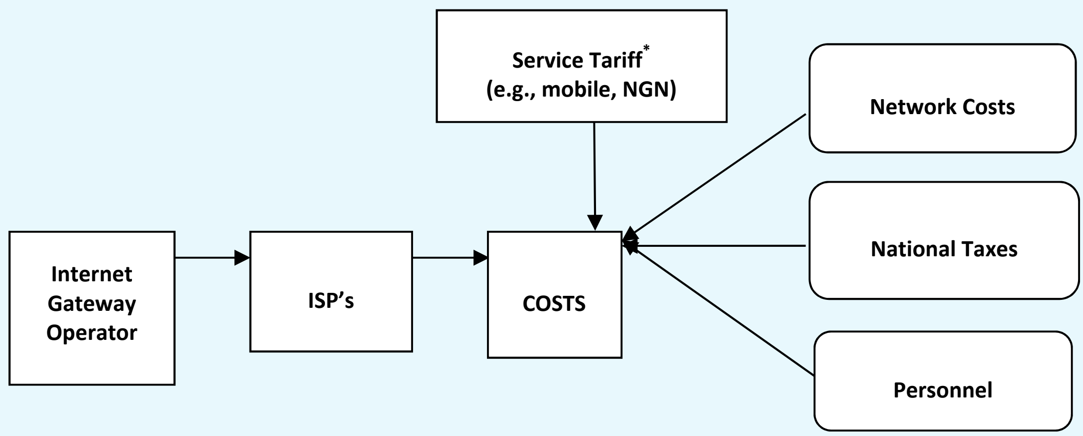
Annex 2: Tariff Considerations for Data Services including NGN

In the voice market, the tariffs are determined by competition. The Regulator sets a uniform interconnection rate across all networks and allows the operators to come up with their own end user rates which are to a large extent determined by competition allowing price differences between the operators. However, tariffs for data services with the advent of NGN's is different, since data services are, in general today, supported by internet interconnected through the gateway.

[Note: In some countries (for example The Gambia), the gateway is still in a monopoly under the incumbent, thus other providers such as mobile operators still need to go through an ISP to get connected to the gateway.]

As regards voice services each operator has the liberty to charge as low as possible to be competitive in price without having to worry much about covering costs. In the case of data services it is not that easy. The extent to which data service prices can be lowered is constrained by the price of bandwidth from the incumbent to the ISP and from the ISP to the other operators, such as mobile operator, in addition to all other network operational costs. The following figure shows this relationship for pricing of data services.

Figure 2-1: An example of pricing on data services



* *This block has been modified from "GSM/NGN tariff" to "service Tariff (e.g., mobile and NGN), because this block shows an input to the costs from other service aspects.*

Annex 3: NGN Functional Architecture/Security

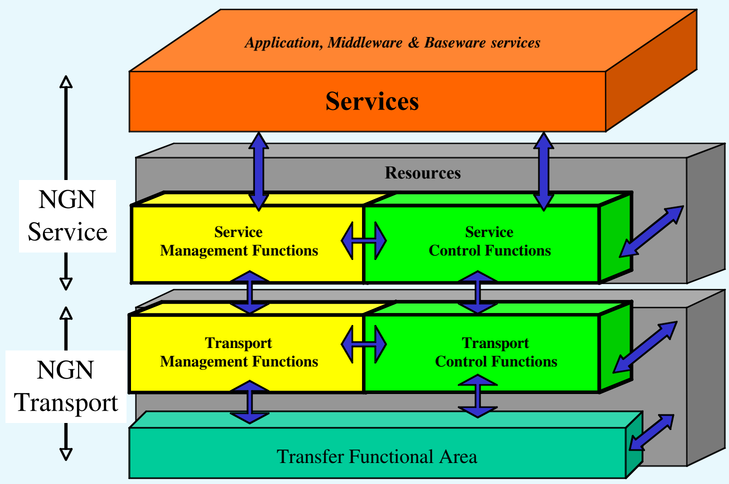
1 NGN Functional Architecture

1.1 General Principles and Reference Architecture Model

As far as NGN systems (non-OSI systems) are concerned, all or some of the following situations may be encountered when considering the OSI 7-layer basic reference model (OSI BRM):

- The number of layers may not equal seven;
- The functions of individual layers may not correspond to those of the OSI BRM;
- Certain prescribed or proscribed conditions/definitions of the OSI BRM may not be applicable;
- The protocols involved may be other than OSI protocols (one notable example being the IP);
- The compliance requirements of the OSI BRM may not be applicable.

Figure 1-1: General functional model of NGN



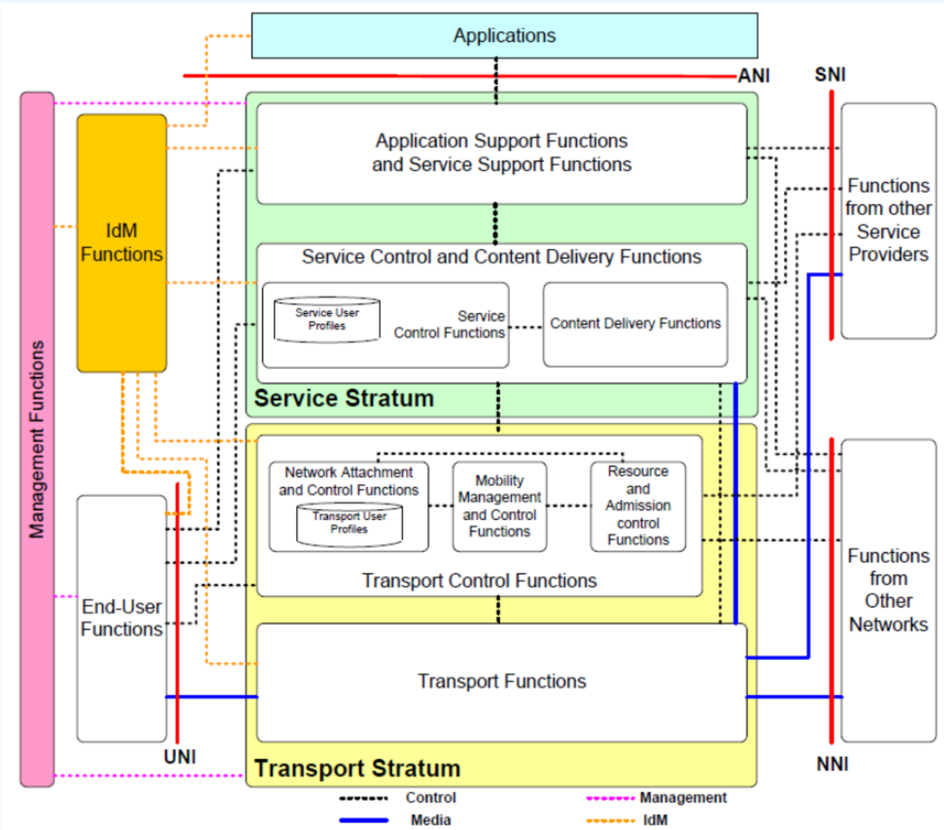
The services and functions are related to each other, since functions are used to build services. It is convenient to assemble functions into two distinct groups, or planes, one comprising all control functions and the other comprising all management functions. The grouping of functions of the same type (i.e., control or management) allows the functional inter-relationships within a given group to be defined, as well as the information flows between functions in the given group.

With this in mind, ITU-T Recommendation Y.2011 goes on to consider the functional aspects of systems implementation. In particular, it develops the following high-level model, which shows how functions may be grouped for the purposes of systems development. The functional blocks shown in Figure 1-1, can then be further decomposed in sub-groups to represent grouping convenient for implementation and distributed system depiction.

1.2 NGN Functional Architecture

NGN services include session-based services, such as IP telephony, video conferencing, and video chatting, and non session-based services, such as video streaming and broadcasting. Moreover, NGN supports PSTN/ISDN replacement.

Figure 1-2: Abstracted NGN functional architecture



The NGN architectural overview shown in Figure 1-2 comes from ITU-T Recommendation Y. 2012. The NGN functions are divided into service functions and transport functions. According to ITU-T Recommendation Y.2011, it is called the functional categories strata.

Customer networks and terminals are connected by UNI. Other networks are interconnected through NNI. Clear identification of UNI and NNI is important to accommodate a wide variety of off-the-shelf customer equipment while maintaining business boundaries and demarcation points for the NGN environment.

1.2.1 Transport Stratum Functions

Transport stratum functions identified in ITU-T Recommendation Y.2012 provide connectivity for all components and physically separated functions within the NGN. IP is recognized as the most promising technology for NGN. Thus, the transport stratum provides IP connectivity for both end-user equipment outside the NGN and controllers and enablers, which usually reside on the servers inside the NGN. The transport stratum is responsible for providing end-to-end QoS, which is a desirable feature of the NGN. The transport stratum is divided into access networks and the core network, with a function linking the two transport network portions.

- **Transport functions**: The transport functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for the transfer of media information, as well as the transfer of control and management information. Transport functions include access network functions, edge functions, core transport functions, and gateway functions.
- **Transport control functions**: The transport control functions include Resource and Admission Control Functions, Network Attachment Control Functions and Mobility management and Control Functions.
  a) Network attachment control functions (NACF): The network attachment control functions provide registration at the access level and initialization of end-user functions for accessing NGN services. The functions provide network level identification/authentication, manage the IP address space of the access network, and authenticate access sessions. The functions also announce the contact point of the NGN Service/Application functions to the end user. That is, the functions assist end-user equipment to register and start the use of the NGN.
  b) Resource and Admission Control Functions (RACF): In the NGN Architecture, the RACF provides QoS control (including resource reservation, admission control and gate control), NAPT and/or FW traversal control Functions over access and core transport networks. Admission control involves checking authorization based on user profiles, SLAs, operator specific policy rules, service priority, and resource availability within access and core transport. Within the NGN architecture, the RACF act as the arbitrator for resource negotiation and allocation between Service Control Functions and Transport Functions.
  c) Transport User Profile functions: These functions take the form of a functional database representing the combination of a user’s information and other control data into a single "user profile" function in the transport stratum. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.
  d) Mobility Management and Control Functions (MMCF): The MMCF provide functions for the support of IPbased mobility in the transport stratum. These functions allow the support of mobility of a single device. The MMCF provides mechanisms to achieve seamless mobility if network conditions permit, but does not provide any mechanism to deal with service adaptation if the post-handover quality of service is degraded from the quality of service before handover. The MMCF assumes that mobility is a service, explicitly specified by parameters in the user service profile. The MMCF is not dependent on specific access technologies, and supports handover across different technologies.

1.2.2 Service Stratum Functions

The service stratum functions provide session-based and non session-based services including subscribe/notify for presence information and the message method for instant message exchange.

- **Service control and content delivery functions** (SC&CDF): The SC&CDF includes service control functions and content delivery functions

    a) Service Control Functions (SCF): The SCF includes resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services.. They can also include functions for controlling media resources, i.e., specialized resources and gateways at the service-signalling level. Regarding the authentication, mutual authentication between end user and the service is performed. The service control functions accommodate service user profiles which represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of functional databases. These functional databases may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

    b) Service user profile functions: The service user profile functions represent the combination of user information and other control data into a single user profile function in the service stratum, in the form of a functional database. This functional database may be specified and implemented as a set of cooperating databases with functionalities residing in any part of the NGN.

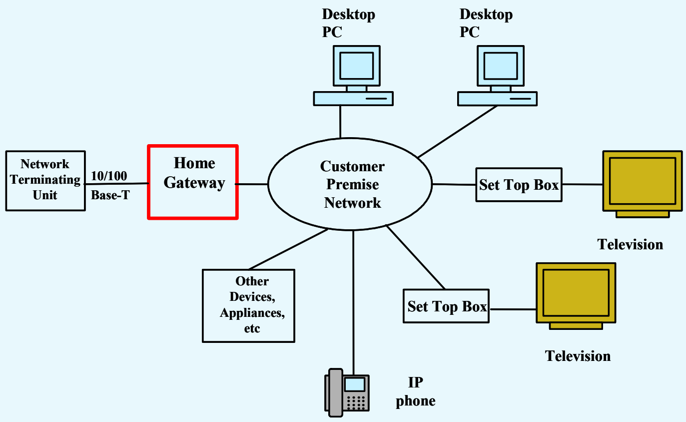
    c) Content Delivery Functions (CDF): The CDF receives content from the application support functions and service support functions, store, process, and deliver it to the end-user functions using the capabilities of the transport functions, under control of the service control functions.

- **Application/Service support functions**: The application/service support functions include functions such as the gateway, registration, authentication and authorization functions at the application level. These functions are available to the "Third-Party Applications" and "End-User" functional groups. The Application/Service support functions work in conjunction with the SCF to provide end-users and third party application providers with the value added services they request. Through the UNI, the Application/Service support functions provide a reference point to the end-user functions. The Third-party applications' interactions with the Application/Service support functions are handled through the ANI reference point.

1.2.3 End User Functions

No assumptions are made about the diverse end-user interfaces and end-user networks that may be connected to the NGN access network. Different categories of end-user equipment are supported in the NGN, from single-line legacy telephones to complex corporate networks. End-user equipment may be either mobile or fixed.

Figure 1-3: Overall configurations of end systems in NGN



1.2.4 *Management Functions*

Support for management is fundamental to the operation of the NGN. These functions provide the ability to manage the NGN in order to provide NGN services with the expected quality, security, and reliability. These functions are allocated in a distributed manner to each functional entity (FE), and they interact with network element (NE) management, network management, and service management FEs. Further details of the management functions, including their division into administrative domains, can be found in ITU-T recommendation M.3060. Management functions apply to the NGN service and transport strata. For each of these strata, they cover the FCAPS.

The accounting management functions also include charging and billing functions (CBF). These interact with each other in the NGN to collect accounting information, in order to provide the NGN service provider with appropriate resource utilization data, enabling the service provider to properly bill the users of the system.

2 Security in NGN

2.1 Security threats and risks

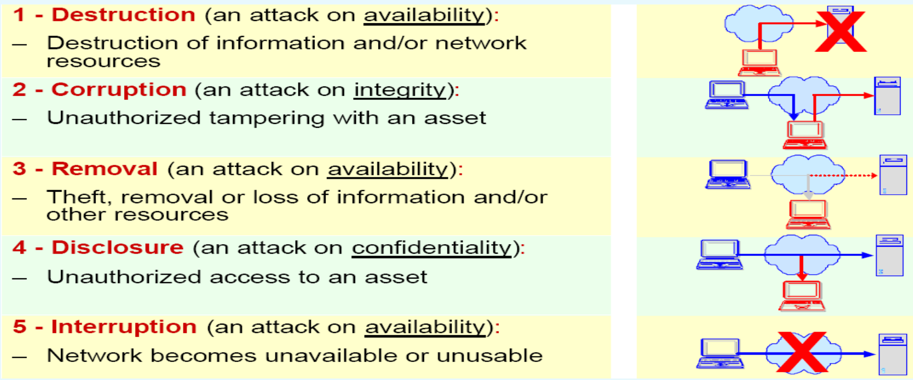
The systems, components, interfaces, information, resources, communications (i.e., signalling, management and data/bearer traffic) and services that make up an NGN will be exposed to a variety of security threats and risks. Those threats and risks will depend on a variety of factors. In addition, end users will also be exposed to certain threats (e.g., unauthorized access to private information). Figure 2-1 illustrates threat model based on Rec. X.800.

Threats to the NGN:

- unauthorized reconnaissance, such as the remote analysis of the system to determine points of weakness (these may include scans, sweeps, port interrogation, route tables, etc.);
- break-in/device takeover resulting in loss of control of the device, anomalies and errors in the configuration audits;
- destruction of information and/or other resources;
- corruption or modification of information;
- theft, removal or loss of information and/or other resources;

- disclosure of information; and
- interruption of services and denial of services.

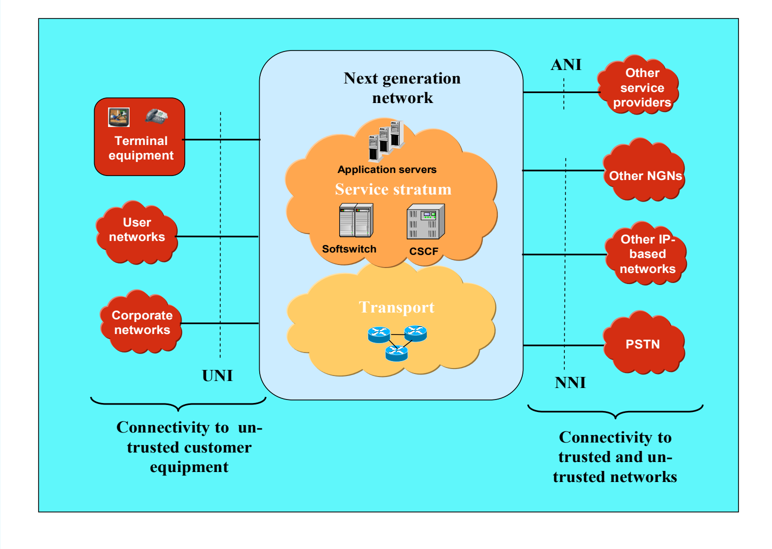
Figure 2-1: X.800 threat model



Further, it is clear that NGNs will be operating in an environment different from the PSTN environment and may therefore be exposed to different types of threats and attacks from within or externally. NGNs will have direct or indirect connectivity to un-trusted and trusted networks and terminal equipment, and therefore will be exposed to security risks and threats associated with connectivity to un-secure networks and customer premises equipment. For example, a provider's NGN may have direct or indirect (i.e., through another network) connectivity to the following as shown in Figure 2-2.

- other service providers, and their applications;
- other NGNs;
- other IP-based networks;
- public switched telephone network (PSTN);
- corporate networks;
- user networks;
- terminal equipment;
- other NGN transport domains.

Figure 2-2: Connectivity to networks and users



In the evolving environment, security across multiple network provider domains relies on the aggregation of what all providers elect to do for securing their networks. Unauthorized network access into one provider's network can easily lead to exploitation of an interconnected network and its associated services. This is an example of the exploitation of the weakest link that can threaten a provider network's integrity and service continuity along with a host of various types of attacks.

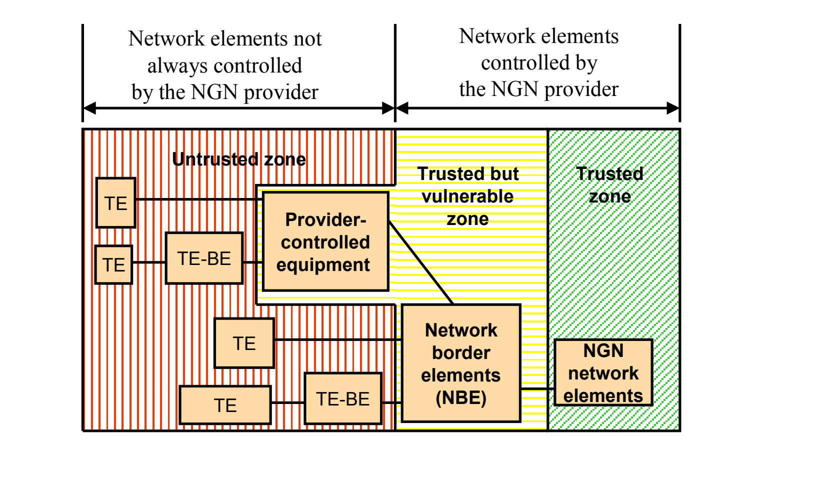
Each NGN provider is responsible for security within its domain. Each NGN provider is responsible for designing and implementing security solutions using network specific policy for trust relations, to meet its own network-specific needs and to support global end-to-end security objectives across multiple network provider domains.

2.2 Security trust model

The NGN functional reference architecture defines functional entities (FEs). However, since network security aspects depend heavily on the way that FEs are bundled together, the NGN security architecture is based on physical network elements (NEs), i.e., tangible boxes that contain one or more FEs. The way these FEs are bundled into NEs will vary, depending on the vendor.

- **Single network trust model**: Three security zones (trusted, trusted but vulnerable, and un-trusted) are dependent on operational control, location, and connectivity to other device/network elements. These three zones are illustrated in the security trust model shown in Figure 2-3.

Figure 2-3: Security trust model



a) "trusted network security zone" or "trusted zone": It is a zone where a NGN provider's network elements and systems reside and never communicate directly with customer equipment or other domains. The "trusted zone" will be protected by a combination of various methods. Some examples are physical security of the NGN network elements, general hardening of the systems, use of secure signalling, security for OAMP messages separate VPN within the (MPLS/)IP network for communication within the "trusted" zone and with NGN network elements in the "trusted-but-vulnerable" zone.

b) "trusted but vulnerable network security zone", or "trusted but vulnerable zone": It is a zone where the network elements/devices are operated (provisioned and maintained) by the NGN provider. The equipment may be under the control by either the customer/subscriber or the NGN provider. In addition, the equipment may be located within or outside the NGN provider's premises. Their major security function is to protect the NEs in the trusted zone from the security attacks originated in the un-trusted zone.

c) "un-trusted zone": It includes all network elements of customer networks or possibly peer networks or other NGN provider domains outside of the original domain, which are connected to the NGN provider's network border elements. In the "un-trusted zone", comprised of terminal equipment, equipment may not be under the control of NGN providers and it may be impossible to enforce provider's security policy on user.

- **Peering network trust model**: When an NGN is connected to another network, the trust depends on:

a) physical interconnection, where the interconnection can range from a direct connection in a secure building to via shared facilities;

b) peering model, where the traffic can be exchanged directly between the two NGN service providers, or via one or more NGN transport providers;

c) business relationships, where there may be penalty clauses in the SLA agreements, and/or a trust in the other NGN provider's security policy;

d) in general, NGN providers should view other providers as un-trusted.

2.3 Design Principles for NGN Security

2.3.1 Objectives and requirements

- **General security objectives**: The following is a list of general security objectives used to guide the requirements in this Recommendation.

  a) NGN security features should be extensible, and flexible enough to satisfy various needs.

  b) Security requirements should take the performance, usability, scalability and cost constraints of NGN into account.

  c) Security methods should be based on existing and well-understood security standards as appropriate.

  d) The NGN security architecture should be globally scalable (within network provider domains, across multiple network provider domains, in security provisioning).

  e) The NGN security architecture should respect the logical or physical separation of signalling and control traffic, user traffic, and management traffic.

  f) NGN security should be securely provisioned and securely managed.

  g) An NGN should provide security from all perspectives: service, network provider and subscriber.

  h) Security methods should not generally affect the quality of provided services.

  i) Security should provide simple, secure provisioning and configuration for subscribers and providers (plug & play).

  j) Appropriate security levels should be maintained even when multicast functionality is used.

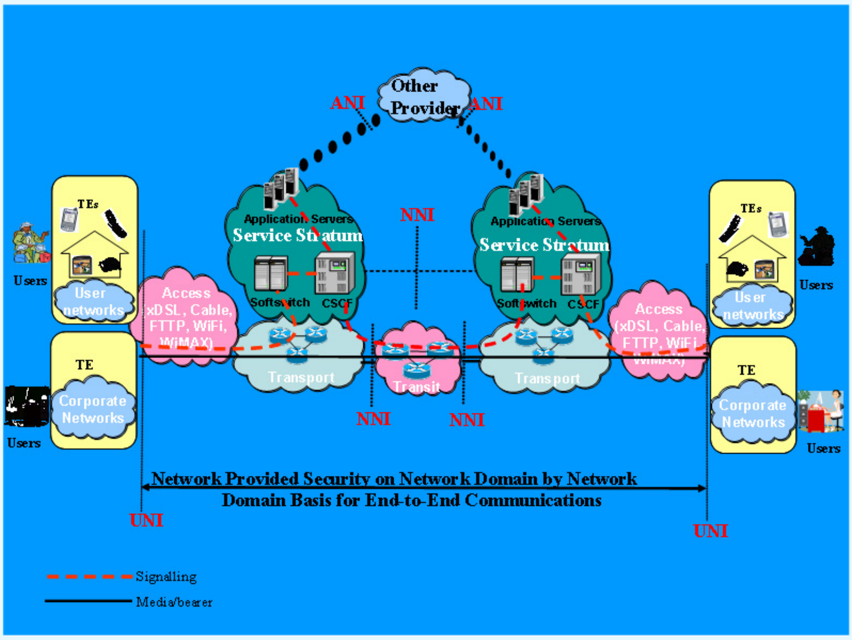
  k) The service discovery capabilities should support a variety of scoping criteria (e.g., location, cost, etc.) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy.

  l) The address resolution system should be a special system used only by this network, and certain security measures are required to be in place. This system may use databases that are internal or external of a domain.

  m) The principles and general security objectives for secure TMN management should be followed.

