TSG-SA WGx #xx **SA-05xxxx**
TSG-CN-WGx #xx **CN-05xxxx**
Agenda Item:

Title: Submission of a high-level architecture and definition for Next Generation Network (NGN) from the perspective of the industry as represented by ATIS, entitled: ì*ATIS Next Generation Network (NGN) Framework, Part I: NGN Definitions, Requirement and Architecture, Issue 1.0, November 2004.*î

Response to:

Source: **Alliance for Telecommunications Industry Solutions (ATIS)**
Tim Jeffries, tjeffries@atis.org // +1.202.662.8669

To: **3GPP SA (SA1 and SA2)**
3GPP CN

Contact Persons:

Name:	Gary Jones, T-Mobile	Stephen Hayes, Ericsson	Randy Wohlert, SBC
E-mail Address	Gary.Jones@T-Mobile.com	stephen.hayes@ericsson.com	Randolph_Wohlert@labs.sbc.com
Tel. Number:			

Attachments: *ATIS Next Generation Network (NGN) Framework, Part I: NGN Definitions, Requirement and Architecture, Issue 1.0, November 2004*

The *Alliance for Telecommunications Industry Solutions (ATIS)* submits the attached document for review and input into 3GPPís work-programs relevant to Next Generation Networks; namely the 3GPP Technical Specifications Groups (TSG) Core Network (CN) and Services & System Aspects (SA) Working Group #1 (Services) and Working Group #2 (Architecture). The attached, referred to as the ATIS NGN Framework, represents the North American marketís requirements for NGN as approved by the ATIS Board of Directors and ATISí 270+ member companies.

Background:

For the past several months, ATIS, through the efforts of its Next Generation Network Focus Group (NGN-FG) -- a group of mid-to-senior management level member company representatives commissioned by the ATIS Board of Directors, has worked towards defining a high-level architecture and set of requirements for NGN from the **business perspective** of the industry as represented by ATIS members.

To ensure the North American marketís requirements for NGN are fully represented in global discussions, as well as to support the development of globally acceptable standards for NGN, these requirements are being submitted/transmitted to help guide relevant national and international standards organizations NGN work programs to address these requirements ñ including, 3GPP, ITU-T FGNGN, and ETSI TISPAN.

The premise of ATISí efforts with respect to the overarching NGN is to develop a broadband system that enables easy integration of network resources, services, and operations across the business units of service providers while decoupling services from underlying network transport technologies. An equally important premise is the potential for (CAPEX and OPEX) cost reductions; *e.g.*, by leveraging commercially available intelligent Consumer Premise Equipment (CPE) and IP-based IT infrastructure and middleware. The ATIS NGN Framework outlines ATISí NGN Definition, Requirements and Architecture towards this end.

Highlights of the ATIS NGN Framework, Part I:

Many efforts towards defining NGN within global standards developers are ongoing and rapidly progressing. And the attached ATIS NGN Framework represents these efforts by either directly utilizing the findings from certain work-programs or by making references to them. Areas where the ATIS NGN Framework differs from these efforts, however, are in the following highlighted areas:

- The scope of the document goes beyond other NGN-related work-programs;
- Provides the unique North American user and regulatory perspective;
- Expands the scope of current NGN-related efforts by scoping out NGN from an ì inter-carrierî perspective;
- Optimizes the NGN for future NGN-type services while providing continued support of vital legacy-based services, and;
- Sets in place explicit criteria for access networks in order to interconnect and interwork with the core NGN.

Of interest, while not unique to the attached, is that the NGN architecture specified builds on the ETSI TISPAN Extended IP Multimedia System (IMS) session-based architecture to consistently support new value-added services. However, ATIS also acknowledges that the NGN architecture may be further enhanced or modified to support other services provided by NGN service providers (*e.g.*, broadband services, L2VPN, L3VPN).

Also of interest is that the Public Switched Telephone Network (PSTN) Emulation subsystem is identified as a mechanism to facilitate migration from legacy PSTN services to NGN. The document identifies key IP access network requirements for compatibility with the core NGN. These include providing IP connectivity, QoS, and policy enforcement.

The NGN also should support mobile network evolution as defined by 3GPP and 3GPP2. As wireless service provider networks may be at any stage in the evolution process, the requirements to achieve convergence will differ depending on which stage is deployed.

Areas of Focus for the 3GPP (CN & SA):

From the document ñ which members of the 3GPP CN & SA and its Working Groups are encouraged to read ñ several areas or sections of the document are considered important to the North American interest; these are:

- Wireline/Wireless Integration
- Network/CPE Integration
- Parlay/OSA based Service Architecture and Open APIs
- Embedded access architecture, DSL and FTTx
- End-to-end QoS

- ENUM
- Presence
- Security

It is important to note that the ATIS NGN Framework document contains a snapshot of NGN target objectives and features, for which phased implementation requirements will be developed. The ATIS NGN-FG will continue to clarify the priorities (*i.e.*, short-term, medium-term, long-term) for these standards initiatives. In addition, ATIS will continue to work with groups (*e.g.*, TISPAN, 3GPP, ITU-T) to develop a consistent set of NGN specifications that meet the needs of ATIS members. To comply with unique North American requirements/standards, ATIS plans to share this document with its internal technical committees and other external groups where and when appropriate.

ATIS welcomes comments on this document. The contacts provided can provide further details on the ATIS NGN Framework, as well as the next steps of the ATIS NGN-FG. They also will ensure comments or requests for clarification are presented to the ATIS NGN-FG for resolution and/or feedback.

ATIS Next Generation Network (NGN) Framework

Part I: NGN Definitions, Requirements, and Architecture

Issue 1.0

November 2004

ATIS is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from more than 350 communications companies are active in ATIS' 22 industry committees, and its Incubator Solutions Program.

< http://www.atis.org/ >

Next Generation Network (NGN), Part I: NGN Definitions, Requirements and Architecture

Is an ***ATIS Work Plan*** developed by the **Next Generation Network Focus Group** for the **TOPS COUNCIL**.

This document is a *work in progress* and subject to change.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document has been prepared as input to the global Next Generation Network (NGN) standards initiatives. ATIS fully supports a consistent set of global NGN standards. The ATIS Next Generation Network Focus Group (NGN-FG[1]) – commissioned by the ATIS Technology and Operations (TOPS) Council – is currently developing an NGN standards gap analysis that will subsequently be input into the global standards process. The ATIS NGN Framework Part I document contains a snapshot of NGN target objectives and features, for which phased implementation requirements will be developed. The NGN-FG will continue to clarify the priorities (*i.e.*,, short-term, medium-term, long-term) for these standards initiatives.

A key motivation for the NGN is to focus on the variety of new, value-added, IP-centric services and applications. An equally important motivation is to reduce Capital Expense (CAPEX) and Operational Expense (OPEX) through more efficient utilization of network resources to provide services (e.g. voice services). The NGN architecture builds on the ETSI TISPAN extended IP Multimedia System (IMS)[2] session-based architecture to consistently support new value-added services. The ATIS NGN architecture may be further enhanced or modified to support other services provided by NGN Service Providers (e.g. broadband services, L2VPN, L3VPN). The PSTN Emulation subsystem is identified as a mechanism to facilitate migration from legacy PSTN services to NGN. This enables expense reduction through more efficient voice services, while still allowing the NGN to be optimized for the future SIP services model. The document identifies key IP access network requirements for compatibility with the core NGN. These include providing IP connectivity, QoS, and policy enforcement.

ATIS will continue to work with groups (e.g. TISPAN, 3GPP, ITU-T) to develop a consistent set of NGN specifications that meet the needs of ATIS members[3]. To comply with unique North American requirements/standards, ATIS plans to share this Framework document with all of its internal technical committees and other external groups where and when appropriate.

ATIS welcomes comments on this document.

[1] Unless otherwise specified, the term NGN-FG refers to the ATIS NGN Focus Group

[2] . The Extended IMS is still being actively defined, with open issues.

[3] This document represents the current North American position as represented by ATIS and its member companies. It has not yet been fully reviewed by the ATIS technical committees.

1 ATIS NGN OVERVIEW

This document defines the current view of the requirements for a Next Generation Network (NGN) architecture with interfaces to existing networks. This multi-service architecture should be viewed from the perspective of service convergence across public mobile, public fixed, and private customer premises networking environments, as shown in Figure 1. Whereas traditional networks have been focused on "unimodal" services (such as voice services), next generation networks are intended to support multimodal communication environments where information can be communicated through a variety of terminal devices, network access technologies, and underlying infrastructures. The information may be presented in real-time (*e.g.,* interactive voice) or time-shifted (*e.g.,* voice mail), in its original format (*e.g.,* analog speech) or transformed (*e.g.,* file attachment.). The information can be delivered by the network to a location, a device, or a person, reflecting personal preferences and mobility options. In this document, a network that uses this multi-service architecture is called the NGN. The scope of the NGN-FG is further refined in clause 1.2 of this document.

1.1 Definition of NGN

The intent of the ATIS NGN-FG is to coordinate with other standards bodies to arrive, to the extent possible, at a consistent global view of the NGN. Therefore this focus group is starting with the current definition of the NGN as defined by the International Telecommunications Union - Telecommunications Standardization Sector (ITU-T).

ITU-T draft Y.2001 provides a definition of NGN as follows:

> **3.1 Next Generation Network (NGN)**: 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 access to different service providers, independent of any access or transport technology[4]. ~~It offers unrestricted access by users to different service providers~~. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.

ITU-T draft Y.2001 goes on to characterize the NGN 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 network, 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 (Quality of Service).

[4] Note this sentence has been proposed by AT&T during the AAP process for Y.2001 as replacement for the text that has been struck out. Final resolution of AT&T's proposal will depend on results of the AAP process.

- Interworking with legacy networks via open interfaces.
- Generalized mobility.
- Access to different service providers, independent of any access or transport technology[5]. ~~Unrestricted 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, and so forth.

1.2 Scope of NGN Focus Group

Figure 1 shows a convergence of *Public Mobile* (Wireless) services, including but not limited to traditional mobile and WiFi hotspot services; *Public Fixed* (Broadband Wireline) services including but not limited to traditional voice and data service; and *Private Customer Premises Networks*, which are typical of today's broadband users. The intersection of these three environments, indicated in green, is the focus of convergent user-centric services. When deployed, services will no longer be associated with the type of network access, but rather with the user need that is satisfied regardless of user terminal or access type.

[5] Note this text has been proposed by AT&T during the AAP process for Y.2001 as replacement for the text that has been struck out. Final resolution will depend on results of the AAP process.

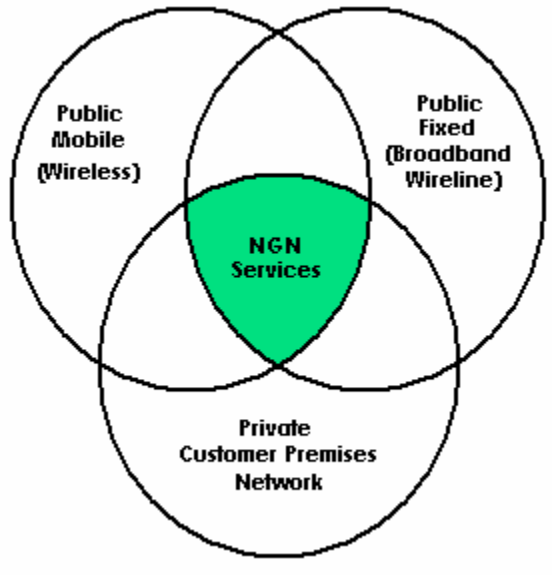

Figure 1 - NGN Context: Convergence of Wireless, Wireline, and Customer Premise Services

In 2003, ATIS began identifying NGN standards gaps with the formation of five ATIS TOPS Council commissioned Focus Groups. The final reports of these Focus Groups provided action plans to address identified standards overlaps and gaps. The NGN-FG is driven by the business needs of the North American market. The goal is to produce, to the extent that it is practical, international NGN standards, consistent with the unique North *American* regulatory, business, and infrastructure requirements. The ATIS NGN-FG will build on the work of the initial focus groups by providing a phased business-driven action plan for achieving implementable and interoperable NGN standards. The NGN-FG will review the existing ATIS Focus Group Work Plans and other NGN-related industry material to identify potential overlaps and gaps.

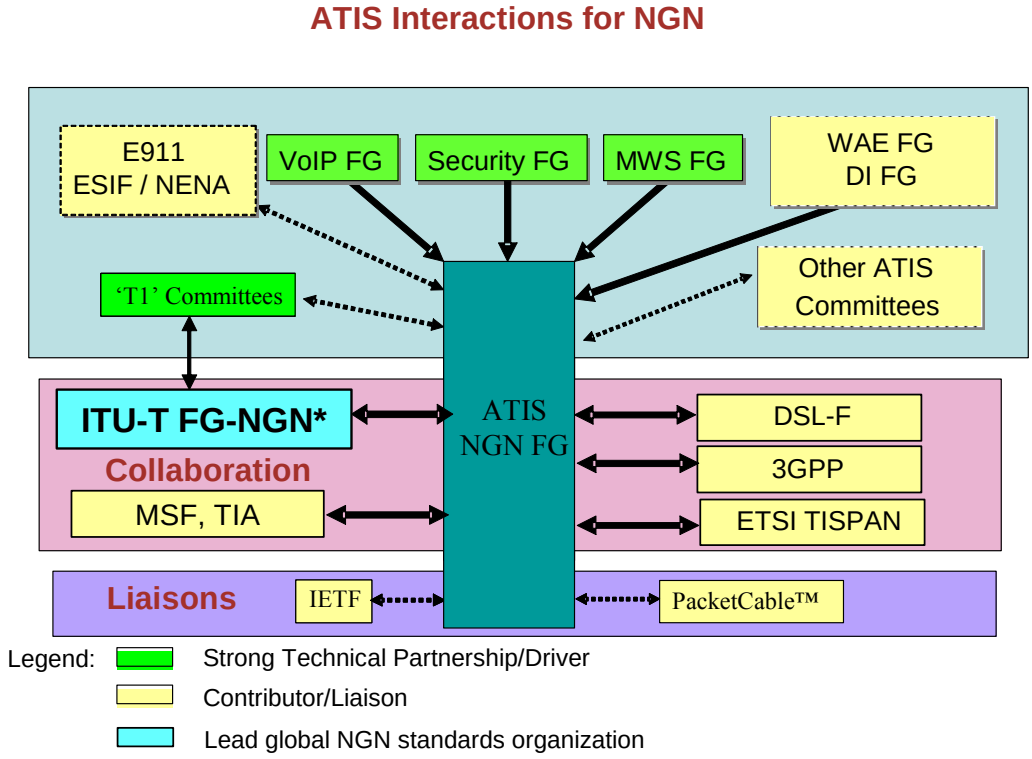

Figure 2 - Potential Standards Collaboration

* NOTE: ITU-T is recognized as the principal global organization for defining a global NGN standard. The ATIS NGN-FG is primarily interacting with the ITU-T FGNGN; however it is recognized that other groups in ITU-T (*e.g.*, SG11, SG13) and other groups in ATIS (*e.g.*, PTSC) that are also concerned with aspects of the NGN.

1.3 Inputs to NGN Focus Group

In 2003, ATIS TOPS Council initiated an analysis of priority areas where additional work was required to realize implementable standards for a multi-service architecture. The following TOPS Focus Groups conducted detailed assessments of standards activities to identify gaps and develop action plans:

- Voice over IP (VoIP)
- Mobile Wireless Services (MWS)
- Network Security
- Data Interchange & Billing (DI)
- Wide Area Ethernet (WAE)

The final reports from these focus groups have now been published and provide an excellent starting point for the NGN-FG group. Figure 2 shows how the output of these TOPS focus groups can feed into

the ATIS NGN-FG. This figure also shows how other activities, such as the ATIS Emergency Services Interconnection Forum (ESIF) E9-1-1 for VoIP standardization effort, could also provide additional input. It is expected that the existing ATIS Committees (*e.g.*, ESIF) and the National Emergency Number Association (NENA) will provide much of the technical expertise required to complete this activity.

Figure 2 also indicates other standards forums that could collaborate closely with the ATIS NGN-FG or provide ongoing liaisons. These include:

- ITU-T: SG13, including the Focus Group on Next Generation Networks (FGNGN)
- 3rd Generation Partnership Project (3GPP)
- European Telecommunications Standards Institute (ETSI) TISPAN
- Multiservice Switching Forum (MSF)
- DSL Forum (DSL-F)
- CableLabs™
- Institute for Electrical and Electronics Engineers (IEEE)
- ATIS Technical Committees *(e.g.*, PTSC, TMOC, NIPP)
- 3rd Generation Partnership Project #2 (3GPP2)
- Telecommunications Industry Association (TIA)
- Internet Engineering Task Force (IETF)
- National Emergency Numbering Association (NENA)
- Emergency Services Interconnection Forum (ESIF)
- TTY Forum
- Industry Numbering Committee (INC)
- FCC Network Reliability & Interoperability Council (NRIC)
- Open Mobile Alliance (OMA)
- Metro Ethernet Forum (MEF)
- MPLS and Frame Relay Alliance

1.3.1 ITU-T:

The appropriate ITU-T Study Groups, including SG13 and its Focus Group on Next Generation Networks (FGNGN), are responsible for the global standards surrounding NGN telecommunications. The ITU-T work can be expedited by having individual organizations or regional SDOs submit contributions to the ITU-T that have a regional consensus. While this approach may not eliminate the

need for collaboration between ATIS and other standards bodies, it should reduce the amount of such collaboration required, while resulting in more harmonized global standards. Such a workflow recognizes the global scope of the ITU-T, while expediting a path for regional input from ATIS into the global standards. Further more, this flow does not exclude the ability for ATIS to develop regional extensions for the ITU-T standards, although such extensions should be minimized and created only when truly needed. The goal is a universal global standard without the need for regional extensions.

1.3.2 ETSI TISPAN

TISPAN is the ETSI core competence center for fixed networks and for migration from switched-circuit networks to packet-based networks with an architecture that can serve in both. TISPAN is the result of the merging of Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) and Service and Protocol for Advance Networks (SPAN) groups in ETSI. TISPAN is the ETSI group responsible for all aspects of standardization for present and future converged networks, including the NGN and including service aspects, architectural aspects, protocol aspects, QoS studies, security related studies, and mobility aspects within fixed networks, using existing and emerging technologies. TISPAN is developing a architecture for NGN based on the 3GPP IMS subsystem (release 6). This architecture is named "extended IMS" throughout this document and is considered the base for ATIS NGN work.

Please, refer to clause 3 for the description of the ATIS NGN Converged architecture based on TISPAN extended IMS.

1.3.3 3GPP

The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. The collaboration agreement brings together a number of telecommunications standards bodies known as *Organizational Partners* (see < http://www.3gpp.org/Management/OP.htm >). The current Organizational Partners are ARIB, CCSA, ETSI, ATIS, TTA, and TTC.

The establishment of 3GPP was formalized in December 1998 by the signing of the *3rd Generation Partnership Project Agreement* (see < http://www.3gpp.org/About/3gppagre.pdf >).

The original scope of 3GPP was to produce globally-applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved Global System for Mobile communication (GSM) core networks and the radio access technologies that they use. The scope was subsequently amended to include the maintenance and development of the GSM Technical Specifications and Technical Reports including evolved network and radio access technologies -- *e.g.*, General Packet Radio Service (GPRS), Enhanced Data rates for GSM Evolution (EDGE), Universal Mobile Telephone System (UMTS) and IP Multimedia Subsystem (IMS).

3GPP2 is a parallel partnership covering specifications for CDMA-2000. Both 3GPP and 3GPP2 are closely aligned with ITU-T 3G standards.

1.3.4 MSF

The Multi-service Switching Forum (MSF) is a global forum with the primary objective of accelerating the commercial availability and interoperability of multiservice networks. The MSF accomplishes this objective by focusing on end-to-end solutions leveraging standards, architectures, and inputs from other SDOs (*i.e.*,, IETF, ITU, Parlay/OSA, 3GPP, etc.) and the prioritization of member companies. The MSF has significant experience in the creation and validation of architectures, Implementation Agreements (IAs), and large scale demonstration of interoperability for VoIP solutions that are fit for use by service providers. The MSF has significant work in progress that may be useful for the ATIS NGN Framework.

More detailed information on the MSF, MSF GMI-2004 Program, and Published documents can be found at < http://www.msforum.org >. Publicly available MSF documents are available at < http://www.msforum.org/techinfo/approved.shtml >.

1.3.5 DSL-F

The DSL Forum, a consortium of industry telecommunications, equipment, computing, networking, and service provider companies, was established in 1994 and continues its drive for a mass market for DSL to deliver the benefits of this technology to end users around the world over existing copper telephone wire infrastructures. The evolution of existing infrastructure towards NGN services provides a significant mechanism for NGN deployment. DSL Forum < http://www.dslforum.org/ > has developed a number of documents regarding the architecture and capabilities of the DSL based access infrastructure. The following published documents are of particular relevance:

- TR-058, *Multi-Service Architecture & Framework Requirements*, September 2003.
- TR-059, *DSL Evolution – Architecture Requirements for the Support of QoS Enabled IP services*, September 2003.
- TR094, *Multi-Service Delivery Framework for Home Networks*, August 2004.

Current work in progress items are also addressing topics of concern including:

- WT-101, *Migration to Ethernet Based DSL Aggregation*
- WT-102, *Architecture & Transport: Service Interface Requirements for TR-058 Architectures*

The architecture described in the DSL Forum documents is one of the inputs that will be considered in the standards gap analysis.

1.3.6 CableLabs®

Cable Television Laboratories, Inc. (CableLabs®) is a nonprofit research and development consortium that is dedicated to helping its cable operator members integrate new cable telecommunications technologies into their business objectives. A significant portion of consumer wireline Internet access is provided via cable infrastructure.

NOTE - Although not further addressed in this document, CableLabs® PacketCable™ Multimedia Architecture (PKT-TR-MM-ARCH-V01-030627) should be considered as another technology for delivery of NGN services. The cable operators are expected to continue to evolve their infrastructure capabilities.

1.3.7 IEEE

The IEEE 802 LAN/MAN Standards Committee develops Local Area Network (LAN) standards and Metropolitan Area Network (MAN) standards. The most widely-used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging, and Virtual Bridged LANs. An individual Working Group provides the focus for each area. The IEEE has significant work in progress that may be useful for the ATIS NGN Framework. This work includes various forms of access to the NGN including: Ethernet in the First Mile (EFM), WiFi, and WiMAX.

1.3.8 ATIS Technical Committees

One of the primary ATIS Technical Committees for NGN standards is the PTSC.

- *PTSC (formerly T1S1): the Packet Technologies and Systems Committee*
  - *Coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S.*
  - *Reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations*
  - *Reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions*

1.4 Expected Results of NGN Focus Group

The ATIS NGN-FG will provide a phased business-driven action plan for achieving implementable and interoperable NGN standards. The initial output of the NGN-FG will consist of Part 1 (this document) and Part 2 (a "gap" analysis). The NGN-FG will work with ATIS Technical Committees to ensure this work plan leads to implementable protocol standards for the North American market, within the context of a common international set of NGN standards. Contributions and liaisons will also be provided to other organizations working on NGN standards, in particular ETSI TISPAN, 3GPP, and ITU-T FGNGN (and any follow-on and related Study Groups or Questions in the next ITU-T study period).

2 HIGH-LEVEL REQUIREMENTS/GUIDING PRINCIPLES

Service providers are highly interested in leveraging existing networks and infrastructure to increase the value of those networks by enhancing their ability to offer customers "seamless" delivery of applications independent of any access or transport technology. This framework provides a common architecture and set of service interfaces to address this basic goal. Adhering to this architecture and to the services and service models set forth provides a common framework for delivering services, irrespective of the network context. Regulatory requirements *(e.g.,* CALEA) may affect any telecommunications services provided.

2.1 General

The NGN-FG activity in ATIS is driven by identified business needs of the North American market. Subsequent clauses discuss each of these drivers in more detail.

To be successful, the new NGN target architecture must not only separate services from transport, but must enable efficient interworking between applications to support innovative converged services. Many of today's services are vertically-integrated which inhibits integration with other applications. This interworking can add value to existing as well as new NGN services by integrating them into the larger convergence of media and access modes, allowing service providers to roll out the kind of customized and convenient advanced services that segments of their markets are already asking for today. By putting the disparate parts of the communications puzzle together (such as wireline and wireless services, switched and IP networks, voice and other media, and access modes of all types), service providers have the flexibility to create the right combinations of services for their markets and deploy them to the benefit of end customers.

