ATIS STANDARD

ATIS-0300104

ATIS Standard on -

Next Generation Interconnection Interoperability Forum (NGIIF)

Next Generation Network (NGN) Reference Document

NGN Basic, Emergency Services, NGN Testing, and Network Survivability

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Published by

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

ATIS-0300104

[Including ATIS-0300109, ATIS-0300111, and ATIS-0300112]

ATIS Standard on

Next Generation Interconnection Interoperability Forum (NGIIF)

Next Generation Network (NGN) Reference Document

NGN Basic, Emergency Services, NGN Testing, and Network Survivability

Alliance for Telecommunications Industry Solutions

Updated September 2019

Abstract

This document provides basic information regarding Next Generations Networks, as applicable to the Next Generation Interconnection Interoperability Forum (NGIIF).

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between service providers (SPs), customers, and manufacturers. The Next Generation Interconnection Interoperability Forum (NGIIF) addresses next-generation network interconnection and interoperability issues associated with emerging technologies. Specifically, it develops operational procedures which involve the network aspects of architecture, disaster preparedness, installation, maintenance, management, reliability, routing, security, and testing between network operators. In addition, the NGIIF addresses issues which impact the interconnection of existing and Next Generation Networks (NGNs) and facilitate the transition to emerging technologies.

The mandatory requirements are designated by the word shall and recommendations by the word should. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word may denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, NGIIF, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, NGIIF, which was responsible for its development, had the following leadership:

K. Riepenkroger, NGIIF Co-Chair (Sprint)

R. Ryan, NGIIF Co-Chair (Comcast)

Table of Contents

Table of Figures

Table of Tables

ATIS Standard on –

Next Generation Interconnection Interoperability Forum (NGIIF) NGN Reference Document

NGN Basics, Emergency Services, NGN Testing, and Network Survivability

1 Scope, Purpose, & Application

1.1 Scope

The suite of NGN Reference Documents provides basic information regarding Next Generation Networks (NGNs), as applicable to the Alliance for Telecommunications Industry Solutions (ATIS) Next Generation Interconnection Interoperability Forum (NGIIF). The NGN is a multi-service, multi-vendor, multi-provider managed packet-based network, which is able to provide telecommunication services and is able to make use of multiple broadband, quality of service (QoS)-enabled transport technologies and in which service related functions are independent from underlying transport related technologies.

This document identifies items that could potentially impact government-managed emergency services, such as Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP) when telecommunications facilities in the NGN are consolidated and newer technologies (e.g., IP, fiber, Ethernet) are implemented.

It also describes the effects of adoption of NGN National Security and Emergency Preparedness (NS/EP) priority services. Included in the document are descriptions regarding Enhanced Overload Performance (EOP) precedence in Code Division Multiple Access (CDMA) networks, Universal Mobile Telecommunications Standard (UMTS) handover to Global System for Mobile Communications (GSM), and the transition to Next Generation 9-1-1 emergency services.

Additionally, this document has been developed to assist network managers by providing guidelines to serve as a general framework in planning for traffic management during high level congestion events or disaster conditions, such as the following (not all-inclusive):

- Network congestion due to facility failures or abnormal calling periods
- Switch or network failures or extended outages
- SS7 network failures
- Voice over IP (VoIP) network failures
- Natural disasters
- Pandemic events
- Major accidents
- Civil disturbances

It also addresses survivability of communications networks and the services those networks provide under failure conditions. Communications networks should be designed and should operate to meet users' expectations regarding network survivability. There should be a common understanding of network survivability assessment techniques. This document references the architectures and services of communications industry segments (i.e., wireline, Internet, wireless, cable, and satellite) and provides references for further information.

1.2 Purpose

The purpose of this document is to outline several aspects of the NGN, some of which include communicating to the industry the effects of transitioning emergency services from circuit switched to NGN and providing basic testing information and references for testing in an NGN environment. It assists interconnected network operators in developing and implementing strategies that ensure the continued operation of communication/facilities before, during, and after an incident.

1.3 Application

This Standard should be used by emergency service providers (SPs) and vendors to understand the effects of transitioning emergency services from circuit switched to NGN.

2 References

The following documents/standards contain information which is referenced within this guideline. At the time of publication, the editions indicated were valid. All documents/standards are subject to revision, and the reader is encouraged to investigate the possibility of applying the most recent editions of the standards and/or documents indicated below.

ITU-T Recommendation Y.2001 (12/2004), *General Overview of NGN.*[1]

ATIS-1000018, *NGN Architecture.*[2]

ATIS-0100002, *Reliability Aspects of Next Generation Networks.*[3]

ATIS-1000113, *Signaling System No. 7 (SS7) – Integrated Service Digital Network (ISDN) User Part.*[4]

IETF RFC 3935, *A Mission Statement for the IETF.*[5]

ATIS-1000061, *LTE Access Class 14 for National Security and Emergency Preparedness (NS/EP) Communications.*[6]

3GPP TS 36.331, version 8 or above, *Evolved Universal Terrestrial Radio Access (E-UTRA), Radio Resource Control (RRC); Protocol specification.*[7]

ATIS-1000009, *IP Network-To-Network Interface (NNI) Standard for VoIP.*[8]

ATIS-1000026, *Session Border Controller Functions and Requirements.*[9]

ATIS-1000038, *Technical Parameters for IP Network to Network Interconnection Release 1.0.*[10]

ATIS-1000039, *Testing Configuration for IP Network to Network Interconnection Release 1.0.*[11]

ATIS-1000040, *Protocol Suite Profile for IP Network to Network Interconnection Release 1.0.*[12]

[1] This document is available from the International Telecommunications Union. <http://www.itu.int>.

[2] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at <https://www.atis.org/docstore/>.

[3] This document is available from ATIS at <https://www.atis.org/docstore/>.

[4] This document is available from ATIS at <https://www.atis.org/docstore/>.

[5] This document is available from the IETF <http://www.ietf.org>.

[6] This document is available from ATIS at <https://www.atis.org/docstore/>.

[7] This document is available from the Third Generation Partnership Project (3GPP) <http://www.3gpp.org>.

[8] This document is available from ATIS at <https://www.atis.org/docstore/>.

[9] This document is available from ATIS at <https://www.atis.org/docstore/>.

[10] This document is available from ATIS at <https://www.atis.org/docstore/>.

[11] This document is available from ATIS at <https://www.atis.org/docstore/>.

[12] This document is available from ATIS at <https://www.atis.org/docstore/>.

ATIS-1000041, *Test Suites for IP Network to Network Interconnection Release 1.0.*[13]

ATIS-1000014, *VoIP Network-to-Network Interface Testing Framework.*[14]

ATIS-1000053, *Emergency Telecommunications Service (ETS) Profile and Tests for IP Network-to-Network Interconnection.*[15]

ATIS-0300100, *IP Network Disaster Recovery Framework.*[16]

ATIS-0300202, *Internetwork Operations – Guidelines for Network Management of the Public Telecommunications Networks under Disaster Conditions.*[17]

ATIS-0100019, *NRSC Hurricane Checklist.*[18]

ATIS-0100018, *NRSC Pandemic Checklist.*[19]

ATIS-1000061, *LTE Access Class 14 for National Security and Emergency Preparedness (NS/EP) Communications, 2015*[20]

ATIS-1000065, *Emergency Telecommunications Service (ETS) Evolved Packet Core (EPC) Network Element Requirements, 2015*[21]

ATIS-1000066*, Emergency Telecommunications Service (ETS) Network Element Requirements for IMS-Based Next Generation Network (NGN) Phase 2, 2016*[22]

ITU-T Recommendation Y.2011 (10/2004), *General Principles and General Reference Model for Next Generation Networks.*[23]

ITU-T Recommendation Y.2012 (04/10), *Functional Requirements and Architecture of the NGN.*[24]

Executive Order No. 13618, 6 July 2012, Vol. 77, No. 133, Federal Register 40779, "Assignment of National Security and Emergency Preparedness Communications Functions," which revoked and superseded Executive Order No. 12472, 3 April 1984, as amended by Executive Order No. 13286 of 28 February 2003.[25]

IETF RFC 3261, *SIP: Session Initiation Protocol.*[26]

IETF RFC 5390, *Requirements for Management of Overload in the Session Initiation Protocol.*[27]

In the Matter of The Development of Operational, Technical and Spectrum Requirements, For Meeting Federal, State and Local Public Safety Agency Communication Requirements Through the Year 2010, WT Docket No. 96-86, *Second Report and Order* FCC 00-242, July 3, 2000.[28]

[13] This document is available from ATIS at <https://www.atis.org/docstore/>.