- **Objectives for security across multiple network provider domains**: The general objective is to provide network-based security for end-to-end communications across multiple provider domains. This is achieved by providing security of the end-to-end communication on a hop-by-hop basis across the different provider's domains. Figure 2-4 shows the general concept of network provided security for end-to-end communications between end users. Each network segment has specific security responsibilities within its security zone to facilitate security and availability of NGN communications across multiple networks.

Figure 2-4: Security of communications across multiple networks



- **Requirements specific for security dimensions**: The objectives described here are specific to particular security dimensions, such as authentication. They are common to all interfaces.

  a) Access control: NGN providers are required to restrict access to authorized subscribers. Authorization may be given by the provider providing the access or by other providers after validation by an authentication and access control processes. The NGN is required to prevent unauthorized access, such as by intruders masquerading as authorized users.

  b) Authentication: NGN providers are required to support capabilities for authenticating subscribers, equipment, network elements and other providers.

  c) Non-repudiation: This document does not specify any non-repudiation security requirements.

  d) Data confidentiality: NGN providers are required to protect the confidentiality of subscriber traffic by cryptographic or other means. NGN providers are required to protect confidentiality of control messages by cryptographic or other means if security policy requests it. NGN providers are required to protect the confidentiality of management traffic by cryptographic or other means.

  e) Communication security: NGN providers are required to provide mechanisms for ensuring that information is not unlawfully diverted or intercepted.

  f) Data integrity: NGN providers are required to protect the integrity of subscriber traffic by cryptographic or other means. NGN providers are required to protect integrity of control messages by cryptographic or other means if security policy requests it. NGN providers are required to protect the integrity of management traffic by cryptographic or other means.

g) Availability: NGN is required to provide security capabilities to enable NGN providers to prevent or terminate communications with the non-compliant end-user equipment. These capabilities may be suspended to allow emergency communications. NGN internal network elements may also be susceptible to viruses, worms and other attacks. Similar measures to quarantine network components are also required. An NGN should provide provision of security capabilities to enable a NGN provider to filter out packets and traffic that is considered harmful by the respective security policy. NGN is required to provide capabilities for the support of disaster recovery functions and procedures.

h) Privacy: NGN is required to provide capabilities to protect the subscriber's private information such as location of data, identities, phone numbers, network addresses or call-accounting data according to national regulations and laws. Specific requirements for privacy are a national matter and are outside the scope of this Recommendation.

2.3.2 Specific security requirements

This clause introduces the specific requirements for security for each of the network elements within the NGN infrastructure.

- **Common security requirements for NGN elements**

  a) Security policy: NGN providers shall prepare appropriate security policy and shall be responsible for applying it to all NEs and devices under its control.

  b) Hardening and service disablement: All NGN elements are required to be capable of being configured to support the minimum services needed to support the NGN provider NGN infrastructure. Any service or transport layer port that is not required for the correct operation of the NGN element is required to be disabled on all systems and network elements. In addition, applications are required to run under minimum privileges (e.g., on "UNIX/Linux" platforms applications should not run as root if root privileges are not indispensable). The base operating system (OS) supporting any NGN element is required to be capable of being specifically configured for security and appropriately hardened. No "backdoors" are permitted (software access which would circumvent usual access control mechanisms) into any NGN element. In addition to hardening, physical and logical access controls are required to be put in place to meet industry best-practices.

  c) Audit trail, trapping and logging: All NGN elements are required to be capable of creating an audit trail that maintains a record of security related events in accordance with NGN provider's security policy. Mechanisms to prevent unauthorized or undetected modification are required. The audit trail is required to be capable of being managed and is required to allow old data in the audit trail to be placed on other media, e.g., removable media, for long-term storage. This interface is required to allow authorized administrators to move old data out of the audit trail onto removable media. This ability is required to be protected by a specific authorization to manage the audit trail.

  d) Time stamping and time source: The NGN element is required to support the use of a trusted time source for both system clock and audit trail item stamping. A trusted time source in this case means a time source that can be verified to be resistant to unauthorized modification. Transitive trust is acceptable, i.e., a time source that relies on a trusted time source is itself an acceptable trusted time source.

  e) Resource allocation and exception handling: Each NGN element is required to provide the capability to limit the amount of its own important resources (e.g., memory allocation) it allocates to servicing requests. Such limits can minimize negative effects of denial of service attacks. Resources used to service requests compete with other resource utilization requests on the system. In addition, each specific NGN application is required to have the ability to limit its own usage of important resources that it allocates for satisfying requests.

f) Code and system integrity and monitoring: The network element is required to be capable of monitoring 1) its configuration and software and 2) any changes to detect unauthorized changes, both based on the security policy. Any unauthorized changes are required to create a log entry and cause an alarm to be generated. Based on the security policy, the network element is required to do the following. The element is required to be capable of periodically scanning its resources and software for malicious software, e.g., a virus. The element is required to generate an alarm if malicious software is discovered during a scan.

g) Patches, hotfixes and supplementary code: To trust signals generated by NGN provider NGN elements within un-trusted networks, say terminal. It is a requirement that software on the system is not compromised. NGN provider network elements and systems are required to provide a capability to verify and audit all their software. The audit results are to be accessible to an OSS. This would allow for an analysis of the security posture of the NGN provider NGN infrastructure and provide guidance to administrators and providers with respect to where mitigation is necessary.

h) Access to OAMP functions in devices: In order to safeguard the OAMP infrastructure, each internal NGN network element is required to be managed through a separate IP address allocated from a separate address block. The NGN network element is required to silently discard all packets received over the non-OAMP interface with source addresses assigned to OAMP traffic. Access to OAMP functions is required to be capable of being controlled by authentication. OAMP traffic is required to be securely protected.

- **Requirements for NGN elements in the trusted zone**: The NGN Release 1 element in the "trusted" zone is to be assigned an IP address in the block reserved for internal NGN elements. All signalling is required to use this address. The NGN Release 1 element is also required to be assigned an IP address in the block reserved for OAMP, and all OAMPs are required to use this address.
- **Requirements for NGN border elements in the "trusted-but-vulnerable" domain**: The network border element is required to support multiple IP addresses, or multiple network interfaces. The NBE is required to silently discard any media packets received that do not correspond to an active session. The NBE is also required to verify that the packet rate is consistent with the negotiated session parameters. The NBE is required to authenticate all requests if required by the service agreement with the customer.
- **Requirements for TE border elements in the "un-trusted" domain**: Physical security is a challenge for equipment placed on customer site. Ultimately, it must be accepted that, to a large extent, the security of these devices is dependent on the customer. In order to preserve the confidentiality of customer communication against eavesdropping on the signalling traffic, signalling messages are required to use a secure signalling connection between the TE-BE and the NBE.
- **Security recommendations for terminal equipment in the "un-trusted" domain**: The terminal equipment (TE) is often outside the control of the NGN provider. Therefore it is not required for the NGN provider to place requirements on its security features or policies, rather it is the function of the various network border elements to adapt to whatever policies are chosen by the customer and to provide the best service under those conditions. Media traffic should be protected from eavesdropping or modification.

2.3.3 NGN security mechanisms and procedures

This clause highlights some important security mechanisms that can be used to realize the requirements in ITU-T Recommendation Y.2701 in each NGN Network Element, and specifies a suite of options to be used for the mechanisms to avoid the mismatch of options.

- **Identification, Authentication and Authorization**: There are identification, authentication and authorization mechanisms, in particular, those concerning SIP-based services.
- **Transport Security for Signaling and OAMP**: Transport security is used in the NGN infrastructure to achieve confidentiality and integrity guarantees of the signalling data and the OAMP messages. It is required to specify profile of TLS and IPsec to be used by the NGN infrastructure network elements as two of the important mechanisms.
- **Media Security**: Media encryption is not required within the NGN infrastructure, but it may be required to be supported for customers that desire its use. Such support may include the support of media encryption protocols, SRTP [RFC3711]. Network Border Elements (i.e., the edge of the network provider's domain) are assumed to implement encryption/decryption although it is possible to do the same in a separate platform shared among NBEs. In either case, the encryption and decryption is required to be collocated with other media processing capabilities such as Dual-Tone Multi-Frequency (DTMF) detection and transcoding.
- **Audit Trail, Trapping, and Logging Systems**: An audit trail is taken all OAMP access attempts (whether successful or not), all OAMP changes made, and all OAMP signoffs. In addition events considered significant by the NGN provider's policy are logged.
- **Provisioning of equipment in untrusted zone**: All customer premise equipments are configured by the TE Provisioning Element. TE Provisioning Element resides in the trusted zone and may only communicate with the TEs via the Network Border Element (NBE). A TE or TE-BE may authenticate and establish a security association with the NBE before it can obtain configuration file from TE Provisioning Element. NBE may support both TLS and IPsec for establishing SA with the TEs (including TE-BE).

2.3.4 Application model for AAA in NGN

Based on security requirements for NGN in Y.2701 and the NGN authentication reference model in Y.2702, the NGN authentication reference model (Figure 2-5) depicts eight authentication reference points. Reference points (1) and (4) refer to transport of user traffic and may be viewed as depending on "horizontal" access control at the transport control level, whereas reference points (2) and (8) may be viewed as depending on control data between the transport and service control layers and therefore as being "vertical." This relationship is displayed in Figure 2-6.

Figure 2-5: End-to-end Reference Architectural Model (Y.2702 NGN Authentication)

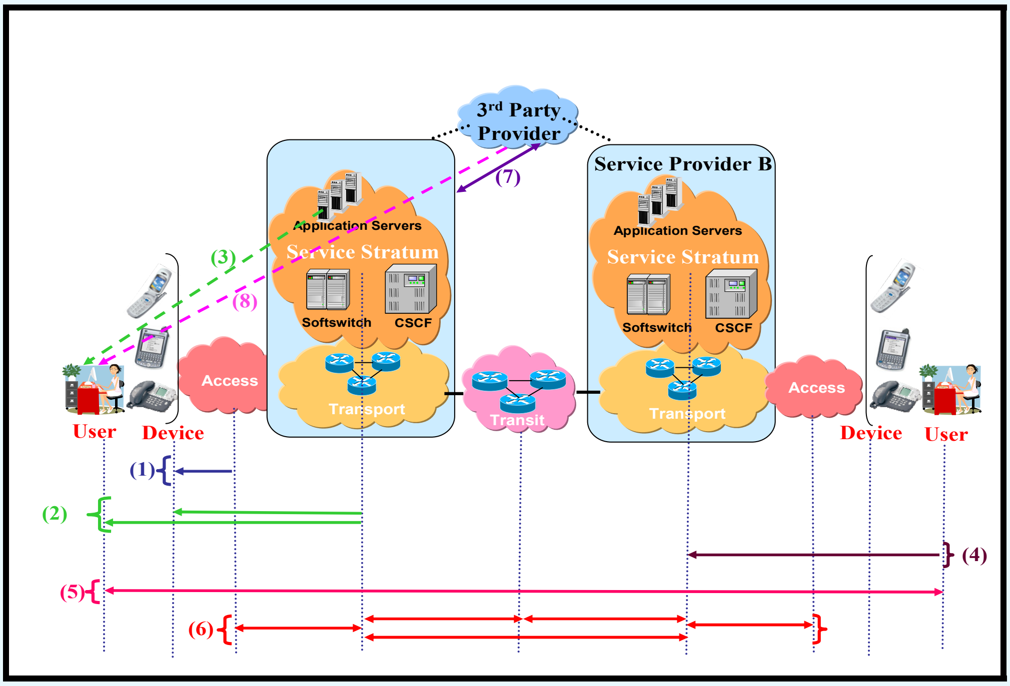
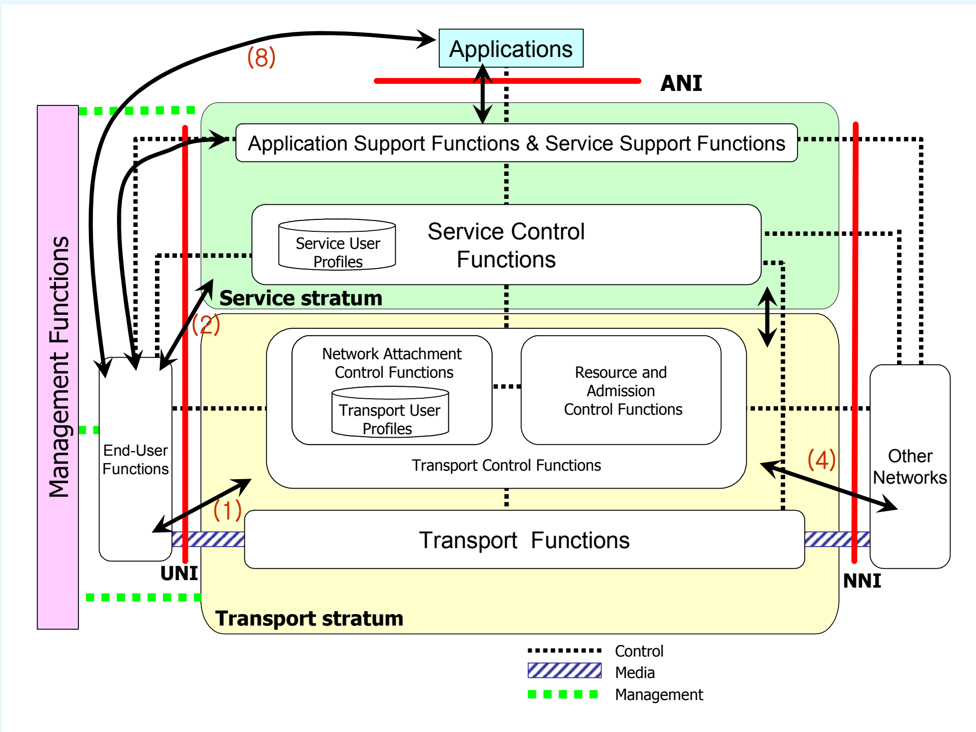


Figure 2-6: NGN Architecture and AAA related domains (Y.2702 NGN Authentication)

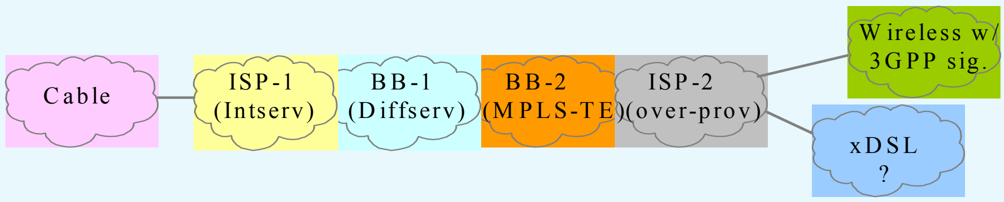


Annex 4: Quality of Service in NGN

1 Overview of QoS and NP in NGN

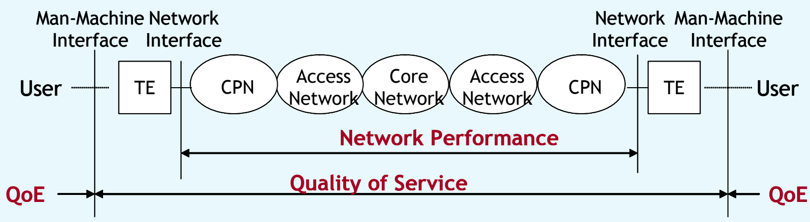
One of the key elements of NGN, which should be based on IP, is the guaranteeing of requested Quality of Services (QoS). The NGN have access and transport agnostic features which should be assumed in heterogeneous environments, so complexity of supporting the QoS is much more complicated. Figure 1-1 shows an example of this complexity.

Figure 1-1: QoS Complexity in Heterogeneous Network Environment



The general aspects of Quality of Service and network performance in NGN are developed to provide descriptions of NGN Quality of Service, Network Performance and Quality of Experience. Figure 1-2 shows the meaning and scope of QoS, QoE and NP with brief explanation about their features.

Figure 1-2: QoE, QoS and NP in NGN environment



Quality of Experience	Quality of Service	Network Performance
User oriented		Provider oriented
User behavior attribute	Service attribute	Connection/Flow element attribute
Focus on user-expected effects	Focus on user-observable effects	Focus on planning, development (design), operations and maintenance
User subject	Between (at) service access points	End-to-end or network elements capabilities

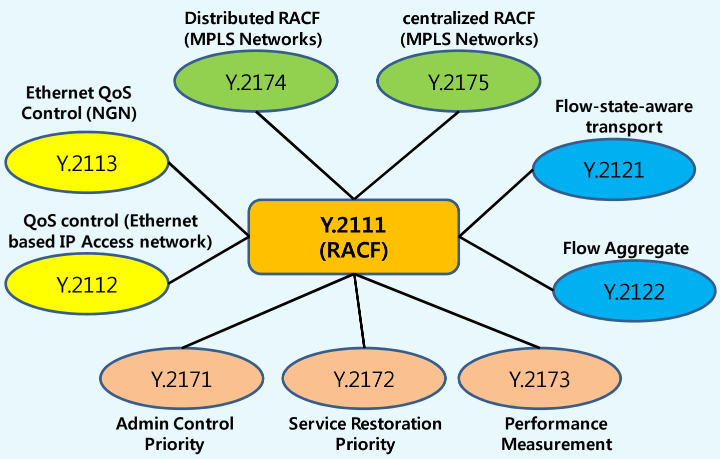
The NGN illustrates how these descriptions are applied in an NGN environment, describe performance aspects of NGN (including performance of service and transport stratum) and provide a basis for common understanding of performance concepts (useful to users and to the industries that compose the NGN – e.g., Fixed & mobile telecommunications, broadcasting, etc.). NGN defines the application QoS classes of the NGN.

The NGN determines the requirements to support QoS across multiple heterogeneous service providers. Existing standards specify several metrics and measurement methods for point to point performance. Notable are ITU-T Recommendations, Y.1540 and Y.1541 standards and the IETF IP Performance Metrics (IPPM) Working Group standards. The NGN considers the options and parameters left unspecified, taking into account the concatenation of performance over multiple network segments, allocation of impairment budgets, mapping between IP and non-IP metrics, accuracy, and data handling.

The network performance parameters of non-homogeneous networks in NGN are developed through the description of performance aspects of the transport layer in NGN. The NGN identifies general performance principles and frameworks that can be applied to the development of specific performance descriptions to support continuing evolution of the NGN. NGN defines the relationship among individual networks' performance which may be observed at physical interfaces between a specific network and associated terminal equipment, and at physical interfaces between specific networks.

A QoS Framework for IP based access networks is also developed in ITU-T through NGN-GSI. Reference architecture for IP access networks for QoS support is provided as well as detailed QoS requirements and validation procedures. The reference model would be part of the overall NGN framework with the service and transport layers, functional entities in each layer, and interfaces between the functional entities, in particular, the functional entities to facilitate interworking with the QoS functionality in the core network as well as that specific to each type of access networks.

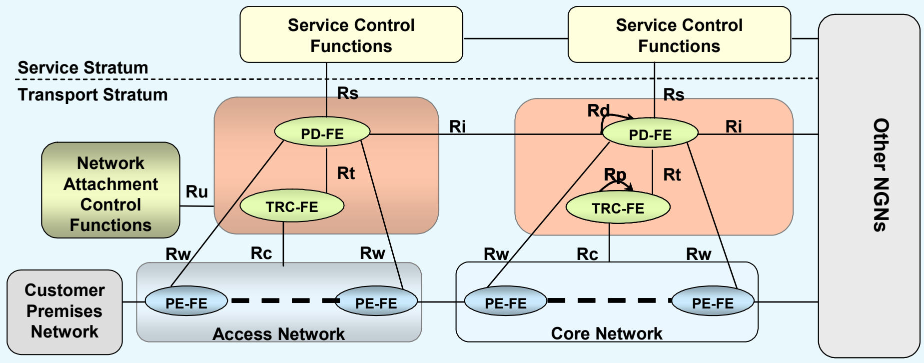
Figure 1-3: ITU-T NGN QoS related standards



2 Resource and Admission Control in NGN

Functional requirements and architecture for resource and admission control in NGN are developed to provide high-level requirements, scenarios and functional architecture. The decomposition to functional entities is specified to provide reference points and interfaces for the control of Quality of Service (QoS), Network Address and Port Translator (NAPT) and/or Firewall (FW) traversal are described.

Figure 2-1: Resource and Admission Control architecture model of NGN



- **QoS capability of CPE**: According to the capability of QoS negotiation, the CPE can be categorized as follows:

  a) Type 1 – CPE without QoS negotiation capability (e.g., vanilla soft phone, gaming consoles)

  The CPE does not have any QoS negotiation capability at either the transport or the service stratum. It can communicate with the SCF for service initiation and negotiation, but cannot request QoS resources directly.

  b) Type 2 – CPE with QoS negotiation capability at the service stratum (e.g. SIP phone with SDP/SIP QoS extensions)

  The CPE can perform service QoS negotiation (such as bandwidth) through service signalling, but is unaware of QoS attributes specific to the transport. The service QoS concerns characteristics pertinent to the application.

  c) Type 3 – CPE with QoS negotiation capability at the transport stratum (e.g. UMTS UE)

  The CPE supports RSVP-like or other transport signalling (e.g. GPRS session management signalling, ATM PNNI/Q.931). It is able to directly perform transport QoS negotiation throughout the transport facilities (e.g. DSLAM, CMTS, SGSN/GGSN).

  Note that the SCF shall be able to invoke the resource control process for all types of CPE.

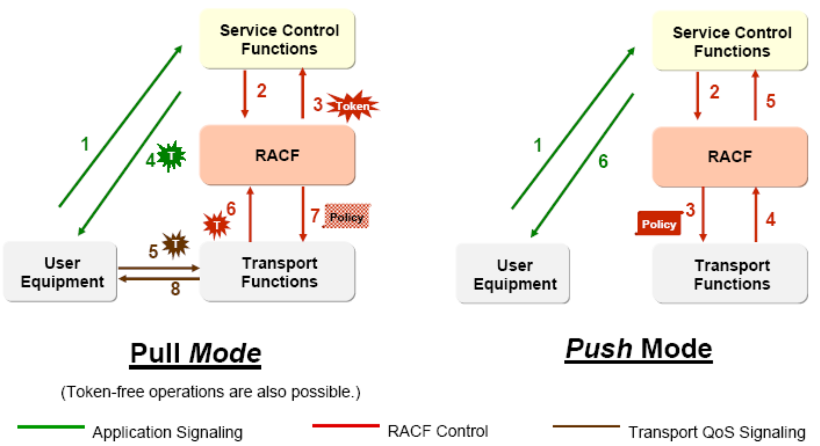
- **Resource control modes**: In order to handle different types of CPE and transport QoS capabilities, the RACF shall support the following QoS resource control modes as part of its handling of a resource request from the SCF:

  a) Push Mode: The RACF makes the authorization and resource control decision based on policy rules and autonomously instructs the transport functions to enforce the policy decision.

  b) Pull Mode: The RACF makes the authorization decision based on policy rules and, upon the request of the transport functions, re-authorizes the resource request and responds with the final policy decision for enforcement.

