

Next Generation Network Architecture

TERJE JENSEN



Terje Jensen is Research Manager in Telenor Group Business Development and Research and Senior Researcher at Q2S/NTNU

The International Telecommunication Union initiated work on the Next Generation Network (NGN) architecture some years ago. Its origin could already be found in the work on Global Information Infrastructure delivering recommendations from around 1998. The NGN work has outlined several important principles regarding layering, mobility and convergence. These are briefly presented in this paper.

1 Introduction

The telecom industry has been motivated by deploying standardized solutions. Two key motivators for this is the *economy of scale* and the *easier interoperability*. Having agreed on a common set of technical solutions allows for the critical mass to initiate research and development of the relevant solutions. One may say that the risk would be lowered while the potential rewards are increased.

The standards are either defined as *de jure* or *de facto*. Looking at great successes within the telecom industry, one finds major networks such as the Public Switching Telephone Network (PSTN), the Global System for Mobile communication (GSM), and the IP-based networks.

In view of this the International Telecommunication Union (ITU) has undertaken activities to elaborate the Next Generation Network (NGN) architecture. This was initiated as an NGN focus group in May 2004. Then the NGN Global Standards Initiative (NGN-GSI) was formed in September 2005. Significant progress has been made during the last years. Some of the main areas addressed are mobility, convergence, system segment decoupling and management.

An objective is to provide recommendations for “*seamless federation of interconnected, interoperable communication networks and information processing equipment, data bases and terminals*”. This is, for example, recognizing the presence of multiple players in the telecom and Internet arena.

As observed when studying the NGN recommendation, several solutions from other international bodies have been incorporated. Examples are the IP protocols and mechanisms from the Internet Engineering Task Force (IETF), the IP Multimedia Subsystem (IMS) from the 3GPP, and the Media-Independent Handover mechanism from the Institute of Electrical and Electronics Engineering (IEEE). This paper elaborates on key principles of the NGN architecture.

2 NGN Principles

2.1 Objectives

The objectives of NGN include to (from [Y.2001])

- Promote fair competition;
- Encourage private investment;
- Define a framework for architecture and capabilities to be able to meet various regulatory requirements;
- Provide open access to network,

while

- Ensuring universal provision of and access to services;
- Promoting equality of opportunity to the citizen;
- Promoting diversity of content, including cultural and linguistic diversity;
- Recognizing the necessity of worldwide cooperation with particular attention to less developed countries.

As stated in [Y.140], the NGN (or GII as it is called in that document) is based upon a seamless federation of interconnected, interoperable communication networks and information processing equipment, data bases and terminals. Interconnection takes on an important role within the context of NGN.

The NGN is based on *packet networks* able to make use of different *broadband technologies*. This is to enable the provision of services where the *service-related functions are independent of transport technologies*. Hence, the philosophy of the ‘hourglass’ model, see Figure 1, can be recognized.

2.2 Definition

ITU-T’s definition of NGN is (ref. [Y.2001], author’s emphasis):

“A Next Generation Network (NGN) is a *packet-based* network able to provide Telecommunication Services to users and able to make use of *multiple broadband, QoS-enabled* transport technologies

and in which *service-related functions are independent of the underlying transport-related technologies*. It enables *unfettered access* for users to networks and to *competing service providers and services* of their choice. It supports *generalised mobility* which will allow consistent and ubiquitous provision of services to users.”

The NGN is characterised by the following fundamental aspects:

- 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 services and multi-media);
- Broadband capabilities with end-to-end QoS and transparency;
- Interworking with legacy networks via open interfaces;
- Generalised mobility;
- Unfettered access by users to different service providers;
- A variety of identification schemes which can be resolved to IP addresses for the purposes of routing in IP networks;
- Unified service characteristics for the same service as perceived by the user;
- Converged services between Fixed and Mobile networks;
- 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 and security/privacy, etc.

These have been specialised for the next phase in the ITU-T’s NGN Global Standards Initiative to cover the following items:

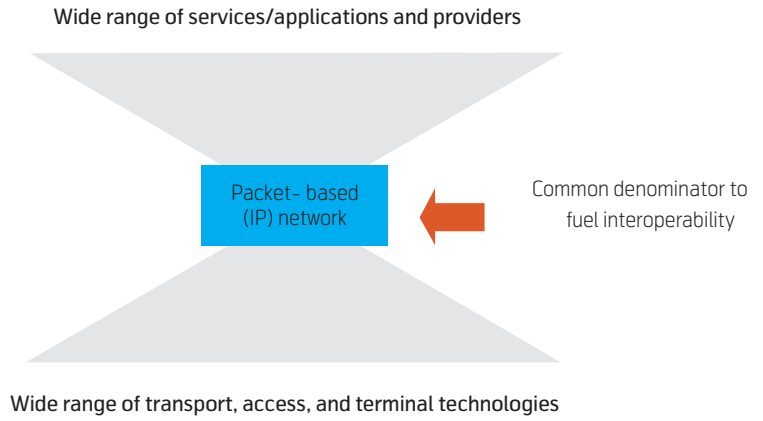


Figure 1 Packet-based network used to decouple applications from transport and terminal solutions

- *Evolution of Networks to NGN*: The evolution of networks to NGNs must allow for the continuation of, and interoperability with, existing networks while in parallel enabling the implementation of new capabilities. Since the realisation and deployment of the NGN will be an evolutionary process, and not all networks will start from the same point, it is necessary to describe a variety of approaches.

The high capital investment in the PSTN (Public Switched Telephone Network) means it must be one of the main work areas for studying evolution to the NGN. The resulting outputs describe possible ways of evolving the PSTN to become an NGN. These outputs provide steps for evolution of transport, management, signalling and control parts of the PSTN to the NGN. Other starting points, notably existing Public Land Mobile Networks (PLMNs), and associated transition scenarios are also under study.

- *QoS (Quality of Service)*: The basic criterion for QoS evolution is ‘subjective user satisfaction’, eg. speed, accuracy, reliability, and security. This involves identification of parameters that can be directly observed and measured at the point at which the service is accessed by users and network providers. Flexibility within the global end-to-end NGN architecture is essential to allow for each recognised operating agency’s different regulatory environment, service offerings, geographic span, and network infrastructure. These factors need to be taken into account when agreeing on parameters for, and levels of, QoS for NGN.
- *Interoperability*: Considering that the NGN will involve a broad series of protocols (including various profiles) at both service and network levels, it is essential to ensure interoperability between different systems and networks.

- *Security*: Security is as crucial to the NGN as it is in today's network environment. The very wide scope of this topic, combined with the number of SDOs (standards development organisations) already involved, underlines the strategic importance of this subject. Within the NGN, security issues interrelate with architecture, QoS, network management, mobility, charging and payment.
- Consideration of the user of generic reference modelling techniques. This is to help identify additional standards needed to support NGN compliant communications services within or between operator domain(s);
- Definition of interworking functions to support legacy (non-NGN-aware) terminals;

Security studies in NGN are addressing

- A comprehensive security architecture for NGNs;
- The preparation of NGN operational security policy and guidelines;
- NGN security protocols and APIs (application programming interface).
- *Generalized Mobility*: NGN will give users and devices the ability to communicate and to access services irrespective of change of location or technical environment. The degree of service availability may depend on several factors, including access network capabilities, service level agreements between the user's home network and visited networks, etc. It includes the ability to communicate from various locations using a variety of terminal equipment, with or without service continuity while in transit or while changing access means. This includes recognition of the need to merge the previously distinct worlds of fixed and mobile telecommunications into a coherent whole.
- *Service Capabilities and Architecture*: Work in this area will continue to
 - Address the telecommunication service capabilities that the NGN should provide, maintaining separation between services and the networks they run on; and
 - Develop a suitable service architecture focused on the interfaces to support different business models and seamless communication in different environments.

Backward compatibility with and the evolution from existing services and systems will be studied in order to meet the needs of end users and service providers.

2.3 Functional Architecture

The *functional architecture* of NGN would define *sets of entities where each provides a unique function*. Relationships and connections between functions are identified in terms of *reference points*. Functions are grouped to represent certain practical physical realizations. Interfaces could be defined at reference points. The following aspects are considered when defining the functional architecture (ref. [Y.2001]):

- Determination of how end-to-end services, call control and user mobility can be supported across heterogeneous networks;
- Functional definition of NGN-aware terminals in terms of software upgrade mechanisms, redundancy and evolution of less expensive terminals, versions negotiation and management.

The NGN functional architecture, ref. [Y.2012], shall incorporate the following principles:

- Support for multiple access technologies: The NGN functional architecture shall offer the *configuration flexibility* needed to support multiple access technologies.
- Distribute 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:
 - May not be distributed over multiple physical units but may have multiple instances;
 - Have no direct relationship with the layered architecture. However, similar entities may be located in different logical layers.

The identified QoS mechanisms are divided into, i) a vertical mechanism linking the upper and lower layer QoS mechanisms, and ii) a layer horizontal mechanism which should link the QoS control between different domains and networks. Relating this to the ‘hourglass’ illustration in Figure 1, there will be notions of service levels at different levels. These should be inter-linked (horizontally and vertically) to combine a good user experience and good network/ system performance.

With regard to end-to-end QoS in NGN, the following aspects need to be considered:

- End-to-end QoS class definition for telephony over packet networks;
- End-to-end multimedia QoS class definition framework and a method of identifying QoS classes of individual media components;
- Specification of how to use lower layer QoS mechanisms to achieve upper layer QoS within the network;
- Inter-domain lower layer QoS control;
- End-user perception of QoS.

The general user requirements for mobility should include:

- Ability to change access point and/or terminal;
- Ability to get access from any network access point, including all access technologies identified above;
- Ability to get services in a consistent manner, subject to the constraints experienced in their current situations;
- User availability and reachability should be known to network functions, and possibly to services and applications, including those provided by a third party.

In order to support generalised mobility, [Y.2001] states that further work is needed to develop network functions at the control layer:

- Identification and authentication mechanisms;
- Access control and authorization function;
- Location management;
- Terminal and/or session address allocation and management;
- Support of user environment management;
- User profile management;
- Access to user data.

As noted from the above list, there is a separation between two distinct blocks or strata of functionality; the transport functions reside in the transport stratum while the service functions related to applications reside in the service stratum.

Each stratum comprises of one or more layers, where each layer is conceptually composed of a data (or user) plane, a control plane and a management plane.