[14] This document is available from ATIS at <https://www.atis.org/docstore/>.

[15] This document is available from ATIS at <https://www.atis.org/docstore/>.

[16] This document is available from ATIS at <https://www.atis.org/docstore/>.

[17] This document is available from ATIS at <https://www.atis.org/docstore/>.

[18] This document is available from ATIS at <https://www.atis.org/docstore/>.

[19] This document is available from ATIS at <https://www.atis.org/docstore/>.

[20] This document is available from ATIS at <https://www.atis.org/docstore/>.

[21] This document is available from ATIS at <https://www.atis.org/docstore/>.

[22] This document is available from ATIS at <https://www.atis.org/docstore/>.

[23] This document is available from the International Telecommunications Union at <http://www.itu.int>.

[24] This document is available from the International Telecommunications Union at <http://www.itu.int>.

[25] This document is available from the Federal Register at < https://www.federalregister.gov>.

[26] This document is available from the IETF at <https://www.ietf.org>.

[27] This document is available from the IETF at <https://www.ietf.org>.

[28] This document is available from the Federal Communications Commission (FCC) at <www.fcc.gov>.

3GPP TR 22.952 version 6.3.0 Release 6, *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Priority service guide.*[29]

TIA/EIA TSB16-A, *Assignment of Access Overload Classes in the Cellular Telecommunications Services.*[30]

3GPP TS 22.011 V13.1.0, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Accessibility (Release 2014).*[31]

CSRIC II WG-4B, *Final Report, Transition to Next Generation 9-1-1*, March 2011.[32]

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions

For definitions of common terms used in this document, please see the ATIS Telecom Glossary, which is located at http://www.atis.org/glossary/.

3.2 Acronyms & Abbreviations

3GPP	Third Generation Partnership Project
AC	Access Class
ACB	Access Class Barring
ANI	Application-to-Network Interface
APCO	Association of Public-Safety Communications Officials
AOC	Access Overload Class
ASC	Access Service Customer
ARP	Allocation and Retention Priority
ASP	Access Service Provider
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
AVP	Attribute-Value Pair
BSC/BTS	Base Station Controller / Base Transceiver Station
CDMA	Code Division Multiple Access
COS	Class of Service
CPC	Calling Party Category
CSN	Circuit-Switched Network
CSRIC	Communications Security, Reliability and Interoperability Council
DHS	Department of Homeland Security
DiffServ	Differentiated Services
DIRS	Disaster Information Reporting System
DRH	Directed Retry Handover
DoS	Denial of Service
DSCP	Differentiated Services (DiffServ) Code Point
EOC	Emergency Operations Center

[29] This document is available from 3GPP at <http://www.3gpp.org>.

[30] This document is available from the Telecommunications Industry Association (TIA) at <http://www.tiaonline.org>.

[31] This document is available from the Third Generation Partnership Project (3GPP) <http://www.3gpp.org >.

[32] This document is available from the Federal Communications Commission (FCC) at <www.fcc.gov>.

ECD	Emergency Communications Division
EOP	Enhanced Overload Performance
EPC	Evolved Packet Core
ESNET	Namespace header for priority calls
ETS	Emergency Telecommunications Service
EV-DO	Evolution Data Optimized
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Administration
FGNGN	ITU-T Focus Group on Next Generation Networks
GETS	Government Emergency Telecommunications Service
GSM	Global System for Mobile Communications
HPA	High Priority Access
HSS	Home Subscriber Server
HSPA	High Speed Packet Access
IAM	Initial Address Message
IETF	Internet Engineering Task Force
IMS	Internet Protocol Multimedia System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
I-CSCF	Interrogating Call Session Control Function
KPP	Key Performance Parameter
LTE	Long Term Evolution
MCS	Mobile Switching Center
MIMO	Multi-Input Multi-Output
MME	Mobility Management Entity
MLPP	Multilevel Precedence and Preemption
MPLS	Multiprotocol Label Switching
MTP	Message Transfer Priority
NACF	Network Attachment Control Functions
NARUC	National Association of Regulatory Utility Commissioners
NCS	National Communications System
NCSL	National Conference on State Legislatures
NE	Network Element
NENA	National Emergency Number Association
NGIIF	Next Generation Interconnection Interoperability Forum
NGN	Next Generation Network
NGN-GSI	NGN Global Standardization Initiative
NNI	Network-to-Network Interface
NORS	Network Outage Reporting System
NRSC	Network Reliability Steering Committee, an ATIS Committee
NS/EP	National Security and Emergency Preparedness
OAM&P	Operations, Administration, Maintenance, and Provisioning
OEC	Office of Emergency Communications

OSS	Operations Support System
P-CSCF	Proxy Call Session Control Function
PCI	Preemption Capability Indicator
PCRF	Policy and Charging Rules Function
PGW	Packet Gateway
PIN	Personal Identification Number
PSAP	Public-Safety Answering Point
PSIST	Persistence Parameter
PSTN	Public Switched Telephone Network
PTSC	Packet Technologies and Systems Committee, an ATIS Committee
PVI	Preemption Vulnerability Indicator
QoS	Quality of Service
QCI	QoS Class Identifier
RACF	Resource and Admission Control Functions
RACH	Reverse Access Channel
RAN	Radio Access Network
RPH	Resource Priority Header
SBC	Session Border Controller
S-CSCF	Serving Call Session Control Function
SGW	Serving Gateway
SIP	Session Initiation Protocol
SONET	Synchronous Optical Network
SP	Service Provider
SR	Selective Router
SS7	Signaling System 7
TAS	Telephony Application Server
TDM	Time Division Multiplexing
TMOC	Telecom Management and Operations Committee, an ATIS Committee
TSP	Telecommunications Service Priority
TR	Technical Report
UMTS	Universal Mobile Telecommunications Standard
UNI	User Network Interface
UTRAN	Universal Terrestrial Radio Access Network
VoLTE	Voice over LTE
VoIP	Voice over Internet Protocol
WATS	Wide Area Telecommunication Service
W-CDMA	Wideband CDMA
WDM	Wavelength-Division Multiplexing.
WPS	Wireless Priority Service

4 General Overview of NGN

In the past, traditional networks, such as the Time Division Multiplexing (TDM)/Public Switched Telephone Network (PSTN), were designed to carry voice traffic. As demand for data communications increased, SPs adapted their networks to also carry data traffic. Rather than replacing the PSTN, SPs began parallel operations, which came to be known as an overlay network. These new overlay networks were designed to carry data traffic. Networks multiplied as network technology continued to grow. As a result, SPs can run six (6) to twelve (12) different networks platforms (i.e., ATM, IP, Relay, X.25 PSTN, VoIP, etc.). NGN is a multi-service architecture that is capable of supporting all traffic types while facilitating service innovation.

NGN is an edge-to-edge packet-based network that seamlessly supports data and voice services, video and multimedia services, and other advanced features (See Figure 4.1).