The Push mode is suitable for the first two types of CPE. For type 1 CPE, the SCF determines the QoS requirements of the requested service on behalf of the CPE; for type 2 CPE, the SCF extracts the QoS requirements from service signalling. The Pull mode is suitable for type 3 CPE, which can explicitly request QoS resource reservation through transport QoS signalling.

Figure 2-2: Pull and Push mode of RACF operation



- **Resource control states**: Regardless of the QoS negotiation capability of a particular CPE and the use of a particular resource control mode, the QoS resource control process consists of three logical states:

  a) Authorization (Authorized): The QoS resource is authorized based on policy rules. The authorized QoS bounds the maximum amount of resource for the resource reservation.

  b) Reservation (Reserved): The QoS resource is reserved based on the authorized resource and resource availability. The reserved resource can be used by best effort media flows when the resource has not yet committed in the transport functions.

  c) Commitment (Committed): The QoS resource is committed for the requested media flows when the gate is opened and other admission decisions (e.g. bandwidth allocation) are enforced in the transport functions.

  d) The general resource control criteria shall be:

  e) The amount of committed resources is not greater than the amount of reserved resources.

  f) The amount of reserved resources is not greater than the amount of authorized resources.

Note that the amount of committed resources typically equals the amount of reserved resources.

- **Resource control schemes**: Given the variety of application characteristics and performance requirements, the RACF supports three resource control schemes:

  a) Single-Phase Scheme: Authorization, reservation and commitment are performed in a single step. The requested resource is immediately committed upon successful authorization and reservation. The Single-Phase Scheme is suitable for client-server-like applications to minimize the delay between the service request and the ensuing reception of content.

  b) Two-Phase Scheme: Authorization and reservation are performed in one step, followed by commitment in another step. Alternatively authorization is performed in one step, followed by reservation and commitment in another step. The Two-Phase Scheme is suitable for interactive applications, which have stringent performance requirements and need to have sufficient transport resources available.

c) Three-Phase Scheme: Authorization, reservation and commitment are performed in three steps sequentially. The Three-Phase Scheme is suitable for network-hosted services in an environment where transport resources are scarce.

- **Information for resource control**: The RACF shall perform the resource control based on the following information:

  a) Service Information: A set of data provided by the SCF for a resource control request, derived from service subscription information, service QoS requirement and service policy rules.

  b) Transport Network Information: A set of data collected from the transport networks, which may consist of transport resource admission decisions and network policy rules.

  c) Transport Subscription Information: A set of data for the transport subscription profile such as the maximum transport capacity per subscriber.

- **Policy rules for the enforcement of resource control results**: The RACF may assist the installation of two types of policy rules related to the enforcement of resource control results:

  a) Policy Decision: A set of policy conditions and actions for the enforcement of resource control results on a per flow basis, which is produced dynamically upon the individual resource request from the SCF. The RACF shall make policy decisions based on the information for resource control described in above paragraph and install the policy decisions to the transport functions autonomously or upon the request of the transport functions. The policy decision can be modified and updated within the lifetime of a resource control session.

  b) Policy Configuration: A set of static policy rules for default network resource configuration. The policy configuration is pre-defined by network operators and does not vary from the individual resource request. The policy configuration can be pre-provisioned statically in transport functions, e.g. mapping rules of the IP layer QoS to link layer QoS. In some cases, the RACF may help install the initial policy configuration for resource control, such as default resource control configuration (e.g. default gate setting).

Note that the RACF may use the soft-state (state that has a lifetime and requires renewal to keep alive) or hard-state (state that is persistent until explicitly removed) approach in support of transport resource control.

Annex 5: NGN Management

1 Objectives of NGN Management

The objectives of the management is to facilitate the effective interconnection between various types of Operations Systems (OSs) and/or resources for the exchange of management information using an agreed architecture with standardized interfaces including protocols and messages. Many network operators and service providers have a large infrastructure of OSs, telecommunications networks and equipment already in place, and which must be accommodated within the architecture in terms of managements. Management also provides capabilities for end-users with access to, and display of, management information, and end-user-initiated business processes. By considering these, it is noted that a management framework contributes to increase customer satisfaction and at the same time underpins a significant reduction in operating costs through new technologies and operational methods.

Within the context of NGN, management functionality refers to a set of management functions to allow for exchanging and processing of management information to assist network operators and service providers in conducting their business efficiently. NGN management (NGNM) provides management functions for NGN resources and services, and offers communications between the management plane and the NGN resources or services and other management planes.

This document introduces summary information about the NGN management based on Recommendation ITU-T M.3060 developed by SG2. M.3060 identifies the management architecture needs to address followings:

- Administrative boundaries amongst operator domains;
- Processes amongst operators across the domain boundaries;
- Processes between Operators and their suppliers' equipments;
- Reference points between the logical functions for Provider and Consumer;
- Provider and Consumer Interfaces between the physical entities used to realize the provider and consumer reference points;
- Information model concepts used to support logical functions.

In addition to this, M.3060 also identifies objectives of NGN management as following:

- minimize mediation work between different network technologies through management convergence and intelligent reporting;
- minimize management reaction times to network events;
- minimize load caused by management traffic;
- allow for geographic dispersion of control over aspects of the network operation;
- provide isolation mechanisms to minimize security risks;
- provide isolation mechanisms to locate and contain network faults;
- improve service assistance and interaction with customers;
- layering of services to enable a provider to provide the building blocks for services and others to bundle the services and its implications on the management architecture;
- business processes as defined in the M.3050.x series and how they would be used in NGN;
- support of applications, both on the same distributed computing platform and those distributed throughout the network.

The following areas are identified for further study issues.

- implications of the need to manage end-to-end services;
- implications of home networks and customer premises equipment.

2 Architecture of NGN Management

2.1 NGN Management Requirements

NGN management supports the monitoring and control of the NGN services and relevant resources for the service and transport via the communication of management information across interfaces between NGN resources and management systems, between NGN-supportive management systems, and between NGN components and personnel of service providers and network operators. NGN management supports the aims of the NGN based on Recommendation ITU-T Y.2201. Followings are key summary of NGN management requirements:

- Providing the ability to manage NGN system resources, both physical and logical including resources in the core network, access networks, interconnect components, and customer networks and their terminals;
- Providing the ability to manage NGN Service Stratum resources and enabling organizations offering NGN end-user services including the ability to personalize end-user services and customer self-service (e.g., provision of service, reporting faults, online billing reports);
- Supporting eBusiness Value Networks based upon concepts of business roles including support of B2B processes;
- Allowing an enterprise and/or an individual to adopt multiple roles in different value networks and also multiple roles within a specific value network;
- Integrating an abstracted view on Resources (network, computing and application);
- Supporting the collection of charging data for the network operator regarding the utilization of resources in the network;
- The ability to provide survivable networks in the event of impairment and proactive trend monitoring;
- Enable service providers to reduce the time-frame for the design, creation, delivery, and operation of new services;
- The ability to manipulate, analyse and react to management information in a consistent and appropriate manner.

2.2 NGN Management Architecture

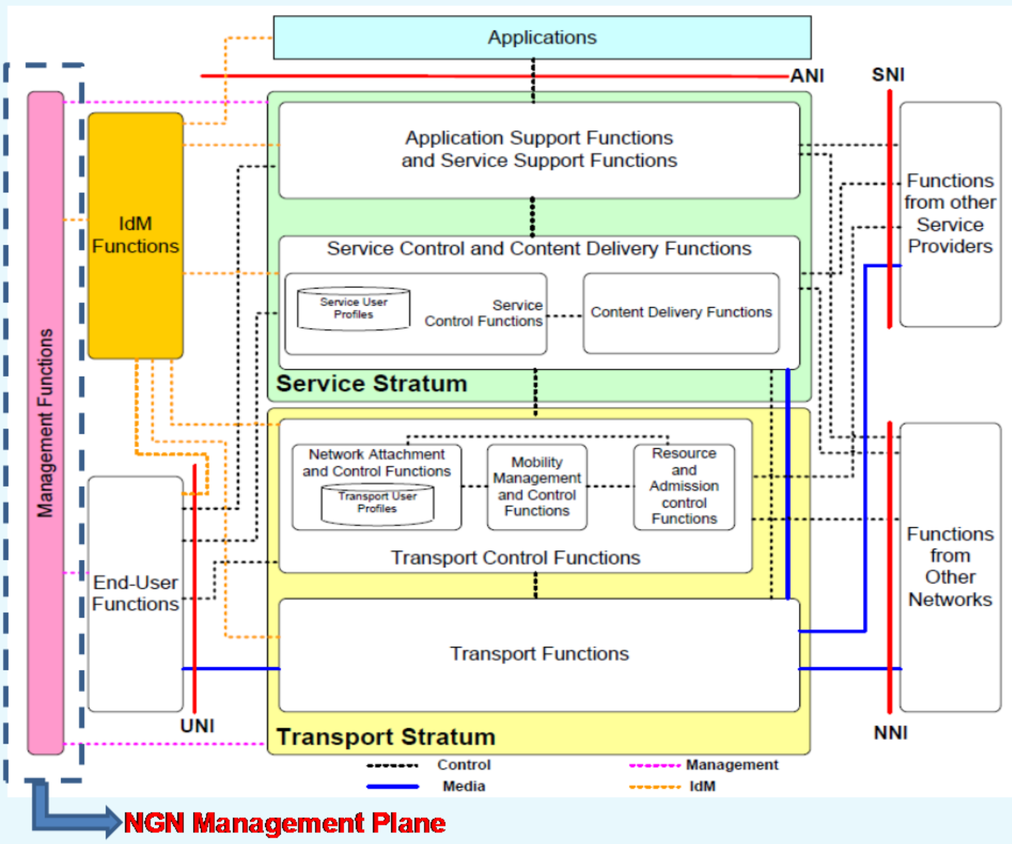
The NGN management plane is the union of the NGN service stratum management plane and the NGN transport stratum management plane following the basis of NGN functional architecture. It may include joint management functions, i.e., functions used to manage entities in both strata plus functions required to support this management.

Referring to Recommendation ITU-T Y.2011 as shown in Figure 2-1, NGN management plane places to cover both transport and service strata as well as other functions such as IdM functions and End-user functions.

The NGN Management architecture will be divided into four different architectural views as shown in Figure 2-2 as followings:

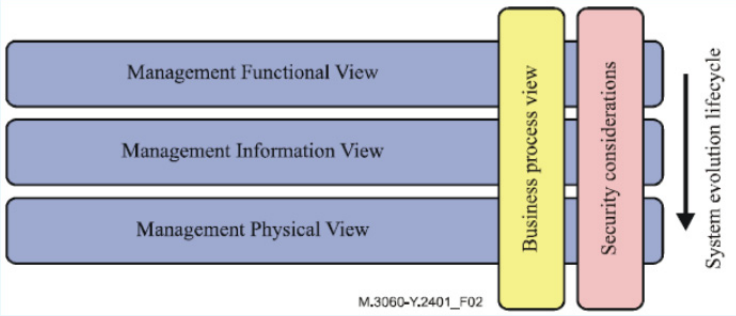
- Business Process View: The business process view, based on the eTOM model (ITU-T Rec. M.3050.x-series), provides a reference framework for categorizing the business activities of a service provider;
- Management Functional View: The functional view permits the specification of what functions have to be achieved in the management implementation;
- Management Information View: The information view characterizes the management information required for communication between the entities in the functional view to enable the performance of the functions to be achieved in the management implementation;
- Management Physical View: The physical view describes the varied ways that management functions can be implemented. They may be deployed in a variety of physical configurations using a variety of management protocols.

Figure 2-1: NGN management plane in the NGN architecture



Each view shows a different perspective into the architecture. These four architecture views also take security into consideration. Figure 2-2 describes the workflow in the creation of management specifications, where first the functional view is defined, followed by the information view and finally the physical view. The Business Process is an influence throughout the lifecycle. Note that, in practice, this process is iterative to enable all aspects of the architecture to evolve over time as required.

Figure 2-2: NGN management architecture



2.3 Relationship to service-oriented architecture (SOA)

One of the architectural principles used in the management architecture for NGN is that of being a Service-Oriented Architecture (SOA). A SOA is software architecture of services, policies, practices and frameworks in which components can be reused and repurposed rapidly in order to achieve shared and new functionality. This enables rapid and economical implementation in response to new requirements thus ensuring that services respond to perceived user needs.

SOA uses the object-oriented principle of encapsulation in which entities are accessible only through interfaces and where those entities are connected by well-defined interface agreements or contracts.

Major goals of an SOA in comparison with other architectures used in the past are to enable:

- faster adaptation to changing business needs;
- cost reduction in the integration of new services, as well as in the maintenance of existing services.

SOA provides open and agile business solutions that can be rapidly extended or changed on demand. This will enable NGN Management to support the rapid creation of new NGN services and changes in NGN technology.

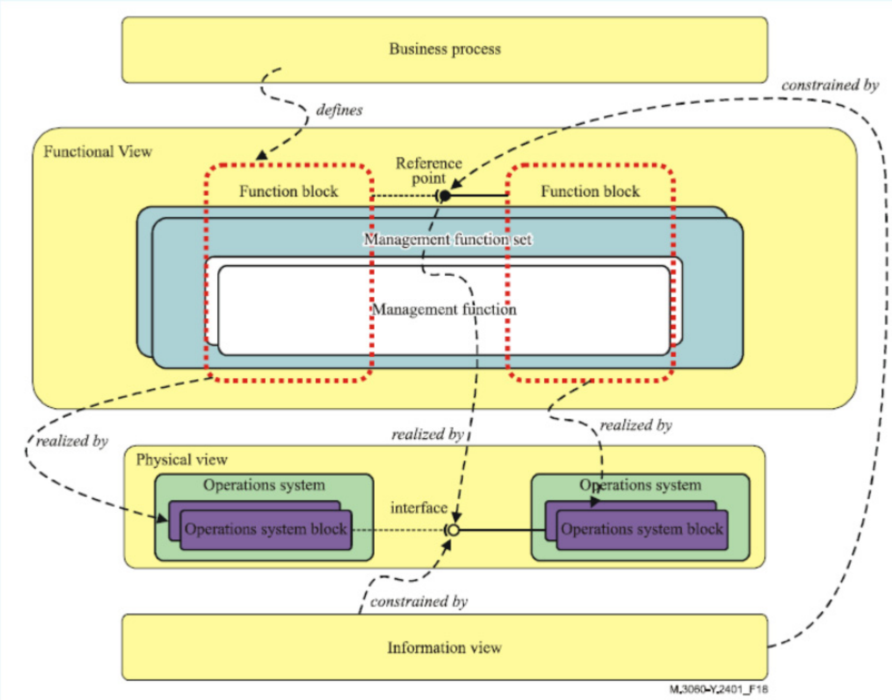
The main features of SOA are:

- loosely coupled, location independent, reusable services;
- any given service may assume a client or a server role with respect to another service, depending on situation;
- the "find-bind-execute" paradigm for the communication between services;
- published contract-based, platform and technology-neutral service interfaces. This means that the interface of a service is independent of its implementation;
- encapsulating the lifecycle of the entities involved in a business transaction; and exposing a coarser granularity of interfaces than OOA.

3 Relationships between management views

A business process provides a set of requirements that defines management functionality in the functional view. This management functionality is composed of management function sets that are composed of management functions. Operations systems realize a number of functional blocks, deployable units of management functionality, in the physical view. The functional view defines reference points that involve interaction between functional blocks. The information view constrains the data and interaction patterns of the interface between operations systems components that are physical realizations of functional blocks. Figure 3-1 shows this relationship between management views and their components.

Figure 3-1: Relationship of management views and their constructs



The management implementation is realized from four different, but interrelated views. These are the business process, functional, information and physical views. Three of these views (business process, functional and information) provide a framework that allows requirements to be documented about what a management implementation should do. The business process view, based on the eTOM model, provides a reference framework for categorizing the business activities of a service provider. The functional view framework permits the specification of what functions have to be achieved in the management implementation. The information view permits the specification of what information (i.e., data) has to be stored so that the functions defined in the functional view can be achieved in the management implementation. The management implementation, that meets the requirements of the management functional and information specifications, may vary greatly from one management solution to another. Management implementations are not currently a subject for standardization.

Annex 6: NGN Testing

1 Background

According to the transition of public telecommunication networks migration from digital circuit-switched to packet switching networks, especially aiming for IP-based network infrastructure, the testing of NGN including equipment testing become of primary importance. Ideally the operator expects to be offered equipment of high quality from the industry. But rapid growth of new technologies and the increase of equipment complexity, it is not easy to confirm the satisfaction of interesting in both operators and industries. However integral testing performed on operator networks is quite costy and it would not be reasonable to wait for external events like incidents affecting the operator networks in order to test them. It seems that the methodology of integral testing may be complemented and updated by the creation of model networks to perform equipment compatibility tests, followed by subsequent resource integration of the model networks to ensure full-fledged integral testing taking into account the interworking testing results.

By considering above, it is required that the study should be covered both compatibility and interoperability testing of various vendors' NGN equipment including new services with the existing ones in the process of NGN equipment operation. ITU-T, especially SG11 is being involved in this study as well as ETSI. This annex introduces summary information about the NGN testing based on Recommendations ITU-T Q.3900 (2006) and Q.3909 (2011) developed by SG11.

2 Technical means and functions to be tested

2.1 NGN technical means to be tested

NGN technical means which identifies as the NGN basic equipment to serve for building NGN solutions including for application shall be implemented taking into account the mandatory NGN function set. It is noted that, at the same time, the composition and number of protocols and interfaces in the specified functionality may be implemented by the manufacturer. For the purposes of standards development, the technical means functionality implemented by the manufacturer, including the requirements for the protocols and interfaces to be implemented in the specified functionality, are assumed to be in complete conformance with the functionality and purpose defined in the NGN requirements (see [ITU-T Y.2012] and [ITU-T Y.2201]).

Recommendation ITU-T Q.3900 introduces following classifications of NGN technical means in public networks as shown in Table 2-1.

Table 2-1: Classification of NGN technical means

System	NGN Technical Means
Call session control system	Media gateway controller (MGC)
	Proxy server SIP (PS)
	IP multimedia subsystem (IMS)
Voice and signalling transmit system	Media gateway (GW)
	Signalling gateway (SG)
	Transport network environment (TNE)
Application servers	Application server (AS)
	Media server (MDS)
	Messaging server (MeS)

System	NGN Technical Means
Management and billing system	NGN management system (NMS)
	Billing system (BS)
Access environment	NGN integrated access devices (NGN-IAD)
	Media gateway for legacy terminal equipment (GW-LTE)

Recommendation ITU-T Q.3900 identifies more details about functionality of the key NGN technical means from above means used in public networks as shown in Table 2-2.

Table 2-2: Functionality of key NGN technical means to be tested

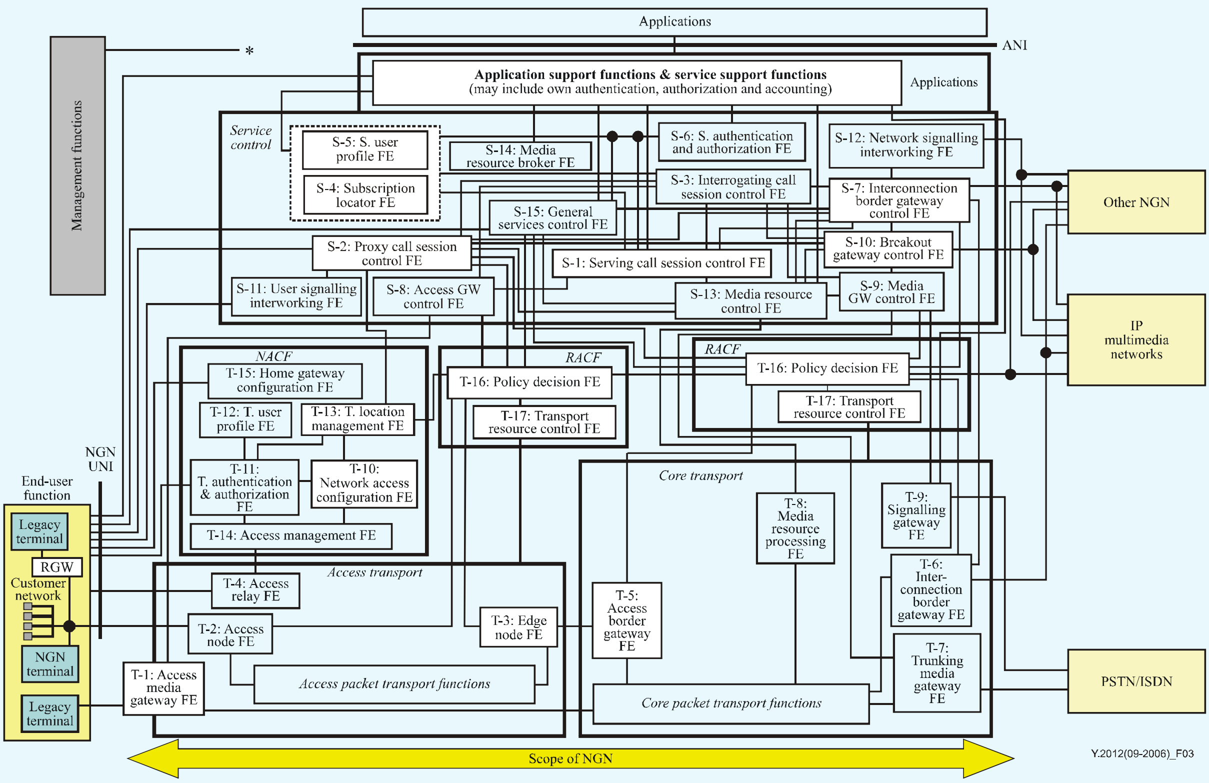
Technical means	Functionality
Media gateway controller (MGC)	• controls the calls among the PSTN subscribers; • provide for a basic part of functionality while controlling the communication sessions (transfer of routing tables, reconfiguring the numbering systems among various numbering plan formats, Media Gateway controlling by means of the signalling protocols (MGCP, H.248/Megaco, H.323, SIP) and etc; • is a main component of softswitch as a part of main switching device in the NGN.
Application server (AS)	• a software server providing new services to the users; • provisioning of new services, for example, e-commerce and electronic trade; • functionally perform as most of the NGN network components in the field of COMMUNICATION SESSION AND SERVICES CONTROL AREA; • a more flexible management of network capabilities and the creation of new and promising network scenarios.
Media server (MDS)	• provides services of interaction between the user and application or other additional communication services by means of voice and DTMF instructions. The MDS architecturally may be divided into: 1) A Media Resource Control Unit ensuring DTMF recognition, speech synthesis, speech recognition, etc; 2) A Service Control Unit ensuring forwarding messages into the message line, message recording, transfer of facsimile services, arranging conference communication, etc; • may be implemented on various software and hardware platforms based on the VoiceXML languages and so on.
Messaging server (MeS)	• responsible for message saving and message transfer to the users; • provide users with additional communication services.
Media gateway (GW)	• provides the functions of transforming the voice information into a digital format and its transfer through the NGN; • performs coding of the amplitude-frequency signals through integrated codecs (G.711, G.723, G.726, G.729, etc.), as well as transfer of digitized signals with the aid of transport protocols RTP/RTCP; • implemented, at least, one of the assortment of protocols (H.323, MGCP, H.248/Megaco, SIP) to establish connection within the GW; • used for the arrangement of interaction on the level of voice circuits between a Circuit Switched Network and NGN.