To make the transition to a fully converged NGN network, service providers need a standards-based, service-enabled network architecture that is ready and able to deliver value-added services. To fulfill these needs, the NGN target architecture should support:

- Open, standards-based interfaces allowing "plug-and-play" integration of any number of applications.
- A standardized session control function through which application servers can signal. This allows full convergence of services over a number of access modes –- blending instant messaging with unified communications and VoIP, for example.
- A logical subscriber database that holds all customer profile data, so that it can be consistently accessed from anywhere in the NGN. This concept, similar to the Home Location Registers (HLRs) and Visitor Location Registers (VLRs) of the wireless world, makes both service rollout and ongoing administration manageable and scalable.

- A set of access-independent application and service creation capabilities, so that these converged applications and services can be adapted to any device the end-user chooses and delivered with consistency (subject to the inherent constraints of the specific access technology and device).

Business drivers are expected to vary depending on market conditions, business focus, timing issues, and other factors. The NGN architecture must support a variety of business models that may apply, including wholesale, retail, Virtual Network Operator (VNO), and Virtual Services Operator (VSO). In developing their NGN strategies, market participants may consider a variety of business model aspects. These include market segment addressed, insourcing vs. outsourcing NGN infrastructure, electronic supply chain and merchandizing model, technology considerations, development and deployment constraints, operating and maintenance models, and regulatory issues. A key consequence of multiple business models is that inter-provider interfaces will emerge at places in the architecture that may not correspond to traditional inter-provider interfaces.

Additionally, accommodation of existing key services and infrastructures through integration and/or interoperability is an important business aspect. The NGN must leverage the deployed base while supporting new services and technologies efficiently.

2.1.1 NGN Network Interconnection

Packet-based networks provide opportunities for enhanced services and reduced costs. The method for interconnecting packet-based networks in the NGN should be through the use of packet-based interfaces. If these packet networks must be interconnected in the interim using TDM and ISUP, then the value of these networks is -- at best -- limited. Network interconnection using packet-based interfaces can address this issue and dramatically increase the value of the NGN. Packet-based interconnection scenarios will increase the importance of an effective and secure mechanism for seamless control and management of network services, as discussed in 2.4.

Services must operate seamlessly across NGN infrastructures provided by multiple network providers. Interconnection should extend to security, OAM, and restoration and repair with the goal of providing consistent service quality end-to-end, improving security and billing/accounting, and reducing operating costs. Providing robust, scaleable, billable, QoS-enabled, and service transparent interconnection arrangements between network providers will require significant enhancements to the definition, specification, and operation of trust-based networks.

The *ATIS VoIP Work Plan* recognized that agreement on protocols and profiles is a necessary part of specifying packet interconnection, but it will not provide sufficient detail for a complete specification (even if this is restricted to a SIP-based carrier packet interconnect). The way in which signaling protocols are implemented in a network and the way services are provided (at least at the interconnect point) must also be specified (either explicitly or implicitly) to provide a full interconnect specification. The network context and service definition for SIP-based interconnect, in essence, provides the architectural framework for a packet-interconnect specification. The main architecture options for SIP-based carrier packet interconnect have been discussed in detail by the VoIP FG in 2.3 of the *ATIS VoIP*

Work Plan This Work Plan also proposes an action plan, which can provide the basis for this work item in the NGN-FG.

The *ATIS VoIP Work Plan* focuses on voice services, but many of the concepts therein can be applied to other services, including VPN, multimedia, and video.

Other areas for consideration are:

- QoS measurements;
- Performance measurements and agreements;
- Robustness, reliability, redundant interfaces, and failover;
- Monitoring;
- Security and trust management;
- Inter-provider Security incident resolution;
- Inter-provider accounting support;
- Default codecs and trans-coding for end-to-end voice and video services;
- IPv4 to IPv6 migration and interconnect;
- ENUM;
- Access to shared directory information.
- Interconnection of services for people with disabilities

In addition, there might be different interconnection and interworking requirements for different service providers. For example, interconnect between two network service providers will require different interfaces and agreements than an interconnect between a network service provider (*e.g.,* ISP) and an application service provider (*e.g.,* email or content provider).

Physical layer network interconnection requirements include, but are not limited to, safety, mechanical (*e.g.,* connectorization), electrical (*e.g.,* waveform and pulse masks), and timing (*e.g.,* bit-rate, jitter, wander, frequency offset).

2.1.2 Interface between Application Service Providers (ASP) and Next Generation Service Providers (NGSP)

For the purposes of this section, an ASP is a business entity that offers application services to its customers via the NGSP and uses communications services offered by the NGSP. Thus the ASP depends on the NGSP for offering services to its customers.

The ASP does not necessarily provide packet transport for customers although it might relay information between customers of the application service.

For example, in the current Internet model, an ASP providing email services to customers (both send & receive) might relay email between customers; however, it wouldn't route IP packets between customers based on IP address. In addition, an ASP typically would provide a value added service to users of an application that requires manipulating the information; for example, the email provider might provide an anti-spam service that filters email based on user-provided criteria.

A different example would be an ASP providing conferencing services. In this case the ASP would terminate the media streams (*i.e.*,, IP packet flows), mix them and send them back out to the participants. In this case, the application information is the media stream and its control protocols.

A complete list of applications provided by an ASP in the NGN model is not attempted here. New applications can be invented and provided over the NGN via software installed at each endpoint without requiring modifications to the NGSP's network or services. Examples of applications currently offered by ASPs over the Internet include email, gaming, e-commerce, web hosting, content caching, etc.. Examples of application services that ASPs could provide over the NGN in the future include web services, grid networking, etc.

The services provided by the NGSP to the ASP can be divided into several categories:

- *Transport services*: The NGSP can provide services that enable the ASP to communicate with its customers efficiently. That is, the NGSP can provide services affecting the transport of packets between the ASP and its customers. For a concrete example of transport services, see the A10 interface in DSL Forum TR-058. Examples of NGSP transport services include:
    - *Basic transport (e.g., best effort):* The NGSP provides connectivity from its network to the ASP. This would include address space, routability, and packet transport.
    - *Quality of Service:* The NGSP could provide varying levels of QoS to the ASP for communicating with its users. This could include basic reliability, differentiated services or dynamically requested QoS. The ASP or the ASP's customer could request the QoS. The NGSP could maintain a business relationship with the ASP such that the cost of the QoS is bundled into the ASP's service. An example of such a service could be video or audio streaming service. When the customer requests a particular audio/video stream, the ASP could generate the request for QoS from the NGSP in the direction from the ASP to the customer. The customer may not even have to know QoS is being used.
    - *Differential Routing*: Transport resources could be reserved for specific customers, specific traffic types, specific times, etc.
    - *Security services:* The NGSP could provide services that enhance the security and operation of the ASPs service.
    - *Multicast services:* The NGSP could provide a multicast service to the ASP. This could provide advantages to the ASP in terms of efficiency of usage of the ASP's bandwidth as well as provide services to the ASP's customers.
    - *Anycast services:* The NGSP can provide anycast services for the ASP resources, such that a resource will exist in multiple locations but appear to have a "close" locator address.

- *Mobility:* The NGSP can provide network capabilities to allow the ASP's customers to access the service independent of access and location. For example, the NGSP could provide Foreign Agent support for Mobile IP.
- *Emergency services:* If the ASP (*e.g.,* PSAP) provides services for Emergency Services, the NGSP can provide the transport prioritization for the packets to be transported in an emergency.
- *Accounting:* The NGSP can provide basic packet accounting information to the ASP (*e.g.,* based on IPFIX info).
- *Usage and Performance:* The NGSP could provide information to the ASP detailing network usage and performance metrics.

♦ *Application Services*: Application services are services offered that operate above the transport of packets. This may include support functions for the transport of packets (and may be included as part of a Transport Service described above) or participation in the application protocols. Examples include:

- *Domain Name System (DNS) Service*: This service would normally be included as part of the basic transport service (see above). However, DNS actually operates as an application running over the basic transport. It is probably the most widely used and successful application service on the Internet. While this service may be bundled into a basic service package, it is possible that enhanced DNS services can be offered.
- *Authentication and Authorization Mechanisms:* The NGSP can provide services that assist the ASP with Authentication and Authorization of customers.
- *Location & Presence:* The NGSP could provide a Location and Presence service to ASPs for its customers. When the user connects to the network, in addition to the Authentication or Authorization info, the NGSP could pass along location information and presence information to a subscribed ASP.
- *Network-Based Storage.* For the use of such applications as global grids, the NGSP can provide transient or long-term storage services.
- *Emergency and Public Safety Services:* the NGSP could provide capabilities that support emergency and public safety services *(e.g.,* can provide geo-location, identity & other call info to a PSAP ASP).

See section 2.3 for further application examples.

A NGSP can choose to bundle a subset of transport services and application services together for particular service offerings. For example, basic transport, basic DNS and AAA can be bundled for a basic connectivity package to an ASP.

In the Internet, new services, applications and markets have been originated by customers of Internet Service Providers (*e.g.,* WWW, Peer-to-Peer networks, e-commerce) that have created new business for ISPs and added value to the Internet. Similarly, given a fertile ground to grow, new services will originate from customers of the NGSP. The ASPs offering these new services could begin by using

Transport Services from the NGSP to connect to their customers and then migrate to Application Services as the services and markets mature. Alternatively, the NGSP can introduce new services to its customers that will generate new markets and ASPs (who will then purchase services from the NGSP) as the markets mature.

The following service enablers are required for ASP support in the NGN:

- *Basic transport (e.g., best effort):* The NGN must provide connectivity from the ASP's customer to the ASP. This includes provision of address space, routability, and packet transport.
- *Quality of Service:*
  - The NGN should support provision of QoS to the ASP for communicating with its customers & partners.
  - The NGN architecture should support both differentiated services (*e.g.,* diffserv) and dynamically requested QoS to the ASP for support of its customer's partners.
    - The NGN architecture should support requests for QoS for sessions between the ASP & its customer from the customer or the ASP.
- *Differential Routing*: The NGN should support reservation of transport resources for specific customers, specific traffic types, specific times, etc. from the ASP.
- *Security*: The NGN should provide services that enhance the security and operation of the ASPs service. This includes, but is not limited to:
  - Availability
  - Cryptographic Services
  - Denial of Service (DoS) (or other attack) detection and mitigation, etc.
  - Packet filtering based on parameters provided by the ASP
- *Multicast:* The NGN should provide multicast capability to the ASP. This includes support of multicast routing as well as the ability for ASP customers to join and leave multicast groups for services offered by the ASP.
  - The NGN should provide anycast services for ASP resources, such that a resource will exist in multiple locations but appear to have a "close" locator address relative to an ASP's customer.
- *Mobility*: The NGN should provide network capabilities to allow the ASP's customers to access the service independent of access and location.
- *Emergency Services:* The NGN should provide the transport prioritization for the packets to be transported to/from an (emergency services) ASP in an emergency.
- *Accounting:* The NGN should provide accounting information to an ASP. This should include at least:
  - Packet flow-based accounting information
  - Session accounting information

- *Usage and Performance*: The NGN should provide information to the ASP detailing network usage and performance metrics.
- *Domain Name System (DNS) Service:* The NGN should offer reliable DNS services including, but not limited to:
  - *DNS hosting for ASPs, including:*
    - Run DNS for a zone, including both primary and secondary DNS servers
    - Run a secondary server for a zone
    - Registration of domain name in DNS
  - *Secure DNS service for ASPs, including but not limited to:*
    - DNSSEC
    - Key management for zones
    - Physical security of hosted DNS servers
    - Network security of hosted DNS servers
    - Hosting PTR records for ASP's IP address block
  - *ENUM support including but not limited to:*
    - NAPTR hosting for ASPs phone numbers under e164.arpa
    - NAPTR hosting under ASP private domain
  - *Hosting of future services based on DNS (new Resource Records)*
  - The NGN should allow the service provider to utilize DNS services offered by ASPs in partnership with the service provider; for example, the ASP could provide DNS hosting for the NGSP's customers including the examples described in the previous bullet item.
- *Authentication and Authorization Mechanisms:* The NGN should provide services that assist the ASP with Authentication and Authorization of customers. This includes but is not limited to:
  - *Connectivity status:* The NGN should be able to support notification of an ASP's customer's connectivity status to the ASP.
  - *AAA proxy:* The NGN should support proxying of Authentication, Authorization and Accounting to the ASP.
- *Location & Presence:* The NGN should provide a Location and Presence service to ASPs for the ASPs customers. When the user connects to the NGN, in addition to the Authentication or

Authorization info, the NGN should support passing of location and/or presence information to a subscribed ASP.

- *Network-Based Storage:* The NGN should support transient or long-term storage services for the use of applications such as global grids.
- *Emergency and Public Safety Services:* The NGN should provide capabilities that support emergency and public safety services (*e.g.,* provide geo-location, identity & other call info to a PSAP ASP).
- *Policy*: Appropriate policies will be required to configure the equipment to support the required QoS and other subscriber preferences
- *Media Resource Functions*: Interactive voice sessions are expected to support the required in-band tones and announcements similar to existing telephony services for the foreseeable future. These in-band tones and announcements can be provided either by the NGSP or by the CPE (stimulated by an out-of-band message from the NGSP).
- *Session Management:* The NGN should support session management services for ASPs. Also, the NGN should support the capability for the ASP to pass session management information transparently to the NGSP. The NGN should also support the capability to provide session management services for ASPs and allow the ASP and its customer to exchange private information inside the session management messages (*e.g.,* using SMIME).

2.1.3 Mechanism to Measure and to Predict Service Quality

The NGN should include mechanisms to measure and to predict service quality. Measurements can be made by intrusive or non-intrusive mechanisms.

2.1.4 Public Service Provider (Fixed & Mobile) Convergence

The NGN must support effective wireless/broadband integration. Specifically, NGN services should be able to be accessed from all types of access networks, including copper DSL, broadband fiber, wireless LAN, cellular wireless, etc.

It will be a requirement that users have the ability to access and use their communications services and network-stored information (service settings, personal data, archives, etc.) from anywhere, any technology, any network, and any device (subject to the inherent service limitations of the access and device). Services (*e.g.,* Internet access or video distribution) should operate seamlessly across wireless and wireline networks in an NGN infrastructure.

NGN convergence can be defined from the user's perspective as the ability to access and use communication services regardless of location, across multiple access technologies, using any of a

variety of terminal devices. This definition represents the ideal. The reality will be gradual evolution towards that ideal.

NGN convergence -- in the broadest context of mobile, broadband integration -- supports a fundamental shift towards an end-user-centric world allowing end-users access to their services from any combination of device and access medium while maintaining a consistent personal profile (*e.g.,* service subscription, personal preferences, single billing, etc.). This transition enables a wide list of new service opportunities, but identifying the most-likely successful services among such a list requires a new way of segmenting the market to better understand end-user needs.

Today, end-users are approached by the telecom industry in a very fragmented way:

- Separate identities for fixed, mobile, broadband, and Internet services (*e.g.,* fixed phone number, mobile phone number, multiple IM-IDs, multiple email addresses, etc.).
- Separate interactions with the service providers (*e.g.,* subscriptions, billing, customer care, etc.).
- Separate service capabilities depending on device used or means of access (*e.g.,* in terms of messaging -- SMS, MMS, IM, email, voice mail, etc.).

Such a fragmented approach may be attributed to external forces shaping the telecom industry, including rapid technology evolution and regulatory changes. However, a result of this fragmented approach is unnecessary complexity, frustration, and cost for the end-user. Given ongoing technological evolution associated with fixed and mobile broadband, VoIP, and the like and the corresponding market dynamics associated with threats of substitution or competition, it is expected that successful service providers will shift from the network-centric to an end-user-centric model.

An end-user-centric market means:

- The emergence of a new generation of end-user services (communication, content, and application) enabled by broadband, without the traditional restrictions of separate networks.
- The capability for end-users to have access to any service over any appropriate access means/device.
- A shift towards service delivery in an end-user-centric way, with a single personal profile (single subscription, single preferences, settings, single bill, etc.) being a key service component.

The new generation of end-user services will consist of innovative combinations of:

- *Communication services:*
    - Voice, text and video conferencing with IM.
    - Messaging interoperability via any device (SMS, IM, email,).

- Video, text and voice communication, conferencing and online multimedia collaboration.
- Content conversion: (e.g. relay services for translating between languages and different media (sign language, text, voice).

- *Content and applications:*
  - *Entertainment:* Gaming, music, broadcast television, on-demand video and interactive services.
  - *Commerce:* Shopping.
  - *Information:* News, traffic.
  - *Productivity:* Intranet Access, VPNs.
  - *Automation:* Home/car/pet security, surveillance, child monitoring, managed homes for elderly care.
- *A personal profile across different access media and end-user devices*.

The convergence of fixed and mobile infrastructure may require additional media resource functions such as the need for transcoding between different speech codecs (such as EVRC in a 3G handset ↔ G.711 in an IP landline phone).

2.1.5 Public Service Provider (Fixed & Mobile) and Customer Premises Network Convergence

NGN services should operate seamlessly and transparently across public mobile/fixed and customer premises networks in an NGN infrastructure. For instance:

- A member of an enterprise can easily, efficiently, and securely access critical enterprise data from a visited location (another person's phone) or from a mobile phone.
- A user with a dual-mode handset that operates as a WiFi cordless phone in the building and a 3G handset outside the building can maintain a telephone conversation continuously while moving in and out of the building.
- A wireless mailbox is accessible from a customer premises network such that a user has the flexibility in selecting the way to retrieve mail based on the networks available.

In more general terms, seamless operations of NGN services across mobile/fixed and customer premises networks imply:

- A user in a public network can communicate (via VoIP, Push-to-Talk, Short Message, or the like) with another user in a customer premises network possibly using a device of a different type (*e.g.,* a multimedia PC versus a 3G handset), and vice versa.
- A user in a public wireless network can maintain existing communication without the associated session or connection being dropped while traveling from the public wireless network to his or her premises network (CP terminal and session mobility), and vice versa.
- A user of a customer premises network can have access to the network and applications remotely through a public network (CP VPN and terminal mobility).
- A user can have access to applications in a public network from his premises network.

In the scenarios above and possibly others, normal expectations of QoS, security, OAMP, etc. are met.

Customer premises networks have made use of diverse technology from user terminals (*e.g.,* IP phones, IP-PBXs, laptops and PDAs) to networking methods (*e.g.,* DSL, Cable, Ethernet, Bluetooth, and WiFi). Given that the trend is expected to continue, full integration of wireless and customer premises network should address, among other aspects:

- Interworking of different types of networks (such as UMTS and IEEE 802.11b), including reconciling any disparities in authorization, authentication and accounting schemes.
- Traversal of firewalls and NAT devices across network boundaries.
- Transcoding between different speech codecs (such as EVRC in a 3G handset ↔ G.711 in an IP landline phone).

2.1.6 Access Criteria for NGN Conformance

The definition of IP Connectivity Access Networks (IP-CAN) is currently being standardized by 3GPP ETSI TISPAN and ITU-T. ATIS will continue to monitor this work.

One of the key objectives of the NGN is having services independent of access; *e.g.,* the ability to use a range of technologies for the IP-CAN. The NGN will place interface requirements on the IP-CAN for any access technology to be included as part of the NGN. An IP-CAN deployment that does not support these requirements may not realize the full set of NGN capabilities. Any IP-CAN that meets these requirements shall be supported by the core IMS network, although it may not support all NGN services. For example, a low bandwidth IP-CAN might support voice services but not video. Similarly, a high latency IP-CAN might support non real-time services, but not interactive voice and video.

The IP-CAN is a subset of the NGN. As the NGN evolves, the IP-CAN may need to evolve as well. Based on the current concept, the anticipated IP-CAN requirements necessary to conform to the NGN architecture include:

- *The IP-CAN shall provide IP transport.* The IP transport may be provided over lower layer technologies (*e.g.,* ATM), but the IP-CAN must present an IP interface to the NGN core transport network, and to the UA in the user terminal.

- *The IP-CAN shall support the provision of QoS consistent with the end-to-end objectives of ITU-T Recommendation Y.1541.* It is recognized that QoS classes of various access technologies may have unique requirements (*e.g.,* 3GPP TS 23.107 "UMTS QoS classes") which must be considered.
- *If the IP-CAN provides encryption at the transport level, it shall only be provided across the IP-CAN, or a portion of the IP-CAN (rather than end-to-end).*
- *The IP-CAN may provide a mechanism to permit or deny a session,* based on the user and the service.
- *If mobility management is provided by the IP-CAN, it shall be done in a way that is consistent with the NGN core.*

2.1.7 Infrastructure Evolution for Incremental Replacement of Legacy Services

The NGN will replace today's telecommunication services (*i.e.,*, "legacy services") over time, although this is not the primary objective of the NGN. The primary service objective of the NGN is to create an open service environment that will support the efficient introduction of new, revenue-generating multimedia services. In this sense, the NGN has three service goals:

1. *Support for converged multimedia services*, based on the 3GPP IMS (SIP based) architecture;
2. *Support for Interconnection and interoperation with the existing PSTN.* This requirement is likely to be an important capability of the NGN for some time. The PSTN requires certain capabilities and functions in connected networks for such areas as security, accounting, etc. To the extent an NGN expects to interwork with the legacy PSTN, including sending or receiving calls to PSTN users or accessing resources in the legacy PSTN, the NGN will need to support appropriate functionality. The necessary capabilities for the NGN to interwork with the PSTN can have implications in the NGN beyond the edge device that provides connectivity to the PSTN; and
3. *Support for legacy services and terminals.* This requirement is not simply based on the need for the NGN to eventually replace the legacy PSTN. There is also a requirement to decouple the replacement of the PSTN network infrastructure from the replacement of PSTN services and terminals. There may be a need for some existing PSTN services to continue to be supported indefinitely, with exactly their current functionality. If the IMS based NGN does not transparently support these services, this could either delay the replacement of the PSTN infrastructure, or force long-term costs into the target network simply to support transient (legacy) service requirements.

It is important that these two goals be kept distinct. If they were to be merged, it is likely that the resulting solution would not be optimal for either goal. It could lead to gaps in the legacy service coverage, and to unnecessary complexity in the target NGN. The NGN will contain distinct subsystems to support:

1. SIP-based multimedia services; and
2. Legacy PSTN services.

These subsystems should share common standards and infrastructure to the extent that this does not compromise the primary objective of optimizing each subsystem for its primary role.

2.1.7.1 PSTN Simulation

The defining characteristic of the PSTN Simulation subsystem is that this subsystem fully complies with the extended IMS standards and service model. This may include extensions to the pure SIP model that have been specified for carrier use (*e.g.,* P-headers).

There will be a desire by some operators to introduce services that are similar to existing PSTN services. These services may even be essentially the same as the existing services, though not necessarily identical in all respects. These services can be provided by the PSTN Simulation subsystem, using capabilities native to extended IMS.

The PSTN Simulation subsystem may use existing PSTN services as a model in an attempt to provide similar services. Existing services could be analyzed to determine if they can be supported, and to identify possible extensions to the SIP standard (new headers or parameters) to more closely replicate the existing services. Proposed extensions could be fed into the regular standardization processes for consideration. However, these will only be added to SIP if they make sense from an extended IMS perspective. There can never be a hard requirement for the PSTN Simulation subsystem to provide a service identical to an existing PSTN service (*i.e.,* PSTN service transparency), as that is the defined role of the PSTN Emulation subsystem.

2.1.7.2 PSTN Emulation

The defining characteristic of this subsystem is that it transparently supports legacy PSTN services, and -- with a suitable terminal adaptor -- legacy PSTN terminals. Therefore, if a service has a hard requirement that it must provide PSTN equivalence and transparency, then this service must, by definition, be supported by the PSTN Emulation subsystem. It is possible for these services to also be supported in the PSTN Simulation subsystem, or even in the extended IMS, but this support must be an "objective" rather than a "requirement."

The ATIS NGN-FG position is that the primary focus of the PSTN Emulation subsystem is to support SS7 based PSTN services and terminals (via a suitable gateway or Terminal Adaptor) in a fully transparent manner. A PSTN based user must not be able to distinguish between a call made to another PSTN user, and a similar call made to a PSTN Emulation subsystem user.

The PSTN Emulation subsystem should use the same standards and capabilities as the extended IMS, to the extent practical while still satisfying the primary requirement of PSTN transparency.