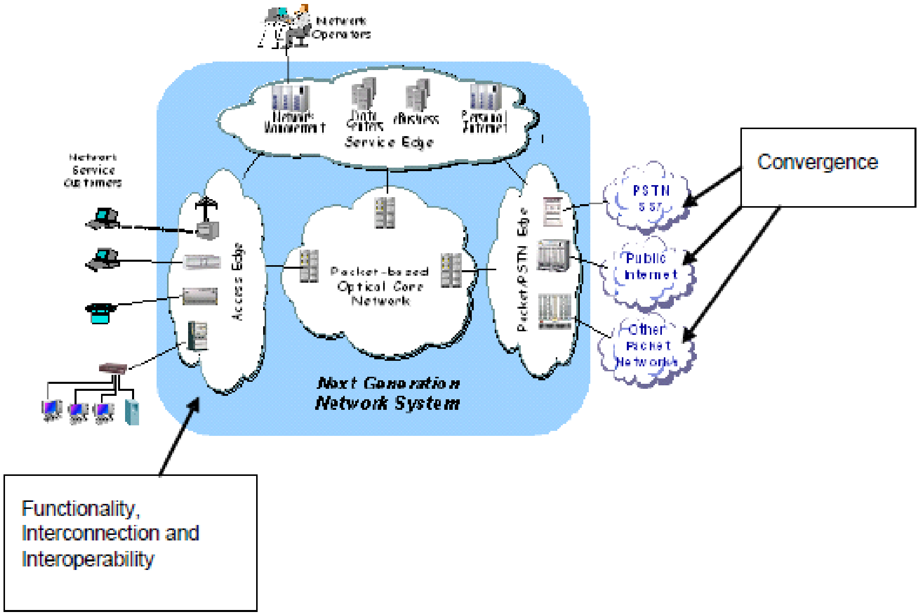


Figure 4.1- NGN Basics

5 Fundamental Characteristics of NGN

The NGN is characterized by the following fundamental aspects:

- Packet-based transfer.
- Separation of control functions among bearer capabilities, call/session, and application/service.
- Decoupling of service provision from transport, and provision of open interfaces.
- Support for a wide range of services, applications and mechanisms based on service building blocks (including real-time/streaming/non-real-time services and multimedia).
- Broadband capabilities with end-to-end QoS and transparency.
- Interworking with legacy networks via open interfaces.
- Generalized mobility.
- Unfettered access by users to different SPs.
- A variety of identification schemes which can be resolved to IP addresses for the purposes of routing in IP networks.
- Unified service characteristics for the same service as perceived by the user.
- Converged services between fixed and mobile networks.
- Independence of service-related functions from underlying transport technologies.
- Support of multiple last mile technologies.
- Compliant with all regulatory requirements, for example concerning emergency communications and security/privacy, etc. Refer to ITU-T Recommendation Y.2001 (12/2004), *General Overview of NGN.*

5.1 Basic NGN Functionality

The NGN levels interoperate to provide end users or end devices with services, and network operators with remote Operations, Administration, Maintenance, and Provisioning (OAM&P) capabilities. The Communication Path level provides connectivity between end user and end devices using Layer 0-3 technologies such as Synchronous Optical Network [SONET], Wavelength-Division Multiplexing (WDM), ATM, Frame Relay, Optical Ethernet, IP, radio, satellite. The Communications Services level enhances communications by providing network management and security capabilities. The Content and Applications level provides end user applications such as voice and video (see Figure 5.1).

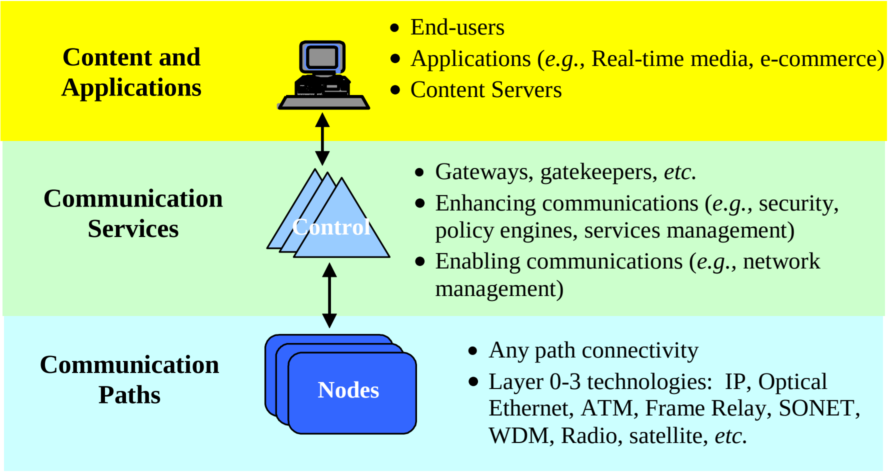

Content and Applications
• End-users
• Applications (e.g., Real-time media, e-commerce)
• Content Servers
Communication Services
Control
• Gateways, gatekeepers, etc.
• Enhancing communications (e.g., security, policy engines, services management)
• Enabling communications (e.g., network management)
Communication Paths
Nodes
• Any path connectivity
• Layer 0-3 technologies: IP, Optical Ethernet, ATM, Frame Relay, SONET, WDM, Radio, satellite, etc.

Figure 5.1- NGN Functionality

5.2 NGN Capabilities

NGN should provide capabilities that would make the creation, deployment, and management of services possible, whether the services are known or unknown. NGN should support the provision of all kinds of services (e.g., multimedia, data, video, and telephony), while relying on a wide range of transfer characteristics, such as real time and non-real time, low to high bit rates, unicast, multicast, and broadcast, messaging, simple data transfer services, etc. The NGN is capable of carrying both voice and data over the same physical network via IP traffic. NGN will change the way SPs offer services, as well as how people communicate. SPs are interested in customizing their services, including offering their customers the option to customize services.

6 Basic NGN Architecture

The ATIS Packet Technologies and Systems Committee (PTSC) published ATIS-1000018, *NGN Architecture*, a technical report describing the ATIS NGN architecture based on the IP multimedia system (IMS) architecture, its subsystems, and the relationships between them. ATIS-1000018 also defines the functional entities, identifies reference points, and provides relationship with other industry NGN architectures.

6.1 Overview of the NGN Architecture

The NGN provides capabilities and resources to applications for value added services. To provide these services, several functions in both the Service Stratum and the Transport Stratum are needed, as illustrated in Figure 6.1, *NGN Architecture Overview*.

The NGN supports a reference point to the applications functional group called Application-to-Network Interface (ANI), which provides a channel for interaction/exchange between applications and NGN elements. This enables the use of NGN capabilities to create enhanced services for NGN users.

The Transport Stratum provides IP connective services to NGN users under the control of Transport Control functions, which includes the Network Attachment Control Functions (NACF) and Resource and Admission Control Functions (RACF).

The User Network Interface (UNI), Network-to-Network Interface (NNI), and ANI should be considered as general NGN reference points that can be mapped to specific physical interfaces depending on the particular physical implementations. The UNI is a demarcation point between the responsibility of the SP and the responsibility of the subscriber. This is distinct from an NNI that defines a similar interface between provider networks. An NNI is an interface which specifies signaling and management functions between two networks. NNI circuits can be used for interconnection of signaling (e.g., Signaling System 7 [SS7]), IP (e.g., Multiprotocol Label Switching [MPLS]), or ATM networks.