Technical means	Functionality
Signalling Gateway (SG)	• allows to convert and send a signalling load of the PSTN network to the MGC and converts such signalling types as ISDN, SS7, etc; • transfer of the SIGTRAN-stack protocols is effected over the SCTP transport protocol; • used at the boarder of the NGN and the PSTN including the arrangement of interaction.
Configuration and management system (MS)	• provide management and control of all the NGN technical means; • construct with the use of distributed and object-oriented structure with multi-protocol; • interfaces should be open using standard protocols (IIOP, CMIP, SNMP, FTP, FTAM, etc.) and the usage of formal languages for description of standard interfaces (CORBA IDL, JAVA, GDMO, ASN.1, etc.).

2.2 NGN functions to be tested

The main NGN functions to be tested as mandatory are classified as Transport stratum functions, Service stratum functions, End-user functions and Management functions. To test such functions, it is necessary to understand in more detail their internal functionality, to determine the purpose and degree of their responsibility (see Recommendation ITU-T Y.2012). An NGN functional architectures showing the detailed functionality is given in Figure 2-1.

Figure 2-1: NGN functional architecture



The presented NGN technical means may implement, within their composition, several functions at a time. The function sets implemented in particular technical means will be defined as following:

1) Transport functions:
   - User connection to the NGN (Access Transport Functions (ATF): T-1, T-2, T-4);
   - Transfer of traffic from the access network to the common transport network with the support of ATF and an additional routing capability (Edge&Access Border Gateway Functions: T-3, T-5);
   - Transfer and management of all types of information (media streams, signalling messages and control system signals) being transmitted over the transport network (Core Transport Functions: T-8, T-9, T-6, T-7).
2) Transport control functions:
   - QoS management including resource management, management of Network Address and Port Translation (NAPT) and NAPT Traversal at the access and transport layer. Testing should be divided for each layer separate with tests both for Access Transport Resource Control (ATRC) and for Core Transport Resource Control (CTRC). Testing of the resource control function should incorporate: packet filtering, traffic classification, service priority policies, passband reservation, network address translation, Firewall (RACF: T-17 for both access and core);
   - Control of user access to the network resources (Admission Control Function) such as user authorization based on the profile should be checked (SLA, service priority, access policies determined by the type of the model network used for testing) and the access and/or transport resources available to the user (RACF: T-16 for both access and core);
   - Control of user access to NGN services such as dynamic allocation of IP addresses and additional configuration parameters needed for user identification/authentication, at the network layer, for access to the network and user localization (NACF: T-10, T-11, T-13, T-14) ;
   - Control of home gateway (HGW) configuration functionality such as configuration of a firewall internally in the HGW, QoS marking of IP packets, etc. (NACF: T-15).
3) Transport user profile functions: checking the possibility of configuring and modifying the information contained in the user profile at the transport layer (Transport stratum: T-12);
4) Service control functions:
   - User registration and authorization at the service layer (S-6);
   - Management media streams, terminal equipment and gateways (S-1, S-11, S-8, S-2, S-3, S-12, S-7, S-10, S-9, S-13).
5) Application/Service support functions:
   - User registration and authorization at the application layer, for user access to the telecommunication services provided by application servers (S-4, S-5, S-6);
   - Management of media streams and telecommunication services (S-14, S-15).
6) Service user profile functions: checking the capability of configuring and modifying the information contained in the user profile at the service control layer and checking the capability of interaction with the user-profile databases of other NGN architecture layers;
7) End-user functions: checking the capabilities of the terminal equipment from the gateway, to which conventional telephone sets are connected, to the multipurpose sets designed specifically for NGN networks include checking codecs, echo-cancellation systems, signalling systems and functions of interaction with the relevant NGN layers;

8) Management functions:

- Error processing management;
- Equipment configuration management;
- Billing system management;
- Service management;
- Security management.

2.3 Conformance of NGN functions to NGN technical means to be tested

The technical means used in NGN networks may implement the functionalities within their composition as shown in Table 2-3.

Table 2-3: Conformance of NGN technical means into NGN functionality

NGN technical means	NGN functionality
Call session control system	
Media gateway controller (MGC)	S-3, S-7, S-9, S-10, S-12 T-10, T-11, T-12, T-13
Proxy server SIP (PS)	S-2, S-3, S-7, S-11, S-12 T-10, T-11, T-12, T-13
IP multimedia subsystem (IMS)	S-1, S-3, S-6, S-7, S-8, S-10, S-12, S-13 T-10, T-11, T-12, T-13, T-14, T-15, T-16, T-17
Voice and signalling transmit system	
Media gateway (GW)	T-7, T-8
Signalling gateway (SG)	T-8, T-9
Transport network environment (TNE)	T-5, T-6, T-8
Application servers	
Application server (AS)	S-4, S-5, S-6, S-14, S-15
Media server (MDS)	S-4, S-5, S-6, S-14, S-15
Messaging server (MeS)	S-4, S-5, S-6, S-14, S-15
Management and billing system	
Management system (MS) Billing system (BS)	– Error processing management – Equipment configuration management – Billing system management – Service management – Security management
Access environment	
NGN integrated access devices (NGN-IAD)	T-2, T-4, T-3, T-5, T-15, T-14
Media gateway for legacy terminal equipment (GW-LTE)	T-1, T-2, T-3, T-4, T-5

3 Model networks for NGN testing

There are two types of model networks for NGN testing: dedicated model and distributed model networks. It should be noted that, although creation of model networks appears to be a promising testing method, not all countries are in a position to implement them to the necessary extent desired. Hence, it is reasonable to create regional model networks whose resources could be employed for testing by various countries located in the given region.

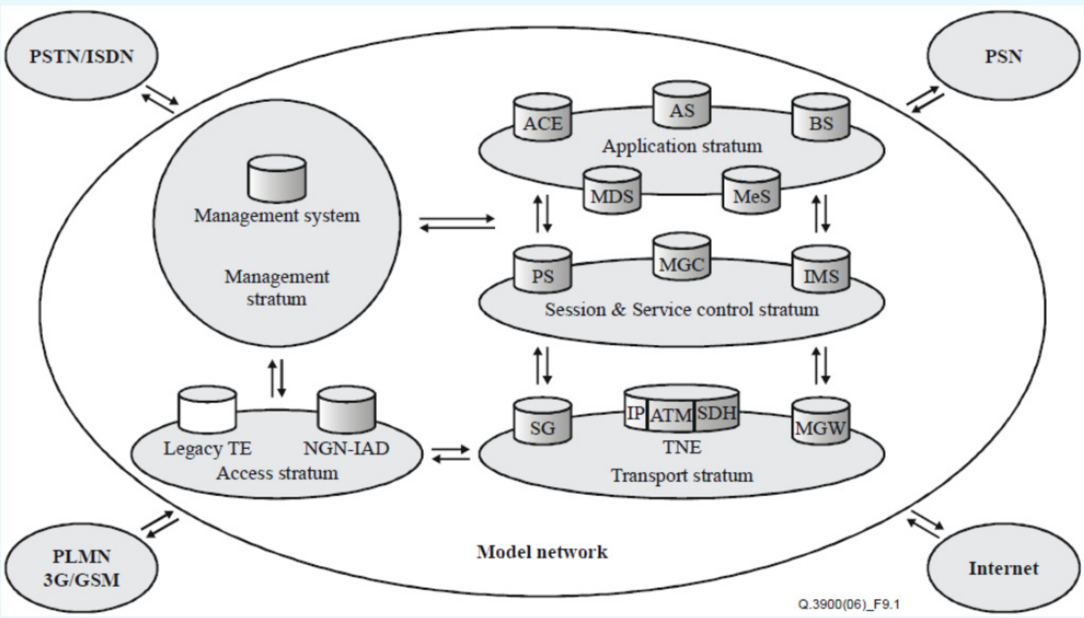
Device Under Test (DUT) may be accessed by the NGN test lab through dedicated model or distributed model. One basic requirement for such a remote testing is that the DUT must appear to the tester as it is connected directly. This is possible by creating a tunnel between the tester and the DUT using appropriate tunneling technology. Tunneling technology can be used, along with pseudo –wire capability in routers, to send the test packets directly to the remotely placed DUT. The available test suits thus become suitable for remote testing.

3.1 Dedicated model network

A dedicated model is a fragment network which is not connected to other model networks and used to perform testing for compatibility and, if possible, for interaction with the technical means employed prior to the NGN development period. The dedicated model network can be connected to a public telecommunication network and/or corporate network.

The basic architecture of a dedicated model network is shown following Figure 3-1.

Figure 3-1: Basic architecture of a model network (form of a dedicated model)



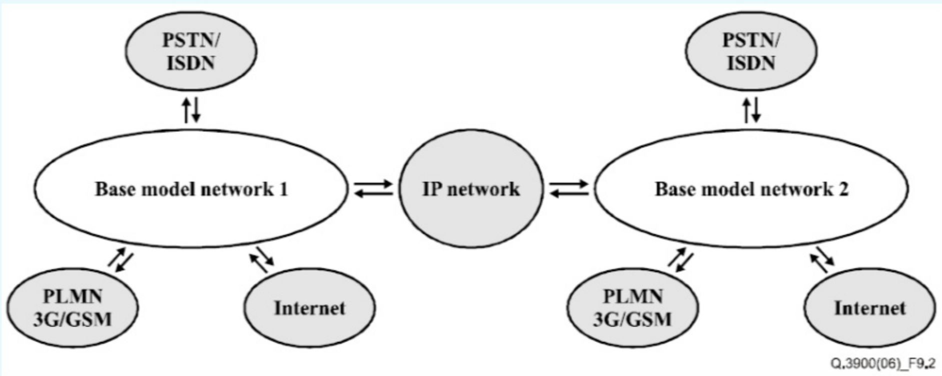
3.2 Distributed model network

A distributed model network is composed of several dedicated model networks, two as a minimum, and should be interconnected by the dedicated Intranet network such as VPN. The distributed model networks can also be connected to public telecommunication networks and/or corporate networks. The distributed model networks are used to perform complex tests for compatibility and interworking as well as to check quality of service parameters, information security requirements and interworking with the technical means. The minimum-size configuration of the model network should have:

- four nodes of the public telecommunication network (three of them should be of different types and two, as a minimum, should originate from different vendors);
- the communication networks inside the dedicated model networks provide internal communication (of the SDH, ATM or IP level) without limitation in types and manufacturers;
- four media gateways, the minimum of three of which should be of different types and the minimum of two should come from different manufacturers;
- four signalling gateways meeting the same different-type and manufacture brand requirements;
- four application servers, out of which at least two should be of different types;
- additional NGN technical means.

The basic architecture of a distributed model network is shown in Figure 3-2.

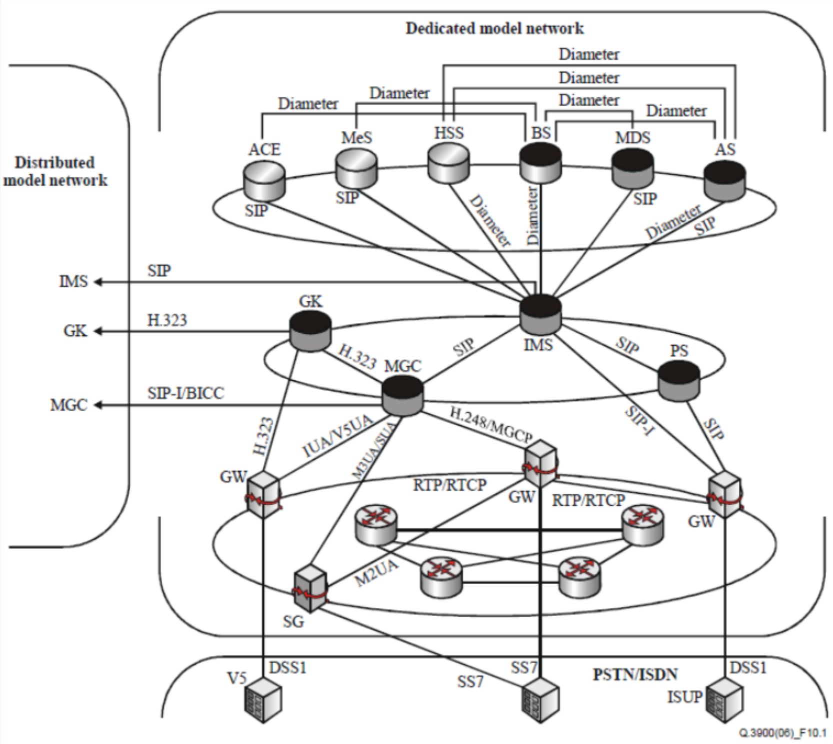
Figure 3-2: Architecture of a distributed model network in minimum-size configuration



3.3 Protocol configuration of model network

The protocols scheme of dedicated and distributed model networks must be realized in accordance with the scheme illustrated in Figure 3-3.

Figure 3-3: Protocol configuration of model network

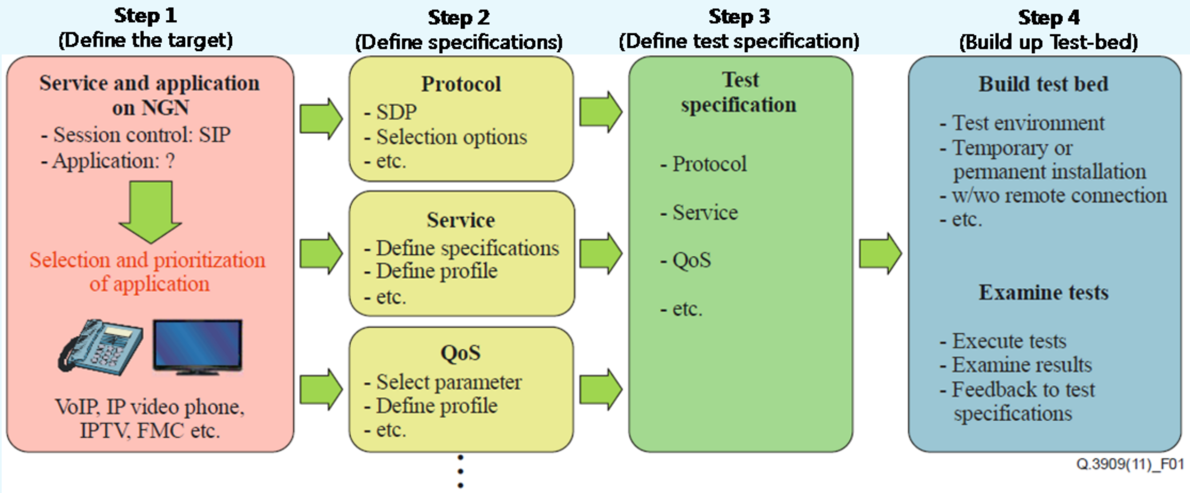


4 NGN conformance testing and interoperability testing

There are two tests to confirm the function of NGN standards: one is for conformance testing and the other is for interoperability testing. NGN conformance testing is able to show that a particular implementation complies with the protocol requirements specified in the associated base standard. However, it is difficult for such testing to be able to prove that the implementation will interoperate with similar implementations in other products. On the other hand, NGN interoperability testing can clearly demonstrate that two or more implementations will cooperate to provide the specified end-to-end functions, but cannot easily prove that either of them conforms to the detailed requirements of the protocol specification. The purpose of interoperability testing is not only to show that target products from different manufacturers can work together, but also to show that these products can interoperate using a specific protocol.

Figure 4-1 shows a four-step approach on the specification process for NGN conformance testing and interoperability testing.

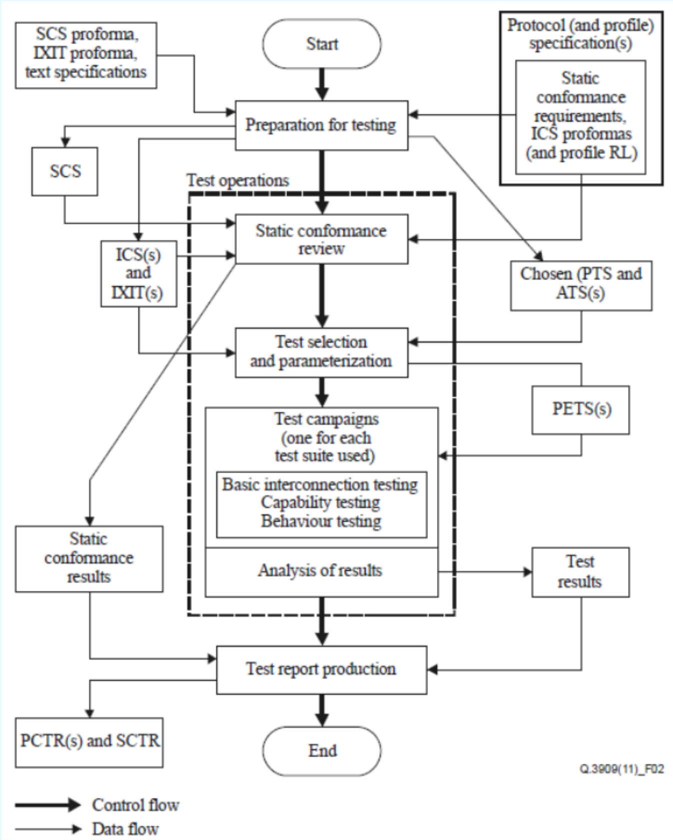
Figure 4-1: Typical NGN conformance and interoperability test specification process



4.1 NGN conformance testing

A conformance testing is performed on a product or a system to confirm that the protocol implemented in the target product (or system) is in accordance with the protocol specification described in specific Recommendations. Therefore NGN conformance testing is performed on NGN systems with relevant Recommendations. It is possible to refer to part of a procedure of the ITU-T X.29x-series as a procedure for NGN conformance testing. Figure 4-2 illustrates the overview of conformance testing of the execution procedure in [ITU-T X.290].

Figure 4-2: ITU-T X.290 conformance assessment process overview



NGN conformance testing should consider specifications on:

- the test subject which is connected to the tester or reference machine and examines conformity with reference Recommendations;
- certifications or the type of approval which may be given to the products passed by the testing authority (this is not a mandatory function of conformance testing);
- test specifications for the conformance testing which are specified in the test specification language (e.g., PICS, PIXIT).

The conformance assessment process involves following three phases: preparation, operation and reporting.

1st phase is the preparation for testing as following step:

1-1) Set the test object, target interface and target Recommendations,

1-2) Set the physical configuration and target products, and

1-3) Define the test scenarios.

2nd phase is for test operations with following step:

2-1) Static conformance review,

2-2) Test selection and parameterization, 2-3) Test campaigns (examine the conformance testing according to the scenarios) and,

2-4) Analysis of results.

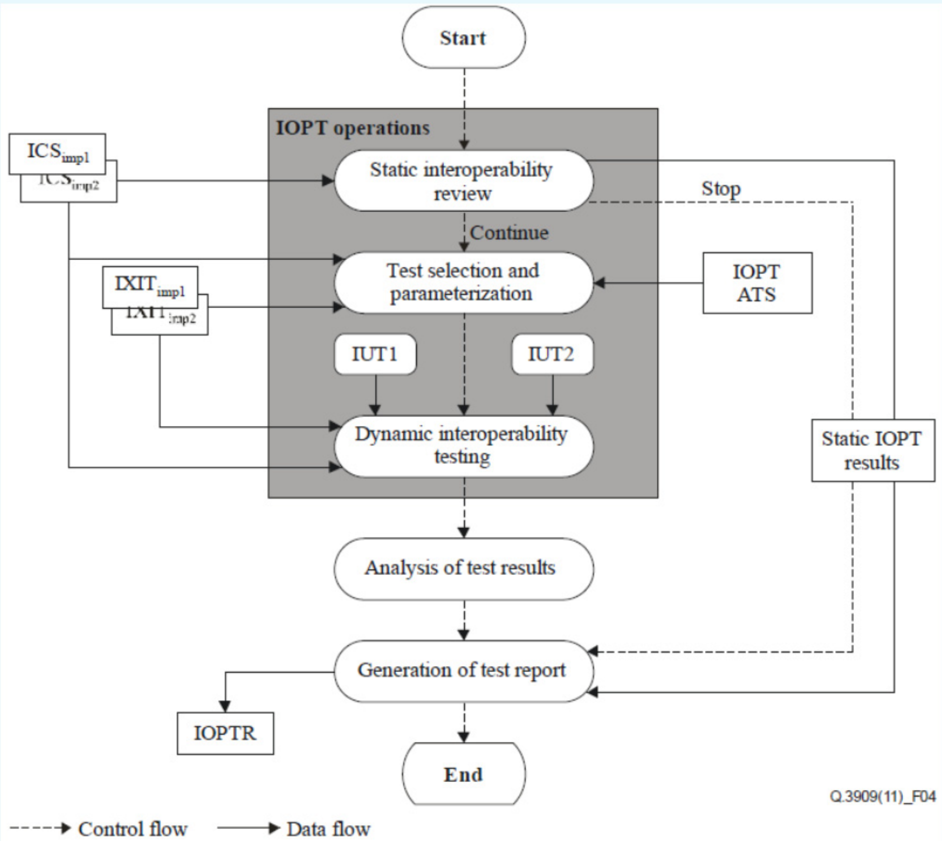
Finally 3rd phase is production of the test report.

4.2 NGN interoperability testing

Interoperability testing for NGNs is performed on two or more products. Its objective is to check the ability and performance of the products implemented by mutually exchanging information. The interoperability testing procedures of [ITU-T X-Sup.4] and [ITU-T X-Sup.5] may be referenced when undertaking NGN interoperability testing,

Figure 4-3 shows the overview of the execution procedure for interoperability testing which identified in [ITU-T X-Sup.4] and [ITU-T X-Sup.5].

Figure 4-3: Interoperability testing procedure



The execution procedure of interoperability testing in [ITU-T X-Sup.4] and [ITU-T X-Sup.5] is described as follows:

- The test operator should receive the information conformance statement (ICS) and implementation extra information for testing (IXIT), described in the applicable reference Recommendations;
- A static interoperability review is executed according to the content described in the ICSs and IXITs;
- If after review of the static interoperability test results, it is judged that interoperability testing does not need to be executed, then the test operation will be ended;
- When it is necessary to execute the tests, the settings of the test method, the test environment architecture and the test specification will be explained in detail during the process of test selection and parameterization;
- Dynamic interoperability testing is executed according to the procedure of the prepared test specification that is built in two or more implementations under test (IUTs) which, as target products, connected mutually;
- The test output in dynamic interoperability testing would be analyzed and the test result report would be generated.

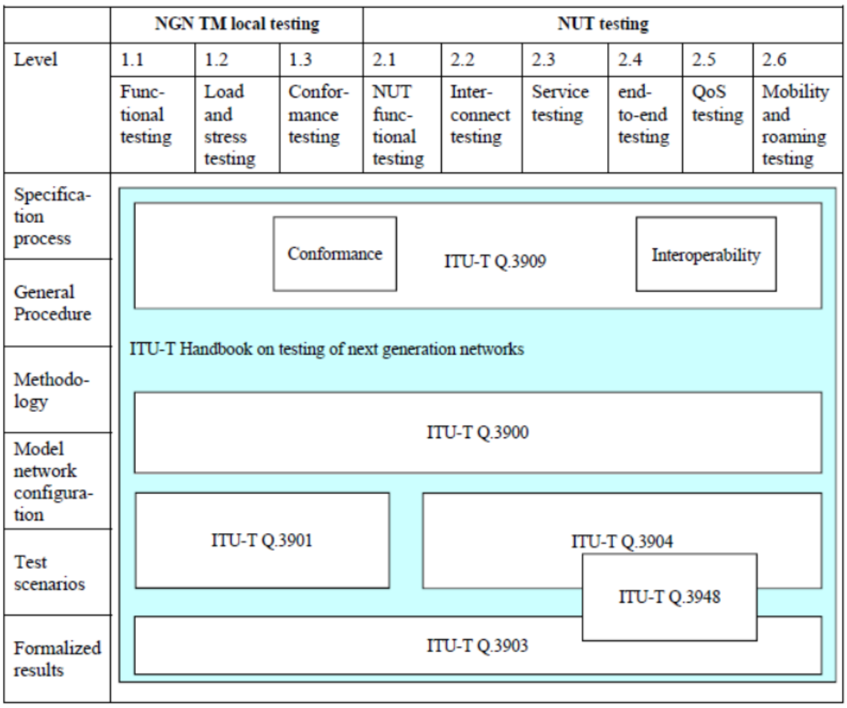
Interoperability testing for NGNs should consider specifications on multiple products from multiple vendors that are connected and tested for interoperability at the service and transport level, or both. And NGN interoperability testing should be conducted in the following steps:

1) Preparation for testing
    1-1) Set the test object, target interface and target Recommendations
    1-2) Set the physical configuration and target products
    1-3) Define the test scenarios.
2) IOPT operations
    2-1) Static interoperability review
    2-2) Test selection and parameterization
    2-3) Dynamic interoperability testing (examine the interoperability testing according to the test scenarios).
3) Analysis of test results.
4) Generation of test report.