2.1.7.2.1 TDM Replacement

TDM network replacement is a subset of the requirements for the PSTN Emulation subsystem. The NGN must have the capability to replace the existing TDM network, and to emulate PSTN services. This is required to ensure an effective migration from the existing PSTN to the NGN. This does not mean that the initial focus of the NGN will be existing TDM services, or that it must provide legacy services immediately, or indefinitely. Initial NGN services will be driven by market requirements.

When the NGN is emulating existing PSTN services, it should not be possible for users to determine whether the service is terminating on the existing PSTN, or being emulated on the NGN.

2.1.7.2.2 Voice Band Data and Relay

Voice Band Data is a subset of the requirements for the PSTN Emulation subsystem. Though voice-band data is normally associated with fax and modem transmissions carried in 3.1kHz analog channels at 64kb/s, a wider scope must be considered by the NGN. This wider scope also includes DTMF signaling, Telephone Devices for the Deaf (TDD), and ISDN B-channel circuit-switched data. While DSL or other forms of digital broadband access will supplant high-speed modem for Internet access in a true NGN deployment, the requirement to support all other voice-band data transmission types carries forward from the PSTN to the NGN. Fax continues to be used for its ability to send hand-written forms and signatures; low-speed modems are widely used by point-of-sale terminals and security systems. DTMF entry is fundamental to IVR and voice mail systems, and is also used by home security systems. The transport of text telephone (TTY) signals will continue to be a requirement in support of TDDs. Finally, NGNs providing tandem switching for legacy Class 5 switches or including access gateways to host analog Plain Old Telephone Service (POTS) lines, must support high-speed modems. Given these requirements, the NGN must include adequate provision for providing reliable transmission (equivalent to the PSTN) of voice-band data signals. Based on business decisions and regulatory requirements, a NGSP might choose not to support all of these services.

Two basic methods exist to transport voice-band data over IP, PCM-based transmission and relay. The first involves transporting voice-band data using the mechanisms specified in ITU-T Recommendation V.152 (targeted for consent by the end of 2004). Relay, on the other hand, involves the demodulation of the analog signal to transport the raw data over the IP network and then re-modulation at the far end. The bandwidth reduction that results will typically allow use of redundancy to withstand packet loss.

2.1.7.3 Mobile Network Evolution

The NGN should support mobile network evolution as defined by 3GPP and 3GPP2. Wireless service provider networks may be at any stage. The requirements to achieve convergence will differ depending on which stage is deployed.

Given the likelihood that softswitch functionality will be deployed prior to a complete IMS-based architecture, mobile network evolution is likely to leverage that functionality as a starting point. Further definition of these functions and a more complete view can be found in the Annex A.

2.1.8 Transparent, End-to-End Communication

End-to-end applications should be able to run transparently over the NGN. However, it is recognized that there may be a conflict between end-to-end transparency, and network services such as those in 2.3. Because of this there are challenges in achieving end-to-end transparency. These are discussed in the gaps clause of this document.

The NGN should continue to offer backwards compatibility to best effort Internet applications. Applications requiring additional network performance or functionality may require additional network services.

2.1.9 Other Services

Other services may also be offered by the NGN over time. In many cases, these services will be tunneled through the NGN, or simply rely on the NGN as a transport service. For example, some LAN services (*e.g.,* point-to-point Ethernet relay services) may become available in the WAN via the NGN. While such tunneled or emulated services may be useful adjuncts to the NGN service repertoire, they are not the main driver for NGN functionality in the short term.

2.1.10 Guiding Principles for Services in a Converged Network

It is important that the technology for developing services should be network and application protocol independent. There are several reasons for this:

- It is not economical to deploy a multiplicity of development and delivery environments.
- It is not economical to deploy separate physical networks for each service as they are rolled out.
- Service development and delivery technologies that are tightly coupled to specific networks and protocols violate the software engineering practice of "separation of concerns." The service developer should concentrate on what's delivered to the user, not how that service is implemented in a particular network.
- The infrastructure that gives users a converged experience can be expected to be a mix of both IP and non-IP technologies for the foreseeable future.
- Service creation could be done by any third party developers (*e.g.,* from the IT environment), and not just by trusted developers working directly within the telecom environment.

Service capabilities are accessible by applications and end users through APIs. Applications can be under direct management of the NGN provider or can be provided by third parties. APIs capture service capability features. For example, OSA/Parlay X specifies web services APIs for Third Party Call, Network-Initiated Third Party Call, SMS, Multimedia Message, Payment, Account Management,

User Status, and Terminal Location services. APIs are not limited a priori regarding the nature of the service capability features they support. In particular, these can be session-based or transaction-based.

The Parlay/OSA model should be given consideration as an appropriate model for the face that's presented to the outside world. As a practical example, consider the TCP/IP protocols. Vast numbers of developers can say they know how to write applications that run on TCP/IP. But nearly all of those programmers see little or nothing of the underlying protocols. They see APIs that abstract those protocols -- the well-known sockets libraries in UNIX or Java class libraries, for example. Parlay/OSA and its descendants could play a similar role for NGN services. In particular, 3GPP OSA Release 6 has defined several service interfaces based on Parlay X Web Services. The web services[6] framework adds a level of abstraction and flexibility to service creation. Parlay X Web Services can be published through a registry, making them available for discovery.

While SIP is the core signaling protocol in IMS, it should be as transparent as possible to application developers. SIP application servers will continue to play an important role in providing services. The development of APIs that abstract protocols generally lags behind the development of those protocols. This is especially true for a protocol that is as extensible as SIP. Nevertheless, the goal should be to bring new capabilities into a higher-level API such as Parlay/OSA.

In order to fulfill their role and depending on the services requested, service capability servers can access IMS components such as S-CSCF, HSS, PDF, and Media Resource Functions (MRF). Interactive Voice Response (IVR) systems, announcement systems, and media servers are examples of MRFs.

2.1.11 Synchronization and Timing Issues

Synchronization and timing requirements for the NGN are for further study.

Historically, synchronization and timing has often been an afterthought, investigated when the QoE (Quality of Experience) of the end-user dropped below an acceptable level. The modern PSTN is well synchronized; with the majority of digital network elements provided a timing reference traceable to a Primary Reference Clock -- mainly because without a "common clock" there were significant problems with voice-band modem performance particularly. The advent of ISDN reinforced the need for good network synchronization. The preponderance of customer premise equipment connected to the network over digital facilities (especially E1 and T1) utilizes the network feed as a timing reference source. Good synchronization is an enabler to elevate performance from mediocre (at best) to carrier-class. Wireless operators have found that attention to good synchronization resulted in fewer dropped calls and customer complaints. It is unlikely that the need for good synchronization will become moot with the advent of NGNs.

Whereas it is the goal to separate services from transport, there are some facets of the underlying physical layer, usually associated with the transport segment, that impact the perceived quality of the

[6] Other standards bodies active in developing web services standards include W3C and OASIS.

service. Synchronization is one such facet and must be considered up front rather than as an after-thought. Samplings of some of the areas where synchronization and timing will need consideration are listed below:

- *Multi-Service Provisioning Platforms (MSPPs)* will be an important building block in NGNs. These need a good synchronization reference, especially if they are used in circuit emulation services.
- *All wireless base stations (Node Bs in 3G parlance) need good synchronization*. This will be especially important if hand-offs are to be made between "wireless" and "wired" stations.
- *All network elements terminating SONET/SDH facilities need good synchronization.*
- *All cross-over points, such as circuit-packet boundaries and analog-digital boundaries will need good synchronization.*
- *All TDM networks inherently need good synchronization*. When a packet segment is interspersed between two circuit-switched segments the increased delay will mandate improved echo return loss enhancement. Slips in the circuit-switched segments will bleed over as echo "blips", and thus it may be necessary to tighten the stratum level requirement of holdover in the remaining circuit-switched segments.
- *Synchronization distribution in the legacy network is hierarchical*, with timing carried over the transport network (typically SONET/SDH) from a PRS-equipped site to subtending nodes. Replacement of facilities with asynchronous methods that cannot carry a timing reference reliably will break the hierarchical distribution model. This is readily addressed by greater proliferation of Primary Reference Sources (PRS).
- For QoS enabling and monitoring Time of Day will be required.

2.2 U.S. Regulatory Requirements:

The regulatory requirements are, to a certain extent, a moving target with evolving legislative and regulatory actions by the governmental bodies of various jurisdictions. In many cases, regulations are service specific, with traditional telecommunications services having a larger regulatory footprint than newer services; for example, voice (telephony) services have a larger footprint of regulatory action and case law than newer services such as instant messaging. The regulatory classification of specific services (*e.g.,* basic telecommunications services vs. information services) significantly impacts the requirements for those services. A number of regulatory requirements have developed from this legacy of voice services, and these regulatory requirements may expand to affect NGN services.

2.2.1 Lawfully Authorized Electronic Surveillance (LAES)

2.2.1.1 U.S. Regulation

The Communications Assistance for Law Enforcement Act of 1994 (CALEA) requires carriers to provide certain electronic surveillance capabilities to law enforcement agencies. Standards work in support of this was performed jointly by ATIS and TIA committees in the Lawfully Authorized Electronic Surveillance (LAES) *ad hoc*, which published a series of standards referred to as J-STD-025. ATIS PTSC and Wireless Technology & Systems Committee (WTSC) have also published American National Standards T1.678 and T1.724 that are concerned with LAES for VoIP in a wireline environment and with LAES for data in a GSM environment, respectively.

2.2.1.2 LAES Industry Direction

The *ATIS VoIP Work Plan* identifies potential work on LAES for ATIS committees.

The NGN LAES service provides the capability for the NGN operator to extract reasonably available information related to a particular subscriber requested in a court order and provide the requested information to one or more Law Enforcement (LE) agencies expeditiously. The information provided can consist of the traffic delivered to or received from the subscriber, call-identifying information, or both.

The intercepted information should be provided in a format that can be delivered electronically to LE.

Only personnel authorized by the network operator for such purposes should have access to this information and only they should have knowledge of the existence of the intercept. The Security Focus Group Work Plan has identified security concerns relative to the protection, in a carrier's network, of the surveillance operations/information in the fulfillment of the court order (see clause 1.6 of the *ATIS Security Work Plan*).

As new services and capabilities are defined for the NGN, consideration should be given as to whether or not new capabilities are required for LAES. Some services may be required by the FCC to support LAES.

2.2.2 Number Portability

2.2.2.1 U.S. Regulation

Number portability is a network capability that allows a NANP telephone number associated with an end-user to be moved from one serving switch in a network to another serving switch in the same or different network without changing the association between the end-user and the number.. In the U.S., only service provider portability is required of most telecommunications service providers. Location portability (which allows an end-user to change its location while retaining the number) and service portability (which allows an end-user to change service while retaining the number) are not required in the U.S. However, certain services are being implemented today by some service providers that blur

this distinction between types of portability. The *ATIS VoIP Work Plan* identifies ongoing work in this area.

2.2.2.2 Industry Direction

Number portability has had significant impact to both wireline and wireless end users. Some VoIP providers are offering any U.S. NANP number to be used anywhere in the country or world as an option. This capability is a function of the VoIP service, not of the number portability function itself. This capability is providing a flavor of location portability that had not previously been available in the U.S. Thus, the continued use of geographic numbers in areas outside of the expected geographic area may be a growing trend with NGN service providers. Previously in the wireline PSTN, number portability was limited to porting a number within a rate center; however, with wireline to wireless portability a wireline TN can be ported to a wireless service provider within the LATA rather than within the rate center. It remains to be determined how these aspects may or may not be applicable within an NGN architecture.

2.2.3 Number Pooling

2.2.3.1 U.S. Regulation

Number pooling is a number administration and assignment process that allocates numbering resources to a shared reservoir associated with a designated geographic area such that blocks of Directory Numbers (DNs) smaller than an entire NXX code are available for assignment by service providers. Thousands-Block Number Pooling shares an NPA-NXX among service providers by allocating numbers in thousands-blocks from the same NPA-NXX to service providers offering service within the same rate center. The Location Routing Number (LRN) Number Portability mechanism is used to correctly route calls to subscribers assigned a directory number within a pooled thousands-block. Only service providers capable of number portability can participate in number pooling. Thousands-Block Number Pooling has been mandated by the FCC in the U.S. in the Top 100 Metropolitan Statistical Areas (MSAs). The *ATIS VoIP Work Plan* identifies ongoing work in this area.

2.2.3.2 Industry Direction

Number pooling may have significant impact to users served by a VoIP technology service provider. VoIP providers are in some instances participating in pooling today. Some VoIP providers participate directly in pooling and others only via underlying carriers. Given the ability, noted above, of VoIP providers to assign geographic numbers to end-users outside of the geographic rate area associated with the NXX code that is pooled, it remains to be determined how these geographic limitations on number pooling may or may not be applicable within an NGN architecture.

2.2.4 E 9-1-1

2.2.4.1 U.S. Regulation

In the United States, the three-digit number "9-1-1" has been designated as the "Universal Emergency Number" to request emergency assistance. Today, most of the U.S. population is covered by the "Enhanced 9-1-1" service. Enhanced 9-1-1, or E9-1-1, directly connects the caller to the Public Safety Answering Point (PSAP) serving the geographic region from which the caller is calling. The E9-1-1 service provides the PSAP call-taker with the telephone number and physical address of the caller as well as the specific police, fire, and EMS for the caller's location. The *ATIS VoIP Work Plan* identifies ongoing work in this area by ATIS ESIF.

2.2.4.2 Industry Direction

In today's network, E9-1-1 service is provided through a complex cooperative effort between the telephone service provider, the 9-1-1 service provider, and the State or local government jurisdictional authority. Accuracy of the data that drives the E9-1-1 service, as well as the continuous availability of the various systems that actually provide the service, are both paramount to providing what is considered to be a "life-critical" service.

The common, converged infrastructure that characterizes the NGN provides both an opportunity for further improvement of the E9-1-1 system and poses a significant challenge to maintaining the status quo. Potential improvements enabled by the NGN and by advances in information technology may include faster emergency call setup, simultaneous delivery of both voice and location data to the PSAP, and integration of rich media like building layouts, maps, etc. Such improvements may also result in more efficient utilization of PSAP resources and more cost effective connectivity. The NGN architecture must enable interworking with the legacy E9-1-1 network for an indefinite period of time. NENA has initiated a Next Generation E9-1-1 program and is currently working with ATIS ESIF in developing requirements for packet-based networks.

For 9-1-1 calls utilizing the IMS-based service, the NGSP must be able to determine the physical location of the caller (to the extent possible given trans-jurisdictional mobility and nomadicity), and must work in a cooperative manner with the PSAPs and 9-1-1 jurisdictional authorities to determine the correct routing treatment for that caller given the location. The NGSP should provide QOS and reliability for 911 calls consistent with or better than currently available on the PSTN.

The inherent mobility afforded by the NGN poses significant challenges for E9-1-1, particularly with regard to pinpointing the current location of the calling device, routing the emergency call to the correct PSAP (based on the caller's current location,) and providing that location to the PSAP. Mobility across facility providers or service providers must not (within reason) inhibit the caller's ability to contact the correct PSAP during an emergency. However, given the mobility and nomadicity that might be available in a NGN, providing this information may not be possible (*e.g.,* if the user calls 9-1-1 from a foreign country).

There are two specific cases that should explicitly be considered for the NGSP determining location capability:

- The first case is that of a legitimate emergency call where the user is unable to provide accurate location information. This case is a valid emergency call where the subscriber has not overtly attempted to withhold the location information nor attempted to suppress or modify any signal that the network could use to derive accurate location information.
- The second case is that of a malicious call where incorrect location information is provided by the caller to direct emergency services to the wrong location. This case adds the complications that rather than not providing data verbally, the subscriber may verbally provide false information and may attempt to block or spoof signaling such that the NGSP fails in deriving location information or delivers a false location. Obviously, it is unrealistic to expect total protection from malicious calls, but it is realistic to report NGSP derived location for comparison (e.g. by the PSAP operator) with verbally reported location. The PSAP responder could be sensitive to mismatches or network location detection failures, and act according based of local policy.

Finally, NGNSP users may need to communicate with the PSAP during an emergency using communications devices other than telephones. If the user contacts the PSAP using the NGSP's IMS-based service, the NGSP should facilitate initiation of the session with the PSAP and delivery of location information to the PSAP. The NGSP must not inhibit customers that don't use IMS-based services from contacting the correct PSAP in case of emergency and must not inhibit the customer (or customer's equipment) from providing his or her location to the PSAP during an emergency.

The NGN may provide additional services to assure the reliability, accuracy and trustworthiness of the reported location information, in response to evolving NENA and NRIC requirements.

2.2.5 Emergency Telecoms Service (ETS)

2.2.5.1 U.S. Regulation

There is no current regulatory requirement for ETS.

2.2.5.2 Industry Direction

Emergency Telecommunications Service (ETS) is currently under development in ATIS Technical Committees (*e.g.,* PTSC) to provide services somewhat analogous to the Government Emergency Telecommunications System (GETS) deployed in the PSTN.

The NGN can facilitate the creation of ETS that can significantly enhance the nation's safety. In particular, the NGN is envisioned to enable improved communication between and among the various

government agencies charged with the protection of the citizens, as well as between these government agencies and the citizens themselves. While E9-1-1 concerns itself with enabling a caller to contact authorities during an emergency, the NGN will provide improved and efficient ways for the authorities to communicate during an emergency.

Providing key officials with a priority calling service, similar to GETS, is critical. The ability for key officials to use the telecommunications system during a crisis, regardless of the type of communications device or access used will help ensure the safety and security of the nation. To ensure that only authorized users can have access to ETS, and to protect network resources from excessive use or abuse, the NGN must support appropriate authentication and authorization mechanisms. In general, these mechanisms should be as strong as possible. The authorization mechanisms should also be flexible enough to provide various levels of restriction and privilege as needed.

The NGN architecture protocols and network elements shall be highly resistant to denial of service attacks or other types of harm that might be perpetrated on the NGN by terrorists or miscreants. Implicit in the idea that the NGN will provide efficient and improved "Emergency Telecom Services" is the notion that the NGN itself is secure, robust, and constantly available for use during an emergency.

As mobility increases, the notion of detecting presence can further enhance ETS by helping to ensure citizens can be contacted who are physically located in an area of interest. Locating and contacting important public officials, regardless of where they might be or which network they might be on, can also significantly improve our nation's ability to respond during a crisis.

2.2.6 FCC Rules and Regulations

The U.S. FCC Rules and Regulations are described in Title 47 of the Code of Federal Regulations (CFR). Other regulatory regimes apply in other countries within the scope of North America. Additional regulations may apply at the state level. It is beyond the scope of this document to presume specific regulatory treatments for specific services in an NGN environment. Of particular relevance for US voice telephony services are the following parts of title 47CFR, which apply to the PSTN. The applicability of these requirements to NGN services remains to be evaluated.

- Part 6: Access to telecommunications service, telecommunications equipment and customer premises equipment by persons with disabilities
- Part 7: Access to voicemail and interactive menu services and equipment by people with disabilities
- Part 22: Public mobile services
- Part 27: Miscellaneous Wireless communications service
- Part 32: Uniform system of accounts for telecommunications companies
- Part 36: Jurisdictional separations procedures; standard procedures for separating telecommunications property costs, revenues, expenses, taxes and reserves for telecommunications companies

- Part 42: Preservation of records of communication common carriers
- Part 51: Interconnection
- Part 52: Numbering
- Part 53: Special provisions concerning Bell operating companies
- Part 54: Universal service
- Part 59: Infrastructure sharing
- Part 61: Tariffs
- Part 63: Extension of lines, new lines, and discontinuance, reduction, outage and impairment of service by common carriers; and grants of recognized private operating agency status
- Part 64: Miscellaneous rules relating to common carriers
- Part 65: Interstate rate of return prescription procedures and methodologies
- Part 68: Connection of terminal equipment to the telephone network
- Part 69: Access charges

As the NGN services extend beyond voice services – *e.g.,* to video and multicast services -- additional parts may apply. NGN services expand the range of personally identifiable information stored by the network operator. Location and identity information, for example, may be the subject of future regulations regarding privacy. Privacy concerns are already an issue regarding the control of updates and disclosure in the context of ENUM. As NGN services include content-based services, and extend into the consumer electronics domain, additional regulations such as the Digital Millennium Copyright Act (DCMA) may result in requirements for various forms of Digital Rights Management (DRM).

In view of the service evolution and consequential market and regulatory evolution, the NGN will require significant flexibility in its architecture in order to support flexible grouping of functions and flexible charging models, as the administrative structure of the operators change in response to market and regulatory evolution.

2.2.7 Accounting

2.2.7.1 U.S. regulations

Various state government agencies (*e.g.,* Public Utility Commissions) have regulatory requirements regarding Intra-state tariffs. FCC Regulations would apply to inter-state tariffs. Taxes and other fees may apply to various commercial transactions with associated requirements for identification and non-repudiation. National Exchange Carrier Association (NECA) rules apply to telecommunication carriers for Universal Service Fund (USF) purposes.

2.2.7.2 Industry Direction

In some cases there may be rules regarding compensation among networks and users that need to be accommodated. In other cases there may be fees or charges due to various governmental agencies, etc. These various rules can require identifying to billing entities the originating and terminating users, their locations, the networks involved, the services used, and the volume and nature of traffic.

2.2.8 Other Mandated Services

2.2.8.1 U.S. Regulations

The FCC has defined numbering resources for various services. The State Governments have in some cases mandated the deployment of these services. The Federal Government may also mandate such services.

2.2.8.2 Industry Direction

There are more services that may be required besides just E9-1-1. Universal Access may require Operator Assistance, Directory Assistance, and Telecom Relay Services (TRS, in many places now accessed via 7-1-1) or their equivalents. Other services that may be required include Community Assistance (2-1-1), Government Assistance (3-1-1), and Transportation Information (5-1-1). As with E-9-1-1, the destination for these additional N-1-1 services is usually dependent on the jurisdiction from which the communication originates.

2.3 End-User Applications

In the current PSTN, applications provided by service providers are typically vertically integrated (*e.g.,* separate networks designed for separate services). In the NGN, applications will be supported on a common, converged infrastructure. The NGN architecture should support the case where the infrastructure is not vertically integrated with the applications and services

New services and applications are expected to require additional functionality from the NGN. The NGN-FG will use selected new applications as use cases to identify requirements for a converged NGN. Particular attention will be given to requirements that are unique to North American service providers. These use cases assume the service is provided by the NGN service provider. It is recognized that some or all of them could be provided by ASPs utilizing the NGN as transport.

2.3.1 Interactive Voice

Voice is an application that, while traditionally associated with PSTN telephony, is an important challenge for IP-based NGNs because of the stringent QoS required to support good voice transmission quality. Indeed, voice is a paradox for IP networks because the per-call bandwidth can be very small

with low bit rate codecs (~8 kb/s), but the stringent delay and jitter requirements are a big challenge for IP networks. Wideband codecs can also be used for higher quality voice over broadband NGN connections.

The requirement for a minimum level of perceived voice quality is independent of the underlying infrastructure.

The most comprehensive treatment of "mouth-to-ear" voice transmission requirements—including specific considerations for the effects of IP networks—has been captured by the ITU-T Study Group 12 (SG12) in its G.100-series Recommendations. This information has been reflected in Recommendation Y.1541, which provides NI-to-NI IP QoS classes, and notes that in order to satisfy the SG12 voice requirements, IP networks should introduce no more than 100 ms of delay, 50 ms of delay variation (jitter), and 1 in 1000 dropped packets. (The "mouth-to-ear" delay that is trying to be satisfied is 150 ms, as per G.114.) As noted in a recent appendix added to G.114, most regional IP-based networks should have no trouble satisfying the 100 ms delay requirement, but long, international paths may have difficulty. As for jitter and packet loss, only well-engineered paths can be guaranteed to satisfy requirements. While "best effort" IP networks may satisfy these requirements for some calls, they cannot make any specific guarantees on a per call basis.

It is worth noting that codecs with better packet loss concealment algorithms are becoming available, and it may be appropriate to re-evaluate the packet loss requirements in the future. In the case of an NGN spanning multiple operators, there is a need for a work item to allocate impairments among the operator networks.

While many of the enablers listed in this section may be required to offer a PSTN-quality telephony service, the NGSP may also choose to offer voice services that don't provide PSTN-quality as defined above or may offer a service that meets a subset of these requirements. For example, the NGN service provider may offer a voice chat service similar to (or integrated with) text-based instant messaging. The NGN architecture must intrinsically support a range of such services.