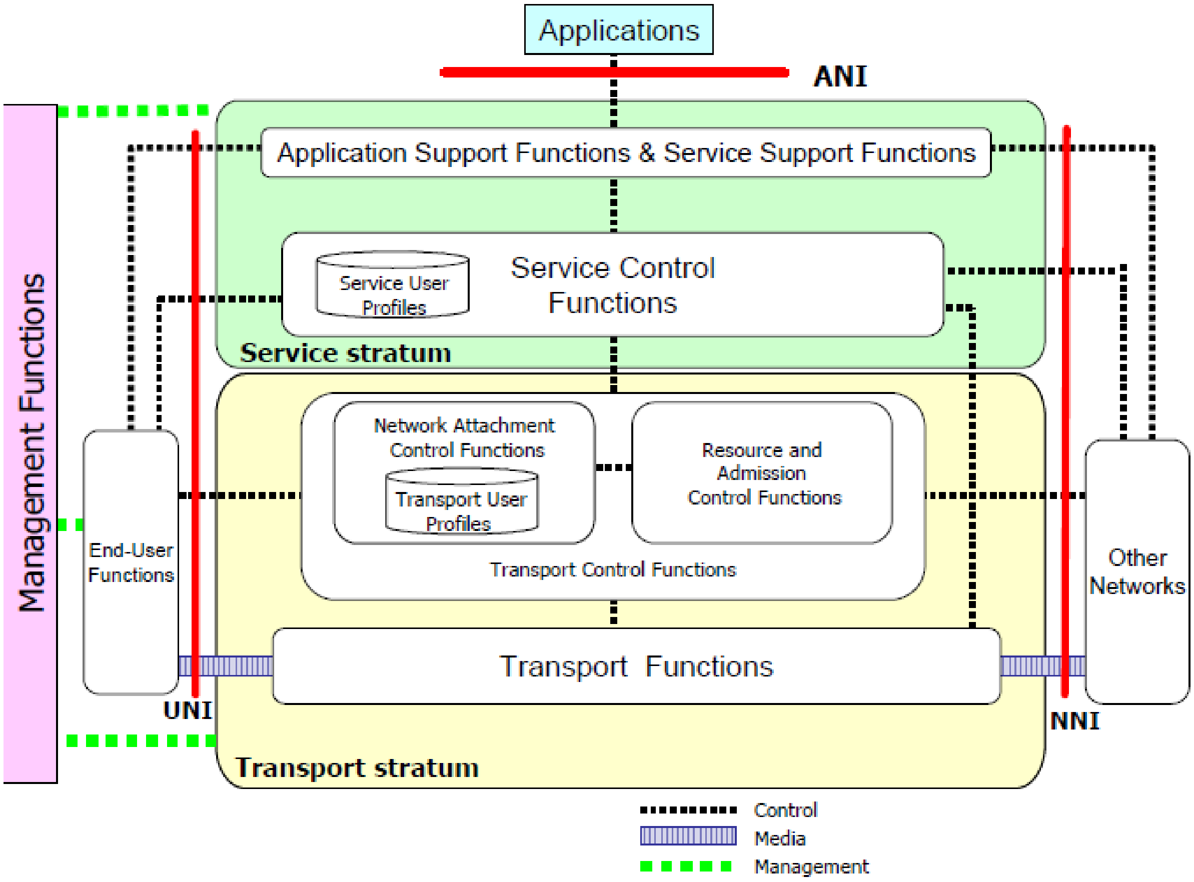


Figure 6.1 - NGN Architecture Overview

6.2 Decoupling of Services & Transport

A main characteristic of NGN is allowing transport services and application services to be offered separately so that they can evolve independently. In NGN architectures, service functions and transport functions should be clearly separated. The separation is by functionality. Transport functions are in the Transport Stratum and service functions related to application are in the Service Stratum. In general, each Stratum has its own set of roles, players, and administrative domains. Each Stratum needs to be treated separately from a technical point of view. A visual of the separation of the Service Stratum and the Transport Stratum can be viewed in Figure 6.1.

6.2.1 Service Stratum Functions

The abstract representation of the functional grouping in the Service Stratum includes the Service Control functions, Service User Profile functions, and the Application/Service Support functions.

6.2.1.1 Service Control Functions

The Service Control functions include resource control, registration, and authentication and authorization functions at the service level for both mediated and non-mediated services. They may also include functions for controlling media resources (i.e., specialized resources and gateways at the service signaling level).

6.2.1.2 Application Support Functions & Service Support Functions

The Application Support functions and Service Support functions include the gateway, registration, authentication, and authorization functions at the application level. These functions are available to the Applications and End User functional groups. The Application Support functions and Service Support functions work in conjunction with the Service Control functions to provide end users and applications with the value-added services they request.

Through the UNI, the Application Support functions and Service Support functions provide a reference point to the end user functions (e.g., in the case of third-party call control for click-to-call service). The Applications' interactions with the Application Support functions and Service Support functions are handled through the ANI reference point.

6.2.1.3 Service User Profile Functions

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

6.2.2 Transport Stratum Functions

The Transport Stratum functions include Transport functions, Transport Control functions, and Transport User Profile functions.

6.2.2.1 Transport Functions

The Transport functions provide the connectivity for all components and physically separated functions within the NGN. These functions provide support for the transfer of media information, as well as the transfer of control and management information.

Transport functions include access network functions, edge functions, core transport functions, and gateway functions.

6.2.2.2 Transport Control Functions

The Transport Control functions include RACF and NACF.

6.2.2.3 Transport User Profile Functions

Transport User Profile functions take the form of a functional database representing the combination of a user's information and other control data into a single "user profile" function in the Transport Stratum. This functional database may be specified and implemented as a set of cooperating databases.

6.3 Performance Measures of NGN Services

6.3.1 Basic Terms

Key Performance Parameters (KPP)

Certain enterprises measure “Key Performance Parameters (KPP)” for services and systems. These parameters, defined as those attributes or characteristics of a system that are considered critical or essential to successful system operation, are used to determine whether a system is (a) functioning and (b) functioning satisfactorily. KPPs normally have threshold and objective performance levels, which, respectively, describe performance levels that are minimally expected to be met at all times, and desired levels that are expected to be met most of the time.

Quality of Service (QoS)

There are several definitions of Quality of Service (QoS), which usually define a level of performance for a service in a communications network in terms of the underlying communications technology (e.g., rate of transfer of bits) or in terms of service characteristics (e.g., speed of delivery of text messages).

Quality of Service can be controlled via various mechanisms; the nature of the specific mechanisms used depends on the network’s underlying technology and transmission protocols. For communications paths that span multiple networks, the interoperation of one network’s QoS control mechanisms with the control mechanisms of the other network is facilitated via standardized mappings. Some common QoS mechanisms include:

- Differentiated Services (DiffServ) Code Point (DSCP).
- QoS Class Identifier (QCI).
- Allocation and Retention Priority (ARP).
- Guaranteed Bit-Rate (GBR).
- Multi-Protocol Label Switching (MPLS).
- And others.

Quality of Experience (QoE)

The Quality of Experience (QoE) is the collective effect of a service’s performance. It determines the degree of satisfaction of a user of the service.

End-to-End

End-to-End refers to the flow of communications between two end points (e.g., end-user devices) and specifically implies taking into account the end points and all intervening elements.

End-to-Middle

End-to-Middle, also known as *end-to-edge*, refers to connections that take into account a single end-point, an element at the edge of a provider’s network (often the far edge), and all intervening elements.

Middle-to-Middle

Middle-to-Middle refers to portions of communications networks that are either contained within one provider’s transit network, or span transit networks. Single provider’s middle-to-middle service is confined to the boundaries of a single provider’s network, edge to edge. Multiple providers’ middle-to-middle service spans multiple providers’ networks, usually from one provider’s near edge to another provider’s far edge, and includes the effects of interoperability between the SPs’ networks.

Throughput

Throughput can be characterized in a variety of ways depending on context. Normally Throughput is defined in the contexts of Internet Protocol (IP) or User Datagram Protocol (UDP) throughput, and Transmission Control Protocol (TCP) throughput.

IP Throughput focuses on the transmission of packets between two adjacent IP nodes (one or more lower layer devices may exist between the two IP nodes but they are transparent in the determination of throughput between the two IP nodes). Factors that determine IP Throughput include transmission delays between the nodes and processing delay within the nodes.

TCP Throughput is defined as the average rate of successful delivery of data from a source IP node to a destination IP node over a TCP network. Factors that influence IP Throughput (described above) contribute to TCP Throughput. In addition, TCP Throughput is also affected by the constraints of this protocol[33]. As a result, throughput of TCP traffic will always be lower than the available raw (IP, or UDP) bandwidth.

6.3.2 Performance Measures

Performance measures may apply to a network, or to a specific service provided by a network.

6.3.2.1 Network Performance Measures

Network performance measures apply to the performance of a network without regard to any specific service. These may include the following:

1. Throughput.
2. Data errors (packet loss).
3. Latency (one-way or round-trip delay).
4. Jitter (variability of latency across multiple packets).
5. And others.

These network performance measures are described in more detail below:

<u>Throughput</u> (“throughput” here refers specifically to IP Throughput)

<u>Short-term (burst) throughput:</u>

Short-term (burst) throughput is the average throughput that a user will receive during the initial, transient period of a transfer. One of the benefits of short-term (burst) throughput is its ability to characterize the throughput of a link on small data transfers.