4.3 Positioning map of NGN testing specification documents

A number of ITU-T Recommendations contain NGN testing specifications. Following Table 4-4 shows the relationship between the ITU-T Handbook on testing of NGN and ITU-T Recommendations specifying NGN testing.

Table 4-4: Recommendations for NGN tests



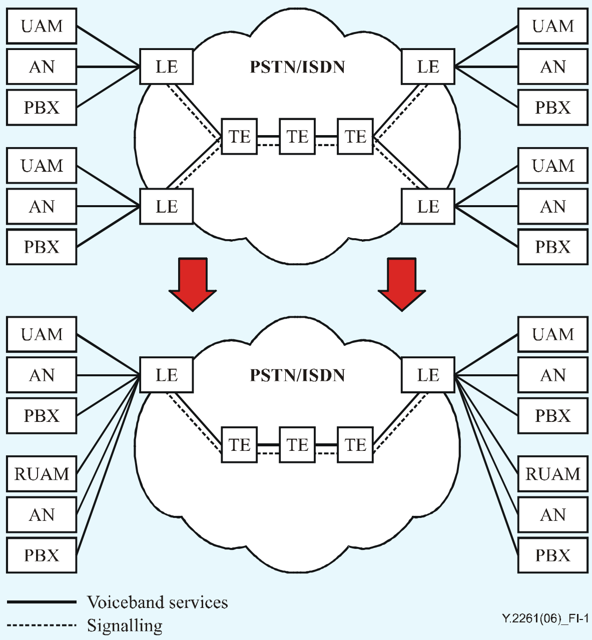
Annex 7: Examples of Migration Scenarios

1 Core Network migration to NGN

1.1 Consolidation of local and remote exchanges for migration to NGN

In order to prepare the PSTN/ISDN for the migration to a NGN, and as an initial step, some of the LEs (Local Exchanges) can be removed and all their functionalities such as control, accounting, etc. transferred to those remaining LEs. The affected UAMs (User Access Modules), PBXs, and ANs (Access Networks) are connected to the remaining LEs. Further consolidation occurs when UAMs become RUAMs (Remote UAMs), which are connected to the remaining LEs. Figure 1-1 shows this preparatory step.

Figure 1-1: Preparation for migration to NGN

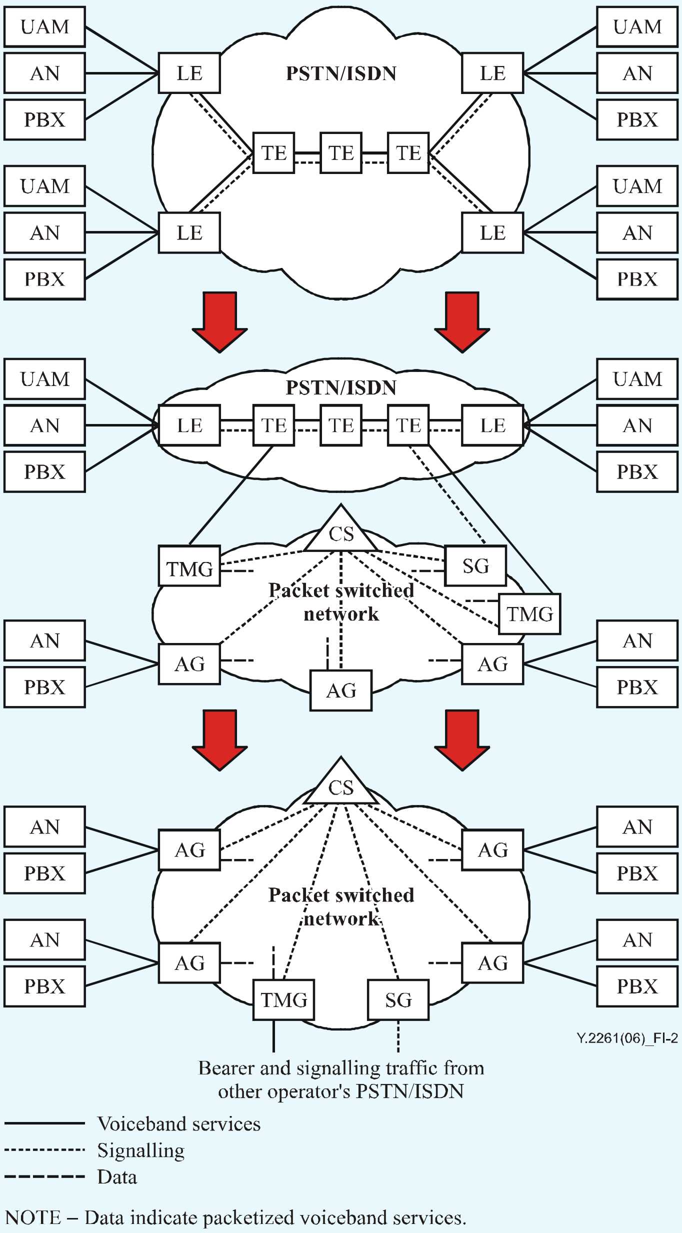


1.2 Scenario 1 – PSTN/ISDN and NGN initially co-exist

In the most likely initial approach for migration of PSTN/ISDN to the NGN, the PSTN/ISDN will co-exist with the NGN during a transition period. There are two steps in this scenario.

- Step 1: In this step, some of the LEs are replaced by AGs (Access Gateways). Functions originally provided by the removed LEs are now provided by the AGs and the CS. In addition, some of the access elements such as UAMs, RUAMs, and PBXs, which were originally connected to the removed LEs, are now directly connected to AGs. Additional AGs may also be deployed to support new subscribers that directly connect to them. The TMGs (Trunking Media Gateways) and SGs (Signaling Gateways) are deployed for interconnection between the NGN and the TEs of the legacy network as well as other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by the CS.
- Step 2: In this step, the remaining LEs are replaced by the AGs, and the TEs are removed and their control functions are performed by CS. The TMGs and SGs are deployed for interconnection between PSN and other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by the CS.

Figure 1-2: Realization of scenario 1



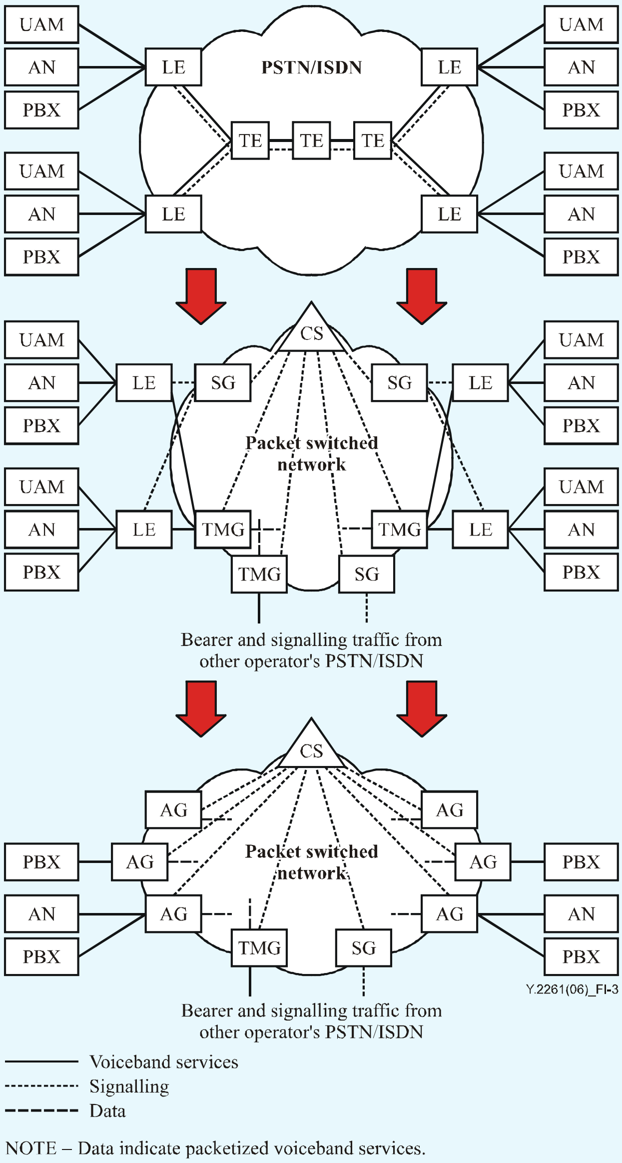
1.3 Scenario 2 – Immediate use of NGN, initially via SGs and TMGs

In this scenario, the PSTN/ISDN is immediately replaced by the NGN. As a first step, the LEs are connected to SGs and TMGs, while later on they are eliminated.

- Step 1: In this step, PSTN/ISDN is replaced by NGN and the TE functions are performed by the TMGs and the SGs under the control of the CS. The LEs are connected to the NGN via TMGs and SGs. The TMGs and SGs are also deployed for interconnection between NGN and other operators' PSTNs/ISDNs.

- Step 2: In this step, the LEs and some of the access elements such as UAMs and RUAMs are removed and their functions are provided by the AGs and CS. The PBXs are directly connected to the AGs. The ANs are either replaced by the AGs or are connected to the AGs. The TMGs and SGs are deployed for interconnection between NGN and other operators' PSTNs/ISDNs. The AGs and TMGs are all controlled by CS.

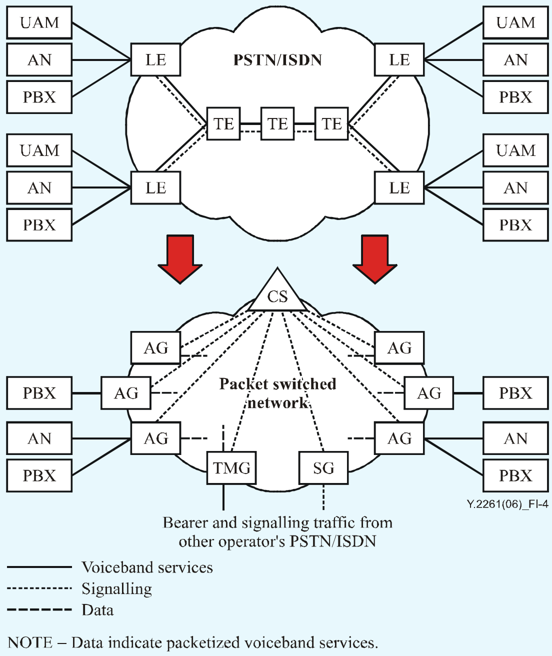
Figure 1-3: Realization of scenario 2



1.4 Scenario 3 – The one-step approach

In this scenario, the PSTN/ISDN is replaced with NGN in only one step. The LEs are replaced by AGs and their functions are divided between the AGs and the CS. Specifically, the call control and accounting functions are all transferred to the CS. All access elements such as UAMs, RUAMs, and PBXs are connected to AGs. The ANs are either replaced by the AGs or are connected to NGN through the AGs. The TMGs under the control of the CS, and the SGs, are deployed to replace the TE functions and provide interconnection between NGN and other operators' PSTNs/ISDNs.

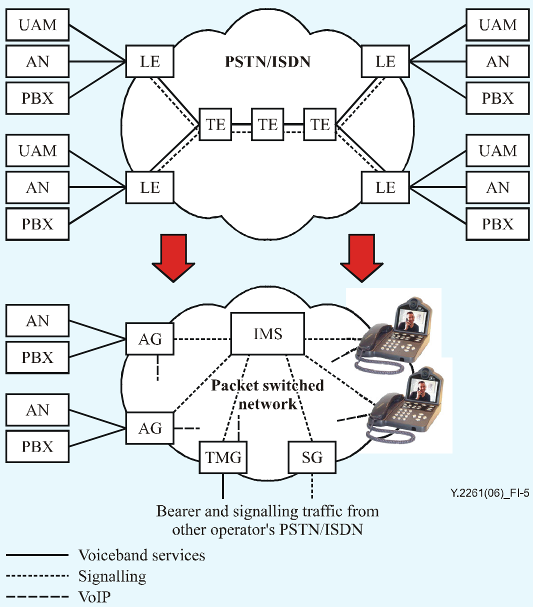
Figure 1-4: Realization of scenario 3



1.5 IMS-based migration to NGN

In the case of where PSTN/ISDN evolves directly to a NGN based on the IMS core network architecture, the end-users access the network using NGN user equipment or legacy user equipment connected via an AG. The TMGs and SGs are deployed for interconnection between the NGN and other operators' PSTNs/ISDNs.

Figure 1-5: IMS-based PSTN/ISDN migration to NGN

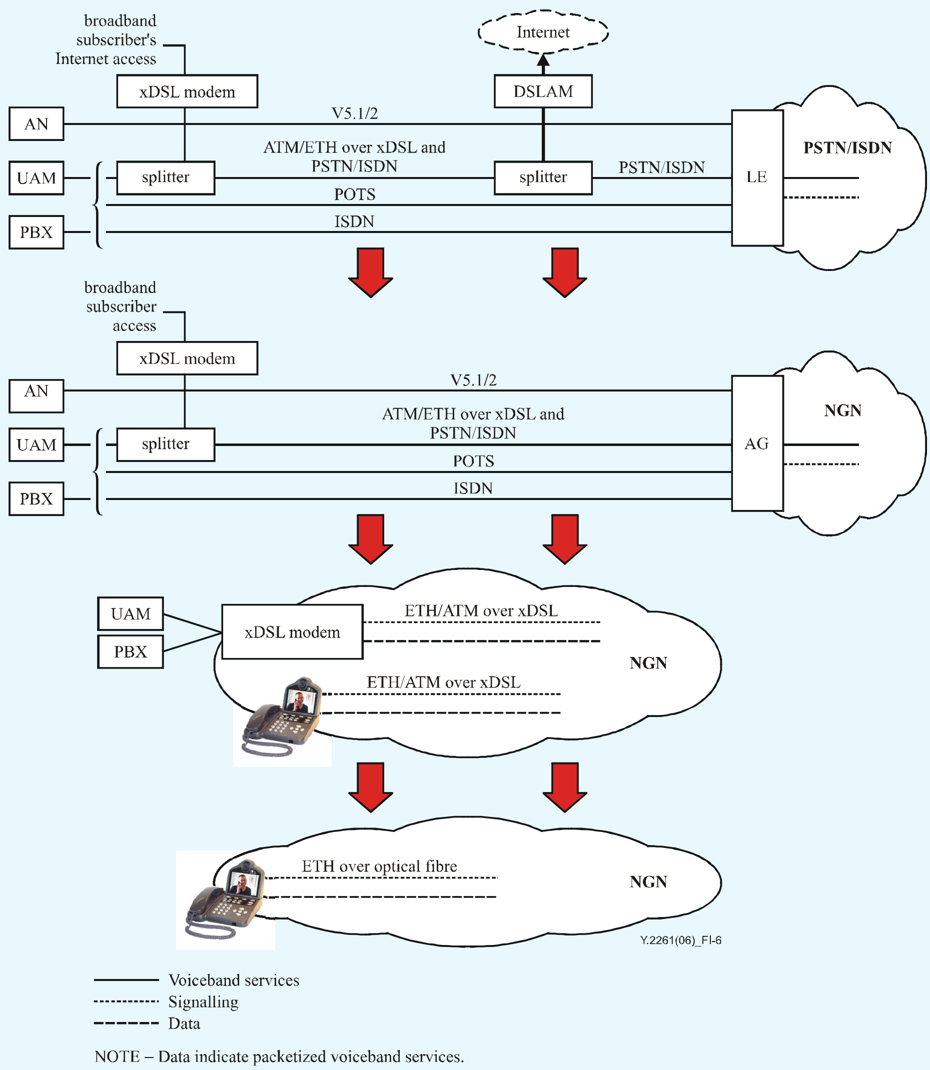


2 Access network migration to NGN

Legacy voice users may also have access to broadband services for example via xDSL (see [G.995.1]). In this case, the customer-located equipment is an xDSL modem and the service provider equipment is a digital subscriber line access multiplexer (DSLAM). Since xDSL interfaces enable users to connect to the Internet, these interfaces may be utilized to connect such users to NGNs. AN, for another user domain with V5.x [G.964] and [G.965] interface can be left as it is shown in Figure 5-6 or it can be completely replaced by AG connected to NGN directly. Migration of access network is shown in three possible steps.

- Step 1: Traditional AN/UAM interfaces include: POTS, ISDN and V5.1/2 [G.964] and [G.965]. Such interfaces connect subscribers to the core PSTN/ISDN via LE.
- Step 2: An IP user may also use xDSL interface as the transport medium to an NGN. Protocol for xDSL interface may be Ethernet which enables broadband data flows and services, e.g., VoD, IPTV, VoIP and Internet.
- Step 3: In this step, the legacy end systems are replaced by NGN end systems and twisted copper lines are replaced by optical fibre, either fibre-to-the-curb (FTTC) or fibre-to-the-home (FTTH) to increase transmission speed.

Figure 2-1: Migration of xDSL access to NGN

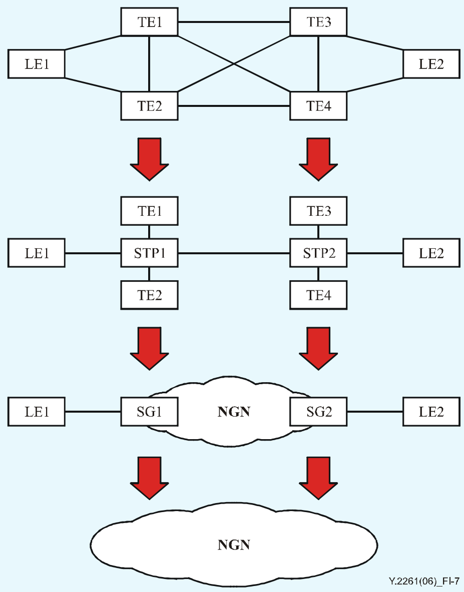


3 Signaling and control scenarios

A possible scenario for migration of signalling in the core network consists of following three steps.

- Step 1: In this step, signalling functions are transferred from the TEs to the independent units creating an STP mesh network (partial or complete).
- Step 2: In this step, STPs are upgraded to the SGs and are placed on the edge between PSTN/ISDN and NGN. In this case, both the legacy network and NGN co-exist with each other.
- Step 3: In this step, all LEs and TEs are replaced by NGN.

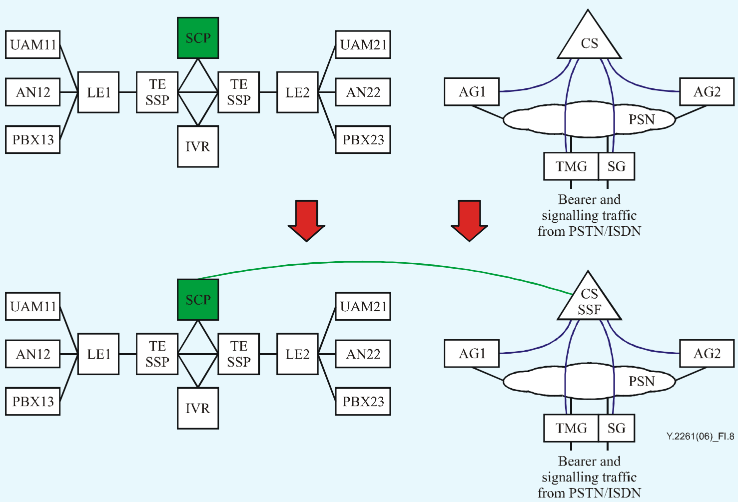
Figure 3-1: Realization of signalling migration scenario



4 Services migration scenarios

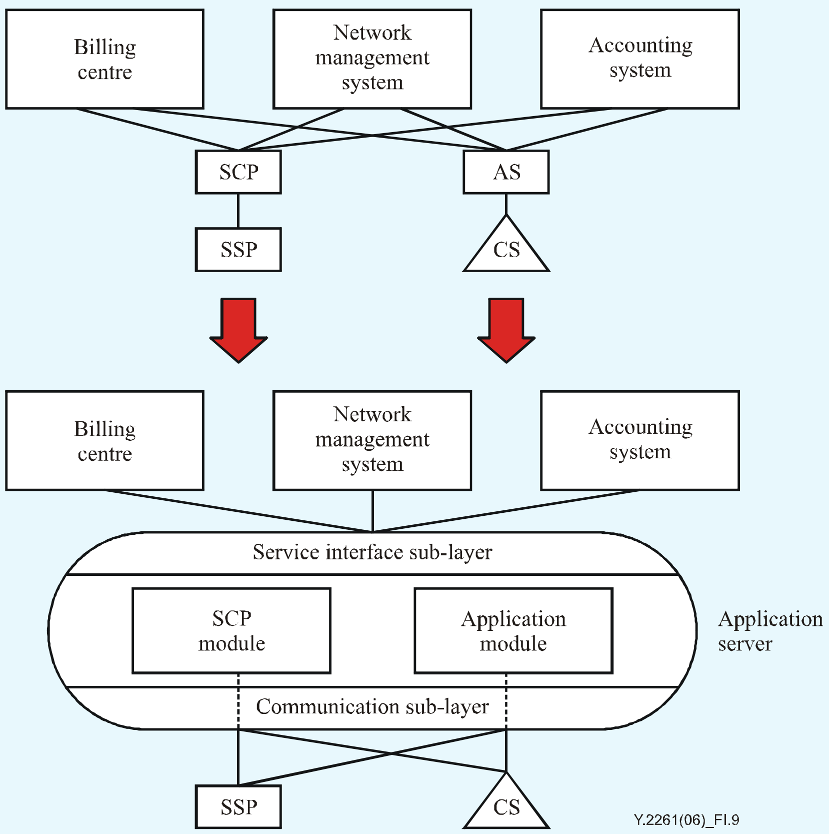
- Scenario 1: In this scenario, existing IN services are reused in NGN by implementing SSF in the CS. Both PSTN/ISDN and NGN exist.

Figure 4-1: Realization of scenario 1



- Scenario 2: In this scenario, the SCP is integrated to the application server. The communication sub-layer is a uniform communication layer which may provide connection between SSP, CS, SCP and the application server. The services created by the service creation environment (SCE) in the IN may be directly loaded into the SCP module of the AS. The SCP and the application module may be connected through a service interface sub-layer to operation and maintenance and external systems (e.g., billing centre, network management centre, accounting system).