The following service enablers support interactive voice services in the NGN:

- *QoS levels:* A service provider may distinguish a variety of voice services through the selection of network parameters and level of QoS associated with those services. Measurement and monitoring of end-to-end and/or cross-segment delay can permit the service provider to manage levels of latency and jitter across the network.
- *Presence:* Existences of an interactive voice session may imply presence that can be leveraged with other terminal capabilities for other applications -- *e.g.,* IM. In addition, other presence services may be used to initiate voice or other multimedia sessions.
- *Policy:* Appropriate policies will be required to configure the equipment to support the required QoS and other subscriber preferences.
- *Media Resource Functions:* Interactive voice sessions are expected to support the required in-band tones and announcements similar to existing telephony services. These in-band tones and announcements can be provided either by the NGN service provider's media server or by the CPE (e.g. stimulated by out of band message from the service provider).

- *Media Gateway Functions:.* Transcoding may be required to adapt between codecs.
- *Unified interface and Service Ubiquity:* The user interface, dialing plan, etc., can be preserved through roaming operations to enable wider nomadicity.
- *Multicast:* Voice conferencing may imply the use of multicast to redirect a copy of the session. Other service possibilities include the use of interactive voice terminals to access audio content which may be multicast (*e.g.,* Internet radio).
- *Communication context:* A combination of session state and personalization features enables customized services. As an example, a subscriber listening to an Internet radio session may require that to be turned off when answering an interactive voice session.
- *Nomadicity:* A coherent set of service features should be obtained regardless of the access network through which service is obtained. For example, the same phone number should allow incoming calls to reach you, whether via the mobile network, an 802.11 hotspot, or a home network, without requiring specific user interaction to register with the access network.
- *Location:* Location information may be required in support of a variety of services associated with interactive voice sessions -- *e.g.,* E.911 services.
- *PIM (Personal Information Manager):* The presence information and other communications context data may be logged to the user's PIM.
- *ENUM:* An ENUM translation service may be required to assist in interactive voice sessions that terminate in the PSTN.
- *Service and content discovery:* User devices should be able to quickly discover the servers in the network needed to support interactive voice services.
- *Digital Rights Management (DRM):* The basic conversational interactive voice service does not require additional DRM services, but does not preclude them.
- *Session Management:* Session management allows a user to initiate, set up, and terminate an interactive voice session with multiparty participation.

2.3.2 Content/Capabilities - Video

The NGN is expected to support a number of content-based services. Additionally, the support of multiple discovery/store-fronts and delivery/fulfillment mechanisms must be considered. Multiple media types can be either downloaded or streamed between the media servers and the end terminals. (Note that the media and end user terminals may be in different networks.) The accounting, settlement and digital rights enforcement for the various types of content will need to be given consideration with respect to cross service/content providers. Examples of such services include web browsing, Internet radio, Internet TV, access to various directory services etc. An Internet TV application is interesting because of its potential to illustrate interactions between IP infrastructure functions (*e.g.,* multicast), session control functions (*e.g.,* admission control), and application functions (*e.g.,* contents storage and distribution). Consider a consumer Internet TV application delivered via a bandwidth-constrained DSL access infrastructure, and leveraging multicast within the IP network to minimize aggregate IP

network resource utilization. Such an application would be expected to require the use of several network service enablers:

- *QoS:* Some specific QoS mechanisms would be required in a bandwidth-constrained access. A bandwidth allocation supported by a session based admission control function may be a reasonable assumption. Note that such a dynamic QoS scheme may require changes in QoS policy to be propagated throughout the network infrastructure.
- *Multicast:* For this example, we can assume a source-specific multicast model. Note that the use of multicast is a convenience for the operator to minimize network resources and not an essential component of the service definition. The NGN should respond appropriately whether the content is unicast or multicast.
- *Authentication/Authorization/Identity:* The service must be authorized for a specific facility, or potential identity. More sophisticated individualized authorization models may be required for some variants of the service -- *e.g.*, parental controls
- *Communication context:* The Internet TV stream may be one element within a communication context. Consider two teenagers watching the same movie (in their respective houses) and instant messaging each other at significant moments during the show. An alternative example may be the TV stream as a Picture-in-Picture option within a multimedia conferencing service.
- *Nomadicity:* For an Internet TV service, nomadicity would normally be interpreted as the user being able to access the same service profile from a different location. Computational power/performance cost trends for handheld devices are likely to produce portable terminals capable of participating in Internet TV sessions within the life of the NGN.
- Emergency *Services:* Existing television services provide content overlays notifying of emergency conditions (*e.g.*, tornado warning). A similar content overlay function is expected to exist in this Internet TV service.
- *Content and service discovery*: Assisted by a centralized or distributed directory, the user is able to search and locate the video content from the terminals. The search can be text- , picture-, or video-based. The content and the service available based on the content should be reported back to the user as the result of search.
- *Digital Rights Management*: Employing the DRM technology, the NGN should allow certification of the legitimacy of the original source of the video content, authentication and authorization of the user to view the content, and clear accounting among content creators, producers, traders, and users.
- *PIM:* This service example does not require it, but in some service variants, the time for watching the Internet TV show may have been scheduled in the PIM calendaring facility.
- *Session Management:* Standard session management control commands must be defined for users to initiate and control a content delivery. Initiation commands may include search, browse, and order. Control commands may include play, rewind, forward, pause, stop, fast rewind, fast forward, etc.

2.3.3 Multimedia (MM) Conferencing

This is the "classic" multi-user conferencing application that would support voice, video, messaging, whiteboards, and so forth. Members to the conference can be on wired or wireless networks with any of a number of terminal devices. The Multimedia Conferencing service would:

- Auto-discover the capabilities of the terminal device and manage the delivery of the media accordingly. An example would be high-levels of video compression for users on low-bandwidth wireless terminals.
- Adapt to changes in the user terminal devices, including handoff between devices, a conference shared across multiple types of devices, or multiple interfaces to a single device.
- Authenticate users.

In addition, MM conferencing would support:

- Integration with calendaring/scheduling applications and data collaboration (*e.g.,* document sharing);
- Different conference setup modes (*e.g.,* instant, scheduled, ad-hoc);
- Access control (*e.g.,* change participant privileges) and call control (*e.g.,* add/drop/mute participant) over each participant leg;
- Floor Control (automatic via loudest/preferred speaker or dynamic via ASR/DTMF control);
- Change of conference model and media ad-hoc (*e.g.,* move from IM session to voice call, from voice call to audio conference, from audio conference to video conference, from audio/video conference to collaboration session,);
- Integration with Presence to complement scheduling of conference features;
- Record of conference participant leg;
- Media (*e.g.,* image, text) insertion;
- Video mixing with simultaneous view of conference participants, dynamic layout according to the number of conference participants and voice activated modes (*e.g.,* auto-zoom on the active speaker).

2.3.4 Content Sharing

The NGN is envisioned to allow users to define "closed user groups" or "virtual peer networks" that allow content -- voice messages, images, videos and so forth -- to be shared amongst the (authenticated) members. Content could be hosted by an information provider (centralized) or it could be stored locally (distributed). Personal content sharing is seen to be analogous to multi-media conferencing, except the content is not real-time (live), but delivered on-demand. An example of such an application may be sharing personal digital photographs amongst family members in different

locations. Another example would be to provide access to a hosted private content repository to the employees of an enterprise. Such an application could support a variety of data formats (*e.g.,* block structured, file structured, XML, etc.).

Alternately, end users and enterprises may form groups and publish content to a large group for sale and distribution through the carrier network -- for example, education, conferences, etc.

The following service enablers support content sharing services in the NGN:

- *QoS:* Some content may require QoS arrangements (*e.g.,* minimum bandwidth requirements to download images or video) for better service.
- *Presence:* Content sharing seems to be a transactional application rather than a session-based application, and transactional applications are unlikely to require presence support.
- *Policy:* There may be security policy to control operations on content such as access, replication, or modification.
- *Media Resource Functions:* May be required for some format conversions (*e.g.,* text–to-speech)
- *Unified interface and Service ubiquity:* A user should be able to store their content on a "network drive" and access their content regardless of the access network using the same network address information -- *e.g.,* it's always the N: drive (for network)
- *Multicast:* While we typically associate content services with relatively static content such as web pages, content could be a stream of data from a web cam or telemetry device. Multicast would seem to be more applicable to the streaming applications than static content.
- *Communication context:* May not be relevant if the content sharing is not session-based.
- *Nomadicity:* A user should be able to store their content on a "network drive" and access their content regardless of the access network.
- *Location:* The definition of the closed user group may include entities such as "anyone at a specific location" -- *e.g.,* home
- *PIM:* There may be some logging of content access to PIM required.
- *ENUM:* May not be applicable to most (data) content sharing.
- *Service and content discovery:* Users should be able to discover the content they want and share the contents in ether a client-server or peer-to-peer technologies.
- *Digital Rights Management (DRM):* Employing the DRM technology, the NGN should allow contents shared in a closed group to be lawfully distributed to and only used by the closed group member.
- *Session management:* Not applicable here.
- *Authentication and authorization* – There must be mechanisms to authenticate users and authorize them to various levels of information or network resources.

2.3.5 Interactive Gaming

Interactive gaming provides an immersive context that can be used for entertainment and communication purposes. Interactive gaming encompasses a broad range of virtual environments and interaction modes that can be used to demonstrate a number of communication capabilities. For example, wireless terminal devices (*e.g.,* PDAs) may be used to interact with game content on game consoles and with other remote players.

The following service enablers support interactive gaming services in the NGN:

- *QoS:* Some media streams within a game may require QoS -- *e.g.,* interactive voice sessions, video clips, etc.
- *Presence:* Presence information may be of value in persistent virtual world games.
- *Policy:* There may be access control policies to restrict who can gain access to a specific game. For persistent world games, there may be further restrictions to recover state information from previous sessions.
- *Media Resource Functions:* Likely implemented in the gaming environment, and not a network requirement.
- *Unified interface and Service ubiquity:* Access into the game should be the same regardless of the terminal type used (within minimal terminal constraints for the game).
- *Multicast:* Multicast group semantics may be used to scope content for sharing – *e.g.,* in a massive multiplayer online game, the players within a specific zone of interaction (like a room) may be communicating via a specific multicast channel. As avatars move between rooms, they communicate via different multicast channels.
- *Communication context:* Given that the subscriber is active in a game session, user preferences may redirect incoming voice calls to voice mail.
- *Nomadicity:* Access to the game should be independent of the access network infrastructure.
- *Location:* Location may be required for some games. Proximity (*e.g.,* same LAN segment or access point) may facilitate additional offline human interactions.
- *PIM:* Online game sessions may be scheduled or logged.
- *ENUM:* May not be applicable to most games.
- *Service and content discovery:* Users will be able to discover available games as well as people available to play a game at any time.
- *Digital Rights Management (DRM):* Employing the DRM technology, the NGN should allow only the paying customers to access and participate in interactive gaming.
- *Session management:* Interactive games is controlled under a session management where multiple parties can join, play, leave, and rejoin the game.
- *Authentication and authorization* – There must be mechanisms to authenticate users and authorize them to various levels of information or network resources.

2.3.6 Sensor and Control Networking

Traditional WAN communication has been user-centric. As the availability of smart sensor devices increases, the public WAN infrastructure should also support these devices (with the appropriate safeguards). For example, consider a future health care scenario where a person is instrumented with several sensors to monitor biological functions. These sensors could communicate through a public wireless network to a medical facility where the data could be monitored. Given the medical nature of the scenario, there arise a number of legal constraints (regarding patient privacy, data integrity, and so on) -- additional network assurances could be useful. This application category also includes Supervisory Control and Data Acquisition (SCADA).

2.3.7 Wireless Terminal Control of Customer Premises Equipment

Wireless terminals (*e.g.,* PDAs) are can be used for a variety of services to control devices in customer premises networks. A more traditional example might be the use of touch-tone signaling to control some home automation function. A more current example might be the use of the mobile handset or wireless terminal as a remote control for consumer electronics devices such as television sets.

2.3.8 Mobility Management (across wireless and wireline)

This application is based on the concept of the migration of a call/connection instance between terminal devices (and by inference, networks). Example use cases:

- A user on a call on a wired terminal in a home or office can transfer the call to a mobile phone and then roam on a cellular network.
- A user with a "dual-mode" wireless terminal can roam between a cellular network and private wireless network (with wired network interfaces, such as a home premise network) and vice versa. The home premise network could use regular telephony (copper wires) or VoIP to access the access provider network. The user could be authenticated and authorized to use a number of different private wireless networks (*e.g.,* home, office or commercial).
- Other use cases can be developed for non-voice applications. For example, mobility for Internet Access, SMS, music delivery, etc.

2.4 Network Service Enablers

Although an NGN does not contain vertically-integrated applications, there are still network-based communication services that bring value to consumer applications. This clause identifies some of the key network services required in the NGN.

2.4.1 QoS

The NGN should enable the provision of end-to-end QoS across different infrastructure technologies and multiple service providers to the extent possible based on the capabilities of those technologies and agreements between service providers (both ASP and NGSP). A NGSP may provide service and connectivity to service providers that do not provide QOS. In these cases, the services requiring QOS may not be available end-to-end or may operate in a degraded manner.

QOS has been treated extensively in ATIS, ITU-T, IETF, and other standards organizations. For VoIP, it has been treated in detail in the report of the *ATIS VoIP Work Plan*. The basic thrust is that QoS is multi-faceted; covering not just transmission quality, but also reliability, availability, security, call set-up, etc.

Thus, in addition to being multi-dimensional, real QoS is end-to-end and must be achieved not only across combinations of access and backbone networks, but also across paths that span multiple carriers and service providers. A feasible NGN QoS solution must evolve incrementally from current (non-QoS-enabled) networks.

Admission control will be addressed in the section on session management.

A variety of network-based mechanisms are required to support different aspects of QoS for different services and infrastructure contexts. In IP (and other packet) networks, one of the major concerns for QoS is largely associated with developing mechanisms to manage congestion. Congestion can be managed by complementary techniques that operate on several timescales, e.g.:

- *Network Engineering* can provide the additional capacity required to avoid congestion, but requires significant time to install and provision that additional capacity. Pre-emptive network engineering can avoid congestion at the cost of lightly-utilized infrastructure.
- *Traffic Engineering* can redirect traffic from heavily-used paths to more lightly-loaded paths, assuming such paths exist. Traffic engineering can increase the utilization of a meshed topology at the cost of some increase in operational complexity.
- *Packet Scheduling* can reprioritize packets on the short timescales that operate within queues in network equipment to provide preferential treatment, assuming some traffic classification mechanism exists. Packet scheduling can increase link utilization at the cost of device complexity and operational complexity. Packet scheduling can also be used to mitigate the problems associated with congestion for a particular traffic flow (*e.g.*, dropped packets, delay, jitter). While packet scheduling can provide better service to some traffic flows, it comes at the expense of other traffic flows on the same path. The congestion experience of the other flows may be worsened by the preferential treatment given to some flows.

Within the IP core, where traffic of multiple classes from multiple customers is aggregated, an operator may choose to simplify operations by reducing the number of traffic classes to be supported. An example may be an operator relying on Best Effort services in the core with appropriate network and traffic engineering support.

Within the access network, there are many more links than in the core, making a pre-emptive network engineering strategy much more expensive. Despite the larger number of links, most of them are not diverse, with access networks typically having a simple star topology. In such a topology, traffic engineering is not applicable as additional paths are not available. Hence, access networks are likely to rely on packet scheduling mechanisms to support QoS requirements. Packet scheduling mechanisms are not unique to IP protocols, with other packet technologies (*e.g.,* Ethernet) supporting packet classification and scheduling regimes. NGN may incorporate IEEE 802.1p classification and scheduling mechanisms in devices that are not IP-aware. Other link specific scheduling mechanisms may be required for other lower layer technologies; *e.g.,* IEEE 802.11e for WiFi and similar mechanisms for Bluetooth, HomeplugAV, etc.

Packet classification and scheduling mechanisms cannot assume to be uniform across the domain of a single operator, let alone the multiple operators assumed to exist in the context of an NGN service. For example, an operator may choose to implement an expedited service with a priority scheduling mechanism at the edge of the network where latency is a concern, and with a WFQ scheduling mechanism in the core where cost allocation across multiple services may be a concern. For this reason, the packet classification and scheduling mechanisms are specified as policies (see 2.4.3 for more details concerning policies) rather than specific mechanisms, providing for some flexibility in terms of network implementation.

QoS in terms of error control is performed by several different mechanisms. Lower layer protocols (*e.g.,* DSL) may provide certain levels of error correction. In addition, TCP provides an ARQ mechanism for latency tolerant applications. For UDP applications requiring additional error control (*e.g.,* video), additional application layer protocols (*e.g.,* RFC 2733, RFC 3640) may be required for FEC and interleaving.

QoS, in terms of availability or reliability is a more complex subject. Beyond device reliability there are a number of strategies that operators may use to increase the reliability of service. These include not just redundant network capacity, but specific protocols to support the use of that capacity. These protocols are of particular importance at network interfaces where they must operate across administrative boundaries. Consider load balancing as a generic mechanism to provide resiliency and increased capacity at a network interface. This can be applied at layer 1 (*e.g.,* current work on "G.Bond" in the context of DSL), Layer 2 (*e.g.,* 802.1ad), or Layer 3 (ECMP) as appropriate.

For each service, there will be a number of other service-specific performance concerns that might be considered under the heading of QoS. For a session-based service such as interactive voice, the call setup delay may be such a performance metric. For an Internet TV service, the channel change time may be such a performance metric. Such service specific performance metrics are beyond the scope of this clause, but they may well be impacted by the performance of various network service enablers.

Many of the techniques for QoS in IP networks have been designed for operation within a single Autonomous System (AS). Some service providers span multiple ASs. The IP peering between service providers, however, is typically an AS boundary. There appear to be two potential mechanisms to support QoS sensitive routing across an AS boundary - QoS extensions to BGP or Application Layer Routing (*e.g.,* using tunnels between Session Border Controllers). The definition of appropriate metrics

for per domain behavior (PDB), and best practices for QoS measurement methodologies are required. The mechanisms to concatenate these metrics across multiple domains are also items for further study.

2.4.2 Presence

Some NGN services require an indication of presence or connectivity -- for example, extensions of Instant Messaging (IM) services.

Presence is a set of attributes characterizing the current properties (*e.g.*, status, location, etc.) of an entity. An *entity* in this respect is any device, service, application, etc., that is capable of providing presence information. *Availability*, on the other hand, denotes the ability and willingness of an entity to communicate based on various properties and policies associated with that entity -- *e.g.*, time of day, device capabilities, etc. The terms presence and availability are almost always used together to provide a complete set of presence information. However, presence is not usually a service that is offered as a stand-alone service, but rather in conjunction with other services -- *i.e.*,, presence is often referred to as an "enabler" in that it enables other services and applications to exist by providing presence information to that service or application.

The basis for presence architectures is based on the IETF model developed for the Internet, which defines some key functions and principals which are subsequently reflected in the other presence architectures used outside the Internet -- *e.g.*, in the telecommunications industry. These same fundamental functions and principles are also valid in an NGN architecture.

For example, the presence service has two distinct sets of "clients." One set of clients, called *presentities*, provides presence information to be stored and distributed. The other set of clients, called *watchers*, receive presence information from the service.

There are two kinds of watchers, called *fetchers* and *subscribers*. A *fetcher* simply requests the current value of a presentity's presence information from the presence service. In contrast, a *subscriber* requests notification from the presence service of (future) changes in a presentity's presence information. A special kind of fetcher is one that fetches information on a regular basis; this is called a *poller*.

This can be illustrated with the following hierarchy:

- *Presence*:
  - Presentities
  - Watchers
    - Fetchers
      - Poller
    - Subscribers

The presence service also has watcher information about watchers and their activities in terms of fetching or subscribing to presence information. The presence service may also distribute watcher

information to other watchers, using the same mechanisms that are available for distributing presence information.

A presence protocol defines the interaction between the presence service, presentity's and watchers. It carries the presence information. Both the Extensible Messaging and Presence Protocol (XMPP) and Session Initiation Protocol (SIP) are the leading presence protocols: XMPP for more of the public Internet-based applications, and -- increasingly -- SIP and its corresponding extensions for the telecommunications industry. The wireless industry (3GPP and 3GPP2) has adopted the 3GPP based presence architecture, designed to interwork with the 3GPP IP Multimedia Subsystem (IMS).

Clearly, presence in an NGN architecture must continue to support privacy issues corresponding to those we have to-day in both the wireless and wireline industries. The ability to manage presence information such that only those with valid subscriptions can access presence information is paramount. Even watchers with valid subscriptions may receive only a subset of the presence information based on certain policies.

Presence includes things such as:

- *Where am I?:* location (LBS),
- *What context am I in?:* Home, restaurant, professional,
- *Who do I know?:* Address book, buddy lists, buddies' location, favorite links,
- *Which access means/devices do I use?:* PC, cellular phone, PDA,
- *Which access rights do I have?:* Parental controls (credit limits, content restrictions)
- *How do I pay?:* E-payment, wallet, split billing, creative pre/post paid,
- *Which identifiers (e.g., numbers, SIP addresses, etc.) do I have?:* Fixed, mobile, SIP-Url, IM-ID,
- *How do I want to appear?:* Ring-tones, ring-back tones, logos, avatars,
- And even more *elements in the future* (such as "My voice-print" for speaker recognition).
- *My willingness* to accept various types of communication.

In an end-user centric world, it is the end-user who decides which access means or which device to use. This end-user decision will be based on a trade-off between access means and devices depending on his personal preference or need of the moment:

- At home;
- On the pause (nomadicity);
- On the move (mobility); and
- In the enterprise.

The decision on which access will be based on the application, service availability, and price without the need to understand the technical attributes of one access mechanism versus another. However, this trade-off will implicitly be based on parameters such as required bandwidth, cost, mobility, QoS needs, ergonomic requirements, and the like. Given the very different nature of these parameters and the applications that heavily exploit one or many of these attributes, the current proliferation of devices (PC, blackphone, cellular phone, multimode/WiFi phone, PDA, TV, etc.) and access types (PSTN, fixed broadband access, cellular access, WiFi, WiMax, etc.) will continue to exist.

This implies that the end-users will value services that can be delivered over any access means and any device allowing them maximum freedom and control –- including the capability to apply the same personalization settings to any of these devices. A typical illustration is the recently introduced Instant Messaging (IM) on mobile phones, which has long been available on PCs. The introduction of IM on mobiles has given people greater freedom to communicate in this form (*i.e.,* being in touch with "buddies" the same as if they were sitting at their PC).

Moving towards an end-user centric vision opens the door to many new service opportunities that will cross the traditional boundaries of fixed, mobile, broadband, ISP, and portal businesses. We anticipate that the migration to these new services will be phased over time, in line with the capability build-up of service providers and the adoption of end-users.

2.4.3 Policy

The NGN communication services identified in this document require a mechanism to ensure consistent application across a range of network types and access technologies. These services must also be applied consistently across various service provider networks. The mechanism to provide this functionality in a converged NGN is *policy*. An effective policy infrastructure can ensure services are applied consistently across various access technologies and multiple service providers. An effective policy infrastructure is essential for network-based services to be practical, useful, and billable in a converged network. The NGN program will identify policy requirements, define a consistent policy architecture, and specify policy protocols as a core capability of NGN.

Services may be invoked at various "levels" within the architecture -- for example, business services at the Business Management Layer, network services at the Network Management Layer and so forth. Similarly, the policy system that implements the decision support should also be "layered" and the policy engine technology should be commensurate with the requirements of the "layer". This implies there is not a single *policy system* but a multiple systems that are able to interact one with another to provide decision support both horizontally (*i.e.*, within a "layer") and vertically (*i.e.*,, between layers). In a similar manner, it is envisioned that multiple policy systems may exist within a single layer. This characteristic could be exploited to provide, for example, a series of layer-specific policies without requiring the complete specification of the "rule set" within one policy system or the use of a single technology (*e.g.,* rule-based) across multiple policy systems. As such, the continuum of "policy systems" exists within and across all layers of the NGN.

The new control and management paradigm required for the NGN is provided through an effective policy mechanism. The application of policy constraints in the control and management flow should be

transparent to the operational aspects of an in-service system. A transparent policy-enabled management paradigm allows for the application of constraints on the observable behavior of a system without modifying existing code within that system. There is also a requirement for mechanisms to quantify Quality of Experience (QoE) for new services (*e.g.,* video conference) and to predict the QoE that will be realized for a given network architecture or configuration.