<u>Sustainable throughput:</u>

Long-term (Sustainable) throughput is the steady-state expected throughput that a user should receive after an initial, transient period of higher throughput. Sustainable throughput needs to be considered for both upload and download, to capture asymmetry in data transfer rates.

<u>Minimum throughput:</u>

Minimum throughput captures degradation in throughput that might result from congestion, throttling, or high network utilization.

[33] As an illustration, the maximum size of the receive buffer of the destination IP node is limited by TCP to 65,536 bytes. Using a slow satellite path of 0.5 seconds as an example, a single TCP connection can then use only a maximum of 1.05 Mbit per second (65,536 Bytes / 0.5 seconds), regardless of the link’s capacity.

Bulk Transfer Capacity (BTC):

Bulk Transfer Capacity (BTC) represents the achievable throughput by a single connection. BTC applies only to TCP connections and depends on how TCP shares bandwidth among individual TCP flows.

BTC is unique among throughput measurements in that it does not directly measure actual throughput, but rather the maximum throughput obtainable.

Goodput

Goodput is the effective transmission rate of the payload data while discounting overhead bits, control messages, re-transmissions, etc.

TCP Goodput measures the number of TCP payload bytes per second that the system can transfer.

Throughput measurements often suffer from high variability due to differences in access technologies, providers' traffic shaping policies, and congestion during peak hours. Additionally, the actual throughput of a TCP connection is very difficult to measure due to complicating factors such as transfer size, types of cross traffic, and the number of competing connections. As a result, BTC may be the most useful of the throughput metrics.

Packet Loss

Loss Rate:

Loss Rate is the average packet loss over a period of time.

Loss Burst Length:

Loss Burst Length is the average duration of a packet loss episode.

Packet loss measurement is valuable in that it has implications for TCP throughput and TCP timeouts. For instance, studies have shown that the loss of even a single packet can severely degrade streaming video quality, and that bursts of loss have similarly deleterious effects on performance.

Latency

Round Trip Time (RTT):

Round Trip Time (RTT) is the time delay between sending a packet and receiving a response. RTT can be measured by sending small UDP packets to a test node and timing the responses (while treating any response receipt delay longer than a specified threshold as packet loss).

Last-Mile Latency:

Last-Mile Latency is the latency between an end-user device and the first device inside a SP's network. Last-Mile Latency characterizes the access link and is therefore more useful for describing short data transfers. Last-Mile Latency is a strong metric because SPs can guarantee a maximum Last-Mile Latency that users should expect even during congestion. The standard deviation of Last-Mile Latency can also be used to estimate jitter in a given segment.

Latency Under Load:

Latency Under Load is the actual latency that a user experiences during an upload or download. Latency Under Load reflects issues with buffer bloat, active queuing, and traffic shaping.

Latency, much like throughput, can be difficult to measure due to complicating factors: The quality of access links, modem buffering, and cross-traffic in customer premise equipment all interfere with latency measurements.

Jitter

Maximum Jitter (i.e., maximum delay variability):

Maximum Jitter is the largest value of jitter that users should experience, and indicates whether the data transmission characteristics are satisfactory for a given application.

Jitter and latency are closely related, as are packet loss and throughput.

6.3.2.2 Service Performance Measures

Service Performance Measures are generally specific to each service: The performance measures that apply to voice over IP (VoIP) service, for instance, are different from the performance measures that are applicable to electronic mail (e-mail). Some performance measures, however, are universal (or nearly so) across multiple services. These generic service performance measures may include the following:

1. Uplink and downlink goodput (i.e., net throughput, discounting overhead transmissions).
2. Round trip latency per transaction.
3. Data session setup time.
4. Data session setup success rate.
5. Percentage of failed transaction.
6. Data session drop rate.
7. Mean Opinion Score (MOS).[34]
8. And others.

The purposes of Service Performance Measures are to allow the SP to measure the users' quality of experience by monitoring their services in near real time, and for identifying and responding to degradations in performance. From a service-user's perspective, Service Performance Measures answer questions such as:

- What is the likelihood that a data session can be completed?
- Responsiveness, i.e.,
  - How long does it take to connect to the server?
  - How long does it take to download/upload the desired information?
  - What is the latency or delay during each transaction or interchange?
- How often is the connection lost?
- Is the transmission consistent enough to support the desired usage?

While it might be possible to answer such questions directly by using custom software on the users' devices, such an approach may be cumbersome to develop, deploy, and maintain. Alternatively, SPs can collect network performance measurements within their networks and use these to assess the factors impacting user experience.

It should be emphasized that the service performance as experienced by the user is an end-to-end measure, regardless of the fact that there may be multiple intervening network technologies and providers. Thus, the ability is required to collect these measures across technologies and providers in a manner that will enable an end-to-end view of the service performance.

Conversely, from the SPs' perspective, Service Performance Measures, i.e., the collection and analysis of service and network measurements enable the providers to answer questions such as:

- What level of service quality is the network delivering to users?
- Is the service functioning normally now?
- Are there any geographic regions where the service is not functioning or functioning less than optimally?
- What percentage of the time has the service been functioning normally for the past hour? Day? Month?
- If/when the service was not functioning normally everywhere, which network element(s) or feature(s) were experiencing and/or causing the problem?
- How often and for how long has the service been down over the last day? Week? Month?

[34] MOS, a numerical value between 0 and 5, started out as a subjective assessment of a telephone connection's voice quality based on human perception. The International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) has redefined MOS [ITU-T G.107] so that it now refers to an objective quantitative score computed from measured data of packet loss-rate, delay, and jitter.

- What fraction of valid service requests has been honored/denied over the last day? Week? Month?
- Is the service affected by the presence or operation of other services on the provider's network?

Note that Service Performance Measures can be used to provide quantitative measures of user Quality of Experience. Also note that they can be measured objectively, either directly or via lower (network) level measures.

6.4 NGN Functional Entities

A functional entity comprises a specific set of functions at a given location. Groupings of functional entities are used to describe practical physical implementations. In the NGN, functional entities controlling policy, sessions, media, resources, service delivery, security, etc., may be distributed over the infrastructure, including both existing and new networks. When these functional entities are distributed, they communicate over open interfaces. As such, the identification of reference points is an important aspect of NGN. Gateways provide a means of interworking between different networks of operators, both existing networks and NGN (NGN, PSTN, Integrated Services Digital Network [ISDN], Global System for Mobile Communications [GSM], and Code Division Multiple Access [CDMA]).

6.5 NGN Functional Architecture

The functional architecture is a set of functional entities and the reference points between them used to describe the structure of an NGN, each providing a unique function. The relationships and connections between functions are identified in terms of reference points.

6.6 NGN Emergency Services

Emergency services include the public 9-1-1 services and the Cybersecurity and Infrastructure Security Agency (CISA) Emergency Communications Division (ECD)[35]-managed Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS), and Telecommunications Service Priority (TSP). As the telecommunications industry consolidates facilities in its transition from circuit- to packet-switching technology, these services, originally deployed in the circuit-switched PSTN, will interoperate with their NGN versions (known as the NGN Priority Services).

6.6.1 GETS & WPS

GETS provides Federal, state, local, territorial, and tribal officials, as well as other authorized personnel with national security and emergency preparedness (NS/EP) responsibilities with the means of obtaining priority in completing telephone calls via the Public Switched Telephone Network (PSTN) during times of emergency or when the wireline telephone network is otherwise congested. WPS enables an authorized NS/EP user to place calls with priority via mobile (cellular) networks after invoking WPS from a WPS provisioned handset on a per-call basis by dialing Feature Code *272, followed by the destination number.

To achieve priority for a connection-oriented priority service in an IP network, the signaling protocol used for setting up the connection (e.g., Session Initiation Protocol (SIP)) uses its priority parameters (e.g., SIP Resource Priority Header) to assign priority to both signaling and transport packets. For wireless calls, call-establishment priority on the radio interface will be achieved via technology-specific mechanisms, e.g., the use of automated access class barring (ACB) in Long-Term Evolution (LTE) networks.

SP interconnection/interoperability will need to support NGN Priority Services. SPs will need to establish trust relationships with interconnected peer SPs to ensure NGN Priority Services calls maintain priority across network boundaries.