Figure 4-2: The SCP is integrated to the application server as a whole

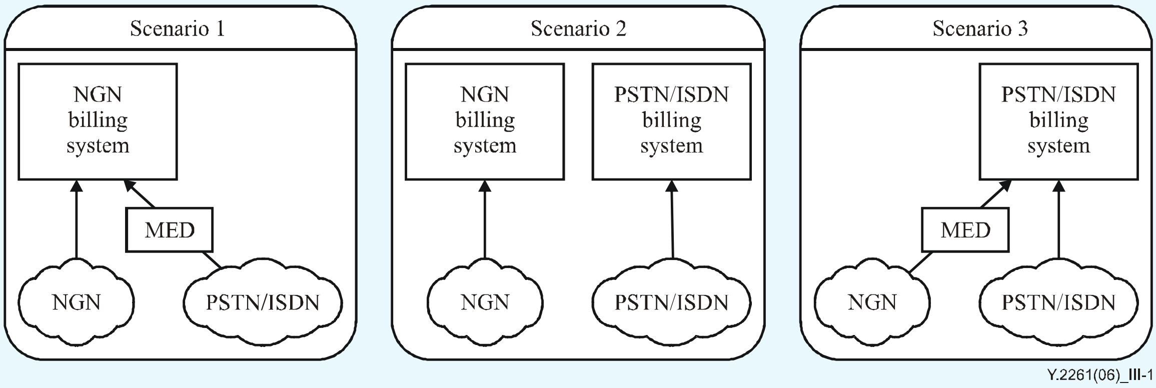


5 Billing system migration scenarios

The following three scenarios are considered when migration to NGN. The timing or preference for selection of these scenarios is service provider dependent. Mediation (MED) is an entity which allows transfer and processing of call detail records (CDRs) from the PSTN/ISDN to the NGN billing system, or from the NGN to the PSTN/ISDN billing system.

- Scenario 1: For this scenario, an NGN billing system is considered to handle both the PSTN/ISDN and the NGN. For this case, all accounting aspects are affected.
- Scenario 2: For this scenario, a new billing system is developed for the NGN, while keeping the existing PSTN/ISDN billing system. For this case, all accounting aspects are to be considered for NGN.
- Scenario 3: For this scenario, a legacy billing system is considered to handle both the PSTN/ISDN and the NGN. For this case, all accounting aspects are affected.

Figure 5-1: Billing system migration scenarios



Annex 8: NGN Issues

NGN should continuously evolve to build up "Connected World" providing more convenient ways to use services and application including to use of relevant network resources allowing from other providers such as 3rd party providers. Another important aspect is that NGN should support Ubiquitous Networking which will represent the situation of "Connect to Anything" in other words called IoT "Internet of Things". For these, service platform aspects and capabilities to support ubiquitous networking of NGN have been seriously considered and developed during the last few years, especially in ITU-T NGN-GSI.

1 Service Integration and Delivery Environments in NGN

NGN-GSI in ITU-T studied on service platform aspects which should support multi-fold telecommunication business model and through this, NGN enhances NGN end-users access to applications. ITU-T Recommendation Y.2240 (approved at January 2011, formerly known as Y. NGN-SIDE) identifies service delivery platform called NGN-SIDE can be viewed as the next generation service delivery platform (SDP) and its framework can conceptually be applicable to other telecommunication environments (e.g. mobile networks).

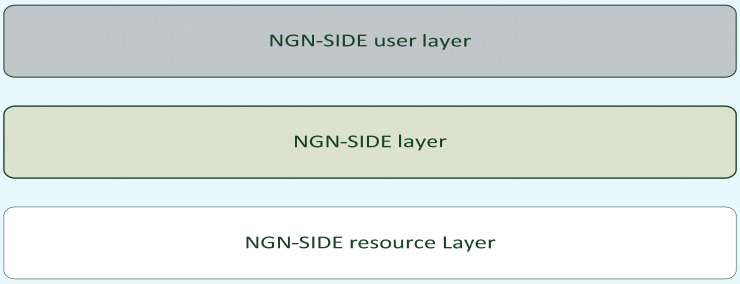
NGN-SIDE is defined as "an open environment in NGN integrating resources from different domains and delivering integrated services to applications over NGN." Here, domains include, but are not limited to, telecommunication domain (e.g. fixed and mobile networks), Internet domain, Broadcasting domain and Content Provider domain.

The following main functionalities are supported in the NGN-SIDE ecosystem:

- integration of resources from different domains (e.g. telecommunication domain (fixed and mobile networks), broadcasting domain, internet domain or content provider domain) over NGN;
- adaptation, including abstraction and virtualization, of resources from different domains;
- resource brokering for mediation among applications and resources;
- support of application development environment for application developers;
- support of different service interfaces across ANI, UNI, SNI and NNI for exposure of NGN-SIDE capabilities and access to resources in different domains;
- provision of mechanisms for the support of diverse applications including cloud services, machine to machine, and ubiquitous sensor network applications;
- provision of mechanisms for the support of applications making usage of context based information;
- provision of mechanisms for content management.

NGN-SIDE has a layered architecture as shown in the following Figure 1-1:

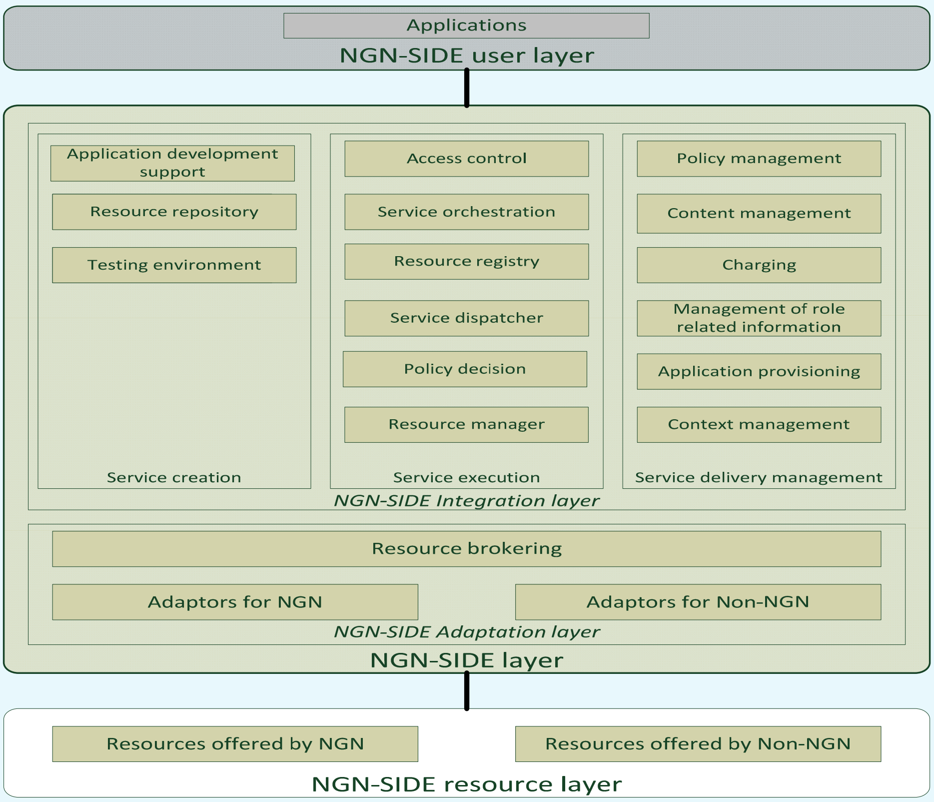
Figure 1-1: Layered View of NGN-SIDE



- The NGN-SIDE user layer uses the services offered by the NGN-SIDE layer, including resource exposure. It includes users accessing the NGN-SIDE, such as applications and other users.
- The NGN-SIDE layer corresponds to NGN-SIDE.
- The NGN-SIDE resource layer includes resources accessible by NGN-SIDE, such as applications, service enablers, network capabilities, connectivity, computing, storage, and content.

The following Figure 1-2 shows a functional view of NGN-SIDE according to the above described layers, the NGN-SIDE layer being comprised of the NGN-SIDE integration layer and the NGN-SIDE adaptation layer:

Figure 1-2: Functional View of NGN-SIDE



In order to reduce the complexity of integrating resources, the NGN-SIDE integration layer provides a unified way for the NGN-SIDE users to access the resources offered by NGN and Non-NGN. It supports the service creation functional group, the service execution functional group and the service delivery management functional group:

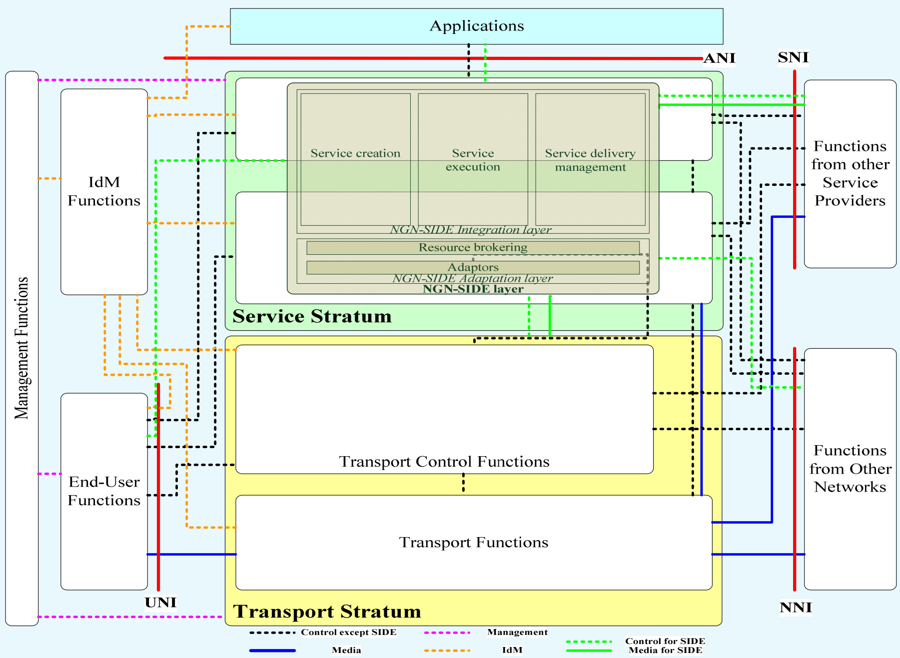
- the service creation functional group provides capabilities to realize an application development environment for application developers;
- the service execution functional group provides capabilities to support the service execution environment;
- the service delivery management functional group provides capabilities to realize the management of different aspects, provisioning of applications and charging for ensuring proper functioning of the service creation and service execution functional groups and providing associated delivery functionalities.

The NGN-SIDE adaptation layer adapts resources offered by NGN-SIDE resource providers such as their own service logic and service control, and related protocols, in order to provide uniformly adapted resources (e.g. control and media format) for interaction with the NGN-SIDE integration layer. NGN-SIDE resource providers use standardized or proprietary interfaces called “NGN-SIDE resource interfaces” to offer resources to NGN-SIDE and these interfaces are adapted by NGN-SIDE.

NGN-SIDE positioning within the NGN reference architecture is shown in the following Figure 1-3:

The NGN-SIDE functional components are positioned inside the NGN service stratum. The NGN-SIDE adaptation layer enables the abstraction of resources, including the resources of the NGN transport stratum (e.g. transport control functions and transport functions related resources) and the NGN service stratum (e.g. service control functions and content delivery functions related resources).

Figure 1-3: NGN-SIDE positioning within the NGN reference architecture



2 Open Service Environments in NGN

Another important aspect of NGN in the sense of services is that enabling new capabilities and supports a wide range of emerging services with advanced and complex functionalities for application providers such as 3rd party providers. In response to a drive from application providers and/or developers to develop new applications and capabilities accessible via standard interfaces, NGN providers should cooperate in the development of standard application network interfaces (ANI) including software reusability and portability. An open service environment (OSE) within NGN aims to provide efficient and flexible capabilities based on the use of standard interfaces to NGN applications thereby enabling applications to take full advantage of the NGN capabilities. Two ITU-T Recommendations address this OSE as follows:

- ITU-T Recommendation Y.2234 (approved at 2008): defines the requirements that are divided into service requirements and functional requirements.
- ITU-T Recommendation Y.2020 (2011): defines the OSE architecture for NGN based on ITU-T Y.2234 and ITU-T Y.2201.

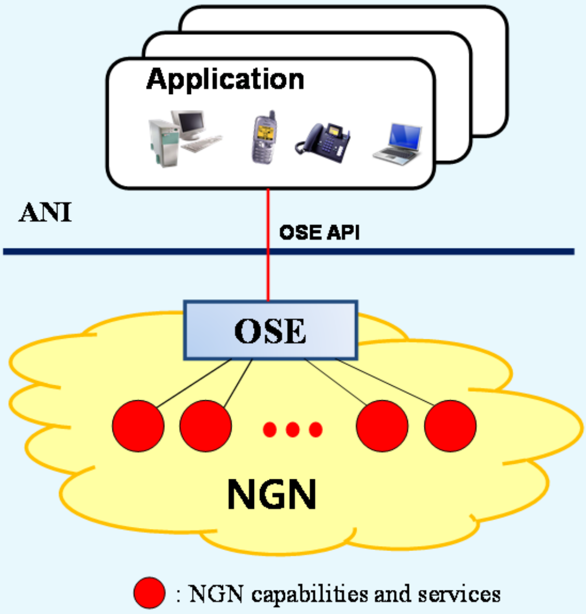
Open service environment provides capabilities to enable flexible and agile service creation, execution and management based on the use of standards interfaces. The use of standard interfaces will ensure NGN OSE based service reusability and portability across networks, as well as accessibility by application providers and/or developers.

OSE capabilities have the following characteristics:

- Flexible development of applications and capabilities by NGN providers, application providers, and other service providers;
- Exposure of capabilities via standard application network interfaces (ANI);
- Portability and re-usability of capabilities across networks (and from other network to NGN or from NGN to other network);
- Leveraging new capabilities enabled by technologies from non-NGN environments

The OSE allows applications to make use of NGN capabilities and/or services offered through the application network interface (ANI) as shown in Figure 2-1. Application providers and/or developers will be able to create and provide new applications via standard interfaces at the ANI as shown OSE API regardless of the type of underlying network and/or equipment.

Figure 2-1: Open service environment capabilities in NGN



Service requirements of NGN-OSE capabilities are defined as followings:

- Provide standard APIs for application providers and/or developers to create and introduce applications quickly and seamlessly;
- Provide the service level interoperability among different networks, operating systems and programming languages (e.g. Web Services are an example of enabling technology for providing service level interoperability);
- Support service independence from NGN provider and manufacturers [ITU-T Y.2201]:
- Support OSE capabilities based on NGN providers' capabilities. However, OSE capabilities based on application providers' capabilities are not supported in this version of the document;
- Support location, network and protocol transparency [ITU-T Y.2201]:
- Provide capabilities for coordinating services among themselves and services with applications;
- Support service discovery capabilities to allow users and their devices to discover the services, applications, and other network information and resources of their interest [ITU-T Y.2201]. In addition, discovery mechanisms for services or components of multiple application providers are recommended to be provided;
- Provide the means to manage the registration of capabilities, services and applications. The technology choice is required to ensure functions for service registration and deregistration, including configuration, activation, publication [ITU-T Y.2201];
- Provide the service management capabilities such as service tracking, update management, auditing, version control, logging, e.g. provide a record of the history of services, access control management, statistical analysis of service registration and utilization.
- Support NGN services reuse by providing service composition capability;
- Support of a service composition language;

- Offer a development support environment which supports construction, trialing, deployment, and removal of applications [ITU-T Y.2201];
- Allow interworking with service creation environments and network entities for creation and provisioning of applications and services [ITU-T Y.2201];
- Provide a secure access to the NGN capabilities in alignment with the general NGN security requirements as specified in clause 5.13 of [ITU-T Y.2201];
- Support policy enforcement capability for resources protection and management, and service personalization.

The functions to support of the NGN-OSE are consisted with service coordination, service discovery, service registration, service management, service composition, service development support, interworking with service creation environments and policy enforcement. In each function has more detail requirements as following:

The NGN service coordination functions are required to:

- Provide coordination of applications and services with capabilities;
- Provide the tracking of NGN capabilities or service components from various application providers, and the relationship between these capabilities or service components;
- Support the information on state change of capabilities or service components for applications and services.

The NGN service discovery functions are required to:

- Provide service discovery for physically distributed NGN services;
- Support a variety of discovering criteria (e.g. specific field based discovery, classification system based discovery). An example of discovering criteria is implemented in the Universal Discovery, Description and Integration (UDDI) specification of Web Services framework;
- Use user and device profile information for discovering the proper service;
- Allow users to discover user-interest services, device-interest services and network information;
- Support a variety of scoping criteria (e.g. location and cost) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy (This allows support of customized discovery for a wide range of scenarios.);
- Use a variety of approaches for discovering services such as client-server, P2P, combination of client-server and P2P;
- Support appropriate mechanisms to ensure security and privacy;
- Take into account scalability (e.g. broadcast mechanisms are recommended to be avoided).

The NGN service registration functions are required to:

- Provide service registration, including configuration, activation, publication and service deregistration;
- Provide a variety of service registration features (e.g. manual, autonomous) for NGN services;
- Support a variety of registration parameters, including mandatory and optional parameters.

The NGN service registration functions may support:

- Registration services in centralized and de-centralized ways;
- Multiple concurrent service registrations.

The NGN service management functions are required to:

- Provide a monitoring function of registered services for availability and predicted response time. NGN services and user applications might need to use monitoring information for the availability or predicted response time of target services before executing services;
- Provide managing functions of QoS information about registered NGN services such as accessibility, performance, integrity, reliability, etc.;
- Provide a version management function to NGN services for interoperability;
- Provide notification service functions for updated services;
- Provide failure detection and recovering functions for unexpected failures;
- Provide service tracking management functions to capture and log all relevant information for each component within a service chain. Service tracking is recommended to allow for an association among the captured data associated with a specific service. Service tracking is required to enable tracking of capabilities or components of multiple third parties, and the relationships between these capabilities or components;
- Provide a service substitution function that considers various kinds of factors to users. It is required to provide mechanisms to capture a set of information including terminal capability, network situation, user preference and substitution policy; and judge whether to substitute the service or not based on the captured information. If there is a need to substitute the service, this function will substitute it;
- Provide service access control functions to control the accessibility of a specific service by applications. (The service access control function provides the necessary authentication and authorization actions required to ensure that the application has appropriate access rights for the requested service.);
- Provide statistical analysis functions to analyze service registration and utilization information (e.g. number of registered services, utilization frequency of registered services, and number of applications using registered services.);
- Provide an auditing function to review the overall operations of open service environment capabilities during a specific period required by the auditor.

The NGN service composition functions are required to:

- Provide a composition language that describes the interaction among services. Additionally, the composition language is recommended to support expression capabilities for describing the composition logic among services;
- Support the composition of services statically or dynamically (i.e. for the static type, the services are composed during service design; while for the dynamic type, the services are composed during service runtime).

The NGN service development support functions are required to:

- Support services re-use and allow for services interchangeability;
- Support mixing-and-matching of services by management of interfaces and consistent semantics of shared data/schema across these services
- Support the full life cycle of services, ranging from installation, configuration, administration, publishing, versioning, maintenance and removal;
- Support delivery-agnostic application designs to allow applications to be implemented without requiring re-design for each subsequent development scenario;
- Support tracking of dependencies among services.

The NGN service creation environment interworking functions are required to:

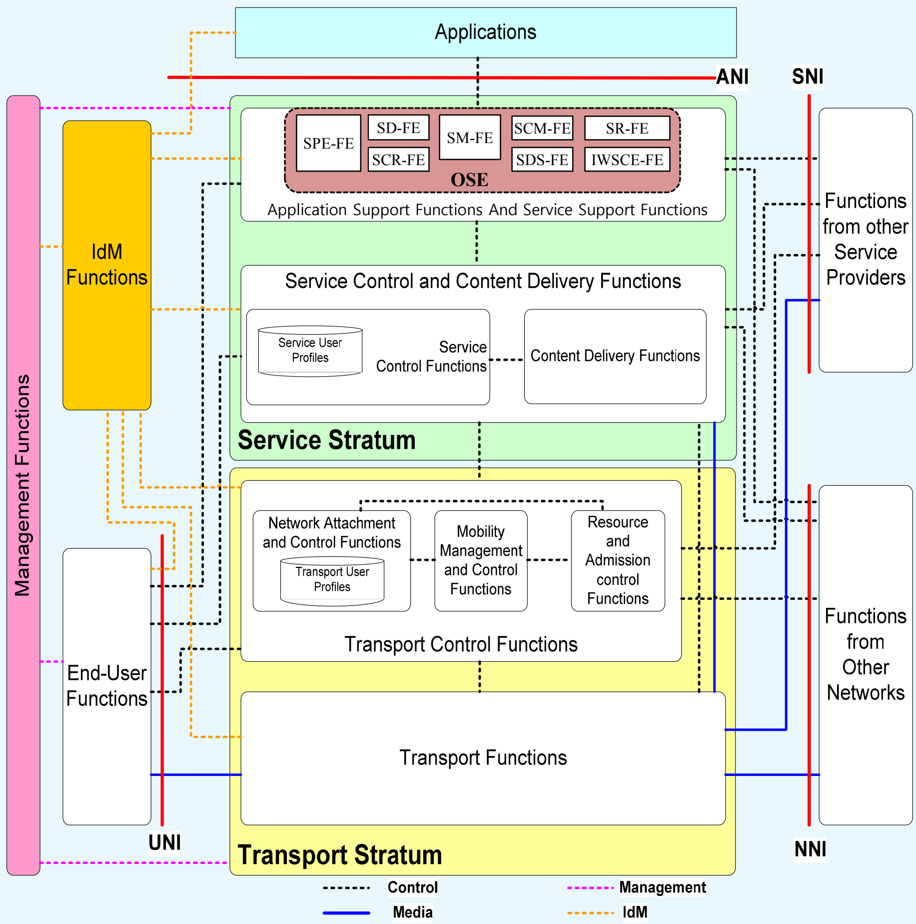
- Support the following three classes of service creation environments

The NGN policy enforcement functions are required to:

- Provide a description language to express various kinds of policy rules such as those related to authorization, charging, service level agreement and logging. This language is recommended to support policy re-use;
- Provide a policy execution framework to interpret and execute the policies;
- Protect services from unauthorized users' requests and manage requests based on the policy rules;
- Support the selection of appropriate services for service composition to respond to the needs and preferences of a user or a group of users.

Figure 2-2 shows the extended NGN architecture overview [ITU-T Y.2012] in order to illustrate the positioning of the OSE functional group.

Figure 2-11: OSE positioning in the NGN architecture



3 Next Generation Ubiquitous Networking (NGUN)

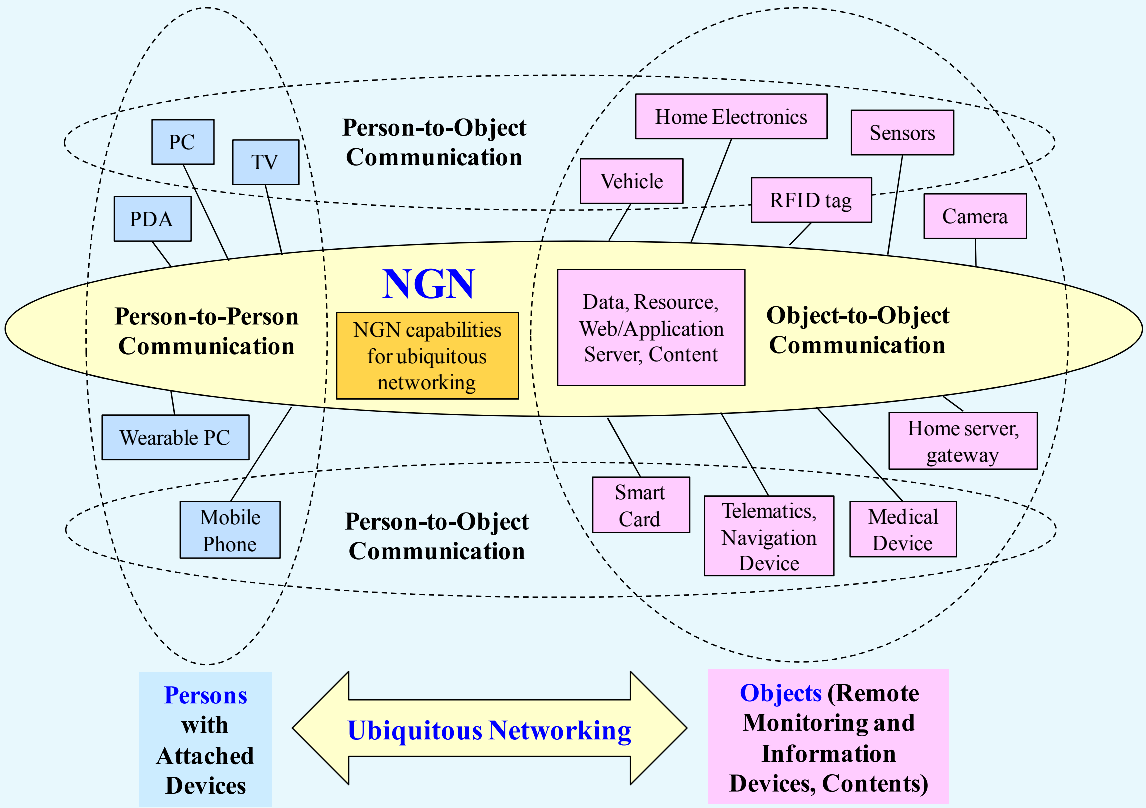
To realize the vision of "Connect to Anything" or in other words IoT "Internet of Things", networks should have capabilities of Ubiquitous Networking. It is not easy to define of "Ubiquitous Networking" because of the conceptual features of "Ubiquitous" or "Ubiquity". ITU-T developed a recommendation to specify the "Ubiquitous" features as a networking capability of NGN. The ITU-T Recommendation Y.2002 (10/2009) specifies "Next Generation Ubiquitous Networking" as a part of NGN recommendations.