The *NGN service stratum* is the part of NGN which provides the user functions that transfer service-related data and the functions that control and manage service resource and network service 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.

The *NGN transport stratum* is the 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.

From an architectural perspective, each layer in the service and transport stratum is considered to have its own user, control and management planes, see Figure 2. The NGN management plane is the union of service stratum and transport management plane. The NGN control plane is the union of the service and the transport stratum control plane.

The concept of NGN planes does not imply virtual integration of planes. The intention is to define reference points between planes of different strata.

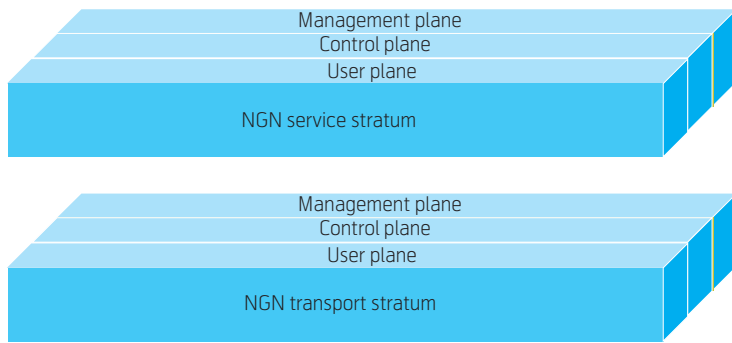


Figure 2 NGN basic reference model (from [Y.2011])

A general function model can formalize a structural model where services and service components are described separately. Different perspectives can be taken, leading to different models such as:

- Enterprise model that identifies players and roles. That is, this describes business activities within value chains, such as structural roles and infrastructural roles.
- Implementation model that is looking at how functions are distributed and implemented. It also identifies the protocols that are passing across interfaces between equipment.

The functions and services are related to each other; functions are used to build services. Moreover, there are similarities between the sub-types of services and functions.

Resources provide physical and non-physical (ie. logical) components. Typical examples are transmission links, processors and memories. Resources should

also be dealt with separately from the functions and the services.

2.4 Multi-layer Principles

In a multi-layer implementation, conflicts and inefficiencies may occur if the layers operate independently. Hence, coordination between layers and associated components are commonly sought. In *cooperating layered networks* there is a controlling entity for each layer.

The ordering of layers within the hierarchy refers to the service requester/provider relationship similar to the protocol stack. The higher layer (*client layer*) requests service from the lower layer (*server layer*).

Depending on the realization of the inter-layer interaction, internal and external interfaces have to be defined to exchange such control information. The exchanged information may include details of the capabilities, topology, and resource information provided by the server layer network to the client layer network.

Intra-layer interaction can occur between functional entities within the same layer to support the existence of multiple networks at another layer, see Figure 3. One type of functions is mapping between address spaces when independent address spaces are used for different layers. Two examples are, i) mapping from IP addresses to Ethernet MAC addresses, and, ii) mapping from domain names to IP addresses (eg. from www.telenor.com to 148.121.139.45).

Coordination among appropriate functional entities in the client layer network and server layer network is required to enable

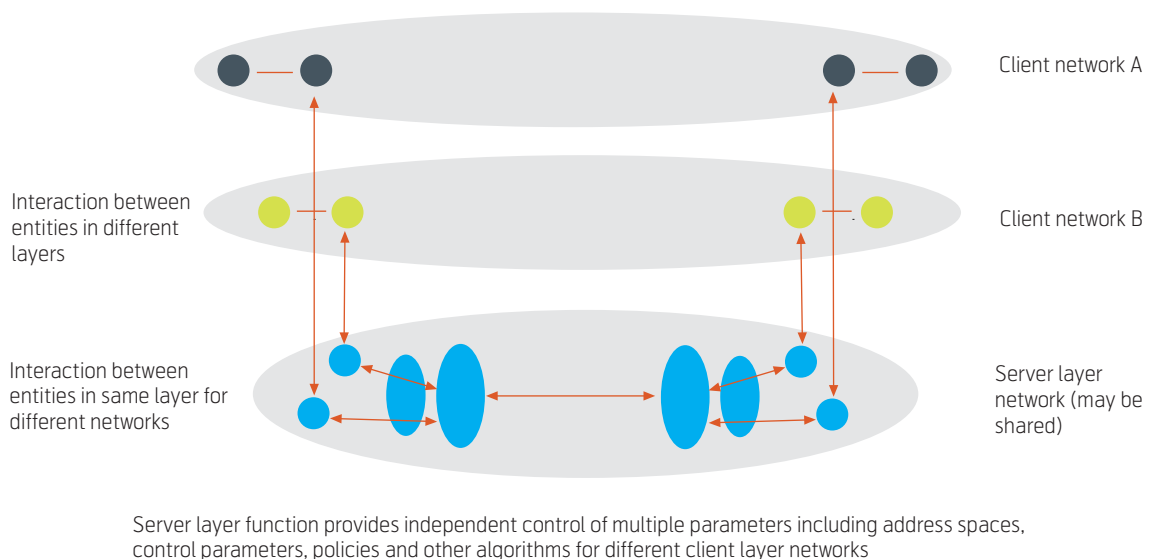


Figure 3 Inter-/intra-layer interactions, multiple client networks on common server layer (adapted from [Y.2011])

- Seamless and economical support of multiple client layer networks by a single server layer network;
- Ability to negotiate and (re-)allocate resources dynamically in the server layer network according to the client layer network requirements;
- Simultaneous and efficient handling of multiple layers' resources;
- Failure detection and coordination of different layers' recovery mechanisms;
- Virtual separation of the control entities as well as policy and management functions for the different client/server layer networks, including independent address spaces for different (layer) networks.

The NGN should be able to support a wide range of QoS-enabled services. To offer the QoS service, it is necessary to define, at least:

- Bearer service QoS classes;
- QoS control mechanisms;
- QoS control functional architecture;
- QoS control/signalling.

2.5 Architecture Overview

An NGN architecture overview is illustrated in Figure 4. Note that user profiles are indicated both in the

service stratum and the transport stratum; these may be co-located or integrated depending on the actors involved. As a minimum the following shall be supported by the service user profile:

- Authentication;
- Authorization;
- Service subscription information;
- Subscriber mobility;
- Location;
- Presence (eg. on-line/off-line status);
- Charging.

The NGN architecture can be specialised for certain application areas. One example is functionality for providing VPN services. This is depicted in Figure 5. Note that it adds on to the general NGN architecture where a number of functional entities have been included.

The VPN membership management functions supports, i) creating and releasing VPNs, ii) users joining and leaving VPNs, and, iii) partitioning a VPN into several groups. The VPN connection management functions manage VPN tunnels.

Returning to the general NGN architecture, Figure 6 illustrates functional entities (FEs) within the Transport functions. The Access Node FE is directly connected to end-user functions. The access link is termi-

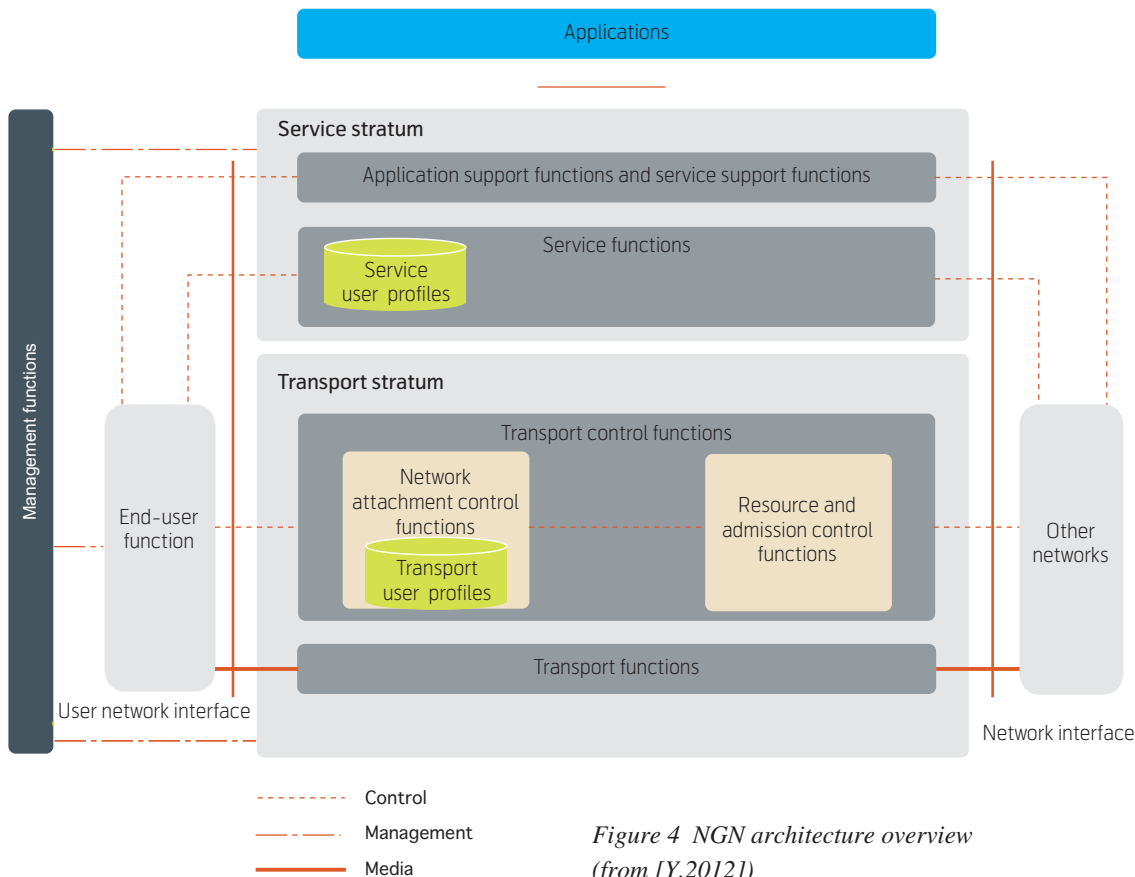


Figure 4 NGN architecture overview
(from [Y.2012])