[35] Formerly the National Communications System (NCS) and Office of Emergency Communications (OEC)

6.6.2 NG9-1-1

There is consensus within the 9-1-1 community that there are shortcomings in the existing 9-1-1 system infrastructure and there is the need to take advantage of advances in information and communications technologies to implement the next generation of the 9-1-1 system. The Next Generation 9-1-1 (NG9-1-1) system is an IP based architecture which is designed to incorporate enhanced multimedia capabilities, improved emergency call routing, improved location determination, and nationwide call-transfer capabilities.

There are over 6,200 Public Safety Answering Points (PSAPs) in the United States which are the recipients of emergency voice calls to "9-1-1". Some of these PSAPs may never convert to NG9-1-1. Consequently, the NGN may have to interface to both legacy PSAPs and NG9-1-1 PSAPs. Both the ATIS Emergency Services Interconnection Forum (ESIF) and Wireless Technologies and Systems Committee (WTSC) continue to develop ATIS standards to define these interfaces.

Although the NG9-1-1 is capable of multimedia communications such as graphics, pictures, and video, the availability of these capabilities to citizens is dependent upon the capabilities of the PSAP systems and the capabilities of the originating SP networks. The deployment of enhanced 9-1-1 services is focused first on emergency voice calls and on SMS to 9-1-1 services.

6.6.3 TSP

The TSP system provides for the priority restoration and provisioning of NS/EP telecommunication services. TSP restoration and provisioning guidelines are provided for access services and generic administrative procedures and interfaces between Access Service Customer (ASC) and the Access Service Provider (ASP).

In order for the TSP system to be effective, it must be incorporated into the day-to-day operating procedures for all ASPs and ASCs. All communications providers are expected to cooperate in the installation and restoration of services with TSP that involves the facilities of more than one SP.

6.6.4 Wireless Emergency Alerts (WEA)

Wireless Emergency Alerts (WEA) [formerly known as the Commercial Mobile Alert System (CMAS)[36] or Personal Localized Alerting Network (PLAN)] is a voluntary services of the wireless operators to provide an authority to citizen emergency alert system that allows wireless customers who are carrying certain wireless phone models and other enabled mobile devices to receive geographically-targeted, 90 English character text-like messages alerting them of imminent threats to life or property in their current location. This voluntary service is supported by all four of the major Tier I wireless operators in the US.

The technology[37] utilized by WEA ensures that emergency alert messages will not get delayed or rejected under network congestion conditions, which can happen with standard mobile voice and texting services especially during disasters or localized emergencies.[38] The technology employed by WEA is a one-to-many broadcast service. The WEA service only supports text messages and does not support other media types such as graphics, maps, videos, or pictures.

[36] The name of this service was changed to Wireless Emergency Alerts (WEA) a few months before the national launch in April 2012. The prior name of Commercial Mobile Alert System (CMAS) is the name referenced in the WARN Act, the FCC NPRM FCC-07-214A1, FCC 1st Report & Order FCC-08-99A1, FCC 2nd Report & Order FCC-08-164A1, and the FCC 3rd Report & Order FCC-08-184A1. The ATIS and 3GPP standards also refer to this service as CMAS.

[37] The WEA solution is standardized in ATIS, 3GPP and joint ATIS and TIA standards. In 3GPP, WEA is part of the international Public Warning System (PWS).

[38] The collapse of the Minneapolis I-35W Mississippi bridge during rush hour on August 1, 2007 is an example where localized network congestion occurred during a localized emergency.

WEA was established pursuant to the 2006 Warning, Alert and Response Network (WARN) Act.[39] WEA enables authorized government officials to target emergency alerts to specific geographic areas (e.g., county, circle, or polygon) through cell towers. The cell towers broadcast the emergency alerts for reception and presentation by all WEA-enabled mobile devices associated with the broadcasting cell towers.

The WEA service does not utilize any media bearers so QoS services are not required for WEA. For GSM and UMTS systems, WEA utilizes control plane signaling resources and a dedicated Cell Broadcast channel. For LTE systems, WEA utilizes only control channel signaling resources.

For additional information on WEA, see both the FCC WEA website[40] and on the CTIA WEA website.[41]

6.6.5 Interim SMS Text-to-9-1-1

The interim text-to-9-1-1 solution is based only upon the wireless operator native Short Message Service (SMS) texting service. Wireless operator native SMS is that feature provided by the wireless operator, and not a third-party texting or messaging application (app) that may be installed on the mobile device. The interim SMS text-to-9-1-1 service provides support for wireless subscribers to send emergency SMS text messages to PSAPs and for subscribers to receive text replies from PSAPs. Wireless customers with SMS service subscription are able to send emergency SMS messages to a PSAP by using the three digits “9-1-1” as the destination address of the SMS message. A dialogue association is maintained to support multiple SMS messages within a conversation between the subscriber and the PSAP telecommunicator.

On December 6, 2012, AT&T, Sprint, T-Mobile, and Verizon entered into a voluntary agreement with the National Emergency Number Association (NENA) and APCO International (APCO) in which each of the four commercial mobile radio service (CMRS) SPs agreed to provide text-to-9-1-1 service by May 15, 2014, to Public Safety Answering Points (PSAPs) that are capable of receiving and request to receive text-to-9-1-1 service[42]. In this agreement, the major SPs also committed to providing a bounce-back message to alert their subscribers attempting to text an emergency message to instead dial 9-1-1 when text-to-9-1-1 is unavailable in a particular area. The agreement stated that all four SPs would provide this capability by June 30, 2013. The associated FCC Report & Order is FCC-13-64A1, *Federal Communications Commission First Report and Order In the Matter of Facilitating the Deployment of Text-to-911 and Other Next Generation 911 Applications*.

The interim SMS to 9-1-1 solution is fully operational by AT&T, Sprint, T-Mobile, and Verizon. However, the availability of SMS to 9-1-1 services in a specific location is dependent upon the readiness of the associated PSAP to receive SMS to 9-1-1 text messages and upon the PSAP initiating the process of requesting receipt of SMS to 9-1-1 text messages.

If a subscriber is in a location where the associated PSAP does not support SMS to 9-1-1 text messages and the subscriber sends an SMS message to 9-1-1, the subscriber will receive a response SMS message stating that text to 9-1-1 is not supported in their current location and that they should place a voice call to 9-1-1.

The interim solution will only process text-to-9-1-1 messages via wireless operator native SMS. This means that photos, videos, and multiple recipients for a text message are not supported.

The interim SMS to 9-1-1 solution is defined in the Joint ATIS/TIA standard J-STD-110, *Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification*, and J-STD-110 Supplement A, *Supplement A to J-STD-110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification*. J-STD-110 and its associated Supplement A provides the assumptions, use cases, requirements, architecture, and call flows for the interim SMS to 9-1-1 solution and defines the new network elements and new interfaces. The companion specification is the Joint ATIS/TIA standard J-STD-110.1, *Joint ATIS/TIA Implementation Guidelines for J-STD-110, J-STD-110, Joint ATIS/TIA Native SMS to 9-1-1 Requirements and Architecture Specification*, which provides implementation

[39] Available at: <http://transition.fcc.gov/pshs/docs/emergency-information/cmas-warn-act.pdf>.

[40] Available at: <http://www.fcc.gov/guides/wireless-emergency-alerts-wea>.

[41] Available at: <http://www.ctia.org/your-wireless-life/consumer-tips/wireless-emergency-alerts>.

[42] See Letter from Terry Hall, APCO International; Barbara Jaeger, National Emergency Number Association (NENA); Charles W. McKee, Sprint Nextel; Robert W. Quinn, Jr., AT&T; Kathleen O’Brien Ham, T-Mobile USA; and Kathleen Grillo, Verizon, to Julius Genachowski, Chairman, Federal Communications Commission, and Commissioners McDowell, Clyburn, Rosenworcel and Pai, PS Docket 11-153, PS Docket No. 10-255 (Dec. 6, 2012) (Carrier-NENA-APCO Agreement).

guidelines for the J-STD-110 solution. The Ad Hoc National SMS Text-to-9-1-1 Service Coordination Group (SCG) developed the *Interim SMS Text-to-9-1-1 Information Planning Guide,* to provide instructions to PSAPs in order to become ready to accept SMS to 9-1-1 text messages.