In this recommendation, "Ubiquitous Networking" identifies as "The ability for persons and/or devices to access services and communicate while minimizing technical restrictions regarding where, when and how these services are accessed, in the context of the service(s) subscribed to". Based on this definition, this recommendation identifies fundamental characteristics of ubiquitous networking as followings:

- IP connectivity: IP connectivity will allow objects involved in ubiquitous networking to communicate with each other within a network and/or when objects have to be reachable from outside their network. Particularly, as many new types of objects will be connected to networks, IPv6 will play a key role in object-to-object communications
- Personalization: Personalization will allow to meet the user's needs and to improve the user's service experience since delivering appropriate contents and services to the user. User satisfaction is motivated by the recognition that a user has needs, and meeting them successfully is likely to lead to a satisfying client-customer relationship and re-use of the services offered
- Intelligence: Intelligence which enables network capabilities to provide user-centric and context-aware service is essential to meet numerous network requirements in terms of data handing and processing capabilities. Introduction of artificial intelligence techniques in networks will help to accelerate the synergies and ultimately the "fusion" between the involved industries
- Tagging objects: Tag-based solutions on ubiquitous environment will allow to get and retrieve information of objects from anywhere through the network. Radio frequency identifier (RFID) is one of tag-based solutions for enabling real-time identification and tracking of objects. As active tags have networking capabilities, a large number of tags will need network addresses for communications. As IP technology will be used for ubiquitous networking, it is essential to develop mapping solutions between tag-based objects (e.g. RFIDs) and IP addresses
- Smart devices: Smart devices attached to networks can support multiple functions including camera, video recorder, phone, TV, music player. Sensor devices which enable detection of environmental status and sensory information can utilize networking functionalities to enable interconnection between very small devices, so-called 'smart dusts'. Specific environments such as homes, vehicles, buildings will also require adaptive smart devices

Figure 3-1 illustrates the different types of communications for ubiquitous networking.

Figure 3-1: Ubiquitous networking communication types



Note: objects include all of things which are attached in the network. Some objects can be attached with persons and others can be located remotely with persons. "person-to-person" communication relies on a "object-to-object" communication.

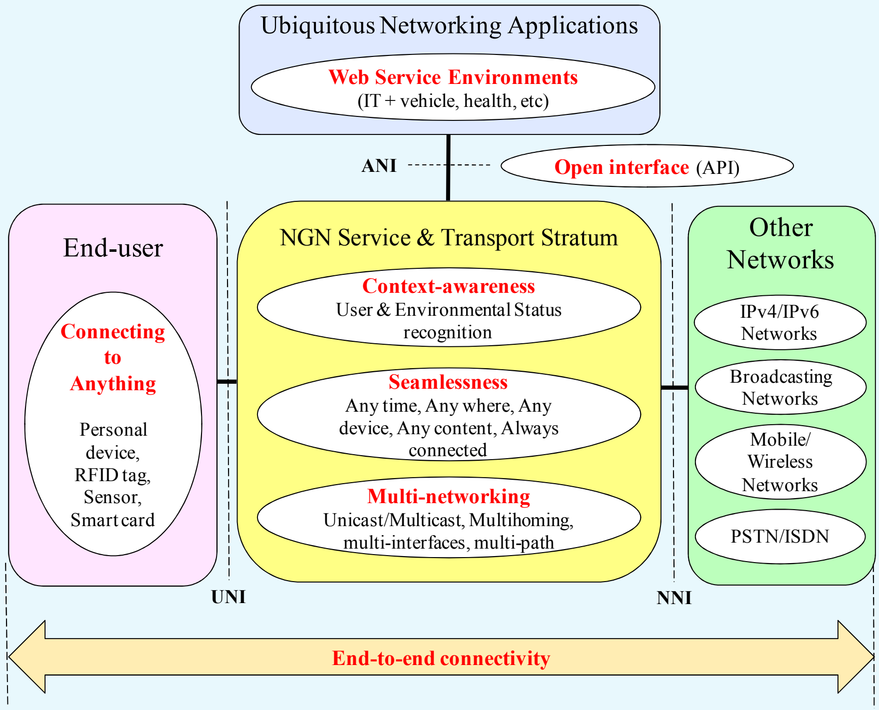
Figure 3-1 makes a distinction between the following users of ubiquitous networking: persons (using attached devices such as PC, PDA, mobile phones) and objects (such as remote monitoring and information devices, contents) and shows three different types of communications:

- Person-to-Person Communication: persons communicate with each other using attached devices (e.g. mobile phone, PC);
- Person-to-Object Communication: persons communicate with a device in order to get specific information (e.g., IPTV content, file transfer);
- Object-to-Object Communication: an object delivers information (e.g. sensor related information) to another object with or without involvement of persons.

Ubiquitous networking aims to provide seamless communications between persons, between objects as well as between persons and objects while they move from one location to another.

Figure 3-2 shows the high-level architectural model for ubiquitous networking in NGN. This model is based upon the NGN overall architecture as described in [ITU-T Y.2012] showing the necessary capabilities to support of ubiquitous networking.

Figure 3-2: High-level architectural model for ubiquitous networking in NGN



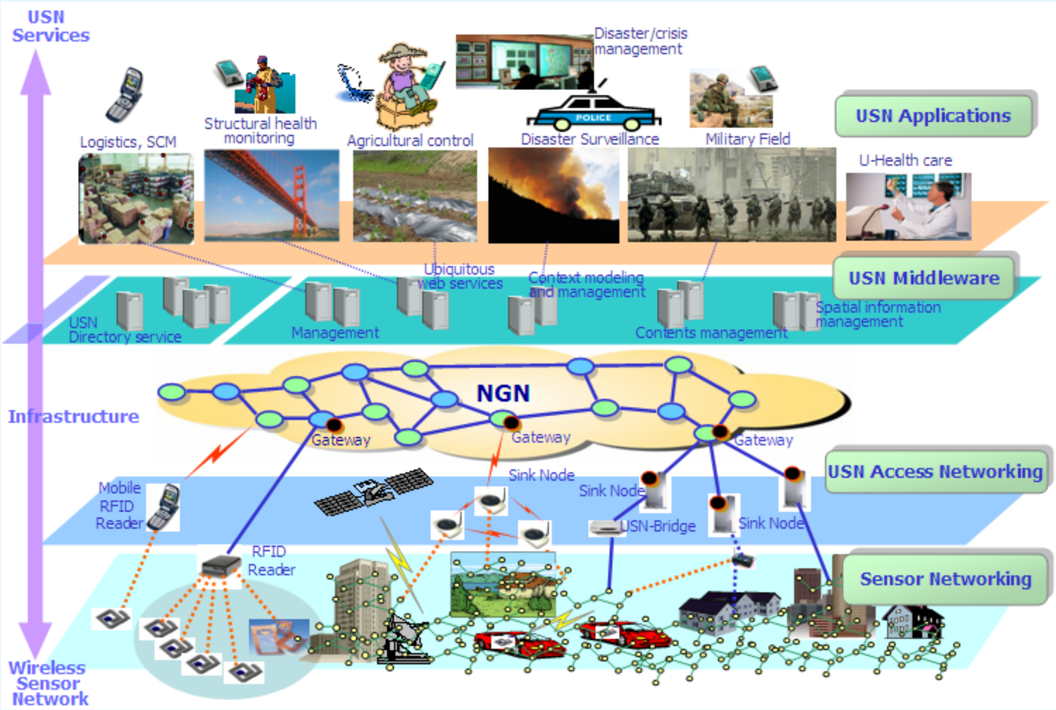
4 Ubiquitous Sensor Networks (USN)

The technology using sensors has huge potential as it could generate applications in a wide range of fields, including ensuring safety and security, environmental monitoring, promoting personal productivity and enhancing national competitiveness. The term of "Ubiquitous Sensor Networks" (USN) is used to describe a network which is configured with sensors that could provide ubiquitous connectivity.

ITU-T Recommendation Y.2221 provides a description and general characteristics of USN and their applications and services. This recommendation also analyzes service requirements of USN applications and services, and specifies extended or new NGN capability requirements based on the service requirements. The main components of a USN, as described in Figure 4-1 are:

- Sensor Networking: Comprising sensors which are used for collecting and transmitting information about their surrounding environment and an independent power source (e.g., battery, solar power);
- USN Access Networking: Intermediary collection of information from a group of sensors through "sink nodes" and facilitating communication with a control centre or with external entities;
- Network Infrastructure: Next Generation Network (NGN);
- USN Middleware: Software for the collection and processing of large volumes of data;
- USN Applications Platform: A technology platform to enable the effective use of a USN in a particular industrial sector or application.

Figure 4-1: Schematic Layers of a Ubiquitous Sensor Network



Sensor is a device that captures a physical stimulus such as temperature, sound, light, pressure, heat, vibration, or magnetism. Sensor data has to be transmitted to users for data processing and corresponding reactions.

Sensor networks can be established by wire-line or wireless. Typical wire-line networking techniques are RS-232, RS-422, RS-485, Power Line Communication, etc. A variety of wireless networking techniques has been used. But nowadays standardized ways have emerged as hot topics and a new term, WSN (Wireless Sensor Network), was made for technology and business marketing. Typical wireless PHY/MAC networking solutions are IEEE 802.15.4, IEEE 802.15.3, Bluetooth, etc. Multi-hop networking solutions over these wireless networks are ZigBee, 6LoWPAN, etc.

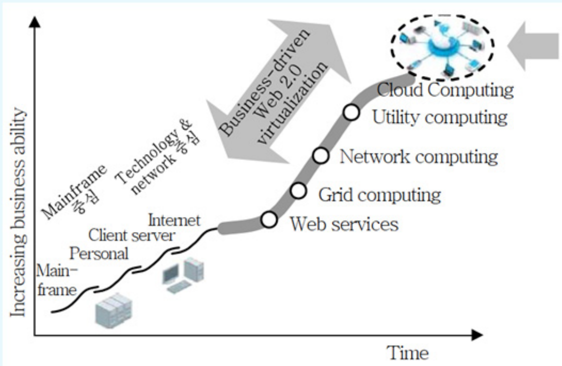
5 Cloud Computing

5.1 Background and definition of Cloud Computing

The background history about the cloud computing may back to the dates when mainframe became available in academia and corporations, accessible via dumb terminals which were used for communications but had no internal computational capacities. Thus it had been required to share main-frame with multiple users by multiple terminals in terms of physical access to the computer as well as to share the CPU time such as time-sharing. In the 1990s, telecommunications with offering virtual private network (VPN) services with comparable quality of service, but at a lower cost, it began to use the cloud symbol to denote the demarcation point between providers including users. Cloud computing extends this boundary to cover servers as well as the network infrastructure. Following Figure 5-1 shows brief summary of such history about cloud computing developments.

According to the developments of computing capabilities, users such as scientists and technologists explored ways to make large-scale computing power available to more users over time sharing, optimal use of the infrastructure, platform and prioritized access to the CPU. In addition, the ubiquitous availability of networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, autonomic, and utility computing have led to growth of cloud computing.

Figure 5-1: History of computing



Cloud computing is defined as a model for enabling service users to have ubiquitous, convenient and on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or resource pooling provider interaction. Cloud computing enables cloud services which identified as a service that is delivered and consumed on demand at any time, through any access network, using any connected devices using cloud computing technologies. It is considered from a telecommunication perspective that users are not buying resources but cloud services that are enabled by cloud computing environments.

The cloud computing model promotes availability and is composed of six essential characteristics, five cloud service categories and four deployment models as followings:

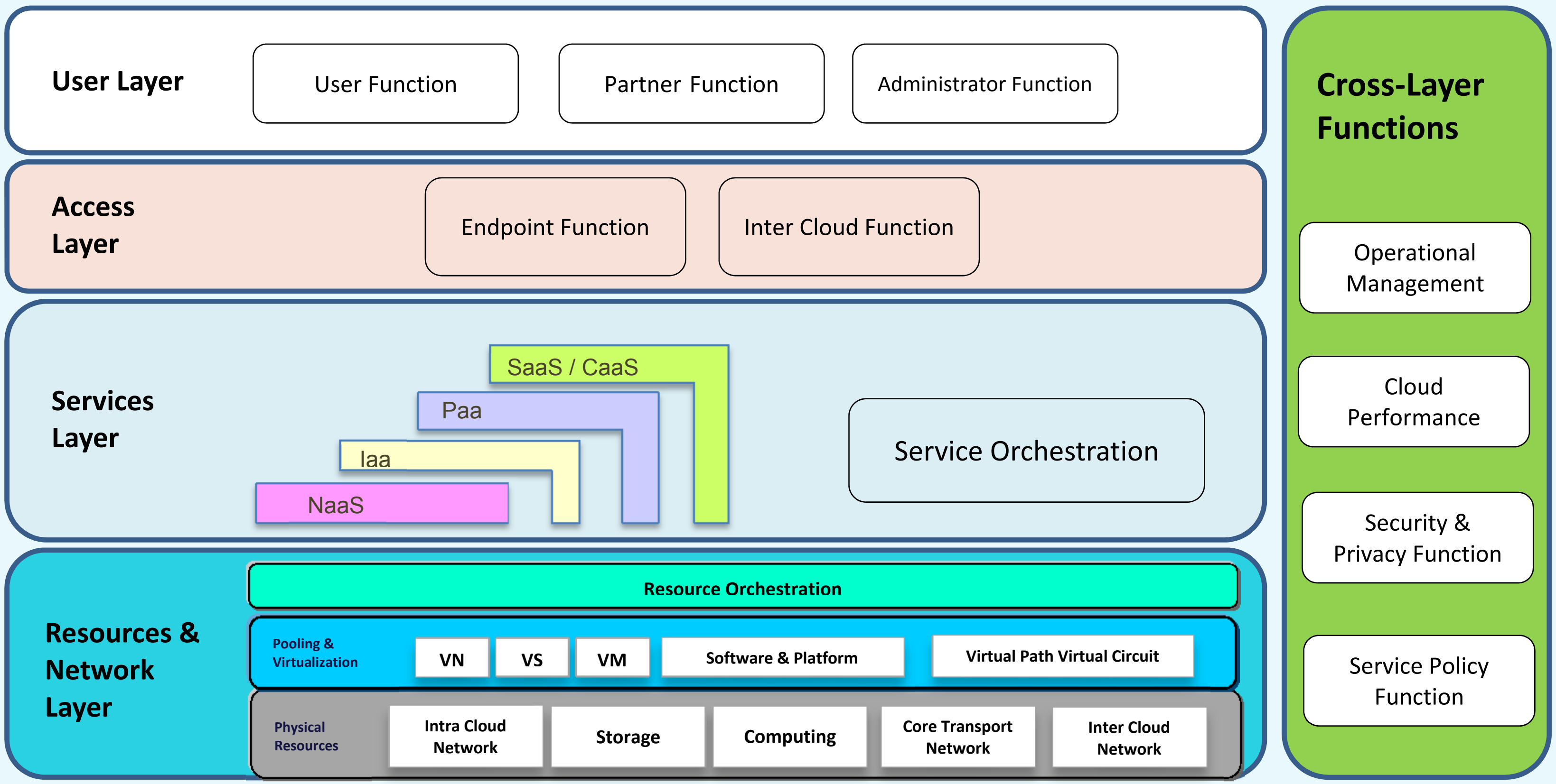
- On-demand self-service: A cloud service user can unilaterally provision computing capabilities, such as server time, network storage and communication and collaboration services, as needed automatically without requiring human interaction with each service's cloud service provider.
- Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- Resource pooling: The cloud service provider's computing resources are pooled to serve multiple users or organisations using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to user demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify the location at a higher level of abstraction (e.g., country, state, data center). Examples of resources include storage (typically on hard or optical disc drives), processing, memory (typically on DRAM), network bandwidth, and virtual machines.

- Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the cloud service user, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Measured Service: Cloud systems automatically control and optimize resource use (e.g., storage, processing and bandwidth) by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., the number of active user accounts). Resource usage can be monitored, controlled, and reported. It provides transparency for both cloud service provider and cloud service users.
- Multi-tenancy: A characteristic of cloud in which resources are shared amongst multiple cloud tenants. Tenant is intended here as any Cloud Service User (CSU) workload that has unique requirements and/or a unique operating agreement with the Cloud Service Provider (CSP). There is an expectation on the part of the cloud tenant that its use of the cloud is isolated from other tenants' use in the same share resource pool; that tenants in the cloud are restricted from accessing or affecting another tenant's assets; that the cloud tenant has the perception of exclusive use of, and access to, any provisioned resource. The means by which such isolation is achieved vary in accordance with the nature of the shared resource, and can affect security, privacy and performance.

5.2 Architecture model

Figure 5-1 shows a functional architecture model of cloud computing. These functional layers in the architecture are derived by grouping cloud related functions.

Figure 5-1: Functional Architecture Model of Cloud Computing



- User Layer: performs interaction between the cloud service user and the underlying cloud architecture layers. The User Layer is used to setup secure mechanism with cloud computing, send cloud service requests to cloud and receive cloud services from cloud, perform cloud service access, administrate and monitor cloud services;
- Access Layer: provides a common interface for both manual and automated cloud service capabilities and service consumption;
- Services Layer: the cloud service provider orchestrates and exposes services of the five cloud service categories. The Cloud Services Layer manages the cloud components required for providing the services, runs the software that implements the services and arranges to offer the cloud services to the cloud service user;
- Resources & Network Layer: The Resources and Network layer is where the physical resources reside including equipment typically used in a data centre such as servers, networking switches and routers, storage, etc, and the corresponding non-cloud-specific software that runs on the servers and other computers such as host operating systems, hyper-visors, device drivers, generic systems management software, etc;
- Cross-Layer Functions: perform overall system management (i.e., operations, administration, maintenance and provisioning (OAM&P)) and monitoring, and provide secure mechanisms.

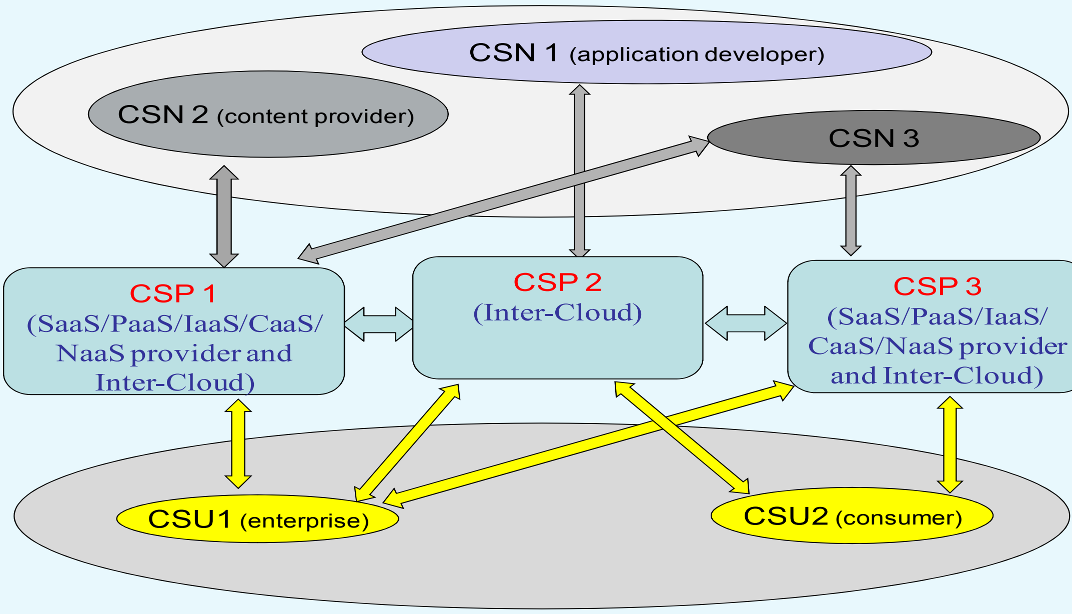
5.3 Cloud Computing Eco-systems

A cloud computing business ecosystem (cloud ecosystem) is a business ecosystem of interacting organizations and individuals - the actors of the cloud ecosystem - providing and consuming cloud services. The following actors are identified in a cloud ecosystem:

- Cloud service users (CSU): A person or organization that consumes delivered cloud services;
- Cloud service providers (CSP): An organization that provides and maintains cloud services to be delivered and consumed;
- Cloud service partners (CSN): A person or organization that provides support to the building of the service offer of a cloud service provider (e.g. service integration).

Figure 5-2 depicts the actors with some of their possible roles in a cloud ecosystem.

Figure 5-2: Actors with possible roles in a cloud ecosystem



5.4 Cloud Service categories

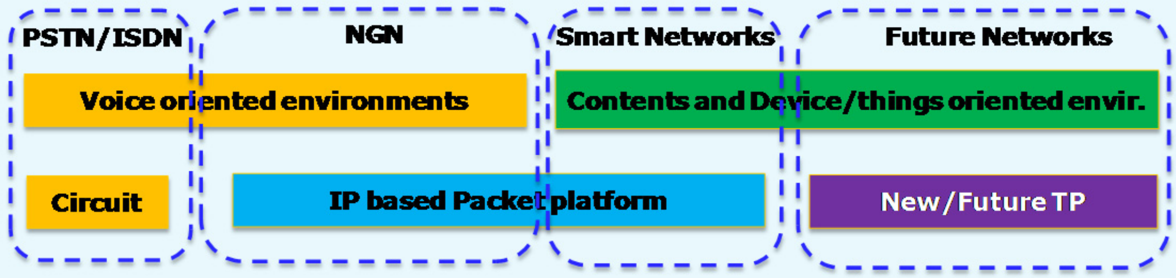
One of the key features of the cloud computing is "Anything as a Service" so called "XaaS". There are plenty of candidate issues to be part of "as a Service", but at this stage, ITU-T, especially SG13 is being discussed about following five services as key service categories.