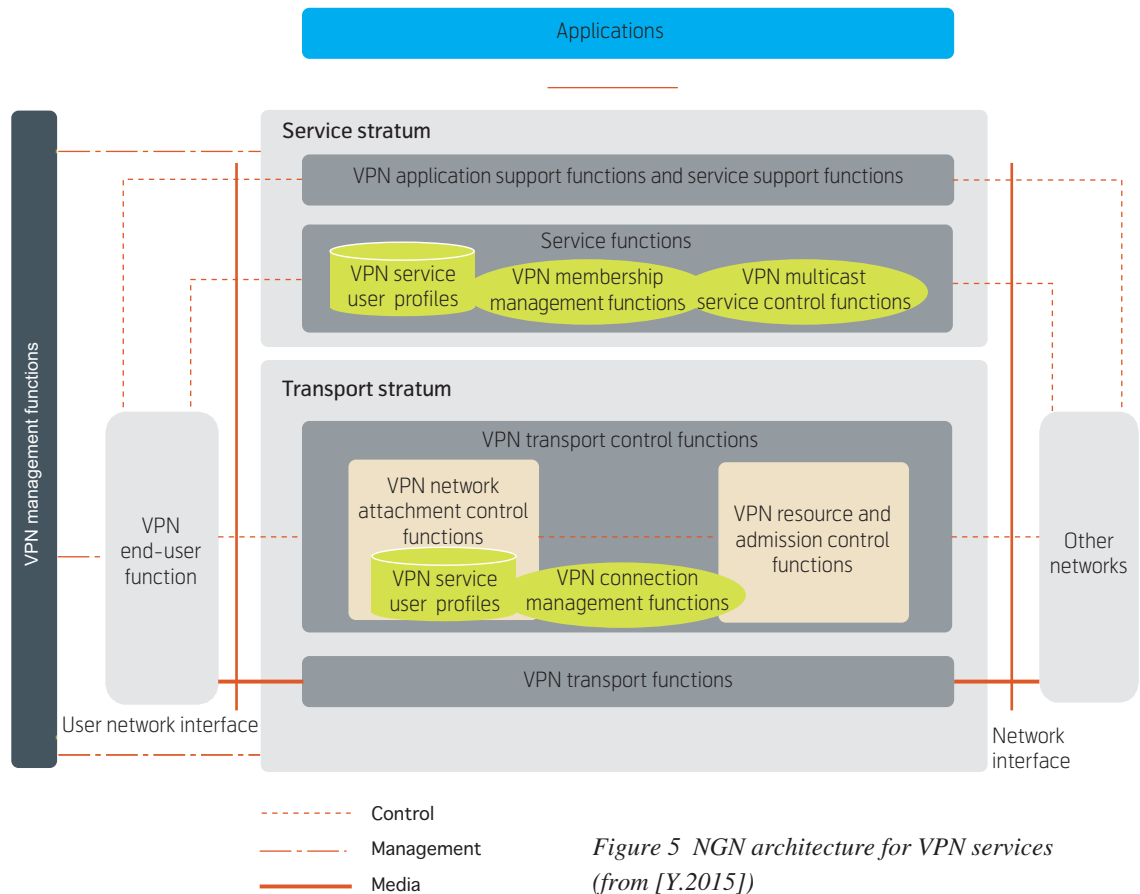


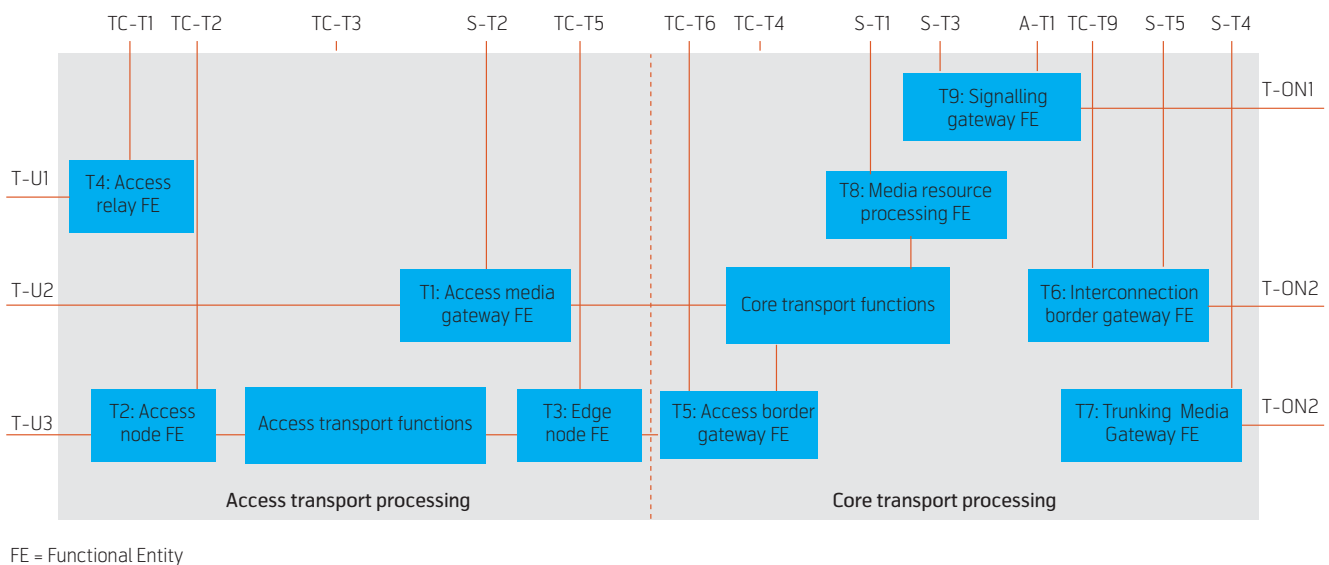
Figure 5 NGN architecture for VPN services (from [Y.2015])

nated in this node. This allows different access types such as Digital Subscriber Line, optical access systems, wireless systems to be used. Commonly, the access node is a layer 2 device, but it can also support some IP functions.

The Edge Node FE connects to core packet transport functions. This node terminates layer 2 access ses-

sions. It shall also be a layer 3 device with IP capabilities in case the core network is an IP-based network.

Functional entities within the service functions group are shown in Figure 7. The proxy call session control function (P-CSCF) acts as the contact point to the user. This has the capability to accept service requests from the user and forward them to the Interrogating CSCF or Serving CSCF.



FE = Functional Entity

Figure 6 Functional entities within the Transport functions group (from [Y.2017])

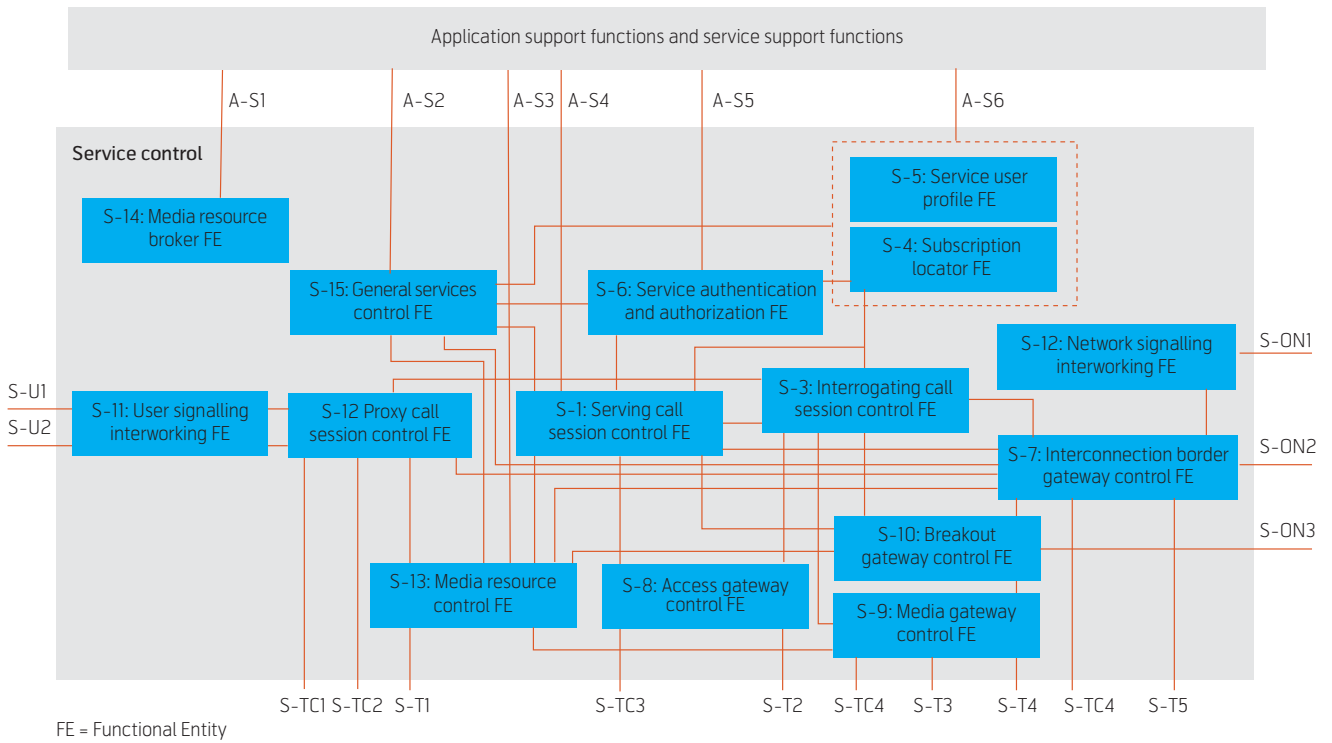


Figure 7 Functional entities in service control group (from [Y.2017])

The service profile function is responsible for storing information about a user, including user authentication and authorization information.

3 Fixed – Mobile Convergence

Steadily more actors are looking for opportunities following from offering so-called converged services and running converged operations. Typically, a converged platform is used when offering services across a range of accesses and terminals. In order to ensure an efficient solution it is necessary to define a *common reference architecture* such that all relevant areas can be related to the same set of functionality groups and reference points.

Convergence may allow for offering the same set of services on different fixed and mobile accesses. Moreover, it may also transfer services between terminals attached to different access networks. This could be decided by reachability, user preferences or at explicit requests, eg. ref [ITU-FMC].