The fundamental attributes of policy control may be summarized as follows:

- Service provisioning system
- Service set-up (control plane)
- Authorization/entitlements
- Service delivery elements
- Billing/metering

2.4.4 Media Resource Functions

Media resources in the NGN provide many roles in conjunction with traditional voice processing services and user interactions via voice and DTMF. These are expanded in the NGN with new data, video and content services. *Media servers* are network elements providing the media resource functions:

- Recorded and composed announcements
- Interactive voice response
- Audio recording
- Voice mail
- Advanced speech recognition
- Text to speech
- Audio conference bridge
- Video/data bridges
- Media forking
- Media insertion (e.g. image, text , video) in multimedia stream
- Content caching/hosting/serving

Media servers terminate media streams, have standard signaling interfaces, and interact with the media session under programmatic control of the application functions via open industry programming languages. In addition, media servers can provide external call control and multimedia interaction programmatic interfaces, based on open industry standard interfaces such as H248, SIP, and W3C VoiceXML and CCXML (as well as forthcoming V2XML, *i.e.,* Voice/Video XML), to allow external network elements providing application functions to access/control the media server capabilities.

2.4.5 Media Gateway Function

Media gateways are used to allow media streams to pass between networks of different technologies or belonging to different operators and use different coding parameters.

Trunk gateways represent the predominant application for media gateways today and are used to interface VoIP NGNs to the PSTN. Gateways are expected to evolve to support packet interfaces between NGN service providers. Trunk gateway functions include:

- Packet stream termination
- QoS statistics gathering
- Transcoding between the packet network codec and μ-law PCM
- Echo cancellation
- Media forking (function may be placed in separate media server)
- Voiceband data detection and processing
- TDM network interfaces, predominantly T1, DS3 and OC3
- Trunk signaling such as SS7, MF and PRI (user-side)
- Audible call progress tones

In addition to interfacing to the PSTN, trunk gateways are the vehicle used by the NGN to interface to legacy mobile networks up to the 3GPP Release 4 architecture. This introduces the possible requirement to support tandem-free operation or transcoder-free operation in NGNs providing tandem switching for mobile networks.

Access gateways have been defined to allow an NGN to provide PSTN emulation. Their functions are similar to trunk gateways but with a focus on the signaling used in access networks. Access gateway functions include:

- Packet stream termination
- QoS statistics gathering
- Transcoding between the packet network codec and μ-law PCM
- Echo cancellation
- Voiceband data detection and processing
- Media forking (function may be placed in separate media server)
- TDM network interfaces, *e.g.*, GR-303, GR-8, PRI (network-side)
- DTMF, BRI and PRI signaling
- Analog and ISDN line interfaces
- Audible call progress tones

Ideally NGNs providing through IP transport for voice or video communication sessions should negotiate a common codec to allow end-to-end transport of the media without transcoding. This allows for the best possible voice and video quality and avoids the need for intermediate media processing resources. Carrying over from the PSTN, the support of G.711 in all devices could guarantee a successful end-to-end media negotiation and so makes a logical choice as a mandatory codec to support at a point of network interconnection. For this and other reasons many wireline

networks may wish to set G.711 as their default network codec and require all NGN devices to support this. However this is not an option for mobile wireless networks which must use low-bit-rate codecs to maximize call capacity over wide-area air interfaces. It is also not always possible in wireline networks providing NGN services over an ADSL interface and cable networks have even more severe bandwidth restrictions which is reflected in PacketCable 1.1 mandating low-bit rate codecs.

As a potential alternative to G.711 a wireless mobile codec, such as the 3GPP AMR codec, could be chosen as the network default codec. However, this would have the result of increasing the cost of the IP end terminals due to the AMR licenses and reducing the voice quality compared with the PSTN today. Other low-bit rate codecs such as G.729 and iLBC are available with lower license fees but these will not be supported by cellular networks and so are unlikely to be provided by dual-mode (cellular/WiFi) terminals. Regardless of the terminal codec choice, the NGN should support G.711 for end-to-end interoperability.

With this in mind, it is apparent that networks must be capable of transcoding between codecs as media streams cross network boundaries. This requirement expands when other factors that may be negotiated in an end-to-end media session are considered:

- Packetization
- Silence suppression
- RFC2833 telephone events and tones
- Voiceband data handling
- Fax, modem and TTY relay
- Redundancy and forward error correction
- Encryption and authentication

Wideband audio and video codecs further expand on the variations that may exist between networks transporting these media. Video, for example, is generally subject to codec, bit-rate, and format adaptation.

The optimum settings for a particular network depend on multiple business and technical factors and it will not always be possible to negotiate common settings across network boundaries even if the underlying codec can be agreed upon. This is especially true for encryption and authentication for which the exchange of keys will be constrained by trust boundaries.

The foregoing identifies the need for the NGN to provide media gateways to support IP network interconnection. Such media gateways may exist at the physical network interface to serve as border elements, they could be inserted between the IP-CAN and the core network, or they could be treated as a network resource pool.

2.4.6 Personal Profiles, "Unified" Interface and Service Ubiquity

In today's networks, the user experience is greatly defined by the terminal characteristics and the user location. A trivial example is dialing and number plans: a user familiar with the North American y have a very difficult time placing a local or long-distance call when traveling outside North America.

In the NGN, users may have *profiles* that allow uniform network interfaces (regardless of location) and service ubiquity (*i.e.*, the users' subscribed services are also available on a "host" network). Thus users may need to identify the person they wished to call and the profile will interact with the network to 'dial' the call irrespective of which country they may be in.

The management and application of these profiles reflect the interaction characteristics of a user at a specific time (*i.e.,* reflect the "role" they have chosen at a time). The system should recognize and modify its presented interface to properly reflect the user "role." Note that the roles of users are independent and dynamic.

The *personal profile* is the cornerstone of an end-user-centric world. Today, end-users are confronted with fragmented service, requiring them to enter and maintain equivalent information several times: address books, buddy lists, billing and payment preferences, phone numbers, presence, ring-tones, etc.

Ideally, the end-user would only require one, single personal-profile containing all of his personal information and preferences:

In order for such a profile to be attractive for the end-user, a number of prerequisites must be fulfilled. The profile must be delivered in a simple way, manageable by the end-user. It also must address fundamental core end-user values such as privacy, security, intimacy, life enrichment, simplification, etc.

2.4.7 Multicast

Multicast capabilities are required for efficient delivery of some services, but these capabilities are not easy to operate in a multi-provider, multi-infrastructure context. Mechanisms are needed to deploy and operate scalable multicast services supported by a single NGNSP and which span multiple transport service providers.

2.4.8 Communication Context

Several aspects of these NGN services may involve the establishment of a communications context. The range of this context can include a profile, an agent, and a virtual environment within which the communication aspects take place.

2.4.9 Nomadism and Roaming

The concepts of nomadicity and roaming in TISPAN [TISPAN-NGNR1] are the following:

- *Nomadism:* Ability of the user to change the network access point on moving; when changing the network access point, the user's service session is completely stopped and then started again -- *i.e.,*, there is no session continuity or handover possible. It is assumed that the normal usage pattern is that users shutdown the service session before moving to another access point.

- *Roaming:* This is the ability of the users to access services according to their user profile while moving outside of their subscribed home network -- *i.e.,* by using an access point of a visited network. This requires the ability of the user to get access in the visited network, the existence of an interface between home network and visited network, as well as a roaming agreement between the respective network operators.

The NGN architecture should support Nomadism and Roaming capabilities. Work is required to define the interfaces and protocols used for Nomadism and Roaming. In the NGN, Nomadism and Roaming should not be restricted to a single administrative domain.

2.4.10 Location

Some NGN services may require location information for devices, people, or information. Mechanisms to determine and report locations information will generally vary by access technology. Given nomadicity, this means that support for location services will have to be implemented within each access technology. Location may also be delivered by the CPE to the NGN using capabilities currently under development (*e.g.,* IETF geopriv). In this case, the location services may not be dependent on the access technology. The NGN should provide additional services to ensure the correctness and authenticity of location information used for its services to mitigate any adversary effects due to fraudulent or false location information. Privacy issues must be taken into account when defining location services. Personal profiles provide a means for the user to control the release of location information.

2.4.11 Personal Information Management and Access

Today, most users locally store contact information (such as names and phone numbers) on individual devices (mobile phones, handhelds, PCs, POTS line phones, and so forth). Managing these devices to maintain synchronization can be complicated and time-consuming. The NGN is envisioned to enable users to manage contact information and provide access to this content in a much simpler way. Example capabilities include:

- Access mode optimized for the input capabilities of the terminal device (speech recognition, keyboard/terminal, pointer device, and so on).
- Integration of the Contact Information Base with call management and control functionality.
- Use of standard protocols for synchronizing information into local devices (*e.g.,* LDAP)
- Privacy/security mechanisms for protecting user data.

2.4.12 Usage of ENUM

ENUM is a method defined in IETF for utilizing the DNS to map telephone numbers into Universal Resource Identifiers (URIs). This provides the capability for, among other things, the user to enter a telephone number and get back a SIP URI, email URI, etc. indicating how to contact the intended party.

The ITU-T is responsible for allocating E.164 Country Codes internationally. The North American Numbering Plan Administration (NANPA) supports the allocation of the E.164 address Space in North America. The association between E.164 addresses and IP addresses for routing purposes can be supported through the ENUM (tElephone NUmber Mapping) standards developed by the IETF. The ENUM Forum is an organization developing proposals for deploying ENUM in North America. The FCC (telecom numbering) and Department of Commerce (DNS) are the two government agencies most involved in monitoring the deployment of ENUM in the USA.

Three variants of ENUM have been proposed:

1) Public ENUM;

2) Carrier (or infrastructure) ENUM; and

3) Private ENUM.

The ENUM Forum is the lead ENUM organization in the USA. The *ATIS VoIP Work-Plan* identifies ongoing work in this area to evaluate industry direction. Public ENUM is the term currently used for the original ENUM RFC's specification of mapping E.164 telephone numbers into DNS. Infrastructure ENUM is a proposal for using the ENUM method to support internal operation of a service provider (or between service providers). Private ENUM is a term used for the use of the ENUM method within private enterprises (*e.g.,* using that enterprise's domain name and DNS zones). Private ENUM should be transparent to the NGN; however, interworking may need to be defined between Private ENUM and Public ENUM.

TISPAN has already delivered a Technical report (ETSI TR 102 055) for Infrastructure ENUM and is developing further work in this area related to its NGN project.

The *ATIS VoIP Work Plan* identifies ongoing work in this area to evaluate industry direction.

2.4.13 Content and Service Discovery

The NGN is expected to support a wide range of services and applications which may also change over time. Therefore, the NGN should support service discovery capabilities to allow users and their devices to discover the services, applications, and other network information of their interest. A service discovery system should allow users and their devices to discover services over any specific underlying networking technology (*e.g.,* cellular systems, wireless local area networks, DSL). However, the service discovery system should be, to the extent possible, independent of the underlying networking technologies so that it can support heterogeneous and changing network technologies.

The service discovery system should allow users to discover *user-interest* and *device-interest* services and network information. *User-interest services and information* can be directly used by human users. Examples of user-interest services and information include existence of networks in nearby locations, directory services, shared facilities (*e.g.,* shared printers), and information contents. The service discovery system should support multimedia user-interest content search (*e.g.,* searching by text, image, and video). *Device-interest services and information* may not be directly usable to human users, but may instead be used by users' terminal devices to support networking functions and/or the applications running on the user terminal devices. Examples of device-interest services and information include the addresses of key networking elements that user devices need to know, such as authentication servers, IP address allocation servers (*e.g.,* DHCP servers), and SIP servers.

The service discovery system should not be limited to only the traditional client-server based systems. Instead, service discovery may be realized using peer-to-peer technologies or a combination of client-server and peer-to-peer technologies. The service discovery system should support a variety of scoping criteria (*e.g.,* location, cost, etc.) to provide appropriate scaling, with appropriate mechanisms to ensure security and privacy.

The service discovery systems developed for the NGN should be independent of lower layer protocols as much as possible and should take into account scalability and bandwidth consumption (*e.g.,* broadcast methods should be avoided).

2.4.14 Digital Rights Management

Digital Rights Management (DRM) represents a range of techniques that use information about rights and rights holders to manage copyright material and the terms and conditions on which it is made available to users. The NGN should permit DRM techniques to ensure the legal rights of all stakeholders of the content in the NGN including creators, producers, publishers, traders, and receivers. There is no requirement for the NGN to employ DRM techniques for content carried over its network or not provided by the NGSP. DRM is an application layer enabler and should not affect the NGN transport. The NGN may provide authentication or location information to a DRM application.

The NGN service provider may make content available through a DRM system. This NGN DRM requires all contents to be not only systematically-identified, but also the information about their legal rights holders and their legal rights associated with the contents faithfully recorded. The NGN DRM uses copyright protection techniques such as encryption, digital watermarking, and digital signatures to ensure these rights are lawfully enforced. To facilitate wide scale adoption, the use of the NGN DRM must be relatively easy. In most cases, the users should not be aware of the DRM system until they attempt unauthorized access to the content in the NGN. Also, different methods of payment should be offered under the NGN DRM. As digital transactions may involve small volumes of material, there will be a need for efficient and cost-effective payment methods such as micro-payments. The NGN DRM should not restrict fair use of copyrighted material. Neither should it restrict copying of material for personal use by the user (*e.g.,* making backup copies). It should facilitate the ability for the user to be able to use the content on multiple personal devices.

The NGN DRM services do not restrict applications from providing their own DRM mechanisms. Other NGN capabilities (*e.g.,* network security capabilities such as authentication) may also be useful to application DRM mechanisms.

2.4.15 Session Management

The goal of session management in NGN is to provide capabilities to setup, manage, and terminate an end-to-end service session that involves a membership of multiple parties, a group of endpoints associated with the membership parties, and a description of multimedia connection among the endpoints.

For example, the session management for delivering a video-on-demand session consists of:

1. *Two parties:* The video server and the viewer;
2. *Four endpoints:* Two endpoints on the viewer's multimedia PC for receiving video and voice, and two endpoints on the video server for delivering video and voice; and
3. *Two media connections:* A unidirectional video and a unidirectional voice.

Moreover, the viewer can use control commands such as play, rewind, forward, pause, stop, fast rewind, fast forward, etc., to control the video delivery.

The session management, when applied to set up a multiparty and multimedia video conference session, will be different than the video-on-demand described above. The NGN provides session management to accommodate different service application requirements as well as to route session signaling to appropriate application servers. Session management may span across multiple services. The NGN shall provide support for sharing of state and status information between services (in other words service interworking or brokering) to allow for blending of the services as desired. It shall also provide support for session admission control and session mobility.

- *Session admission control* only admits the sessions that can achieve some defined level of QoS and security control.
    - *There are four primary mechanisms for QoS-related session or call admission control as the following:*
        - *Maintaining session counts which admits session requests according to the knowledge of how many sessions (or how much bandwidth) has been allocated*
        - *Out-of-band measurement which admits session requests based on measured network resource availability through periodic polling of routers or switches*
        - *In-band measurement which admits session requests based on the measured network performance through active probes or other in-band performance metrics*
        - *Reservation based mechanisms which admit calls/sessions or flows only if an explicit request for bandwidth reservation for that session/flow is successful*

These mechanisms should be supported in the NGN.

- The admission control mechanisms must span multiple service types (*e.g.,* voice and video).

- *Session mobility* allows the persistence of a session when users leave and rejoin the session, move to different endpoints, or change the media connections. *For example, a user can suspend a video delivery session to his IP TV at home and then resume the session on his laptop in a hotel home.*

2.5 Underlying Network/Support Capabilities (not directly accessible by applications)

Simplified control and management of network services is critical to the success of NGN. Existing control and management paradigms (*e.g.,* PSTN/AIN) are designed to support vertically integrated services and infrastructure. In contrast, the NGN requires mechanisms to support service delivery where the infrastructure is not closely integrated; specifically, multiple operators may own and operate independent parts. This is discussed in more detail in clause 6 of this document.

2.5.1 Operations Administration Maintenance and Provisioning

Management of telecommunications networks is intended to support a wide variety of management areas which cover the planning, installation, operations, administration, maintenance and provisioning of telecommunications networks and services. The ITU-T has categorized management into five broad management functional areas (Recommendation X.700 [1]).

The five FCAPS management functional areas identified to date are as follows:

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

The classification of the information exchange within the management framework is independent of the use that will be made of the information. The management of the NGN needs to be aware of networks and services as collections of cooperating systems. The architecture is concerned with orchestrating the management of individual systems so as to have a coordinated effect upon the network.

Management objectives for Next Generation Networks include:

- 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, and;
- Converge on a single, secure network and set of protocols for managing equipment and carrying management information.

Policy-based management systems may be used to improve the reuse of successful (proved as correct) management decisions (embedded into policy rules). The policy management system is a collection of rules (some can be grouped into policies; simpler policies can be grouped into more complex policies), as finer pieces that can individually constrain the behavior of an operational system. Many approaches and technologies have been proposed to build such management systems (rule-based, scripts-based, model-based, etc.). Multiple policy-based management systems may be simultaneously required. How to build such a management system, what mechanisms are required, and what challenges these systems are raising may be crucial for the NGN. The policy based management systems are an item for further study.

The new NGN elements and the new services provided by them place new demands on the OAMP environment. Careful consideration to the Next Generation OSS (NGOSS) environments must be given around the adoption of industry NGOSS standards and which specific interfaces will be used for all OAMP functions for both internal and inter-carrier functions. Additionally, self-care and self-provisioning (personalization) of new services should be further placed in the end users' control using Internet technologies. The requirements and specifications being developed within ATIS Technical Committees (*e.g.,* Telecom Management and Operations Committee (TMOC), formerly T1M1) and the adopted specifications by TISPAN, TMF and the ITU-T NGN Management Focus Group will be reviewed for adoption within the NGN OAMP framework.

The NGN infrastructure is built upon a foundation of IP-based network services; these have been developed and deployed in the context of best effort IP services. While IP protocols have been developed and deployed for many years, ongoing improvements are required to ensure the continued scalability of the IP infrastructure in the context of QoS and other network services. OAM support for validation of QoS operation may require additional support.

The NGN assumes the existence of intelligent terminal devices. Intelligent terminal devices require configuration and software updates to maintain compatibility with WAN network service features. The

Automatic Configuration Server (ACS) in the context of DSL networks provides a mechanism for the network operator to provide required configuration information to subscriber equipment such as a residential gateway. Other provisioning support mechanisms -- *e.g.,* Local Management Interface (LMI) protocols -- may enhance the automated configuration of interfaces. In the context of home networks and consumer electronics devices as terminals for WAN services, there needs to be an appropriate balance between ad-hoc home network configuration mechanisms and the needs of WAN network services.

In many cases the IP network services rely on adequate support from lower protocol layers. MPLS, Ethernet, and 802.11, HomeplugAV are examples of lower layer protocols of particular relevance, where OAM functions to determine connectivity, available bandwidth, etc, require additional support. Mechanisms to support the detection and diagnosis of network faults in such networks are also required.

For example, the advent of Ethernet as a Metropolitan and Wide-Area Networking technology has driven the need for a new set of OAM protocols. Ethernet OAM functions are rapidly evolving in the standards bodies: IEEE 802.1ag Connectivity Fault Management, IEEE 802.3ah OAM, and Ethernet Local Management Interface (E-LMI). Each of these different OAM protocols has unique objectives and is complementary to the others. The ATIS Wide Area Ethernet Focus Group has identified requirements for Ethernet OAM.

Standards work for Ethernet OAM is underway in various SDOs and industry Fora such as:

- *ITU-T SG 13 and SG 15:*
  - Ethernet Layer Network Arch (G.8010 SG 15)
  - Ethernet OAM Functionality (Y.ethoam SG 13)
  - Requirements for OAM in Ethernet based networks (Y.1730 - SG 13)
- *IEEE:*
  - 802.1ad - Provider Bridges
  - 802.1ag - Connectivity Mgmt (Per VLAN OAM)
- *TMF:*
  - Multi-Technology Network Management – Ethernet (TMF *513/608/814)*
- *MEF:*
  - E-LMI
  - Service OAM Requirements and Framework
  - Performance Monitoring

ITU-T (in collaboration with other committees/forums) initiated a NGN Management Focus Group in November 2004 to coordinate NGN Management (OAM&P) work efforts across interested committees/forums. Participation is open to individuals from organizations with expertise and specifications applicable to NGN management interfaces, including the following:

- ITU-T SG 4 and SG 15

- TISPAN WG 8
- ATIS TMOC
- 3GPP SA5
- 3GPP2 TSG-S WG5
- TeleManagement Forum
- IETF Operations and Management

2.5.2 Security

The NGN should provide the same level or better security as the current PSTN. To be successful, effective security policies must be developed and implemented in a systematic, consistent, and rigorous manner for these services and networks. Developing effective security policies is best achieved by using a comprehensive security model such as the ITU X.805 Security Architecture. The X.805 Security Architecture allows for a structured approach to developing security policies and determining what security services need to be deployed. The use of this (or other) security framework is essential when examining gaps in security standards that can be barriers to implementing security policies needed for Next Generation Networks (NGN). These policies must take into account the risks and benefits of deploying specific security technologies by systematically evaluating the service in light of each of the eight "Security Dimensions" listed in the following diagram:

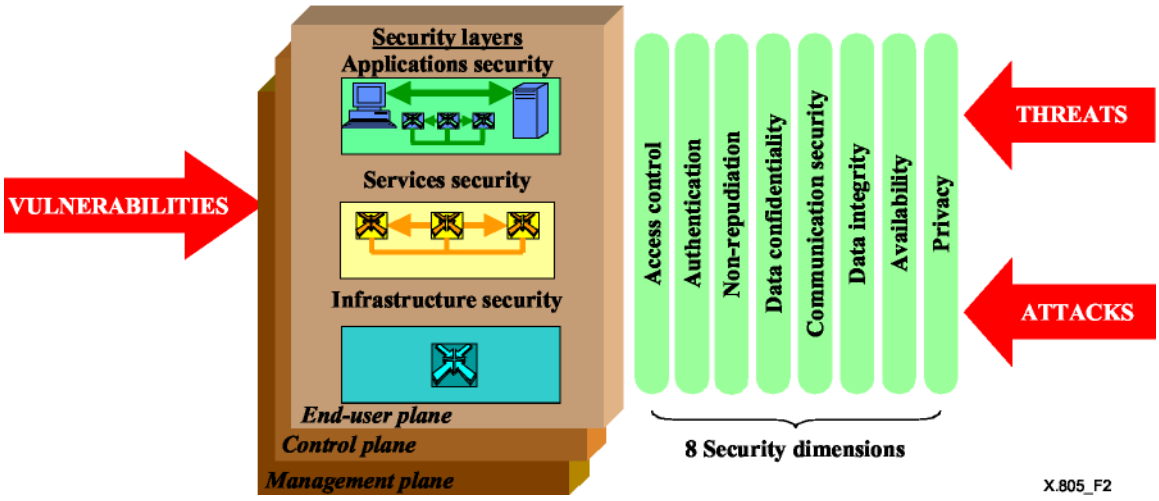

Figure 3 - The Eight Security Dimensions

Moreover, the requirements and specifications being developed within ATIS Technical Committees and the adopted specifications by ITU-T and IETF will be reviewed for adoption within the NGN security framework for both internal and inter-carrier functions.

The Security Dimensions are described in the following clauses. Identity is an essential concept to Authentication and Authorization. Identity management is a key network support capability in the NGN. In the NGN, identity can be used as an addressing mechanism rather as location has been used in the traditional PSTN.

The ATIS Security Focus Group has developed a Work Plan detailing a number of issues that are being worked within ATIS Committees. This work should be taken into account when developing the NGN Work Plan.

2.5.2.1 Authentication, & Authorization

This clause will explore the requirements for *Authentication* functions as they pertain to signaling and bearer traffic within the NGN and its new services. We will focus on what is needed for authentication for both device and end users and how far authentication goes:

- User to phone (for highly secure environments)
- User Agent to IMS
- IMS to User Agent
- User to IP-CAN
- IP-CAN to User
- User Agent to User Agent
- Cross domain authentication
- Authentication of Signaling messages
- Authentication of media packets
- Authentication of messages that traverse PSTN<-> Packet Networks through Signaling/Media gateways

The NGN should allow a variety of authentication techniques to be used against the single user profile, such as name and password, SIM card, smart card, token etc. Thus the NGN may require an authentication broker and the IMS architecture may need to be expanded to support it.

Whereas authentication provides a mechanism for ensuring that the user is who they claim to be, be it a person or a machine. Authentication does not, per se, allow the user access to the services of the NGN:

this is the function of *Authorization*. The Authorization function provides information about what services an authenticated user may use within the NGN. Authorization may include not only the right to use basic communication functions, but also the authority to use Confidentiality services, priority service, etc. Access Controls are the mechanism that actually control access to an object based on whether the subject is authorized to access the object.