The interim SMS text-to-9-1-1 solution supports interfaces for both legacy PSAPs and NG9-1-1 PSAPs (see clause 6.6.2). Specifically, the interim SMS to 9-1-1 solution provides the following three interface options for PSAPs:

- TTY interface.
- HTTP interface (e.g., web page).
- NG9-1-1 i3 based IP interface.

When the PSAP informs the wireless operators of their readiness to accept SMS to 9-1-1 message, the PSAP has to indicate which of the above three interfaces they will be using for the SMS to 9-1-1 messages.

The interim SMS text-to-9-1-1 solution does not utilize QoS services because the solution does not use bearer resources associated with voice or data communication sessions. The interim SMS text to 9-1-1 solution is implemented on specialized communications paths which are separate from the emergency voice communication paths.

The interim SMS text to 9-1-1 solution is applicable to legacy networks, UMTS, and LTE networks. This solution is applicable as long as wireless operator native SMS services are still supported.

There is no association or relationship between voice 9-1-1 emergency calls and SMS to 9-1-1 text messages. The PSAP which responds to the SMS to 9-1-1 text messages may not be the same PSAP which would respond to a voice call to “9-1-1” from the same location. For example, some municipalities or regions may have multiple PSAPs to handle voice 9-1-1 emergency calls from different locations within their area but may have only one designated PSAP to respond to all SMS to 9-1-1 text messages.

The development of the interim SMS text to 9-1-1 is a joint development between ATIS and TIA and is led by the ATIS Wireless Systems and Technologies Committee (WTSC).

7 ATIS Committees & Forums

Various ATIS committees and forums are working on different aspects of NGN. Committee work related to NGN can be found on the ATIS website, http://www.atis.org.

This clause lists a few of the ATIS committees that have NGN related Issues and/or documents that have been completed or are in progress.

7.1 Emergency Services Interconnection Forum (ESIF)

ESIF provides a venue to facilitate the identification and resolution of technical and/or operational issues related to the interconnection of emergency services networks with other networks (i.e., wireless, wireline, cable, satellite, Internet, etc.).

7.2 Packet Technologies & Systems Committee (PTSC)

PTSC develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC 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. International Telecommunications Union – Telecommunication Standardization Sector (ITU-T) and U.S. International Telecommunications Union – Radio Communication Sector (ITU-R Study) Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions. There is also an ongoing joint effort between ATIS and the SIP forum, the IP-NNI Task Force.

7.3 Telecom Management & Operations Committee (TMOC)

The Telecom Management and Operations Committee (TMOC) develops operations, administration, maintenance and provisioning standards, and other documentation related to Operations Support System (OSS) and Network Element (NE) functions and interfaces for communications networks – with an emphasis on standards development related to U.S.A. communication networks in coordination with the development of international standards.

7.4 Wireless Technologies & Systems Committee (WTSC)

WTSC develops and recommends standards and technical reports related to wireless and/or mobile services and systems, including service descriptions and wireless technologies. WTSC develops and recommends positions on related subjects under consideration in other North American, regional and international standards bodies. WTSC is the lead committee on multiple joint industry standards projects including SMS to 9-1-1, Wireless Emergency Alerts (WEA), and public safety Mission Critical Push to Talk (MCPTT) voice interoperation between Land Mobile Radio (LMR) and Long Term Evolution (LTE) systems.

8 Other Industry Activities Related to NGN

8.1 ITU-T NGN Global Standards Initiative (NGN-GSI)

The ITU-T NGN-GSI focuses on developing the detailed standards necessary for NGN deployment to give SPs the means to offer the wide range of services expected in NGN. NGN-GSI harmonizes, in collaboration with other bodies, different approaches to NGN architecture worldwide.

8.1.1 NGN-GSI

The results of the Focus Group on Next Generation Networks (FGNGN) (Release 1) provided the building blocks on which the world's systems vendors and SPs could begin to transition to the NGN. This work is now continued by ITU-T's NGN-GSI, which encompasses all NGN work across ITU-T Study Groups. It has been implemented by co-located meetings of concerned Study Groups and Rapporteur Groups from the various study groups to jointly progress the work under the auspices NGN-GSI.

The ITU-T Y-series recommendations[43] may be of interest to the industry in ensuring an interoperable product from a global perspective.

8.2 Internet Engineering Task Force (IETF)

The Internet Engineering Task Force (IETF) is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The mission of the IETF is to make the Internet work more efficiently by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. The IETF Mission Statement is documented in IETF RFC 3935, *A Mission Statement for the IETF*.

[43] https://www.itu.int/en/ITU-T/gsi/ngn/Pages/default.aspx

9 NGN GETS

As the telecommunications industry consolidates facilities in its transition from circuit to packet switching technology, the CISA/ECD[44] managed GETS and its wireless counterpart, WPS, will interoperate with NGN Priority Services.

9.1 GETS

GETS was established in the U.S. in the mid-1990s in accordance with Executive Order No. 12472. Executive Order No. 12472 was subsequently amended in 2003 by Executive Order No. 13286 and revoked in 2012 by Executive Order No. 13618. The purpose of this wireline service is to provide federal, state, local officials, and other authorized personnel associated with NS/EP responsibilities, with the means of obtaining priority in placing telephone calls via the PSTN during times of emergency or when the telephone network is otherwise congested.

The CISA/ECD contracts with commercial wireline and wireless telephony SPs to provide GETS and the WPS over their networks. The CISA/ECD also authorizes potential GETS and WPS users and issues each GETS user a unique Personal Identification Number (PIN), which can be used to place priority telephone calls in a manner similar to placing a calling-card call.

High probability for call completion of NS/EP calls in a damaged or congested telephone network is achieved through a set of specialized treatments, including routing calls to certain GETS-enabled public SPs, queuing calls to overcome temporary blocking situations, additional re-routing attempts to overcome link damage or route congestion, and exemption from restrictive network controls. In addition, SS7 signaling message priority is associated with GETS calls. GETS call messages are routed with higher priority than are signaling messages associated with non-priority calls.

The number of authorized GETS users has been growing steadily. At present, there are more than 300,000 CISA/ECD-authorized GETS users. GETS and WPS users include officials of the federal, state, and local governments, first responders such as fire fighters, medical personnel, law enforcement organizations, and other authorized users.

9.2 WPS

WPS is implemented in accordance with the rules in the Federal Communications Commission (FCC) *Second Report & Order* WT Docket No. 96-86 FCC-00-242, July 2000. WPS enables an authorized and provisioned NS/EP user to invoke WPS on a per-call basis by dialing Feature Code *272, followed by the destination number. If all radio channels in the user's cell sector are busy, the user's call will be queued for access to the next available radio channel in accordance with the user's assigned priority and the order in which the call was received. Furthermore, WPS provides queuing to congested PSTN interfaces for calls originated at a Mobile Switching Center (MSC) and traversing another SP's network. Regardless of whether a WPS call traverses the PSTN or simply connects within the same MSC, queuing is also applied when terminating a WPS call into a cell where all radio channels are busy. WPS and GETS integration provides end-to-end priority treatment for NS/EP calls, including calls that originate, transit, and/or terminate in wireless and/or landline networks that are equipped with WPS or GETS features.

WPS makes use of several congestion control mechanisms to optimize the probability of call completion during congestion. These include the Precedence Parameter, UMTS Redirection to GSM, also known as Directed Retry Handover (DRH), Enhanced Overload Performance (EOP) signaling priority, and other features.