3.1 Reference Model

The ITU NGN reference model discusses different convergence options as depicted in Figure 8. Note

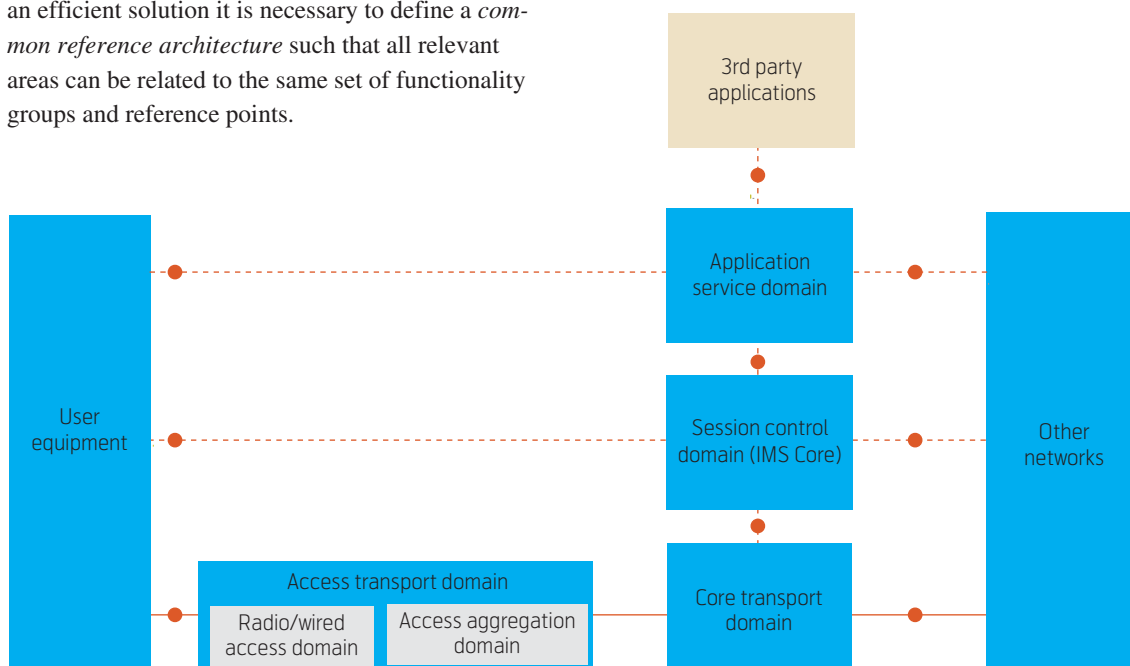


Figure 8 IMS-based NGN reference model (from [ITU-FMC])

that this is a model as seen from a service provider's perspective. The following description is based on [ITU-FMC].

There are two aspects that motivate the user of service level convergence, ie. common session control domain:

- The user's demands to always benefit from the best possible performance/cost ratio in any given network environment;
- The operator's desire to optimize the allocation of network resources, extend services to new network environments and diversify the service portfolio.

The *access transport domain* provides the connectivity between the user equipment domain and the core transport domain. Within the access transport domain we distinguish between

- The physical access media-dependent radio/wired access domain (eg. DSLAMs, 3G base stations and RNCs, WLAN access points, etc.); and
- The access aggregation domain that aggregates the traffic flows from multiple radio/wired access domain instances to an edge node. GPRS, part of the 3GPP IP connectivity access network, is one example of an access aggregation domain and so is the network that connects DSLAMs to a BRAS/IP service edge. A mobile access aggregation domain will contain mobility management functions.

The *core transport domain* may also contain mobility functions in order to support mobility across different access domains (eg. Mobile IP home agents). The core transport domain interconnects with access domains and core transport domains of other networks. It also supports media processing capabilities as found necessary. Network attachment, resource and admission control functions are contained in both the access and core transport domains.

IP in the transport domains bridges diverse fixed and wireless technologies. However, interoperability of various access technologies at the transport layer only is not sufficient to support global mobility in such a heterogeneous environment. For this a common control layer is needed. This include mechanisms such as:

- Identification and authentication mechanisms;
- Access control and authorization function;
- IP address allocation and management;
- User environment management;
- User profile management and accessibility to user data.

All these are required to achieve true convergence across different access technologies and across different networks.

Session control of connectivity between user equipment and between user equipment and other networks is provided by the session control domain. This also contains functions supporting presence and location services. The session control domain interfaces with the core transport domain to convey transport resource requests and Network Address Translation (NAT) binding information, if applicable. It may also interface with the access transport domain, for instance to convey location information in case of a wired access domain.

The *application service domain* contains functionality that supports so-called application services. These include messaging and information services that may be built on top of session control services.

IP Multimedia Subsystem (IMS)-based service convergence enables a number of FMC service capabilities:

- Access to the same IMS services from different terminals with different public identities. These may be implemented as a single physical terminal with different public identities.
- Access to the same services from different terminals using the same public user identity. This allows the user to decide which services are directed towards which terminal and in which order, whilst the calling party only needs to know one public identity.
- Service continuity on a multi-mode terminal whilst moving between a home or enterprise fixed network environment and the mobile network. This could for example be a dual-mode UTRAN and WLAN/Bluetooth handset or a device that can connect either to a UTRAN base station or to a private WLAN/Bluetooth access point.

In terms of the domain model, the IMS-based FMC architecture is based on the following principles:

- The architecture is required to provide access to IMS-based services from any type of user equipment with IMS compatible interfaces.
- The user equipment may be connected to any type of packet-based access transport domain with compatible interfaces that are able to convey transparently the protocols between the user equipment and IMS.

- Access transport domains may be connected to multi-access core transport domain, which implies that the interface between access and core may be specific for the access technology.
- The interfaces between the core transport domain and the IMS service platform are independent of technology. It is also based on the required functionalities to support IMS-based services and capabilities. This does not preclude the use of other service platforms to support this interface.
- The interfaces shall support sharing of access and core transport domain facilities by multiple service platform providers.

3.2 Convergence

[Q.1762] mentions the following fundamental characteristics of fixed mobile convergence (FMC):

- *Consistency of user experience* is provided through a generic service delivery environment. This satisfies the needs of the fixed network and of the mobile network. The user is able to obtain services in a consistent manner as allowed by the connectivity and terminal/device capabilities. Services are offered in accordance with FMC capabilities. For example, an on-going session could be downgraded for some reason, such as change of access technology or terminal/device capability. A video communication may be downgraded to a voice communication when the user migrates to mobile-only coverage where the access technology is not able to support it.
- Subscriptions and service provisioning are *access-technology agnostic*. The service stratum may be aware of the access and terminal/device capabilities involved in a session instance. Services are supported by all fixed and mobile access technologies where possible and subject to user preferences. Service registration, triggering and execution adapt to network and terminal/devices capabilities. The user's availability, reachability, and the terminal/device's capabilities are perceptible to network functions, and as needed to services and applications, including those provided by a third party; assuming that FMC respects
 - The user's privacy and privacy-sensitive data (eg. address book, preference, presence settings, billing/payment settings and other security settings) contained in the user's profile;
 - The user's personal preferences (eg. availability, reachability);
 - The terminal/device's capabilities,

and adequately protects this information

- Against loss of privacy and loss of confidentiality;
- Against unauthorized access;
- Against unauthorized manipulation,

during storage and/or during communication within and beyond a service provider's domain.

- FMC's service and application processing may *depend on terminal/device capabilities*. Compatible terminal/device capabilities may be selected by end-to-end interaction between terminal/devices, or between the terminal/device and the FMC service stratum according to the service and application needs.

- Support of *generalized mobility*, which includes service mobility, user, terminal/device and network mobility. Reduced or partial mobility may be supported in some specific networks.
- A *generic user profile* for services which contain the criteria for session establishment and connectivity and is applicable both in fixed and in mobile networks, and which is specific to an individual user's subscription, containing eg. the user's address book, preferences, presence options, billing and payment options, service subscriptions and authentication parameters.

These are reflected in the following general requirements for FMC capabilities as listed in [Q.1762]:

- **Access independent:** Services and features offered are required to be independent of access.
- **Uniform authentication and uniform authorization mechanism:** This encompasses a single, common, generic security mechanism in the sense to bridge different access networks at the service stratum. As there may be access-specific or -dependent parts related to the transport stratum, the uniform authentication and authorization mechanisms may not be available at this stratum.
- **Charging and management:** Includes collecting and managing resource usage information.
- **Service access environment.**
- **Quality of service mechanisms:** Enabling service level agreement supporting user and service requirements, like dynamic negotiation of QoS parameters between the service and transport layers.
- **Interworking,** eg. with existing networks.

- Reliability, including appropriate overload control and failure recovery mechanisms.
- Security requirements.
- Public services issues, eg. required by regulations or laws, including lawful interception, malicious communication identification, unsolicited bulk telecommunications, emergency telecommunications, location information related to emergency telecommunication, user identity presentation and privacy, network or service provider selection, users with disabilities, number portability and service unbundling.
- Network selection: Supports a provider being able to define preferred access network for service delivery.
- Location identification: Offering the location information to relevant services given user's permission.
- Personalized configuration.
- Personal data network storage.
- Accounting support capabilities: Collect Charging Data Record (CDR) information to gather relevant usage data to initiate a unified bill.
- Message processing: Support storage, transcoding, conversion and relay of different message types (eg. SMS, MMS, IM, e-mail).
- Presence information: Collect, store, transpose and distribute relevant presence information.
- Mechanisms for applications to access user data.
- User identifier management: Provide a unique user identifier at the transport stratum which allows differentiation among user terminal/devices. Additional identifiers may be used at the service stratum to identify the user.

4 Mobility Aspects

4.1 Mobility and Continuity Cases

One may separate between staying connected for:

- The registration (no need to re-register); and
- On-going sessions (a.k.a. handovers).

Registration service continuity provides transparent registration services across different terminal boundaries or across different network boundaries [ITU-FMC].

Multimedia session continuity refers to the continuation of service components and the required synchronization between them. These might further be divided into:

- Session continuity on the same user device;
- Session continuity on different terminals.

Example cases of the latter are to, i) obtain better in-house coverage without dual-mode terminal, ii) conserve bandwidth by using fixed broadband technology whenever possible, iii) enjoy services provided by powerful terminals with higher bandwidth fixed access.

[Q.1706] classifies the mobility according to service continuity (see Figure 9):

- Service continuity: The ability for a moving object to maintain on-going services including current states, such as user's network environment and session for a service. This category includes
 - *Seamless handover*: Preserves the ability to provide services without any impact on their service level agreements to a moving object during and after movement;
 - *'Non-seamless' handover*: The ability to provide services with some impact on their service level agreement to a moving object during and after movement.
- Service discontinuity: The ability to provide service irrespective of environment changes of a moving object, but not to be able to maintain on-going services:
 - *Nomadism*: Ability of the users to change their network access point when moving. When changing the network access point, the user's service session is completely stopped and then started again. That is, there is no service continuity or handover used. It is assumed that the normal usage pattern is that users shut down their service session before attaching to a different access point.
 - *Portability*: Ability of a user identifier to be allocated to different systems when the user moves from one location to another.