The requirements and specifications being developed within industry organizations such as ATIS PTSC/TMOC, ETSI, IEEE, IETF, and ITU-T will be reviewed during the "gap analysis" phase of the ATIS NGN-FG effort.

2.5.2.2 Integrity

Integrity is the capability of ensuring that what goes in, comes out without having been modified. Integrity can be applied at different levels in a network. For example, it may be required that a packet injected into the network is transported to its destination with integrity; however, if that packet is lost, it is of no substantial consequence (this might be true for an "unsecured" VoIP connection). In another scenario where dropping packets has major consequences (*e.g.,* video), integrity may be measured at the session level, as the requirement here is that the complete session information be transferred to its destination without loss or manipulation of the data. The requirements for integrity need to be specified across all "planes" of the network across all security layers.

Note that the introduction of middle-boxes (*e.g.,* NATs, Firewalls, Media Resource Functions) can affect end-to-end integrity mechanisms.

2.5.2.3 Confidentiality and Privacy

Confidentiality ensures that data is protected against unauthorized viewing in transit and that data is not disclosed to unauthorized parties. The application of data confidentiality mechanisms such as encryption and access control lists ensure that data cannot be understood by unauthorized entities, and that information cannot be intercepted as it flows between authorized entities.

The need for confidentially will vary depending on the network "plane" being considered and the particular security layer. For example, whereas as a service provider may consider confidentiality of signaling information a requirement to preserve the integrity of the network functions, confidentiality of user data may be considered a user responsibility. Thus, the requirements for confidentiality need to be specified across all "planes" of the network, across all security layers.

Privacy relates to preventing the unauthorized dissemination of information. For example, in the end user plane, we need to ensure that network elements, services, or applications do not provide information pertaining to the end user's network or use of services or applications to an unauthorized entity. Similar needs are defined for the Control and Management planes.

2.5.2.4 Non-Repudiation

Non-repudiation is the ability to be able to prove that an action was performed -- *e.g.,* if a message is sent from an entity "a" to "b" and subsequently "a" denies having sent the message, with non-repudiation capability, "b" is able to prove that "a" did, in fact, send the message. This can be done by retaining records of all actions that were performed within the network by applications, management systems, or network services for a period of time.

In the context of an NGN, an example of a situation requiring network support capability for non-repudiation is an action where the network triggers a billing event. User-to-user interactions may use other non-repudiation mechanisms and may not require network non-repudiation capabilities.

2.5.2.5 Communications Security and Availability

Communications Security refers to the need to ensure that communications between endpoints cannot be unlawfully intercepted or redirected.

Availability is the need to ensure that the network infrastructure, services, and applications are available for use. This means protection from physical misadventures by the use of alternate routing and duplicated facilities, and also protection from such activities as DoS attacks and other malicious activities that would prevent access to facilities.

Metrics for availability are discussed along with other performance metrics in the clause on QoS. Mechanisms for availability and survivability are also discussed in a later section.

2.5.2.6 3GPP Security

3GPP security mechanisms are detailed in the following specifications:

- TS 33.203, *Access Security for IP based services*.
- TS 33.210, *Network Domain Security: IP network layer security*.

Access security relies on the use of USIM Integrated Circuit Card (UICC) as the platform in which all IMS authentication keys and functions at the user side will be stored.

TS 33.203 sets specific requirements on the ISIM application to support IMS access security, so that the service is not provided until a security association is established between the UE and the network. The IMS AKA method is used for authentication as defined in TS 33.203.

For network domain security, 3GPP has specified security to be provided at the network layer using hop-by-hop security protocols as defined by TS 33.210. For intranetwork security TS 33.210 specifies the use of security gateways between disparate networks and the use of IKE to negotiate and establish secure ESP tunnels between the gateways. Internetwork security is optional, but TS 33.210 recommends the use of IPsec with ESP and IKE.

The security services that have been identified in 3GPP as needed are: confidentiality, integrity, authentication, authorization, some of the dimensions already identified by X.805, and anti-replay protection. These are ensured by standard 3GPP procedures, based on cryptographic techniques.

ETSI TISPAN is endorsing the security mechanisms specified by 3GPP for access and network security, and further enhancements are being studied to accommodate those requirements not currently considered by 3GPP.

As an example, the access security solution might need to work with NATs in between the terminal and the IMS network. This might imply changes in the mechanisms already standardized for Integrity protection.

The already-standardized procedures and services in 3GPP will need to be reviewed in conjunction with the requirements and specifications being developed within ATIS and ETSI TISPAN, for adoption within the NGN security framework for both internal and inter-carrier functions.

2.5.2.7 Attack Mitigation & Prevention

A NGSP should deploy mechanisms to mitigate attacks against its users and connected networks. It should also provide capabilities to shut down or prevent attacks originating from its network.

2.5.3 SLAs

Service Level Agreement (SLA) parameters depend on the service being offered. A set of those parameters (MTTF, MTTR, etc.) is common among different services which will be offered via NGN. The SLA parameters may be defined for both "signaling and control plane" and for "transport plane" for services on the basis of end-to-end and per network segment (both Intra-provider and Inter-provider).

2.5.4 Accounting (Ordering & Billing)

NGN services need to support a variety of commercial arrangements for settlement of transactions, both with the service providers and between the communicating entities. While telephone service billing has also been used to support other billing arrangements, perhaps the stereotypical example is the ability to use a mobile phone to purchase a soda from a vending machine. A further extension would be the ability to transfer value between communicating consumers, rather than just select merchants.

Flexible settlement arrangements may be required. It is desirable that these be based on consistent, scaleable, accounting metrics and settlement models (*e.g.*, "sender pays," "receiver pays," etc.), and a level of aggregation that supports scalability. It shall also be possible to charge through various charging techniques such as prepay, post pay, advice of charge, and third party charging.

2.5.5 Trust

A commercially adequate basis for authentication and trust is required for commercial services to cross administrative boundaries in which the different administrations are involved in the service.

NOTE - A commercial service can cross an un-trusted administrative boundary if it provides sufficient security -- *e.g.*, encryption.

2.5.6 Ad-hoc and Zero Configuration Networking

A consequence of mobility in devices, people, and information is the need to be able to support communications regardless of the network context. As the user moves to a new network context the ad hoc assemblage of available network services should automatically be reestablished based upon the set of available options. For example, as subscribers move within reach of their home networks, their cell phones should operate via the home wireless network rather than via the service provider's WAN wireless network.

The system should be capable of auto-configuration and this capability should be invoked without overt intervention from a (human) operator -- other than possible (re-)authentication -- where possible.

Ad-hoc networking and mesh networking are areas of active research and development. The inter-connection of (mobile) ad-hoc and mesh networks with the NGN needs to be studied. In addition, the use of ad-hoc and mesh networking technologies within the NGN needs to be studied.

2.5.7 Service Quality Measurements

In the traditional voice context, QoE for a voice service is well understood and established mechanisms (*e.g.,* MOS) exist to quantify it. In the NGN context, a variety of services other than voice are to be offered, and indeed those services present much of the rationale for evolution beyond the PSTN to an NGN. Perceptual quality metrics will be required for these non-voice services also. Specific non-voice services requiring standardization efforts to include the equivalent of a MOS score for service quality include:

- Internet TV
- High Definition Internet TV
- Web site browsing
- Multimedia conferencing
- Internet radio
- High definition (stereo) audio

Additional services may also require such metrics as the services become better defined and more widely available.

The performance of the NGN infrastructure is expected to significantly affect the perceived performance of the applications. Performance metrics associated with NGN functions will also be required, particularly when they are invoked in response to human-triggered actions. Latencies associated with service selection or session establishment are examples of areas where NGN performance metrics will be required.

Service quality should be measured actively for each service. The frequency of measurement should depend on the flexibility with which the Service Level Specification parameters are guaranteed.

2.5.8 Mechanisms to Predict Service Quality

In the existing network and given a combination of network equipment and defects, mechanisms exist to predict the expected QoE (*e.g.,* E-model for voice). Similar mechanisms will be required to predict the QoE for future services.

In the context of voice telephony, a MOS score can be predicted given certain information regarding the choice of codec and various network transmission performance metrics (*e.g.,* loss, delay). The E-model is a formalization of this algorithm. Similar mechanisms are required to predict service quality metrics for other services, again largely based on network performance metrics and codec options. While (hopefully) standard IP network performance metrics can be used, the codec information may be more complex in some cases. If we consider a video codec such as MPEG4, there are a variety of implementation options for decoding and error concealment techniques that can impact perceived quality in the presence of errors and loss.

2.5.9 Mechanisms for Network and Service Survivability

Network and service survivability in an NGN is affected by the planning, installation, operations, administration, maintenance and provisioning of networks and services. NGN infrastructure and service survivability is also affected by a range of external threats, *e.g.,* failure of commercial power, terrorist attack. The high-level goal will be to provide survivable and cost-effective networks.

Survivability should be built into the design and operation of the NGN, and should be based on open and interoperable standards rather than proprietary technologies.

For example, for telephony services over IP, the call server can be deployed in split or load-shared mode so that when disasters happen in one geographical location, customers can still obtain service from the call server in another location. Similar mechanism can be utilized for intra-and inter-domain transmission devices and gateways in both wireline and wireless networks.

2.6 Business Model driven requirements

A significant industry standardization effort such as NGN represents significant expense to the participants. In order to balance this expense, the expected deliverables from the standardization effort should promise reasonable potential profits to the market participants. Business model requirements will provide a significant influence to the evolving NGN architecture. The market and industry drive the direction of communications technology and services, which in turn provides the basis for the NGN business model. The business model demands reduced operating costs as well as new sources of revenue. New revenues can be achieved through new end user applications as described in 2.2, through growth of existing markets and from increased market shares of existing services. Each of these efforts can be supported through the use of new technologies plus greater economies enabled by changes in architecture.

A key motivation behind the NGN target architecture is to develop a broadband system that enables easy integration of network resources, services, and operations across the business units of service provides while insulating services from underlying network transport technology. The separation of services from transport will enable a wide range of value-added services, allowing service providers to differentiate products from underlying transport capabilities. This assists the economies that can help maximize the efficiency of the service delivery infrastructure.

Additionally, accommodation of key existing services and infrastructure through interworking and/or interoperability is an important business aspect. For existing service providers, the NGN must leverage the deployed base while supporting new services and technologies efficiently.

Business drivers are expected to vary between firms depending on market conditions, etc. Business drivers for NGN deployments are expected to include:

- Revenue from new retail services enabled by the new architecture.
- Revenue from new wholesale services enabled by the new architecture
- Revenue from existing services able to be offered more cost effectively over the new infrastructure.
- Regulatory requirements (cost of doing business).

2.6.1 Operational Expense (OPEX)

The NGN will enable significant operational efficiencies over existing vertically-integrated networks. Functions today that are provisioned, configured, or manually manipulated using OSS and engineering tools should be done near real-time using network management and signaling processes. The result should be simplified control, network, and service management that may be extended to the end customer.

A converged NGN -- with increased self-provisioning, auto-provisioning, and end-user control -- should create greater economies of scale and simplified operations with the adoption of new network and service management systems.

2.6.2 Implications for Service Providers

The end-user profile (subscriptions, billing, preferences, etc.) has key implications for service providers when moving towards an end-user-centric world with an economically-viable model. From a service development and delivery point of view, a capability needs to be developed to flexibly define, prototype, launch, and modify new services leveraging the user profile. This capability must also orchestrate a complex end-to-end service delivery chain, including third parties. Service providers may also need to complement their own access portfolio through partnerships or wholesale agreements (*e.g.,* MVNO). They may need to adjust their marketing strategy in terms of branding, pricing, etc. Finally, service providers could integrate operational activities across fixed, mobile, broadband, and Internet divisions to benefit from synergy and scale effects.

To avoid commoditization, service providers must carefully decide which position to adopt along the value chain for delivering end-user services. Recognizing different service roles (*e.g.,* wholesale, retail, full service provider), the outcome of competitive dynamics between the service roles may be determined by which actor is the first to successfully transform. This implies that service providers need to move forward with a sustainable position in the service delivery value chain. A key to this will be enabling the end-user profile and allowing services growth, which benefits the user.

In order to enable the end-user profile, service providers should consider the following set of capabilities:

- *The NGN should support bundling based around the end-user, rather than siloed services based on technology*. From a marketing point of view, a consistent branding, go-to-market, and pricing approach across broadband, mobile, and Internet services is needed for these new service bundles, targeted at socio-demographic or vertical end-user segments.
- *From a service development and delivery point of view, a capability needs to be developed to flexibly define, prototype, launch, and modify new services.* Moreover, another capability is needed to orchestrate a complex end-to-end service delivery chain, including third parties.
- *From an operational point of view, sales, marketing, OSS/BSS, network infrastructures, and the like must be integrated* to benefit from scale and synergy opportunities.
- *From an organizational point of view, internal objectives and processes need to be aligned between mobile and broadband activities such that end-users are offered a single point of contact for customer support.* Moreover, potential gaps in a service provider's access, applications, or content portfolio may require augmentation through wholesale partnerships or other activities.

Having identified key capabilities for a service provider to successfully leverage the end-user profile, three capabilities have a profound implication on the underlying technology and solution architecture:

1. The need to complement a service provider's access portfolio with third party access, through different types of business models (*e.g.,* MVNO).

2. The need to rapidly prototype and deliver new services across different access networks, with the end-user profile being a key service component.
3. The need to consolidate operations, including OSS/BSS systems.

For each of these capabilities, the high-level business requirements for the underlying technology and Solution architecture are discussed in the following clauses.

2.6.2.1 Third party access

A list of business requirements for third-party access relates to the need to benefit from a single user profile, even when this user is not on the home network of the service provider:

- End-users should be able to access their services through a simple access and service authentication process.
- Service providers must be capable of securely accessing specific user profile information (*e.g.,* preference settings) from different networks.
- The NGN should support flexible consolidated collection of settlement information such as usage. For example, all services for an end-user may be charged through a single bill for postpaid, or a single account for prepaid, for seamless roaming services between access types such as mobile access and wireless broadband access.
- Service providers must also be capable of collecting user information from different access networks to the service providers' home network (*e.g.,* location information).

Another set of business requirements relate to the challenge of delivering the same service from the service provider who owns the end-user profile (including the service subscriptions) over a third party access network:

- Communication services must be delivered from any access network or technology to any other access network or technology.
- Application and content services must be delivered from the Service Delivery Environment to any access network.
- The solution architecture must accommodate different types of mobility between access networks (*e.g.,* nomadic services, roaming seamless handover, etc.), depending on the service providers' offering and interconnection relationships.

Business requirements that relate to the handling of the different access characteristics are inherent to each access medium (*e.g.,* DSL broadband versus wireless 2.5G):

- Services must be adjusted to fit the terminal and media characteristics of each access network (*e.g.,* bandwidth, QoS).
- Where necessary, different session related control protocols in access networks must be interworked with SIP in the NGN core.
- QoS and security (data integrity, data confidentiality, network security) must be maintained from a user viewpoint (or managed within the constraints of different technologies) across the access networks and the NGN core.
- The end-to-end service instance may span access networks that are independently administrated by separate service providers or use different technologies.

2.6.2.2 Service Delivery Environment

Business requirements for a service delivery environment relate to the delivery of new services using service capabilities -- *e.g.,* based on the information from the end-user profile:

- New services should be able to make use of the service providers' existing service capabilities (*e.g.,* presence), both from the 'telecom world' (*e.g.,* prepaid) and the 'IT world' (*e.g.,* AAA) in the context of NGN.
- New services should also be able to make use of third party service capabilities (*e.g.,* location).
- The Service Delivery Environment (SDE) should support third party applications by sharing service capabilities in a secure way, in order to create a kind of "eco-system."
- The service creation process should be supported by a service creation environment that encompasses both "Telecom" and "IT" services.

Business requirements relate to the openness to the service provider environment:

- The SDE should also be open to the end-user for self-management purposes -- *e.g.,* through web interfaces.
- The SDE should be able to interface with different access networks, through the appropriate protocols.
- The SDE should be capable of supporting a wide range of devices and CPE operating systems.
- The platform of the SDE should be highly scalable and reliable, as it will host most of the new revenue generating services.
- The SDE should be capable of interfacing with the new generation of operations systems (*e.g.,* OSS/BSS), without unnecessarily duplicating information

2.6.2.3 Consolidated operations

Operations consolidation covers BSS, OSS, network management, service provisioning, etc. Given its high level of complexity on the one hand, and a high degree of variation per service-provider on the other hand, further clarification is not provided in this document.

TMF has adopted an NGOSS architecture and data model that is applicable to this area. The ATIS Data Interchange FG has also addressed this. NGN operations are an area for further study as the NGN evolves.

3 ATIS NGN CONVERGED ARCHITECTURE

This clause provides the reference architecture diagrams to delineate the scope of work. It will provide examples of the interfaces that will need to be defined and the functionality that will need to be supported.

Figure 1 identifies the converged environment in which NGN services operate.

Figure 4 provides a reference architecture for NGN integration that elucidates some of the major interfaces that will need to be defined. This list includes:

- Customer premise interface to the access provider network. For Wireline access, these interfaces could include DSL technologies, optical technologies (such as GPON or WDM-PON), and so forth.
- Interfaces between the network infrastructure provider and the service and application providers.
- Interfaces between service providers.

3.1 Converged Architecture

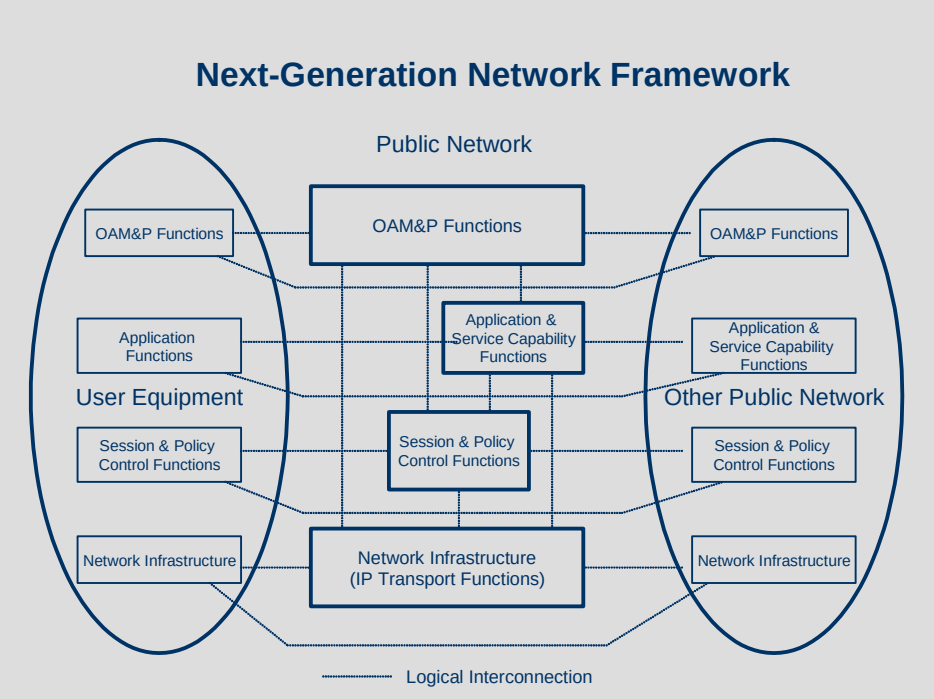

Figure 4 - Framework for a Common Architecture

The framework architecture shown in Figure 4 is based on the NGN Functional architecture currently under development by ETSI TISPAN [NGN Functional Architecture Release 1]. Figure 5 shows a high-level view of the TISPAN NGN architectural approach. The current TISPAN view of the functional components of the IMS, the components outside the IMS and the reference points between them are shown in Figure 6.

This view is still under development within TISPAN. To the extent possible, this functional view will be mapped to the ATIS NGN Framework in Figure 2. TISPAN is working with 3GPP to extend IMS to support additional access types. TISPAN is also defining non-IMS components (*e.g.*, NASS, RACS) as part of TISPAN's NGN architecture.

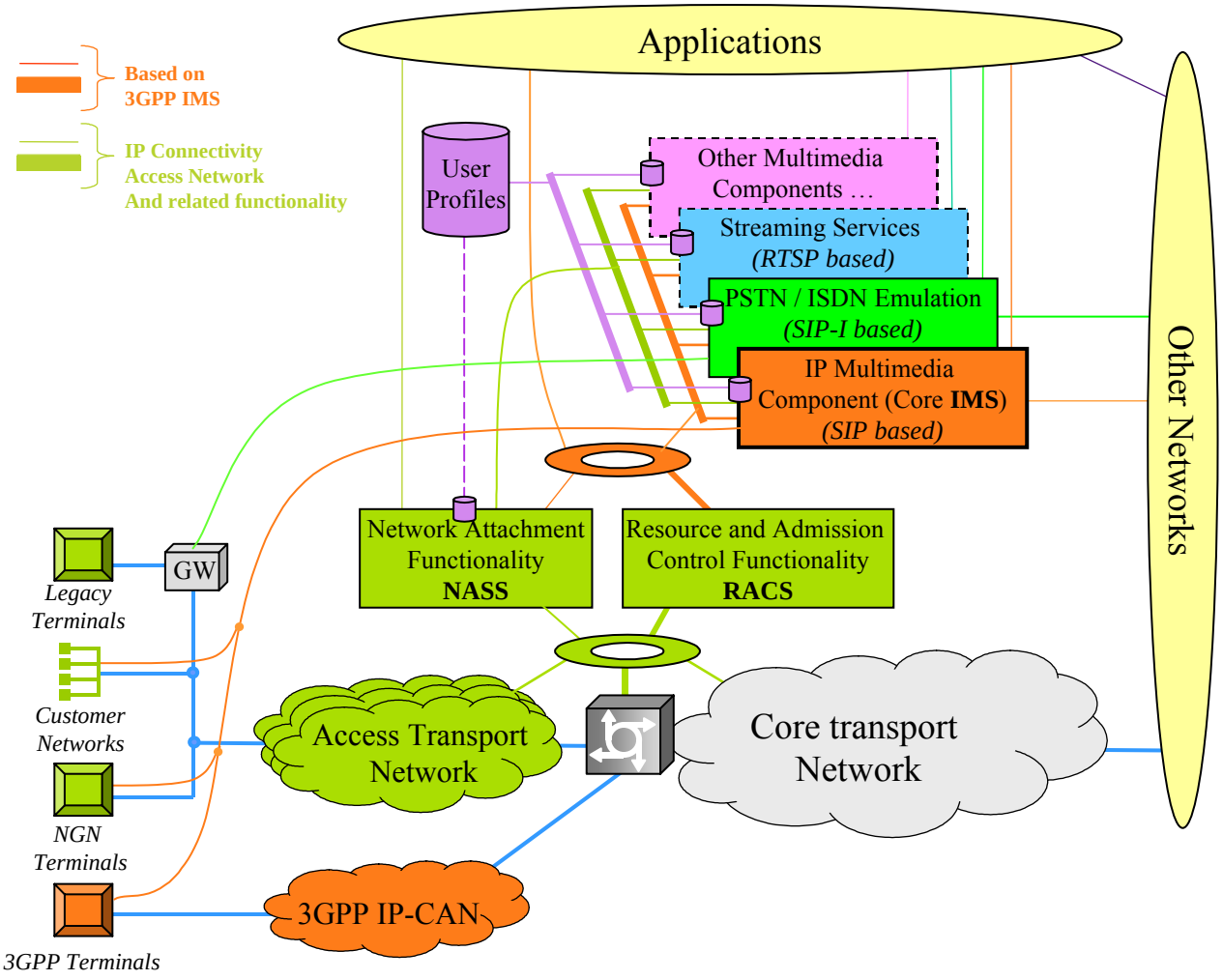

Figure 5 - TISPAN View of the NGN Architecture

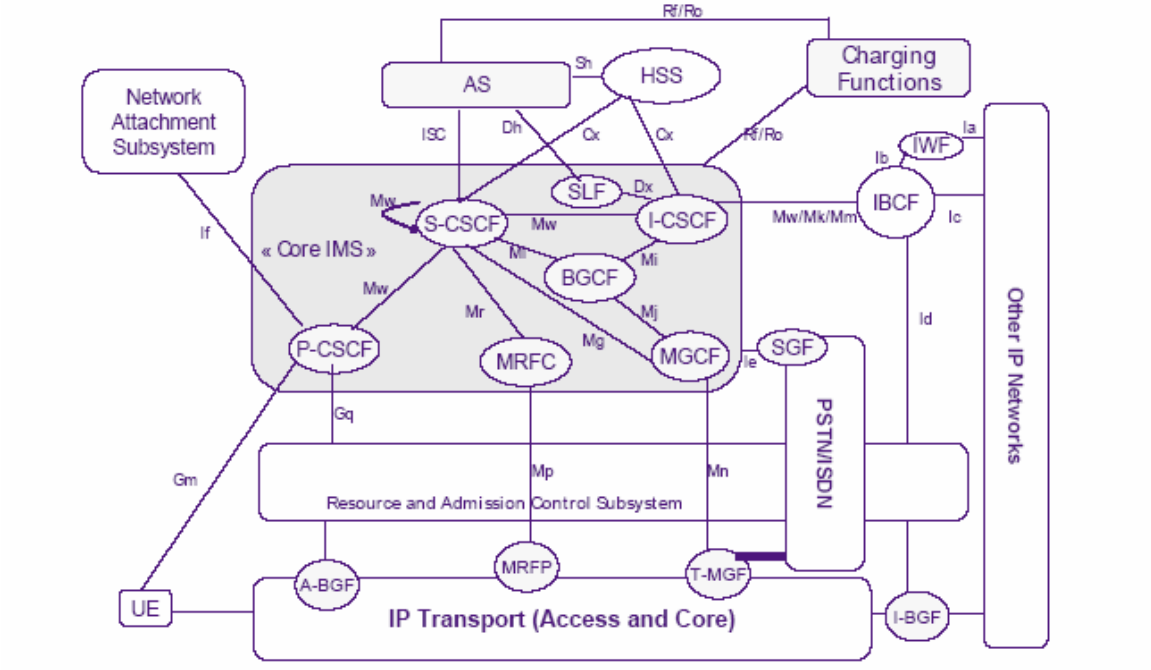

Figure 6 - ETSI TISPAN Extended IMS Architecture

3.2 Functional Components of the Converged Architecture

The following descriptions of the functions in the next-generation network framework are provided to help interpret Figure 4, and the diagrams after each clause provide a mapping of the different functions in ATIS NGN Framework to the TISPAN architecture shown in Figure 6. Figure 4 is not attempting to address the physical packaging of functions in the network or between networks. Nor is it attempting to address the deployment of functions in a centralized or distributed manner.