- Cloud Software as a Service (SaaS): A category of cloud services where the capability provided to the cloud service user is to use the cloud service provider's applications running on a cloud resources;
- Communications as a Service (CaaS): A category of cloud services where the capability provided to the cloud service user is to use real time communication and collaboration services. NOTE - Communication and collaboration services include voice over IP, instant messaging, video conferencing, for different user devices;
- Cloud Platform as a Service (PaaS): A category of cloud services where the capability provided to the cloud service user is to deploy user-created or acquired applications onto the cloud resources using platform tools supported by the cloud service provider;
- Cloud Infrastructure as a Service (IaaS): A category of cloud services where the capability provided by the cloud service provider to the cloud service user is to provision processing, storage, intra-cloud network connectivity services (e.g. VLAN, firewall, load balancer, application acceleration), and other fundamental computing resources of the cloud resources where the cloud service user is able to deploy and run arbitrary application;
- Network as a Service (NaaS): A category of cloud services where the capability provided to the cloud service user is to use transport connectivity services and/or inter-cloud network connectivity services.

6 Future study direction of NGN

Considering this, ITU-T based on the NGN-GSI is continuing of their developments for the NGN will play a crucial role in a future environment as well. For this, as shown in Figure 6-1, ITU-T NGN GSI will continue their study covering various technical subjects. Recently one of the important subjects is providing smart and intelligent capabilities into the NGN as well as its beyond. This issue has been raised mainly from network providers considering the difficulties to provide better services to meet end user's requirements taking into account the status of network resources. Under this subject, NGN-GSI is now develop various solutions and mechanisms to resolve "smart usage of network resources" and "being pipeline of networks" This study will contribute in the development of called "Future Networks" which is being developed as a new paradigm of networks (for example, could be not use of IP).

Figure 6-1: Future study direction of NGN



Annex 9: ITU NGN standards

Internet Protocol Aspects

1 General aspect of IP based networks

Y.1001: IP framework – A framework for convergence of telecommunications network and IP network technologies

2 Architecture, access, network capabilities and resource management

Y.1221: Traffic control and congestion control in IP-based networks

Y.1222: Traffic control and congestion control in Ethernet-based networks

Y.1223: Interworking guidelines for transporting assured IP flows

Y.1231: IP Access Network Architecture

Y.1241: Support of IP-based services using IP transfer capabilities

Y.1242/G.769: Circuit multiplication equipment optimized for IP-based networks

Y.1251: General architectural model for interworking

Y.1261: Service requirements and architecture for voice services over Multi-Protocol Label Switching

Y.1271: Framework(s) on network requirements and capabilities to support emergency telecommunications over evolving circuit-switched and packet-switched networks

Y.1281: Mobile IP services over MPLS

Y.1291: An architectural framework for support of Quality of Service in packet networks

Y.1292: Customizable IP networks (CIP): Framework for the requirements and capabilities related to the customization of IP service networks by customers

3 Transport

Y.1310: Transport of IP over ATM in public networks

Y.1311: Network-based VPNs – Generic architecture and service requirements

Y.1311.1: Network-based IP VPN over MPLS architecture

Y.1321/X.85: IP over SDH using LAPS

Y.1370/G.8110: MPLS layer network architecture

Y.1370.1/G.8110.1: Architecture of Transport MPLS (T-MPLS) layer network

Y.1371/G.8112: Interfaces for the Transport MPLS (T-MPLS) hierarchy

Y.1374/G.8151: Management aspects of the T-MPLS network element

Y.1381/G.8121: Characteristics of Transport MPLS equipment functional blocks

Y.1382/G.8131: Linear protection switching for transport MPLS (T-MPLS) networks

4 Interworking

Y.1401: Principles of interworking

Y.1402/X.371: General arrangements for interworking between Public Data Networks and the Internet

Y.1411: ATM-MPLS network interworking – Cell mode user plane interworking

Y.1412: ATM-MPLS network interworking – Frame mode user plane interworking

Y.1413: TDM-MPLS network interworking – User plane interworking

Y.1414: Voice services – MPLS network interworking

Y.1452: Voice trunking over IP networks

Y.1453: TDM-IP interworking – User plane interworking

Y.1454: Tandem free operation (TFO) – IP network interworking – User plane interworking

5 QoS and Network Performance

Y.1501/G.820/I.351: Relationships among ISDN, IP-based network and physical layer performance Recommendations

Y.1530: Call processing performance for voice service in hybrid IP networks

Y.1531: SIP-based call processing performance

Y.1540: Internet protocol data communication service – IP packet transfer and availability performance parameters

Y.1541: Network performance objectives for IP-based services

Y.1542: Framework for achieving end-to-end IP performance objectives

Y.1543: Measurements in IP networks for inter-domain performance assessment

Y.1544: Multicast IP performance parameters

Y.1560: Parameters for TCP connection performance in the presence of middleboxes

Y.1561: Performance and availability parameters for MPLS networks

6 Operation, administration and maintenance

Y.1704/G.7713: Distributed call and connection management (DCM)

Y.1704.1/G.7713.1: Distributed Call and Connection Management (DCM) based on PNNI

Y.1704.2/G.7713.2: Distributed Call and Connection Management: Signalling mechanism using GMPLS RSVP-TE

Y.1704.3/G.7713.3: Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP

Y.1710: Requirements for Operation & Maintenance functionality in MPLS networks

Y.1711: Operation & Maintenance mechanism for MPLS networks

Y.1712: OAM functionality for ATM-MPLS interworking

Y.1713: Misbranching detection for MPLS networks

Y.1714: MPLS management and OAM framework

Y.1720: Protection switching for MPLS networks

7 IPTV

Y.1901: Requirements for the support of IPTV services

Y.1902: Framework for multicast-based IPTV content delivery

Y.1910: IPTV functional architecture

Y.1911: IPTV services and nomadism: Scenarios and functional architecture for unicast delivery

Y.1991: Terms and definitions for IPTV

Next Generation Networks

1 Frameworks and functional architecture models

Y.2001: General overview of NGN

Y.2002: Overview of ubiquitous networking and of its support in NGN

Y.2006: Description of capability set 1 of NGN release 1

Y.2007: NGN capability set 2

Y.2011: General principles and general reference model for Next Generation Networks

Y.2012: Functional requirements and architecture of next generation networks

Y.2013: Converged services framework functional requirements and architecture

Y.2014: Network attachment control functions in next generation networks

Y.2015: General requirements for ID/locator separation in NGN

Y.2016: Functional requirements and architecture of the NGN for applications and services using tag-based identification

Y.2017: Multicast functions in next generation networks

Y.2018: Mobility management and control framework and architecture within the NGN transport stratum

Y.2019: Content delivery functional architecture in NGN

Y.2020: Open service environment functional architecture for next generation networks

Y.2021: IMS for Next Generation Networks

Y.2022: Functional architecture for the support of host-based ID/locator separation in NGN

Y.2023: Functional requirements and architecture for the NGN for multimedia communication centre serviceY.2031: PSTN/ISDN emulation architecture

Y.2051: General overview of IPv6-based NGN

Y.2052: Framework of multi-homing in IPv6-based NGN

Y.2053: Functional requirements for IPv6 migration in NGN

Y.2054: Framework to support signalling for IPv6-based NGN

Y.2055: Framework of object mapping using IPv6 in next generation networks

Y.2056: Framework of vertical multi-homing in IPv6-based NGN

Y.2057: Framework of node identifier and routing locator separation in IPv6-based next generation networks

Y.2058: Roadmap for IPv6 migration from the perspective of the operators of next generation networks

Y.2062: Framework of object-to-object communication for ubiquitous networking in NGN

Y.2091: Terms and definitions for next generation networks

2 Quality of Service and performance

Y.2111: Resource and admission control functions in next generation networks

Y.2112: A QoS control architecture for Ethernet-based IP access networks

Y.2113: Ethernet QoS control for next generation networks

Y.2121: Requirements for the support of flow-state-aware transport technology in NGN

Y.2122: Flow aggregate information exchange functions in NGN

Y.2171: Admission control priority levels in Next Generation Networks

Y.2172: Service restoration priority levels in Next Generation Networks

Y.2173: Management of performance measurement for NGN

Y.2174: Distributed RACF architecture for MPLS networks

Y.2175: Centralized RACF architecture for MPLS core networks

3 Service aspects

Y.2201: Requirements and capabilities for ITU-T NGN

Y.2205: Next Generation Networks – Emergency telecommunications – Technical considerations

Y.2206: Requirements for distributed service networking capabilities

Y.2211: IMS-based real-time conversational multimedia services over NGN

Y.2212: Requirements of managed delivery services

Y.2213: NGN service requirements and capabilities for network aspects of applications and services using tag-based identification

Y.2214: Service requirements and functional models for customized multimedia ring services

Y.2215: Requirements and framework for the support of VPN services in NGN, including the mobile environment

Y.2216: NGN capability requirements to support the multimedia communication centre service

Y.2221: Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment

Y.2232: NGN convergence service model and scenario using web services

Y.2233: Requirements and framework allowing accounting and charging capabilities in NGN

Y.2234: Open service environment capabilities for NGN

Y.2235: Converged web-browsing service scenarios in NGN

Y.2236: Framework for NGN support of multicast-based services

Y.2237: Functional model and service scenarios for QoS-enabled mobile VoIP service

Y.2240: Requirements and capabilities for next generation network service integration and delivery environment

Y.2251: Multi-connection requirements

Y.2261: PSTN/ISDN evolution to NGN

Y.2262: PSTN/ISDN emulation and simulation

Y.2271: Call server-based PSTN/ISDN emulation

Y.2281: Framework of networked vehicle services and applications using NGN

Y.2291: Architectural overview of next generation home networks

4 Network Management

Y.2401/M.3060: Principles for the Management of Next Generation Networks

5 Security

Y.2701: Security requirements for NGN release 1

Y.2702: Authentication and authorization requirements for NGN release 1

Y.2703: The application of AAA service in NGN

Y.2704: Security mechanisms and procedures for NGN

Y.2705: Minimum Security Requirements for Interconnection of Emergency Telecommunication Services (ETS)

Y.2720: NGN identity management framework

Y.2721: NGN identity management requirements and use cases

Y.2722: NGN identity management mechanisms

Y.2740: Security requirements for mobile remote financial transactions in next generation networks

Y.2741: Architecture of secure mobile financial transactions in next generation networks

Y.2760: Mobility security framework in NGN

Y.2770: Requirements for Deep Packet Inspection in Next Generation Networks

6 Generalized Mobility

Y.2801/Q.1706: Mobility management requirements for NGN

Y.2802/Q.1762: Fixed-mobile convergence general requirements

Y.2803/Q.1763: FMC service using legacy PSTN or ISDN as the fixed access network for mobile network users

Y.2804/Q.1707: Generic framework of mobility management for next generation networks

Y.2805/Q.1708: Framework of location management for NGN

Y.2806/Q.1709: Framework of handover control for NGN

Y.2807: MPLS-based mobility capabilities in NGN

Y.2808: Fixed mobile convergence with a common IMS session control domain

Y.2809: Framework of mobility management in the service stratum for next generation networks

Y.2810: Mobility management framework for IP multicast communications in NGN

7 Supplements and Handbooks on NGN (use cases)

Y Suppl. 1: ITU-T Y.2000 series – Supplement on NGN release 1 scope

Y Suppl. 2: ITU-T Y.2012 – Supplement on session/border control (S/BC) functions

Y Suppl. 3: ITU-T Y.2000 series – Supplement on service scenarios for convergence services in a multiple network and application service provider environment

Y Suppl. 4: ITU-T Y.1300 series – Supplement on transport requirements for T-MPLS OAM and considerations for the application of IETF MPLS technology

Y Suppl. 5: ITU-T Y.1900-series – Supplement on IPTV service use cases

Y Suppl.6: ITU-T Y.2000-series – Supplement on the use of DSL-based systems in next generation networks

Y Suppl.7: ITU-T Y.2000-series – Supplement on NGN release 2 scope

Y Suppl. 8: ITU-T Y.2000-series – Supplement on a survey of global ICT forums and consortia

Y Suppl. 9: ITU-T Y.2000-series – Supplement on multi-connection scenarios

Y Suppl. 10: ITU-T Y.2000-series – Supplement on distributed service network (DSN) use cases

Y Suppl. 12: ITU-T Y.2720 – Supplement on NGN identity management mechanisms

Y Suppl. 13: ITU-T Y.2000-series - Scenarios for the evolution of NGN network capabilities to include information storage, processing and delivery

Y Suppl. 14: ITU-T Y.2000-series – Supplementary service scenarios for fixed-mobile convergence

Y Suppl. 15: ITU-T Y.2000-series – Profile-based application adaptation service using NGN

Y Suppl. 16: ITU-T Y.1900-series – Guidelines on deployment of IP multicast for IPTV content deliveryHandbook: Converging networks (2010)

NGN Related ITU-T SG11 Approved Q-Series Supplements

1 Network signalling and control functional architecture

Q.3030: Signalling architecture for the NGN service control plane

Q.3040: Signalling architecture for IPTV control plane

2 Bearer Control Signalling

Q.3150/Y.1416: Use of virtual trunks for ATM/MPLS client/server control plane interworking

Q.3151/Y.1417: ATM and frame relay/MPLS control plane interworking: Client-server

3 Signalling and control requirements and protocols to support attachment in NGN environments

Q.3201: EAP-based security signalling protocol architecture for network attachment

Q.3202.1: Authentication protocols based on EAP-AKA for interworking among 3GPP, WiMax, and WLAN in NGN

Q.3203: Signalling requirements and architecture of network attachment control functions to support IP mobility

Q.3220: Architectural framework for NACF signalling interface Recommendations

Q.3221: Requirements and protocol at the interface between the service control entity and the transport location management physical entity (S-TC1 interface)

Q.3222: Requirements and protocol at the interface between transport location management physical entities (Ng interface)

Q.3223: Requirements and protocol for the interface between a transport location management physical entity and a policy decision physical entity (Ru Interface)

4 Resource control protocols

Q.3300: Architectural framework for the Q.33xx series of Recommendations

Q.3301.1: Resource control protocol No. 1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity

Q.3302.1: Resource control protocol No. 2 (rcp2) – Protocol at the Rp interface between transport resource control physical entities

Q.3303.0: Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Overview

Q.3303.1: Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE): COPS alternative

Q.3303.2: Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and a Policy Enforcement Physical Entity (PE-PE) (Rw interface): H.248 alternative

Q.3303.3: Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Diameter

Q.3304.1: Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity (TRC-PE) and a transport physical entity (T-PE): COPS alternative

Q.3304.2: Resource control protocol No. 4 (rcp4) – Protocols at the Rc interface between a transport resource control physical entity (TRC-PE) and a transport physical entity (T-PE): SNMP alternative

Q.3305.1: Resource control protocol No. 5 (rcp5) – Protocol at the interface between transport resource control physical entity and policy decision physical entity (Rt interface): Diameter-based

Q.3306.1: Resource control protocol No. 6 (rcp6) - Protocol at the interface between intra-domain policy decision physical entities (PD-PE) (Rd interface)

Q.3307.1: Resource control protocol No.7 - Protocol at the interface between inter-domain policy decision physical entities (Ri interface)

Q.3308.1: Resource control protocol 8 (rcp8) Protocol at the interface between Resource Admission Control Physical Entity (RAC-PE) and CPN Gateway Policy Enforcement Physical Entities (CGPE-PE) (Rh interface): COPS alternative

Q.3309: QoS coordination protocol

Q.3311: Enhancement of resource and admission control protocols to use pre-congestion notification

Q.3312: Use of the access node control protocol on the Rp interface

Q.3313: Signalling protocols and procedures relating to flow state aware QoS control in a bounded subnetwork of a next generation network

5 Service and session control protocols

Q.3401: NGN NNI signalling profile (protocol set 1)

Q.3402: NGN UNI signalling profile (Protocol set 1)

6 Service and session control protocols – supplementary services

Q.3610: Signalling requirements and protocol profiles for customized ring-back tone service

Q.3611: Signalling requirements and protocol profiles for NGN customized ringing tone service

Q.3612: Signalling requirements and protocol profiles for IP Centrex service

7 Testing for NGN networks

Q.3900: Methods of testing and model network architecture for NGN technical means testing as applied to public telecommunication networks

Q.3901: Testing topology for networks and services based on NGN technical means

Q.3902: Operational parameters to be monitored when implementing NGN technical means in public telecommunication networks

Q.3903: Formalized presentation of testing results

Q.3904: Testing principles for IMS model networks, and identification of relevant conformance, interoperability and functionality tests

Q.3906.1: Test scenarios and catalogue for testing fixed-broadband access networks using a model network - Part I

Q.3909: The framework and overview of NGN conformance and interoperability testing

Q.3910: Parameters for monitoring NGN protocols

Q.3911: Parameters for monitoring voice services in NGN

Q.3925: The types of traffic flows which should be generated for voice, data and video on the Model network for testing QoS parameters

Q.3931.1: Performance benchmark for the PSTN/ISDN emulation subsystem of an IP multimedia system - Part 1: Core concepts

Q.3931.2: Performance benchmark for the PSTN/ISDN emulation subsystem of an IP multimedia system - Part 2: Subsystem configurations and benchmarks

Q.3941.1: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 1: Test suite structure and test purposes for SIP-ISDN

Q.3941.2: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 2: Abstract test suite and partial protocol implementation extra information for testing proforma specification for SIP-ISDN

Q.3941.3: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 3: Test suite structure and test purposes for SIP-SIP

Q.3941.4: Network integration testing between SIP and ISDN/PSTN network signalling protocols – Part 4: Abstract test suite and partial protocol implementation extra information for testing proforma specification for SIP-SIP

Q.3945: Test specifications for next generation network services on model networks - Test set 1

Q.3948: Service testing framework for VoIP at the user-to-network interface of next generation networks

Q.3950: Testing and model network architecture for tag-based identification systems and functions

8 Supplements and Handbooks

Q Suppl. 51: Signalling requirements for IP-QoS

Q Suppl. 52: NNI mobility management requirements for systems beyond IMT-2000

Q Suppl. 53: Signalling requirements to support the International Emergency Preference Scheme (IEPS)

Q Suppl. 54: Signalling requirements at the interface between SUP-FE and I/S-CSC-FE

Q Suppl. 55: Signalling requirements at the interface between AS-FE and S-CSC-FE

Q Suppl. 56: Organization of NGN service user data

Q Suppl. 57: Signalling requirements to support the emergency telecommunications service (ETS) in IP networks

Q Suppl. 58: Organization of NGN transport user data

Q Suppl. 59: Signalling flows and parameter mapping for resource control

Q Suppl. 60: Supplement to Recommendations ITU-T Q.3610 and ITU-T Q.3611 - Service flows for customized multimedia ring-back tone (CRBT) and customized multimedia ringing tone (CRT) services

Q Suppl. 61: Evaluation of signalling protocols to support ITU-T Y.2171 admission control priority levels

Q Suppl. 62: Overview of the work of standards development organizations and other organizations on emergency telecommunications service

Handbook on deployment of packet based networks (2009)

Handbook on Testing (2011)

IMT related Recommendations

Q.1711: Network functional model for IMT

Q.1721: Information flows for IMT capability set 1

Q.1731: Radio-technology independent requirements for IMT layer 2 radio interface

Q.1741.1: IMT references to release 1999 of GSM evolved UMTS core network with UTRAN access network

Q.1741.2: IMT references to release 4 of GSM evolved UMTS core network with UTRAN access network

Q.1741.3: IMT references to release 5 of GSM evolved UMTS core network

Q.1741.4: IMT references to release 6 of GSM evolved UMTS core network

Q.1741.5: IMT references to Release 7 of GSM-evolved UMTS core network

Q.1741.6: IMT references to Release 8 of GSM-evolved UMTS core network

Q.1741.7: IMT references to Release 9 of GSM-evolved UMTS core network

Q.1742.1: IMT references to ANSI-41 evolved core network with cdma2000 access network

Q.1742.2: IMT references (approved as of 11 July 2002) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.3: IMT references (approved as of 30 June 2003) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.4: IMT references (approved as of 30 June 2004) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.5: IMT references (approved as of 31 December 2005) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.6: IMT references (approved as of 31 December 2006) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.7: IMT references (approved as of 30 June 2008) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.8: IMT references (approved as of 31 January 2010) to ANSI-41 evolved core network with cdma2000 access network

Q.1742.9: IMT references (approved as of 31 December 2010) to ANSI-41 evolved core network with cdma2000 access network

Q.1751: Internetwork signalling requirements for IMT capability set 1

Q.1761: Principles and requirements for convergence of fixed and existing IMT systems

Operation & Tariff related Recommendations

D.271: Charging and accounting principles for NGN

E.370: Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks

E.4110: Framework for operations requirements of next generation networks and services

NGN Management related Recommendations

M.3210.1: TMN management services for IMT-2000 security management

M.3340: Framework for NGN service fulfilment and assurance management across the business to business and customer to business interfaces

M.3341: Requirements for QoS/SLA management over the TMN X-interface for IP-based services

M.3342: Guidelines for the definition of SLA representation templates

M.3343: Requirements and analysis for NGN trouble administration across B2B and C2B interfaces

M.3344: Requirements and analysis for NGN appointment management across the business-to-business and customer-to-business interfaces

M.3345: Principles for self-service management

M.3347: Requirements for the NGN service activation of NMS-EMS interface

M.3348: Requirements of the NMS-EMS management interface for NGN service platforms

M.3350: TMN service management requirements for information interchange across the TMN X-interface to support provisioning of Emergency Telecommunication Service (ETS)

M.3361: Requirements for business-to-government management interfaces - B2G interfaces – Introduction

M.3400: TMN management functions

M.3410: Guidelines and requirements for security management systems to support telecommunications management

NGN Related ITU-R Recommendations

Recommendation S.1806: Availability objectives for hypothetical reference digital paths in the fixed-satellite service operating below 15 GHz

Report ITU-R M.2176-1: Vision and requirements for the satellite radio interface(s) of IMT-Advanced

Preliminary draft new Recommendation ITU-R S.1897: Cross-layer based QoS provisioning in IP-based hybrid satellite-terrestrial networks

Recommendation F.1094-2: Maximum allowable error performance and availability degradations to digital fixed wireless systems arising from radio interference from emissions and radiations from other sources

Recommendation F.1704: Characteristics of multipoint-to-multipoint fixed wireless systems with mesh network topology operating in frequency bands above about 17 GHz

Recommendation F.1763: Radio interface standards for broadband wireless access systems in the fixed service operating below 66 GHz

Recommendation M.819: International Mobile Telecommunications-2000 (IMT-2000) for developing countries

Recommendation M.1457: Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (IMT-2000)

Recommendation M.2012: Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications Advanced (IMT-Advanced)

International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Office of the Director
Place des Nations
CH-1211 Geneva 20 – Switzerland
Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Deputy to the Director and Director，Administration and Operations Coordination Department (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Infrastructure Enabling Environmnent and e-Applications Department (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Innovation and Partnership Department (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Project Support and Knowledge Management Department (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia

International Telecommunication Union (ITU)
Regional Office
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia
Email: itu-addis@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon

Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroon
Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal

Union internationale des télécommunications (UIT)
Bureau de zone
19, Rue Parchappe x Amadou Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Senegal
Email: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe

International Telecommunication Union (ITU)
Area Office
TelOne Centre for Learning
Corner Samora Machel and Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe
Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil

União Internacional de Telecomunicações (UIT)
Regional Office
SAUS Quadra 06, Bloco "E"
11° andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil
Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados

International Telecommunication Union (ITU)
Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados
Email: itubridgetown@itu.int
Tel.: +1 246 431 0343/4
Fax: +1 246 437 7403

Chile

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile
Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras

Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras
Email: itutegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

Arab States

Egypt

International Telecommunication Union (ITU)
Regional Office
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt
Email: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia and the Pacific

Thailand

International Telecommunication Union (ITU)
Regional Office
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand
Email: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia

International Telecommunication Union (ITU)
Area Office
Sapta Pesona Building, 13th floor
JI. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia
Email: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

CIS countries

Russian Federation

International Telecommunication Union (ITU)
Area Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation
Email: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Switzerland

International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Europe Unit (EUR)
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5111

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

Printed in Switzerland
Geneva, 2014

01/2014