One may also make a distinction between horizontal mobility (mobility on the same 'layer', eg. same access technology) and vertical mobility (mobility between different 'layers', eg. between different access technologies).

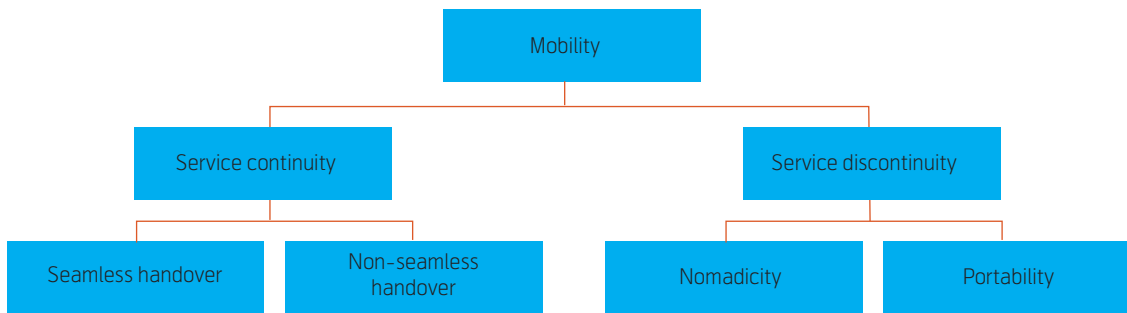


Figure 9 Classification of mobility schemes (adapted from [Q.1706])

4.2 Mobility Management

According to which objects that are moving, mobility management can be categorised accordingly:

- *Terminal* mobility: The same terminal equipment is moving or is used at different locations. The ability of a terminal to access telecommunication services from different locations and while in motion, and the capability of the network to identify and locate that terminal.
- *Network* mobility: A set of fixed or mobile nodes are networked to each other, to change, as one unit, its point of attachment to the corresponding network upon the network's movement itself.
- *Personal* mobility: The user changes the terminal used for network access at different locations. The ability of a user to access telecommunication services at any terminal on the basis of a personal identifier, and the capability of the network to provide those services delineated in the user's service profile.
- *Service* mobility: Mobility applied for a specific service. That is, the ability of a moving object to use the particular (subscribed) service irrespective of the location of the user and the terminal that is used for that purpose.

[Q.1706] outlines a number of requirements on mobility management:

- General requirements:
 - Harmonization with IP-based networks: As the NGN is IP-based, mobility management protocols should be well harmonized with IP technology.
 - Separation of control and transport functions: Such a separation provides architectural flexibility that facilitates the introduction of new technologies and services. Open interfaces between the control plane functions and the transport plane functions are necessary to implant their separation.

- Provision of a location management function: The location of users/terminals is tracked and maintained by one or more location management function. Location management can be expanded to provide location information to service applications.
- Provision of mechanisms for identification of uses/terminals: Specify how the users/terminals are to be identified in the networks or systems for mobility management.
- QoS support: What service levels required by mobile users and services must be managed.
- Interworking with established AAA and security schemes: Specify how users/terminals are to be authenticated, authorized, accounted, and secured for services using standard AAA and security mechanisms. The results of the AAA functionality will be a yes/no decision on the service request made by a user. As a next step, the access network configuration will be adapted to the mobile/nomadic user such that it satisfies the particular Quality of Service (QoS) level and security association for the requested service. These mechanisms should be based on the user's subscription profile and the technical resource constraints of the respective access networks.
- Location privacy: Location information of particular user should be protected from non-permitted entities. This requires mutual authentication, security association, and other IP security requirements between the mobile terminal and the location management function.
- Support of network mobility: examples of moving networks could be bus, train, ship, aeroplane, etc.
- Support of ad hoc networks.
- Resource optimization: Eg. in order to save power consumption in the terminals and signal-

ling overhead on the network side. Resource optimization should be provided to the terminals in idle mode as well as in active mode.

- Support of IPv4/IPv6 and public/private addresses: Both IPv6 and IPv4 must be supported. The same is valid for both public and private addresses. A proxy agent might be needed to support mobility management-related operations such as location update and paging for private addresses.
- Provision of personal and service mobility.
- User data accessibility: Services and other network functions require some user data in order to be appropriately customized. These can be either 'user subscription data' or 'network data'.
- Support of several kinds of mobile end-points: A mobile end-point can be an application in Session Initiation Protocol (SIP), interface in Mobile IP, and so forth. It can also be a core network, an access network, a user-premises network, or a service platform.
- Maintenance of binding information: There are several types of bindings for services:
 - Between a user and a service application;
 - Between an application and a network interface card;
 - Between a service platform and a network termination;
 - Between a network termination and a network access point;
 - Between two different access networks.
- Requirements for inter-core network mobility management
 - Independence from network access technologies: Provide mobility between either homogeneous or heterogeneous types of access network that belong to the same or different operators;
 - Effective interworking with existing mobility management protocols.
- Requirements for inter-access network mobility management:
 - Independence from network access technologies;
 - Provision of mechanisms for context transfer: When a mobile terminal moves across different network, the context information of the current session, such as QoS level, security method, AAA mechanism, compression type in use, etc., might be helpful in performing the handover of

the session to the new access network (eg. minimizing the latency involved in handing the session over to new serving entities). The proper use of a context transfer mechanism could substantially reduce the amount of overhead in the servers that are, respectively or in a combined manner, used to support QoS, security, AAA, and so forth;

- Effective interworking with existing mobile management protocols;
- Provision of a handover management function for seamless services: For maintaining session continuity during movement. The handover might be vertical (between different access technologies);
- Support of policy-based and dynamic network selection: Possible for the user to choose to connect to one of the networks to obtain service, based on the following policies driven by the requirements of the service or application to be used, and presented to the user. The terminal should be able to track information of the current network.
- Requirements for intra-access network mobility management:
 - Provision of mechanisms for context transfer (see above);
 - Provision of a handover management for seamless services (see above).

4.3 Supporting Mobility in NGN

[Y.2018] elaborates on how mobility is supported in the NGN model. Functional elements are depicted in Figure 10. The Handover Control and Decision provides session continuity for on-going sessions when users are moving. Mobility service authentication can be integrated into or separated from network access authentication. When integrated, both mobility services and network access are authenticated by the same operator. Then the transport user identifier will be the same as the mobility service subscriber identifier. When separated (split scenario), mobility service authentication will be done after network access authentication is completed.

The user identity shall be used to get authentication, authorization and accounting services. A user identity will typically refer to a domain name, eg. from a home operator, such as user@home.domain.

Two types of IP addresses are needed: i) a persistent IP address, and ii) a temporary IP address. The persis-

tent IP address is allocated in the anchoring network and maintained regardless of a user's location within a given scope. The temporary IP address is allocated when a user attaches to an access network with a different subnet prefix from the persistent IP address.

The home address in Mobile IP is one example of a persistent identity, while the care-of-address in Mobile IP is an example of a temporary identity.

The Mobility Location Management (MLM) has the following responsibility:

- In case of network-based mobility, initiating location registration on behalf of the User Equipment (UE);
- Processing location registration messages sent from or on behalf of the UE;
- Optionally, maintaining the binding between the mobility service user identity and persistent IP address assigned to the UE;
- Management of the binding between the persistent address assigned to the UE and its temporary address, in the case of host-based mobility, or the address of the lower tunnel end-point, in case of network-based mobility;
- Optionally, holding two location bindings for the mobile UE by marking the binding for the serving network as active state and marking the binding for target network as standby state;
- Supporting separation of control and data plane by allowing the address of the MLM and data forwarding end-point address (ie. tunnelling end-point address) to differ;
- Indication of a new mobility location binding and distribution of binding information to the Handover Decision and Control entity.

The Handover Decision and Control (HDC) has the responsibility to

- Receive a list of candidate access links for handover from the UE and invoking Resource and Admission Control Function (RACF) to verify session QoS availability for each candidate access links for handover. In the case where the UE makes the handover decision the HDC provides the acceptable subset of links to the UE;
- Request RACF to re-provision the resource and QoS for the sessions of the moved UE by submit-

ting binding information to the Policy Decision entity of RACF with the options to

- Request release of resource and QoS configuration for the previous data path while configuring resource and QoS for the new data path;
- Request to leave the previous data path as it is while configuring resource and QoS for the new data path, which makes make-before-break handover possible.
- Request RACF to release resource and QoS for the data path which is verified not to be used anymore;
- Trigger handover upon request from the UE, in the case of network-triggered handover;
- Invoke handover action at the Layer 2 Handover Control in the case of intra-sub-network handover, and at the layer 3 Handover Control in the case of handover between sub-networks;
- Possible coordinate between Layer 2 Handover Control instance to achieve handover in the case of movements within the same sub-network;
- Communicate with Layer 2 handover execution to perform i) relay link layer reports to the handover decision function, and ii) upon request, invoke handover action at the appropriate instance of the Layer 2 Handover Execution;
- Communicate with the Layer 3 Handover Execution to invoke and coordinate handover action at the appropriate instances.

The Network Information Distribution communicates with the entity making the handover decision during the network discovery phase. Handover decision can be made by the UE or by the HDC. It has the responsibility to

- Distribute handover policy, which is a set of operator-defined rules and preferences that affect the handover decisions;
- Distribute other information provided by the Network Information Repository.

The Network Information Repository provides static information on neighbouring networks to assist the access network discovery and selection decision. This information may include:

- Information on neighbouring access network in the vicinity of UE. This may give access network iden-

- tifiers, access types, operators, security and network QoS capabilities, etc.;
- Information on attachment points (base stations, NodeB, access points, etc), such as attachment point identifiers, L1/L2 addresses, bit rates supported, and network address configuration policy;
- Operator policies such as charging mode and rates (cost for the usage of the network), roaming agreements, mobility mechanisms, selection policies, etc.

The Layer 2 handover execution acts on command from the HDC to:

- Take access-technology-specific actions as required to preserve flow continuity during handover;
- Complete handover execution in the direction toward the UE when it has determined that the UE has executed handover.