3.2.1 User Equipment

The user equipment comprises all the CPE including private networks and terminal devices. At its simplest, the user equipment may be a single device (*e.g.,* a mobile handset). The intent is to provide flexibility such that a variety of customer networks and end user equipment will be supported. A customer network may be self-managed, provider-managed, or unmanaged, using a variety of wired or wireless technologies. User equipment could consist of SIP phones, multi-media terminals, mobile phones, set top boxes, IP-PBXs, NAT/FW, servers, or residential gateways.

3.2.2 Other (Public) Networks

The NGN scope includes multiple administrative domains and their interconnections. The NGN also interconnects/interworks with other (non-NGN) networks to allow for end-to-end communications with users attached to these other networks. Examples include:

- IP network providers interworking with other access network technologies, such as wireline and wireless carriers; and
- IP network providers interworking with non-IP network technologies -- for example, the PSTN.

In mobile and nomadic service scenarios, application and control entities within one network may need to communicate with the infrastructure of another network. For example, one can consider a handoff for a cellular handset roaming onto a wireline infrastructure.

3.2.3 Public (NGN) Network

This clause provides an explanation of the functional block within a single instance of an NGN (*i.e.*,, a single service provider) as shown in Figure 4. Figure 4 is not attempting to address the physical packaging of functions, nor to specify whether these functions should be implemented in a centralized or distributed manner.

3.2.3.1 Network Infrastructure IP Transport Function

The network infrastructure IP transport function provides for the transport of IP data, control, and management plane traffic to and from all elements of the NGN. This function also provides for the bearer-data, control, and management plane peer interworking of traffic to and from other networks where required. This includes public and/or private access, core networks, and interworking functions and devices. A variety of wireline and wireless broadband access technologies are supported. Media gateways are elements of the network infrastructure. The network infrastructure IP transport function provides mechanisms to enforce the admission control decisions of the control block. The network infrastructure IP transport function also provides mechanisms to classify and differentiate network treatments between different classes of traffic -- *e.g.*, differentiated services and other transport services.

Figure 7 maps TISPAN extended IMS functional entities onto the network infrastructure IP transport function of the ATIS NGN Framework:

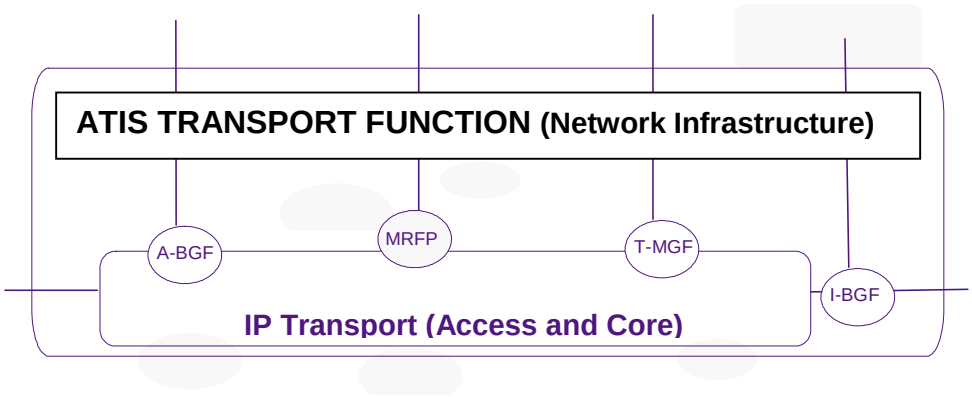

Figure 7 - Network Infrastructure IP Transport Functions

3.2.3.2 Session and Policy Control Functions

This block provides the session and policy control functions that implement all aspects of session management including session establishment, session continuity, session modification, and session termination. Examples of functions contained within the control block are Session Control, Authentication, and Admission Control (administrative and resource constraint policy decisions) across all types of sessions – unicast, multicast, unidirectional, bi-directional, multi-connection.

Control functions also include subscriber location and other capabilities offered by the network providers.

Figure 8 maps TISPAN extended IMS functional entities onto the ATIS Session and Policy Control functions.

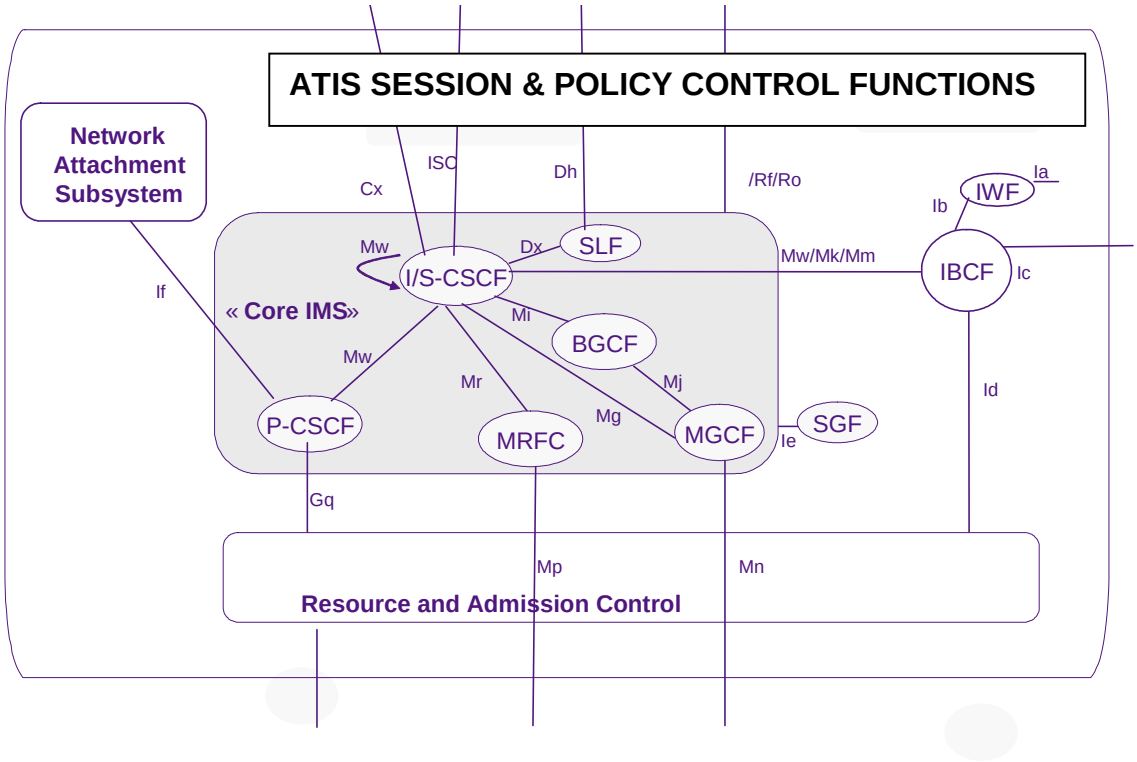

Figure 8 - Session & Policy Control Functions

3.2.3.3 Application and Service Capability Functions

The application and service capability functions block supports application processes that can be invoked by the application subscriber or the application control to perform value added services for end users. Common services such as user database and presence are examples. This layer may also include media resources such as: IVRs, announcement systems, and media servers.

Service capability consists in different Service Capability Servers (SCS) and a service framework. Examples of SCSs are user location and call control. The service framework includes functions such as service discovery and authentication. A SCS may invoke other SCSs as appropriate within the service framework in order to create complex services. Web services technology can be used for the service framework.

Figure 9 maps TISPAN extended IMS functional entities onto the ATIS Application and Service Capability functions.

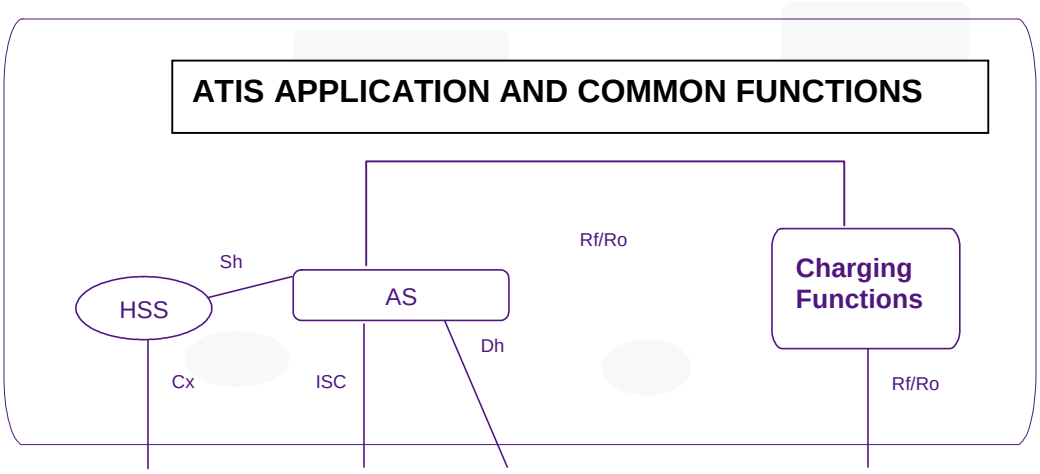

Figure 9 - Applications and Service Capability Functions

3.2.3.4 OAM&P Functions

This block contains Operations, Administration, Maintenance and Provisioning (OAM&P) functions required for an NGN. Fault, Configuration, Accounting, Performance, Security (FCAPS) functions are the basis for OAM&P.

As an example, provisioning/configuration may include such functions as required to enable subscriber creation of service instances through web portals, etc. Management services may also provide some control of network infrastructure in other networks for dynamic QoS -- for example, see DSLF WT102 for control of a DSL access network.

3.3 Multi-provider Perspective on NGN Architecture

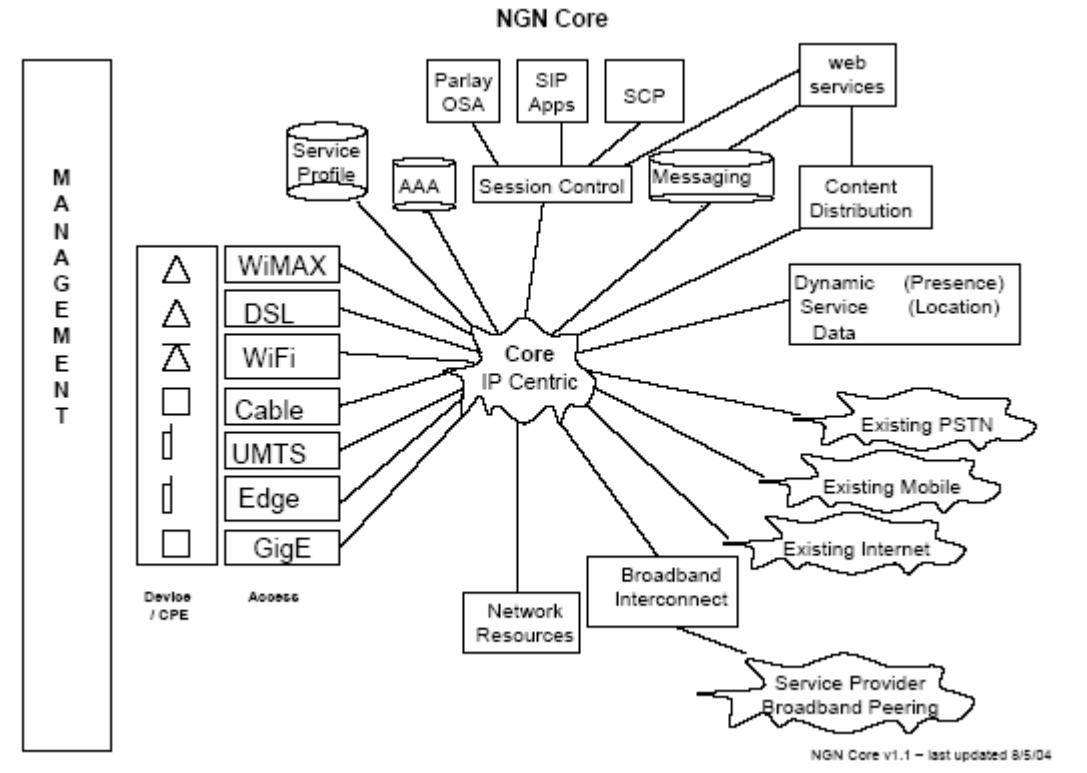

Figure 10 - Illustration of connectivity in a single provider NGN

Figure 10 provides a perspective of the functional components for service control and a variety of access mechanisms communicating through a common IP core. While this is one potential physical configuration, there may be other impacts to the configuration of the network based on the existence of various service provider boundaries. Figure 11 provides an example of a more decentralized physical perspective where different access mechanisms are supported by different service providers, including the possibility of some service providers' IP networks that provide transit rather than access services. The point is not to be prescriptive about a particular configuration of administrative boundaries, but rather to recognize the potential for their existence. In general, wide area services may reasonably expect to involve multiple service providers. A mapping of the control plane (IMS) infrastructure onto this physical infrastructure perspective is required. In general, there will be a requirement for multiple IMS instance to interoperate, and also for IMS systems to provide some level of service across infrastructures administered by other service providers where an IMS infrastructure may not exist.

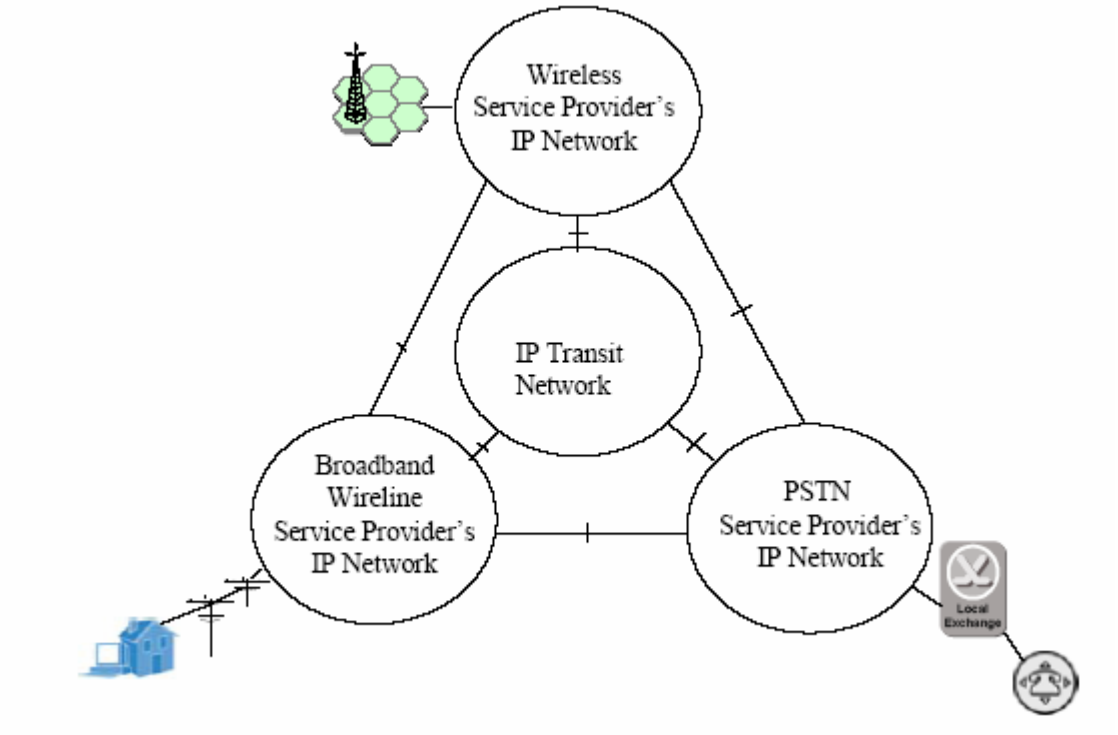

Figure 11 - Multiple Service Provider Connectivity Example

4 CONCLUSIONS

This document has been prepared as input to the global NGN standards initiatives. ATIS fully supports a consistent set of global NGN standards. A standards gap analysis is currently under way in ATIS NGN-FG. This will be input into the standards process. The draft Framework Part I document contains NGN target objectives and features. Phased implementation requirements will be developed for these target objectives and features. The NGN-FG will continue to clarify the priorities (*i.e.*,, short-term, medium-term, long-term).

A key motivation for the NGN is centered on the variety of new, value-added, IP centric services and applications. An equally important motivation is reduced CAPEX and OPEX through more efficient voice services. The ATIS NGN architecture described herein builds on 3GPP's IMS and TISPAN's NGN architecture to consistently support these new value-added services. The PSTN Emulation subsystem is identified as a mechanism to facilitate migration from legacy PSTN services to NGN. This enables expense reduction through more efficient voice services, while still allowing the NGN to be optimized for SIP services. The document identifies key IP-CAN requirements for compatibility with the core NGN. These include providing IP connectivity, QoS and policy enforcement.

ATIS will continue to work with groups such as TISPAN, 3GPP and ITU-T to develop a consistent set of NGN standards that meet the needs of ATIS members. To comply with unique North American requirements/ standards, ATIS plans to share with all internal technical committees and others where appropriate. ATIS welcomes comments on this document.

5 REFERENCES

ITU-T

TBD

3GPP

TBD

MSF

Final Implementation Agreements

MSF-IA-BICC.001-FINAL, *Implementation Agreement for BICC.*[7]

MSF-IA-MEGACO.001-FINAL, *Implementation Agreement for MEGACO/H.248 Profile for Media Gateway Controller/Access Gateway using ATM Trunks.*[3]

MSF-IA-MEGACO.002-FINAL: *Implementation Agreement for MEGACO/H.248 Profile for Media Gateway Controller/Trunking Gateway using ATM Trunks*

MSF-IA-MEGACO.003-FINAL: *Implementation Agreement for MEGACO/H.248 Profile for Media Gateway Controller/Trunking Gateway using IP Trunks*

MSF-IA-MEGACO.005-FINAL: *Multi-service Access Gateway Implementation Agreement (UK Market)*

MSF-IA-MGCP.001-FINAL: *Implementation Agreement for MGCP Profile for Call Agent to User Agent Interface*

MSF-IA-SDP.001-FINAL: *Implementation Agreement for SDP Usage and Codec Negotiation for GMI 2004*

MSF-IA-SIP-T.001-FINAL: *Implementation Agreement for SIP-T Profile for Media Gateway Controller*

MSF-IA-SIP.001-FINAL: *Implementation Agreement for SIP Profile, for Voice over IP, Between a Line-Side Media Gateway Controller and a Trunks Media Gateway Controller*

[7] This document available at < http://www.msforum.org/techinfo/approved/ >.

MSF-IA-SIP.002-FINAL: *Implementation Agreement for Core SIP Profile for Voice over IP*

MSF-IA-SIP.009-FINAL: *Implementation* Agreement for SIP Media Server Interface Final Physical Scenarios

MSF-TR-SCN04-001.00-FINAL: GMI *2004 Physical Test Scenarios Final Product Specifications*

MSF-PS-MTG-REQ-001.00-FINAL: *Product Specification for the Functional Requirements of an MSF Trunking Gateway* Draft *Implementation Agreements*

Draft Implementation Agreement for RSVP-TE

Draft Implementation Agreement for BGP/MPLS VPN

Draft Implementation Agreement for IP Line Side Gateway

Draft Implementation Agreement for Megaco/H.248 Profile for Media Gateway Controller and DSL Gateway

Draft Implementation Agreement for MPLS Support for Differentiated Services

DSL Forum

TBD

PacketCable™

TBD

6 ACRONYMS & ABBREVIATIONS

2.5G	2.5nd Generation Wireless	ARQ	Automatic Repeat Request
2G	2nd Generation	AS	Autonomous System
3G	3rd Generation	ASP	Application Service Provider
3GPP	3rd Generation Partnership Project	ATIS	Alliance for Telecommunications Industry Solutions
3GPP2	3rd Generation Partnership Project #2	AuC	Authentication Center
AAA	Access Authorization and Authentication	BB	Broadband
ACS	Automatic Configuration Server	BGCF	Breakout Gateway Call Function
AIN	Advanced Intelligent Network	BGP	Border Gateway Protocol
AP	Access Point	CALEA	Communications Assistance for Law Enforcement Act
API	Application Programming Interface	CAPEX	Capital Expense
ARIB	Association of Radio Industries and Businesses	CCSA	China Communications Standards Association

CDMA	Code Division Multiple Access
CP	Customer Premises
CPE	Customer Premises Equipment
DCMA	Digital Millennium Copyright Act
DHCP	Dynamic Host Configuration Protocol
DI	Data Interchange (& Billing)
DNS	Domain Name System
DoS	Denial of Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DSL-F	DSL (Digital Subscriber Line) Forum
DTMF	Sual Tone Multi-Frequency
E2E	End-to-End
E9-1-1	Enhanced 9-1-1
EDGE	Enhanced Data rate for GSM Evolution
EF	Expedited Forwarding
EFM	Ethernet in the First Mile
E-LMI	Ethernet Local Management Interface
EMS	Emergency Medical Service
ENUM	tElephone NUmber Mapping
ESIF	Emergency Services Interconnection Forum
ETSI	European Telecommunications Standards Institute
EVRC	Enhanced Variable Rate Codec
FCAPS	Fault, Configuration, Accounting, Performance, Security
FCC	Federal Communications Commission
FGNGN	Focus Group on Next Generation Networks
GETS	Government Emergency Telecommunications System
GGSN	Gateway GPRS Support Node
GMSC	Gateway Mobile Switching Center
G-PON	Gigabit Passive Optical Network
GPRS	General Packet Radio Service
GSM	Global System for Mobiles
HLR	Home Location Register
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
IA	Implementation Agreements
I-CSCF	Interrogating-Call Session Control Function
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Instant Messaging
IM-HSS	IM-Home Serving System
IMS	IP (Internet Protocol) Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP Connectivity Access Networks
IPFIX	IP Flow Information Export
IPGW	IP (Internet Protocol) Gateway
IPsec	Internet Protocol Security
ISP	Internet Service Provider
ISUP	ISDN (Inegrated Services Digital Network) User Part
IT	Information Technology
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector
IVR	Interactive Voice Response
LAES	Lawfully Authorized Electronic Surveillance
LAN	Local Area Network
LBS	Location Based Service
LE	Law Enforcement
LMI	Local Management Interface
LSP	Local Service Provider
MAN	Metropolitan Area Networks
MCU	Multi-Conference Unit
MGW	Media Gateway
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
MRF	Media Resource Functions
MSC	Mobile Switching Center
MSF	Multiservice Switching Forum
MTTF	Mean Time To Find
MTTR	Mean Time To Repair
MVNO	Mobile Virtual Network Operation
MWS	Mobile Wireless Service
NANP	North American Number Plan
NANPA	North American Numbering Plan Administration
NAT	Network Address Translation
NENA	National Emergency Numbering Association
NGN	Next Generation Network
NGN-FG	NGN Focus Group
NGOSS	Next Generation OSS
NGSP	Next Generation Service Provider
NI	Network Interface
NSP	Network Service Provider
OAM	Operations, Administration ,and Maintenance
OAMP *or* OAM&P	Operations, Administration, Maintenance, & Provisioning

OPEX	Operational Expense
OSA	Operator Service Agreements
OSS	Operations Support System
PBX	Private Branch Exchange
PC	Personal Computer
PCM	Pulse Code Modulation
P-CSCF	Proxy-Call Session Control Function
PCX	Private Communications Exchange
PDA	Personal Digital Assistant
PDB	Per Domain Behavior
PDF	Policy Decision Function *or* Portable Document Format
PLMN	Public Land Mobile Network
POTS	Plain Old Telephone Service
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee
QoS	Quality of Service
RAN	Radio Access Network
RFC	Request For Comment
RGW	Residential Gateway
SCS	Service Capability Servers
S-CSCF	Serving -- Call Session Control Function
SDE	Service Delivery Environment
SDO	Standards Development Organization
SG	Study Group
SGW	Signaling Gateway
SIM	Subscriber Identify Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SP	Service Provider
SPAN	Service and Protocol for Advance Networks
SS7	Signaling System 7
TCP	Transmission Control Protocol
TDD	Terminal Device for the Deaf
TDM	Time Division Multiplex
Telco	Telecommunications Company
TIA	Telecommunications Industry Association
TIPHON	Telecommunications and Internet Protocol Harmonization Over Networks
TISPAN	Telecommunications and Internet Converged Services & Protocol for Advance Networks
TMF	Telemanagement Forum
TOPS	Technology and Operations (Council)
TTA	Telecommunications Technology Association
TTC	The Telecommunications Technology Committee
TTY	Text Telephony
UDP	User Datagram Protocol
UE	User Entity
UICC	USIM Integrated Circuit Card (UICC)
UMTS	Universal Mobile Telecommunications System
USIM	Universal Subscriber Identity Module
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VNO	Virtual Network Operators
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual Private Network
VSO	Virtual Service Operations
WAE	Wide Area Ethernet
WAN	Wide Area Network
WDM-PON	Wavelength Division Multiplexing Passive Optical Network
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
XMPP	Extensible Messaging and Presence Protocol

ANNEX A

The information in this Annex represents a snapshot of the evolution to NGN being considered in 3GPP and ETSI TISPAN. This information may change.