Layer 3 Handover executions also act on command from the HAC to:

- Execute tunnel setup, modification or release during handover;

- Buffer user packets as required to preserve flow continuity during handover;
- Following handover, encapsulate user packets received from the UE (at the tunnel lower end in case of network-based mobility) or from correspondent nodes (at the tunnel upper end) and forward them through the tunnel. Similarly, de-capsulate packets received from the tunnel and forward them to the UE (at the tunnel lower end in case of network-based mobility) or to the correspondent node (at the tunnel upper end).

[ITU-HFC] describes the following basic functions to support handover control:

- Handover detection:* Detecting or predicting a need for handover. This can be classified into layer 2 and layer 3 handover detections.
- Network discovery:* A user equipment may have one or more network interface to access heterogeneous networks. These interfaces can be used to connect to one or several of the reachable networks through a point of attachment (PoA) selected based on a profile. In order to control handovers between different access networks, the mobility management protocols should specify how a user equip-

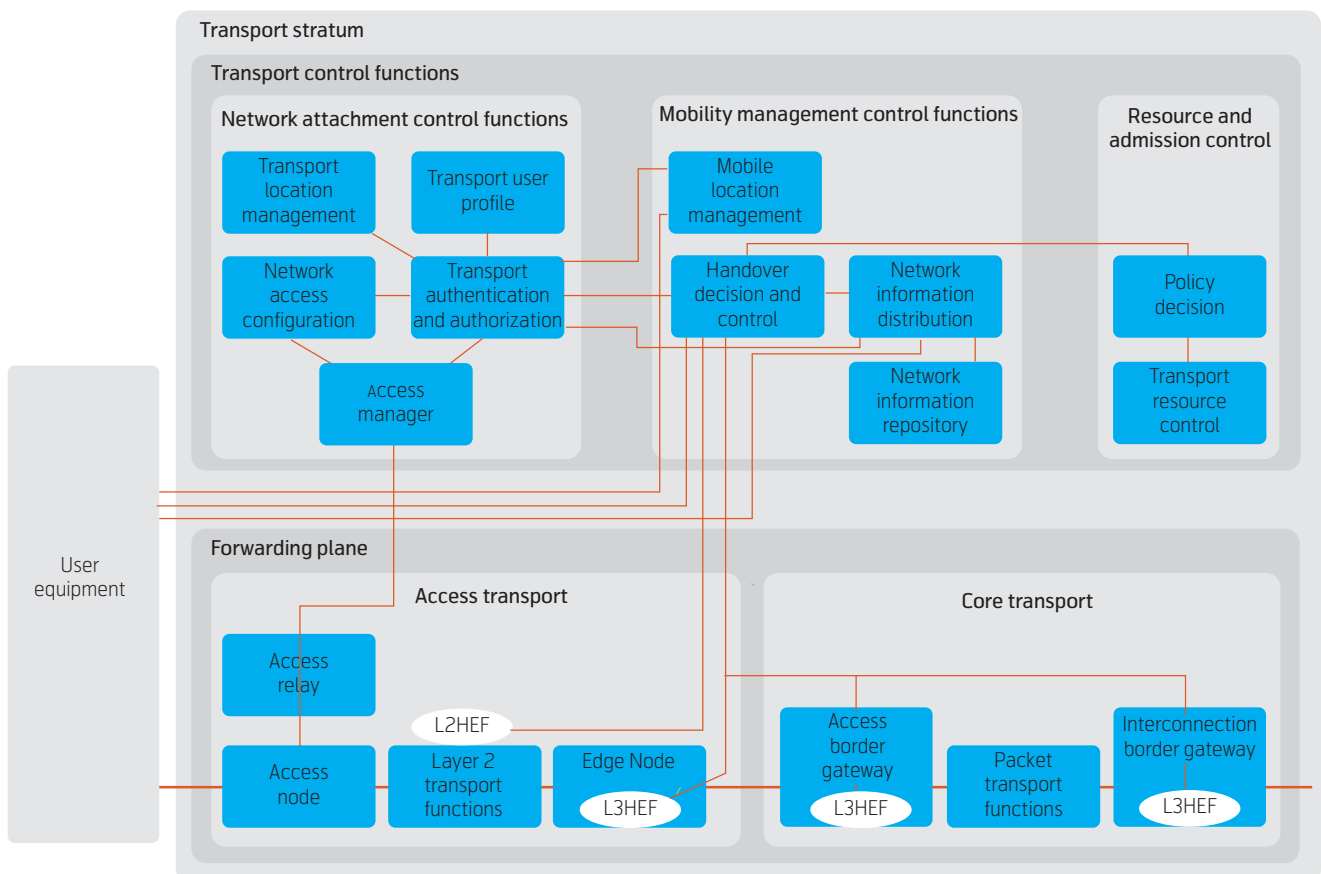


Figure 10 Reference models for functional elements in NGN supporting mobility

ment determines which access networks that are currently accessible and when the determination is needed.

- *Network selection:* When user equipment faces that one of the reachable PoAs (or access networks) is to be chosen to establish a communication link. The network selection functionality should give mobility management protocols a capability that controls the choice of a target PoA for a layer 2 handover depending on either the static network information (eg. access type, cost, provider, etc.), or dynamic network information (eg. signal quality, available resources, etc.).
- *Location update trigger:* Location management procedure should be performed as soon as possible after detecting a layer 3 handover.
- *Routing path adjustment:* The mobility management protocols should specify how to adjust the routing path from/to a user equipment according to the change of location.
- *Attachment point change:* Change of PoA associated with a UE is performed by layer 2 operations. The handover control function should be able to instruct a user equipment to perform a layer 2 handover to the designated PoA requested by upper mobility management protocols. Additionally, the access authentication for a handover can be performed by the handover control functions instead of the user equipment for further performance improvements.

The IEEE 802.21 is an emerging standard that defines a framework for seamless service across different access network involving IEEE 802 technologies. IEEE 802.21 consists of a *Media Independent Handover Function* (MIHF) that provides three services to achieve efficient handover decisions, ref. Figure 11:

- *Event service:* Notifies upper layer users about dynamic events such as link up, link down, link parameter change, etc.;
- *Command service:* Enables higher layers to control the layer 1 and layer 2 of the terminal. Examples are get status of link, scan for new link, switch link, etc.
- *Information service:* Provides information about surrounding network such as neighbour list technology, neighbour operator list, etc.

Mobility is supported by transferring services from one access to another to provide service continuity. This is utilising two functions:

- FMC application server that, i) collects information from the HSS on the user's profile and the operator's policy and charging model, ii) receives information from the user equipment on the user's preferences for a session, based on a user defined policy, iii) receives information from the user equipment on its location, eg. in the `P-Access-Network-Info` in SIP messages that convey information about the radio access technology and eg. the radio cell identity, iv) obtains information from the MIIS in its domain on available access network for the user equipment, v) applies operator policies to the information received and may initiate handover accordingly, and vi) executes the handover using third party call control.
- Media-Independent Handover Information Server (MIIS) collects information about available access networks and capacity and may also provide cost information. It may be organised in a hierarchical manner where the server in the IMS home domain of the user can collect access network information from other servers in the visited domains. Each MIIS may collect information from one or more type of access network in its domain.

In case the handover is based on SIP signalling between the user equipment and the FMC server, it can be supported by the regular roaming interfaces for the IMS services.

In case the service continuity is achieved by transport level mechanisms, eg. through Mobile IP, and the mobile and fixed access provide equivalent QoS

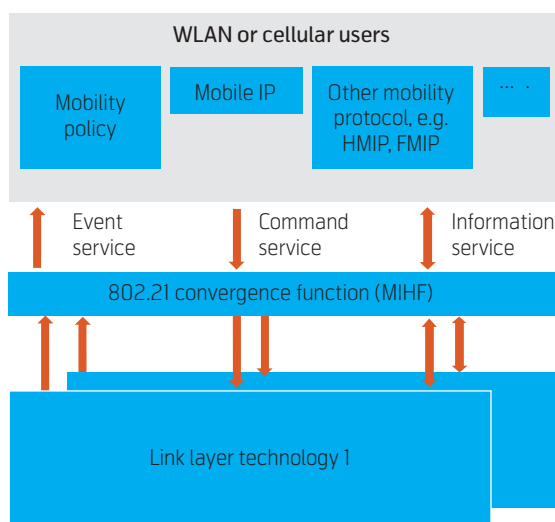


Figure 11 Illustration of 801.21 applied across different accesses (link layers), based on [ITU-HFC]

(bandwidth, delay, packet loss) the transport level handover can be transparent to the service level. In case the QoS of both accesses is substantially different, the service level needs to be involved in the handover decision process. Providing the service level with full control of the handover process as described above offers the advantage that the service that is provided to the user can continuously be optimized for the access network conditions.

When the user equipment is switched on and tries to connect to the network, it should authenticate itself to the network. An authentication might also be performed when the user equipment performs handover to a new access network. Handovers between different access networks incur delay, in particular when re-authentication is performed. Some methods to reduce this delay are pre-authentication and context transfer. The latter means that a mobility management entity in the core transfers its context information to a neighbouring mobility management entity (meaning that these need to have a trust relationship pre-established).

[ITU-FMC] states that an FMC terminal should implement the ISIM functionality to provide the same user identity information and the same security level across different access types. An ISIM could be implemented in different ways, such as a UICC (ie. a card) or 'soft' SIM (ie. a software).

As several terminals do not support ISIM or IPsec, other authentication means have also been defined:

- SIP HTTP digest, ref. IETF RFC 2617: User log-in applying user id and password;
- NASS-IMS bundled: Relying on bearer level security for fixed access networks provided by the Network Attachment SubSystem (NASS). NASS allocates an IP address to the terminal during network attachment. The P-CSCF queries NASS to obtain location information (ie. access line identity) of the terminal. This location information is forwarded to S-CSCF for verification;
- Early IMS: Utilising GPRS level security based on SIM or USIM.

A location management function has two main roles (ref. [ITU-LFM]):

- To manage the transport and/or geographical locations of mobile user equipment;

- For the user equipment, to manage the relation of user identity and location identities (persistent location id and temporary location id).

5 Middleware

[Y.130] elaborates on a number of aspects related to the middleware function. In the ITU NGN model, the middleware is placed between the baseware and the application functions. The middleware assists the separation between applications and networks.

The following requirements are listed in [Y.130] for the middleware layer (named information communication architecture in that document):

- General:
 - Modular;
 - Allow separation between terminal, access and core (transport and control) components;
 - Allow evolution from GSM, ISDN, IN, etc.;
 - Define open, secure, generic interfaces and protocols, eg. Application Programming Interfaces (APIs), Middleware Programming Interfaces (MPIs) and Baseware Programming Interfaces (BPIs);
 - Allow architectural components and different federated administrative domains to inter-operate in a consistent manner for seamless execution of services and management;
 - Allow maximum flexibility in the ways in which architectural components may be geographically distributed, within the constraints of maintaining the required defined interrelationships. This will allow varying degrees of bundling/unbundling, whilst maintaining multi-supplier interoperability.
- Reuse of architectural components:
 - Enable design reuse of architectural component specifications when new services or management capabilities are created;
 - Enable run-time reuse of architectural components so that the architectural components can be accessed in providing new services and management capabilities;
 - Define means by which existing architectural components can be reused to build services and management capabilities.

- Distributed execution:
 - Not dictate the location of architectural components;
 - Facilitate transparent distributed computing. Allowing architectural components to use all the distribution transparency defined in ODP-RM¹⁾ or a subset according to the needs. This does not imply that every node needs to provide all the transparencies.
 - Allow services to be provisioned and accessed from anywhere in the information communication system except that such access is subject to the security control implemented in that information communication system.
 - Be applicable to architectural components for customer domains, including low-end systems (such as PCs, set-top boxes, mobile terminals). This also includes options for scalability, eg. downsizing.
- Support of services:
 - Support, but be free from the limitations of traditional call models (eg. call-associated triggers, protocol-dependency) so that it can support new types of services, such as multimedia communications and information services;
 - Support (terminal, personal and session) mobility services;
 - Facilitate cooperation between service and management capabilities in customer premises equipment/network and in other domains in the information communication system. This includes both network-based distributed services and end-user services. Examples are multimedia libraries and interactive games. Then, the user can utilize the distributed processing capability of the information communication system;
 - Enable end user services to be tailored to meet different customer requirements;
 - Facilitate creation of end-user services together with their associated management services;
 - Include fail-safe mechanisms for handling unexpected service interactions. The fail-safe mechanisms will ensure that predictable and stable system behaviour occurs across all architectural components.
- Support for management:
 - Contain no obvious impediments to the management of relevant components distributed across different domains and players;
 - Enable effective management of information communications systems in which architectural components are supplied by multiple vendors;
 - Enable, and make available, a collection of metering information from resources suitable for further processing by billing entities;
 - Provide means to deal with the availability and congestion aspects of the appropriate architectural components.
- Security:
 - Support authentication and authorization of entities involved in an interaction. The entities are, in general, stakeholders and they may reside in different administrative domains. Mutual identification and authorization should also be supported;
 - Enable collecting and maintaining audit information about actions performed by entities (defined as in above item). This is required to maintain accountability within the system conformant to the middleware;
 - Provide means for preventing stakeholders from performing actions that they are not entitled to perform. This is required to maintain integrity, confidentiality and availability of the system conformant to the middleware;
 - Enable monitoring of rogue and unusual activities, and adoption of counter-measures. This is required to maintain integrity, confidentiality and availability within the system conformant to the middleware;
 - Support protection of information (messages and stored data). This includes maintaining integrity of information and confidentiality within the system conformant to the middleware;
 - Enable realization of security controls across equipment provided by different vendors. Some are required by national regulation to provide certain security and safeguard features as built-in features.

¹⁾ ODP Reference Model identifies access, location, migration, federation, transaction, group, failure, resource, and replication transparency.

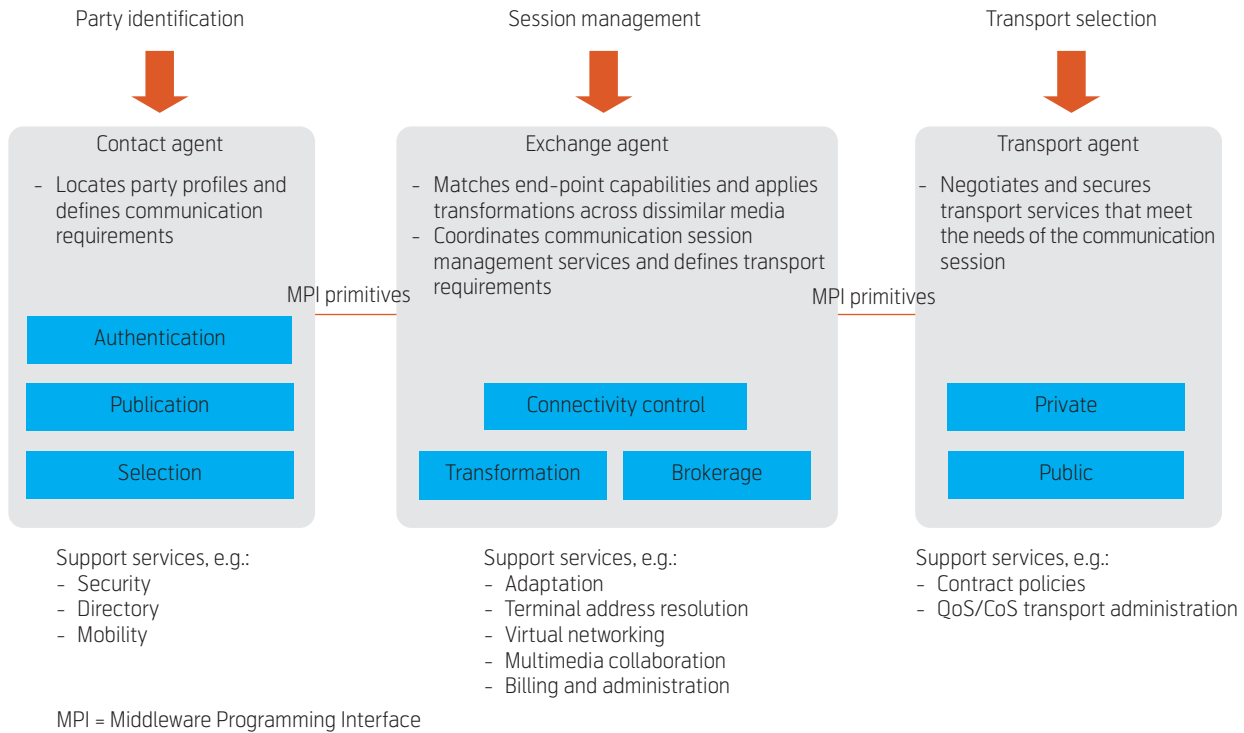


Figure 12 Conceptual architecture for the middleware area (adapted from [Y.130])

- User control: Future services and/or features offered by service providers will permit a degree of user control over such services. Hence, the middleware must support the user to select from a variety of services for any instance of communication. Main objective is to allow the user to select services required on a dynamic basis, which may vary from one communication instance to another. Typically this may include some combinations of
 - Service type, eg. voice service, video service, data service (IP service);
 - Session type, eg. connection-oriented service, connectionless service, multicast service;
 - Quality of Service (QoS), eg. throughput, delay, jitter, etc.;
 - Additional encryption services;
 - Additional authentication service;
 - Mediation services, eg. device adaptation, user presentation, etc.;
 - Other appropriate services /features.
- Operator control: This includes the following aspects of service provision:
 - Policy;
 - Contractual;
 - Service availability and advertising.
- Scalability: Accommodate and allow the evolution of the scale of networks and services and management capability from very small to very large (of global scale) in terms of the number of users, the number of physical entities, the number of administrative domains, etc.
- Mobility: In general all aspects of mobility are embraced, including both personal mobility and terminal mobility. For the majority of cases the middleware assumes the existence of a mobility-supporting system.
- Compatibility with existing telecommunication systems: Accommodate interworking between existing and future infrastructural components and systems. This includes:
 - Enabling access from existing legacy systems to services deployed in future systems;
 - Enabling access from future systems of the middleware to existing services.

The conceptual architecture is depicted in Figure 12. A schematic example of implementation is shown in Figure 13.

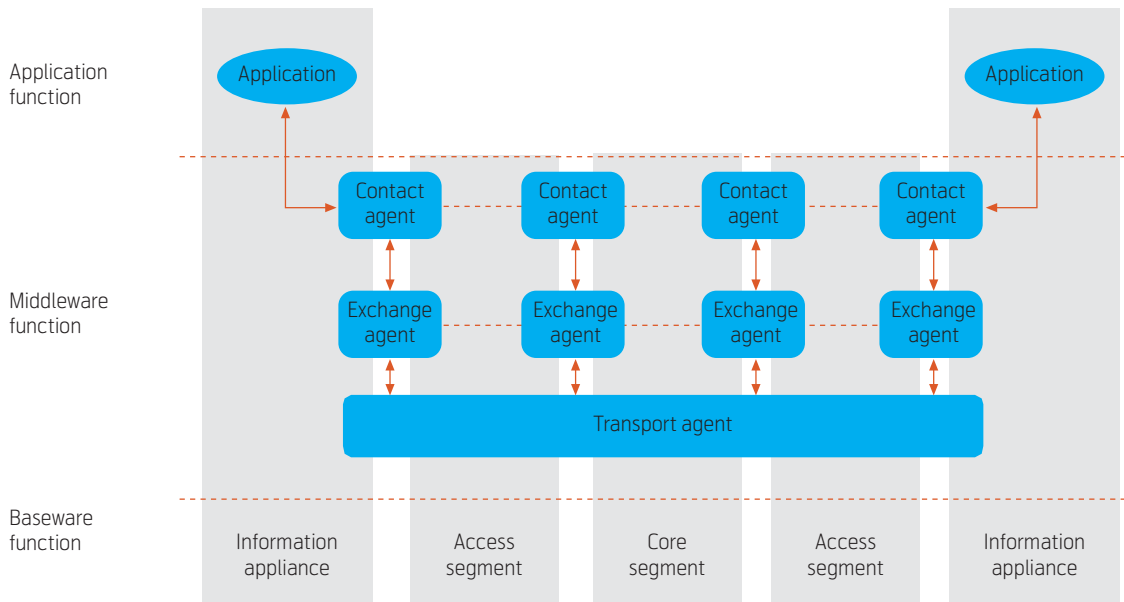


Figure 13 Schematic implementation case for middleware (from [Y.130])

6 Management

Management functions mentioned for NGN follow the traditional *FCAPS model* (ref. [M.3060]):

- *Fault* management;
- *Configuration* management;
- *Accounting* management;
- *Performance* management;
- *Security* management.