A.1: SM Release 99

Given this starting point, the following focuses on evolution of the mobile network to leverage this common infrastructure. Figure 12 shows a first phase of achieving convergence for a carrier-hosted

enterprise communications and a Release 99 cellular implementation. With Release 99 deployment, 3G components are introduced in both the Wireless Home Network and the Cellular Affiliate Serving Network. Thus a Release 99 network can provide 2G/3G functionality from the start. However, having 3G components in the network does not presuppose the availability of IMS, since IMS is only possible starting from Release 5 implementations. Accordingly, both 2G and 3G network elements are shown.

Note that the media gateway is directly connected to the PSTN as opposed to a direct connection to the gateway MSC. This allows hosted communications users to interoperate with the PSTN without passing through the gateway MSC before connecting to the rest of the PSTN. Connections between hosted communications uses and Release 99 cellular users are routed through the PSTN using the normal routing procedures.

In this phase, the level of convergence that the NGN should support is access to common data applications and circuit-switched interoperation for cellular users. Convergence services based on existing terminal capabilities of the legacy networks can also be offered. The call control and the service logic for such are contained in the Application & Serving Complex.

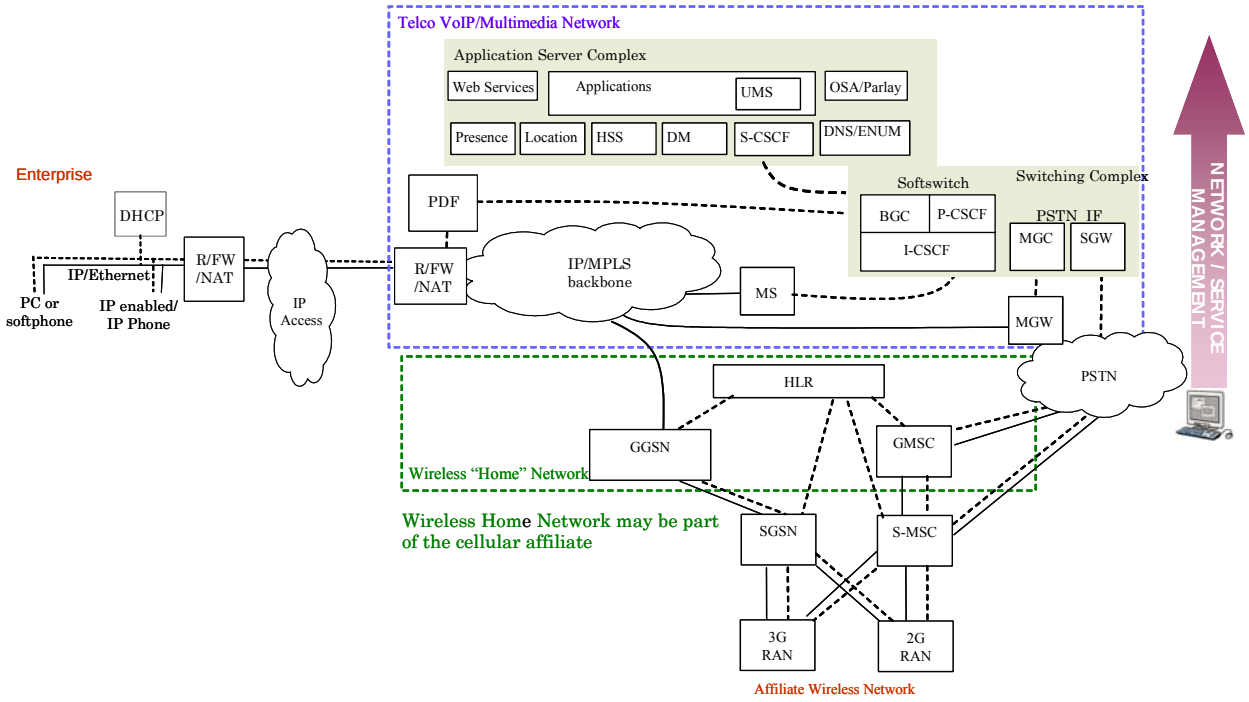

Figure 12 - Convergence with GSM Release 99 implementation

A.2: UMTS Release 4

From a service convergence point-of-view, this scenario is identical to the previous one. The NGN inter-network connectivity can be optimized if the converged service provider owns the MSC server. In this case, the MSC server can be connected directly to the IP backbone of the converged service

provider. In the previous scenario, this connection is made through PSTN connections. As shown in Figure 13 below, the MSC Server and MGW are introduced to support the option of an initial NGN architecture in the Mobile Circuit-Switched Domain.

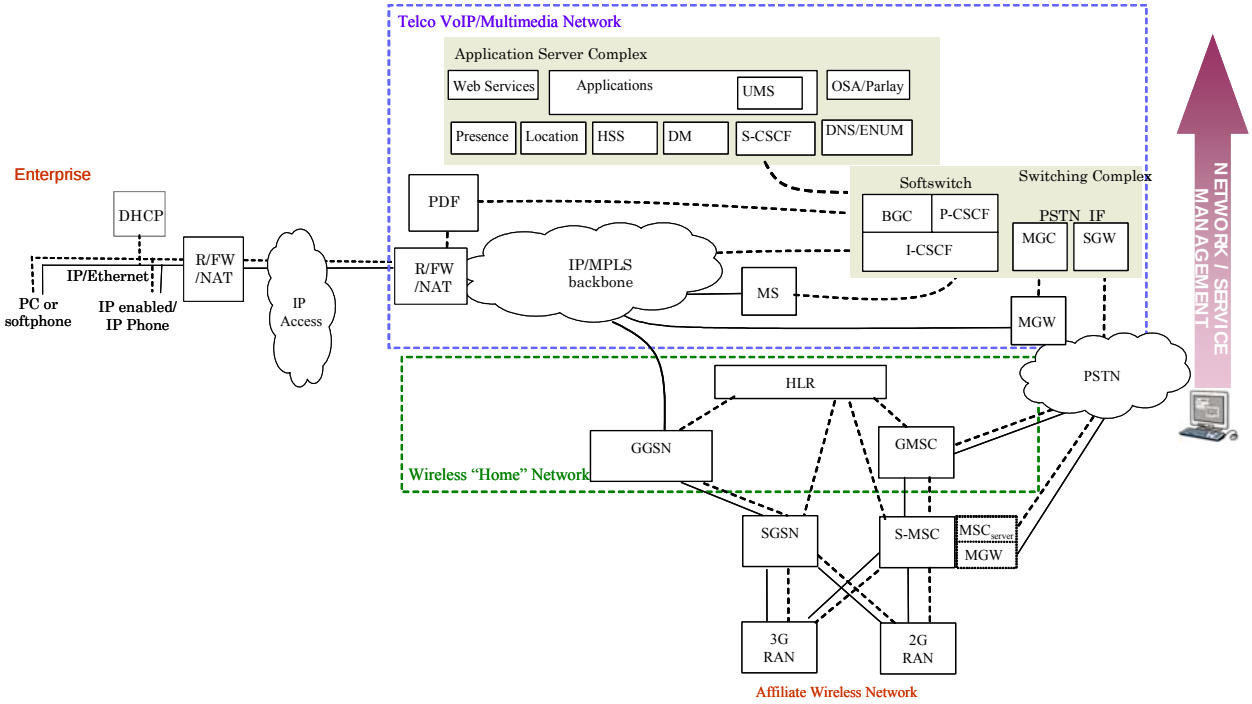

Figure 13 - Convergence with UMTS Release 4 core network implementation

A.3: UMTS Release 5-6

The next evolution stage that should be supported by NGN introduces the 3GPP-defined IMS. This IMS compliant architecture as shown in Figure 14 below indicates the first IMS component that is encountered in the SIP signaling path as the P-CSCF shown in the Wireless "Home" Network. The P-CSCF is connected through the GGSN, SGSN, and 3G RAN to the end user terminal upon registration of the terminal in the network.

The second IMS component encountered in the signaling flow is the I-CSCF. The SIP signaling flows between the P-CSCF and the I-CSCF. In the reference architecture, a BGCF is also present. This can be either in the fixed network via the MGCF and the media gateway, or it can be in the mobile network via the MSC server and the media gateway. This function is used to determine the network where a breakout to the PSTN has to occur.

The P/I-CSCF and the BGCF are present in the Wireless Home Network if the converged service provider does not own this network. The converged service provider network also contains these elements; however, it also contains the S-CSCF by definition, which is associated with the Application & Serving Complex.

The HSS is positioned in the converged service provider network. According to 3GPP standards, the HSS can contain the HLR/AuC and the IM-HSS, which is the IMS database containing IMS subscriber data.

The PDF function has been added to the wireless network to provide policy control. The difference between Release 5 and Release 6 is the following: in Release 5, the PDF is integrated within the P-CSCF using a proprietary interface, while in Release 6 this interface becomes standardized and can be shared with other applications.

The connection between the GMSC (MSCserver/MGC) is retained to indicate the capability remains to establish normal circuit switched calls.

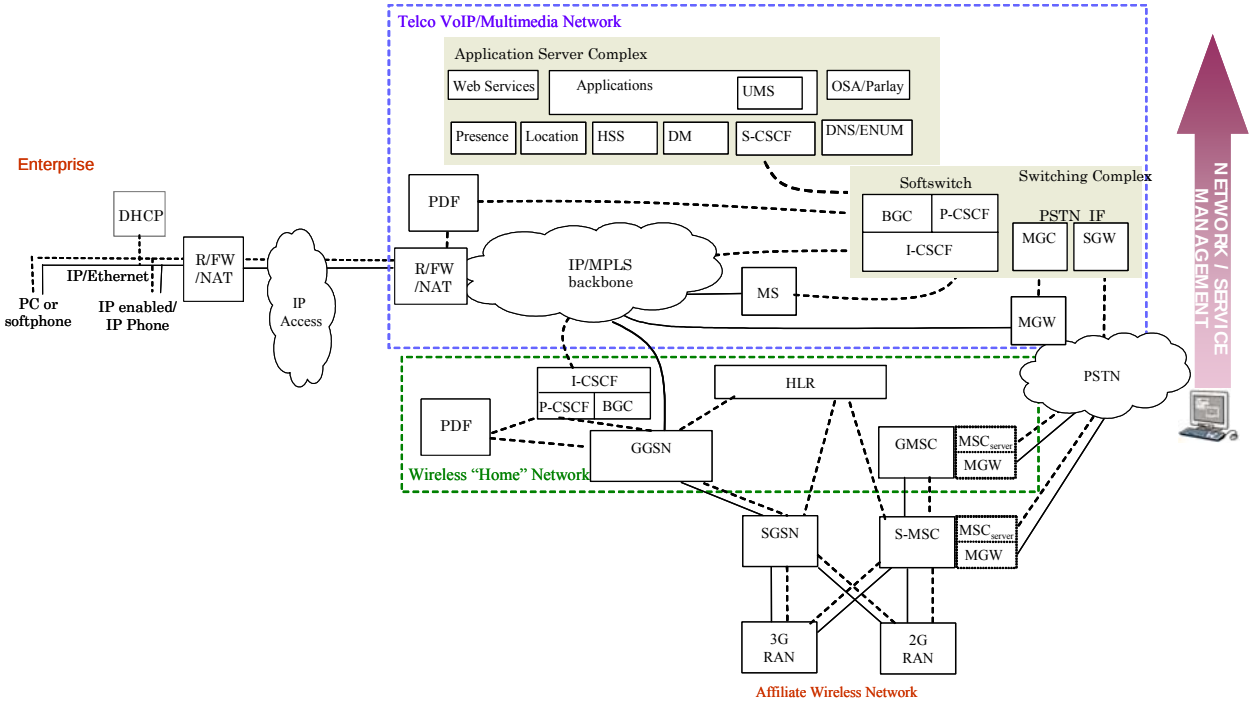

Figure 14 - Convergence with UMTS Release 5-6 core network implementation

A.4: Interworking with WLAN

Interworking with WLAN access can be easily obtained by extending the IMS architecture to WLAN components. The following figure indicates this with interconnections of WLAN users achieved by integrating the WLAN GW functionality into the GGSN in Wireless "Home" Network. This approach allows a single signaling connection towards the already present IMS components. A link towards the PDF is also leveraged. The WLAN AAA function handles user subscription information and access

authentication data. For this purpose, a link towards the AAA/HLR function is added supporting SIM-based authentication.

A public WLAN architecture is completed with a WLAN Access Control thereby completing the architecture to provide the common applications using common enablers over a common core to all connected users; WLAN, Enterprise, Residential, or Cellular.

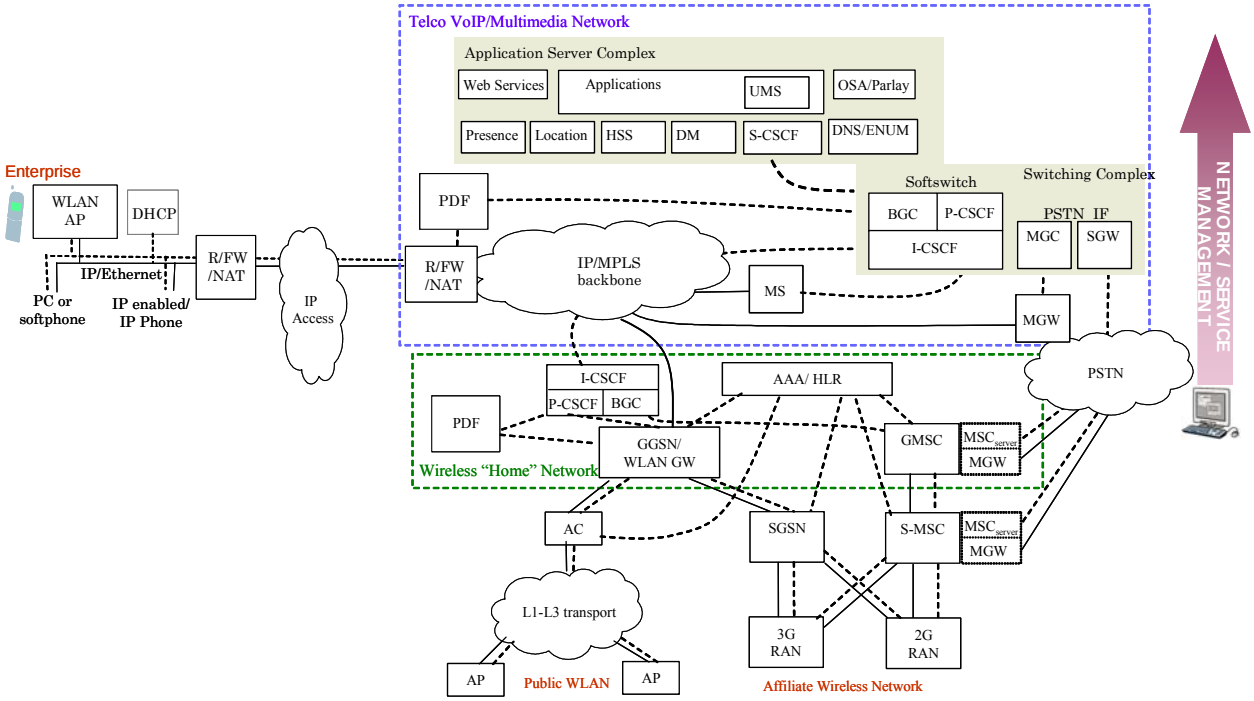

Figure 15 - Convergence with Wireless LAN access

A.5 Generic Access

Generic access provides wireless LAN or Bluetooth access to the wireless home network, without changes to the underlying infrastructure. It can therefore be viewed as equivalent to the traditional wireless access. There is no need to consider this further in the NGN context.

A.6 Extended IMS

Figure 16 below has been drawn to reflect consistency with our previous drawings; however, the functional blocks previously shown in the "Telco VoIP/Multimedia" and Wireless "Home" networks are now shown within a single Converged VoIP/Multimedia Network to reflect the architecture when a single service-provider operates both. In this case, there is no need to duplicate functions such as the P-CSCF, I-CSCF, and PDF in the operator network.

The enterprise environment has been redrawn as a Converged Enterprise indicating network interoperation. The figure also highlights support of a VoIP architecture for residential consumers. Please note that the "Telco VoIP/ Multimedia Network" is identical to those represented in the previous figures. The DSL or other broadband access network may be owned and/or operated by the Telco, although it is not required.

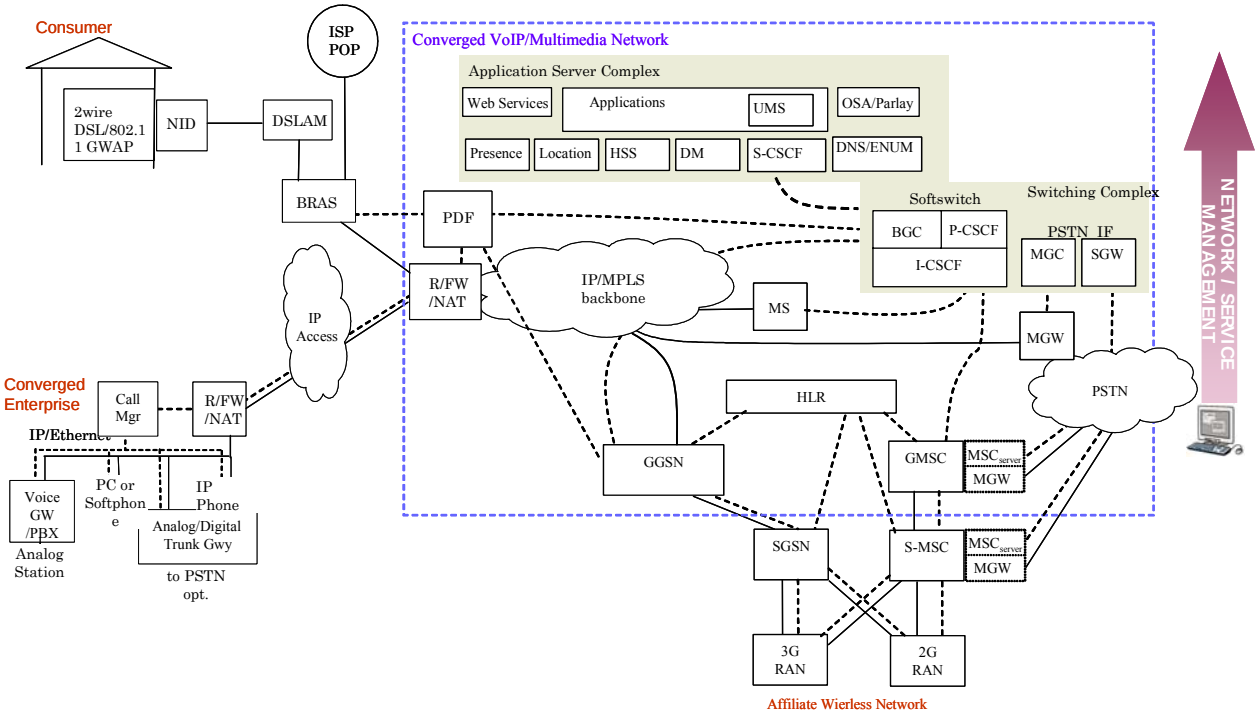

Figure 16 - Converged Service-Provider Architecture

FOCUS GROUP MEMBERS

Company	Name
Nortel Networks	Greg Mumford, Leader
Acterna	Jay Stewart
ADC Wireline Business Unit	Dieter Nattkemper
ADTRAN	Kevin Schneider
ADTRAN	David Williams
ADTRAN	Marc Kimpe, Ph.D.
Agilent	Larry Holmberg
Alcatel	Frederick H. Skoog
Alcatel	Gary Hanson
Alcatel	Ken Biholar
Alcatel	Larry O'Pella
AT&T Labs	Charles Dvorak
BellSouth	Steven Wright
BellSouth	Andrew Vernon
BT Group	Keith Dickerson
CenturyTel	Wayne Davis
Ciena Corporation	Andrew Deczky
Ciena Corporation	Dr. Rajender Razdan
Cisco	Chip Sharp
Cisco	Monique Morrow
Cisco	Art Reilly
Cisco	Dave Meyer
Ericsson, Inc.	Asok Chatterjee
Ericsson, Inc.	Stephen Hayes
Ericsson, Inc.	Susana Sabater
Harris Microwave Communications Division	Carl Day
Harris Corporation	Jerry Sonnenberg
Intrado	Ray Paddock
Intrado	Mike Nelson

Company	Name
Intrado	Larry Ciesla
Leapstone Systems, Inc.	Matt Milford
Leapstone Systems, Inc.	Chris Daniel
Lucent Technologies, Inc.	Hui-Lan Lu
Lucent Technologies, Inc.	Stu Goldman
Lucent Technologies, Inc.	William (Bill) J. Bushnell
Net.com	Craig Forbes
Net.com	Colin Mead
Nokia	Ed Ehrlich
Nortel Networks	Jim McEachern
Nortel Networks	Ron Ryan
Qwest	Mike Fargano
Qwest	Joe Huggins
Qwest	Balan Nair
SBC	Jeff Johnson
SBC	Will Chorley
SBC	Steve Mueller
SBC	Bernard Ku
SBC	Chuck Bailey
Siemens ICN	Rudolf Brandner
Siemens ICN	David Francisco
Siemens ICN	Derek Underwood
Siemens ICN	Dr. Klaus Pulverer
Telcordia Technologies	Dave Sincoskie
Telcordia Technologies	Dr. Tao Zhang
Telcordia Technologies	Fuchun Joe Lin
T-Mobile	Gary Jones
Verizon	Bhumip Khasnabish

- End of Part I -