As the NGN is composed of a number of individual systems, the management architecture is concerned with orchestrating the management of the individual system so as to have a coordinated effect upon the network. Management objectives include (from [M.3060]):

- 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;
- Support business processes and the way they would be used in NGN;
- Support applications, both on the same distributed computing platform and those distributed throughout the network.

The management architecture is divided into four different views, see Figure 14:

- *Business process* view: Providing a reference framework for categorizing the business activities of a service provider. Business processes are organized in the form of a multi-level matrix. This is referred to as the enhanced Telecom Operations Map, see [Jens09t]. It divides the processes into process areas, horizontal functional process grouping, and vertical flow-through process groupings. It also provides basic mappings between business processes and management function sets.
- *Management functional* view: Permits the specification of what functions have to be achieved in the management implementation. This is a structural and generic framework of management functionality. The view is structured from, i) management function blocks, ii) support function blocks, iii) management functionality, iv) provider reference

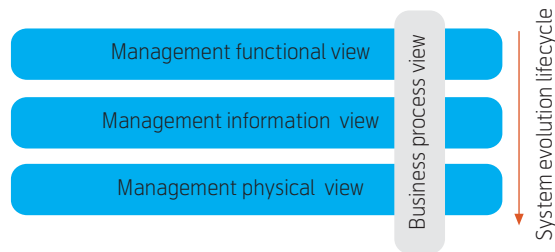


Figure 14 NGN management architecture (adapted from [M.3060])

points and consumer reference points, and v) logical management function layers.

- *Management 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. This view is structured from, i) interaction models, ii) information models, iii) information elements, and iv) information model of a reference point (information-specified reference point). The management information exchanges to be implemented can then be described in terms of these fundamental elements.
- *Management physical view*: Describes the various ways that management functions can be implemented. Management systems may be deployed in a variety of physical configurations using a variety of management protocols.

As stated in [M.3060] the NGN management architecture is a Service-Oriented Architecture (SOA). SOA is a software architecture and further described in [Jens09t].

7 Interworking/Inter-domain

Interworking between different NGN instances can be either service or network interworking, see Figure 15. To provide any instance of an interworking function, the following may be considered, [Y.2011]:

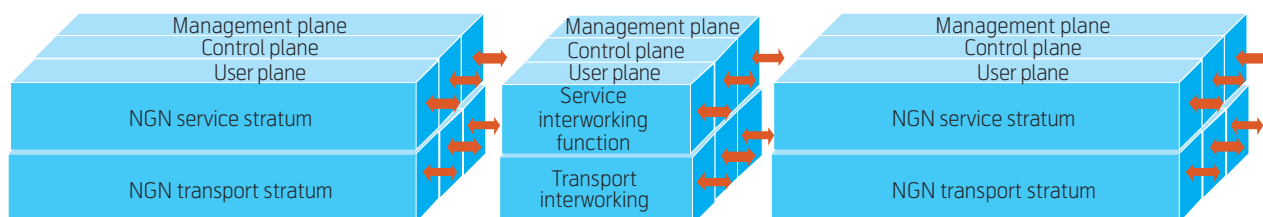


Figure 15 Interworking between different strata of two NGN instances (adapted from [Y.2011])

- User plane's interworking may have responsibility for media flow processes, such as NAT, firewall operation, link mapping, QoS-relative processing, codec converting, etc.
- Control plane's interworking may have responsibility to exchange processing, such as connectivity control, service logical control, user policy negotiations, call signalling, addressing and routing.
- Management plane's interworking may be used for such operations, when necessary, as settlement, bandwidth limitation policy, usage measurements, etc.

Interworking functions are unique and differ from each other when located in different layers.

8 Brief Example – NGN for Tag-based Identification

Depending on the actual applications, functional entities in the NGN architecture have to be populated. One example, from [Y.2016], is shown in Figure 16. This describes the functional entities involved for tag-based identification, such as identifying different devices carrying a tag to be read by a terminal. An example is ticket reader on a bus, another example is bar code reader in a shop.

9 Concluding Remarks

This paper has presented ITU's NGN results so far. There are considerable efforts behind the progress in this area, both by the standardisation bodies and by other projects. One observation is that on-going standards seem to re-use existing and well-adopted protocols and mechanisms. Hence, the various standardisation activities build onto each other's result.

A key characteristic of the NGN architecture is the modularisation. This can be observed by the layering, and also by the way separate areas are linked to a common basic architecture. This has been illustrated by the way mobility is to be supported and the way of implementing convergence.

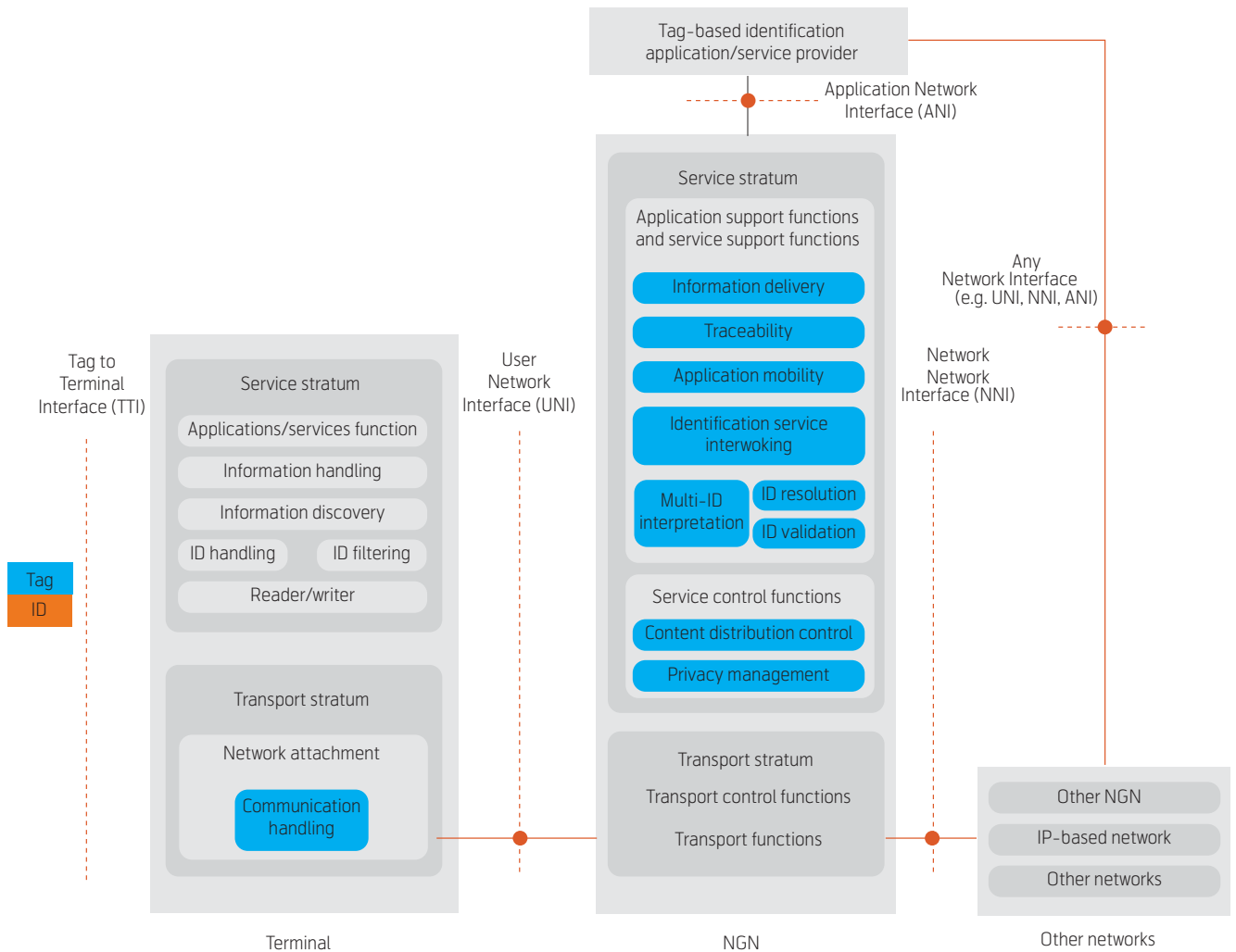


Figure 16 Functional architecture for tag-based identification (from [Y.2016])

Work on the NGN architecture is on-going and latest updates on this can be found on the ITU home page (www.itu.org).

References

[ITU-FMC] ITU. *Fixed mobile convergence with a common IMS session control domain*. ITU-T draft recommendation, May 2009.

[ITU-HFC] ITU. *Framework of handover control for Next Generation Networks*. ITU-T draft recommendation, January 2008.

[ITU-LMF] ITU. *Framework of location management for Next Generation Networks*. ITU-T draft recommendation, January 2008.

[Jens09t] Jensen, T. Technical aspects to consider in an architecture. *Teletronikk*, 105 (2), 4-31, 2009. (This issue)

[M.3060] ITU. *Principles for the Management of Next Generation Networks*. ITU-T Recommendation M.3060, May 2009.

[Q.1706] ITU. *Mobility Management Requirements for NGN*. ITU-T Recommendation Q.1706, May 2009.

[Q.1762] ITU. *Fixed-mobile Convergence General Requirements*. ITU-T Recommendation Q.1762, September 2007.

[Y.130] ITU. *Information communication Architecture*. ITU-T Recommendation Y.130, 2000.

[Y.140] ITU. *Global Information Infrastructure (GII): Reference points for interconnection Framework*. ITU-T Recommendation Y.140, 2000.

[Y.2001] ITU. *General overview of NGN*. ITU-T Recommendation Y.2001, 2004.

[Y.2011] ITU. *General principles and general reference model for next generation networks*. ITU-T Recommendation Y.2011, 2004.

[Y.2012] ITU. *Functional requirements and architecture of the NGN*. ITU-T Recommendation Y.2012, 2009.

[Y.2015] ITU. *General requirements for ID/locator separation in NGN*. ITU-T Recommendation Y.2015, 2009.

[Y.2016] ITU. *Functional requirements and architecture of the NGN for applications and services using tag-based identification*. ITU-T Recommendation Y.2016, June 2009.

[Y.2018] ITU. *Mobility management and control framework and architecture within the NGN transport stratum*. ITU-T Recommendation Y.2018, June 2009.