9.2.1 Precedence

To provide priority treatment for WPS calls, the SS7 Initial Setup ISDN User Part (ISUP) Precedence Parameter will be sent from the originating MSC across the PSTN to a terminating MSC. The Precedence Parameter is defined as an optional parameter within the SS7 ISUP Initial Address Message (IAM) and is specified in 3GPP TR 22.952 version 6.3.0 Release 6, *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Priority service guide*, Table A.2. This parameter ensures that a priority call

[44] Formerly the National Communications System (NCS) and the Office of Emergency Communications (OEC).

originated at an MSC will receive the same priority-level treatment at a terminating MSC (i.e., queuing and servicing before lower priority calls). Without transmission of the Precedence Parameter, all terminating WPS calls would have the same default priority and treatment at the terminating MSC. The precedence parameter is passed along across any intervening networks between the originating and terminating MSCs according to ATIS-1000113, *Signaling System No. 7 (SS7) – Integrated Service Digital Network (ISDN) User Part*. All en-route switches are required to pass optional parameters and values, such as the Precedence Parameter with WPS values.

9.2.2 UMTS Redirection to GSM (also known as Directed Retry Handover)

To support users as they upgrade their mobile equipment to 3rd generation (3G), commercial GSM-based SPs have been deploying UMTS, also known as Wideband CDMA (W-CDMA), as an overlay to their GSM networks. Because UMTS is an overlay, commercial users will continue to receive their wireless service in all markets, whether GSM alone, GSM and UMTS together, or UMTS alone (when available), via the use of dual-mode handsets. However, for WPS calls to or from users with dual-mode handsets in a market with both GSM and UMTS technologies or with UMTS alone, it was necessary to require that WPS calls that originate from a UMTS subscriber or NS/EP calls that terminate to a UMTS subscriber should be redirected to a GSM system if radio resource congestion occurs on the Universal Terrestrial Radio Access Network (UTRAN), the air interface part of UMTS. This approach is called DRH and is a bridging strategy for an immediate UMTS solution.

9.2.3 Enhanced Overload Performance (EOP)

During the first minutes after rare and highly unusual “mass calling events” (potentially triggered by unexpected disasters such as severe earthquakes), the public wireline and wireless networks become extremely congested in and near the affected areas. Various analyses conclude that, in the wireless networks, the problem is primarily caused by call attempt overload on the signaling channel (called reverse access channel, or RACH) needed for a user’s mobile handset to signal to the network a request for a call.

To address this issue, beginning with the CDMA air interface technology, the CISA/ECD process to enhance WPS to protect NS/EP performance during periods when surges in signaling risks congestion of signaling resources. The CISA/ECD contracted with network vendors to design and develop a solution – known as WPS EOP – that would not only overcome congestion on the RACH that could impact WPS calls, but also provide a high assurance that, once getting past the RACH, WPS calls would also receive priority treatment through the base station controller/base transceiver station (BSC/BTS) and MSC processors involved in call setup that could also become overloaded. The CISA/ECD also required that each vendor’s CDMA WPS Overload solution address potential congestion on the RACH that can occur in response to terminating public and NS/EP calls that use the paging channel (PCH), as well as the RACH, for portions of call termination signaling.

The enhancements require WPS mobiles be provisioned with a distinct Access Overload Class (AOC) as permitted in the standards. AOCs are defined in TIA/EIA TSB16-A, *Assignment of Access Overload Classes in the Cellular Telecommunications Services*, and apply for all TIA TR-45 air interfaces – not just CDMA. The user device is provisioned by the wireless SP with a 4-bit number known as the AOC. There are sixteen (16) possible AOCs. Public user devices are assigned random AOCs in the range of 0-9. AOC 10 is defined for system test purposes and is typically used by network technicians. AOC 11 is defined for authorized emergency use for law enforcement, fire, medical, and rescue services; and AOCs 12-15 were reserved for future use. In order to avoid conflict with other federal, state, and local law enforcement, fire, and/or emergency uses for AOC 11, the CISA/ECD proposed use of AOC 12 for NS/EP communications. Both 3GPP2 (the standardization group for CDMA 2000), and the TIA TR 45.5 Subcommittee have accepted the use of AOC 12 by the NS/EP community for voice, video, data, and multimedia.

WPS EOP utilizes the CDMA broadcast Persistence (PSIST) Parameter to control signaling load as provided in the standard. The standard permits assigning separate PSIST Parameter values, individually or collectively, for public AOCs 0-9 and for AOCs 10-15. The WPS EOP exercises the PSIST capability to control public load via AOC 0-9 while enabling WPS AOC 12 to retain a high likelihood of successful signaling. This WPS EOP use of load control also improves the number and percentage of public signaling successes.

The CISA/ECD has instructed the CDMA SPs that AOC 12 should only be provisioned on WPS user devices, as authorized by the Executive Office of the President. In addition, all CDMA SPs should ensure that properly provisioned user devices with AOC 12 function as appropriate, and that any existing overload controls do not impact AOC 12.

9.2.4 Access Class Barring on LTE

The last several years have seen an unprecedented increase in consumer demand for mobile broadband service, proliferation of Smart Phone-type user devices, and a massive increase in data services such as multimedia, messaging, and texting. These changes to the wireless environment can affect the WPS users' ability to make voice calls, placing WPS call completion at risk.

Similar to its efforts to provide WPS over CDMA networks, the CISA/ECD is acquiring WPS over voice LTE networks (VoLTE). Similar to introducing the EOP technology in CDMA networks, the CISA/ECD is taking steps to protect NS/EP priority call performance in LTE networks during periods when surges in network demand risks congestion of the signaling, transport, and media resources necessary to access the network. These capabilities include Automatic Access Class Barring and High Priority Access, which leverage existing features of the 3GPP Radio Resource Control standard.[45] Priority is afforded to NS/EP-authorized user equipment (UEs) due to the reservation and provisioning of special Access Class (AC 14) exclusively for NS/EP-authorized UEs, and the requirement that "AC 14 shall not be subject to barring until after AC 10, 11, 12, and 13 are subject to barring".[46] Provisioning of WPS-subscribed UE, and only WPS-subscribed UEs with the special AC 14 permits radio network access when network congestion requires public UEs (AC 0-9) be barred from sending mobile originated signaling, such as Radio Resource Control Connection Requests and mobile originated data, such as a SIP INVITE.

In addition, radio resource control requests from UEs with AC 11-15 will have the establishment cause set to *highPriorityAccess,* enabling further priority treatment.

The CISA/ECD has instructed the LTE SPs that AC 14 should only be provisioned on WPS user devices, as authorized by the Executive Office of the President or the CISA/ECD on behalf of the Executive Office of the President.[47] In addition, all LTE SPs should ensure that properly provisioned user devices with AC 14 function as appropriate, and that any existing overload controls do not impact AC 14.

9.2.5 Wireless Priority Service (WPS) on Long Term Evolution (LTE) Networks

Commercial SP cellular networks are transitioning from second (2nd)- and third (3rd)-generation cellular protocols to fourth (4th)- generation Long Term Evolution (LTE) protocols. LTE protocols have the capability to prioritize traffic and to meet established quality of service (QoS) requirements for different types of applications. Furthermore, it is possible to apply prioritization levels to different classes of users. Users such as National Security and Emergency Preparedness (NS/EP), public safety, or law enforcement can be afforded higher priority over the public, so that when networks become congested, these high priority users can continue to communicate.

Wireless Priority Service (WPS) provides authorized NS/EP users a means to achieve a higher likelihood of success in making wireless calls across commercial wireless networks during times of severe network overload and congestion. Originally developed as a circuit-switched service, WPS has now been enhanced to operate on fourth (4th)-generation Voice-over-LTE (VoLTE) packet-switched networks as well. The Federal Communications Commission requires commercial cellular providers that choose to offer WPS to do so in accordance with a set of uniform operating protocols.[48]

The high-level framework described below allows commercial cellular providers to develop WPS on VoLTE NS/EP priority services. The recommended WPS on VoLTE NS/EP priority functions and parameter value assignments are designed to meet the Department of Homeland Security (DHS) Emergency Communications Division's (ECD) NS/EP Key Performance Parameter (KPP) objectives and functional requirements when implemented.

To be fully effective, the enhancements require WPS mobile phones be provisioned with a distinct Access Class (AC) as permitted in the standards. For WPS on VoLTE, this AC is 14. It is important that all WPS on VoLTE

[45] 3GPP TS 36.331, Release 8 and above, *Evolved Universal Terrestrial Radio Access (E-UTRA), Radio Resource Control (RRC), Protocol specification.*

[46] ATIS-1000061, *LTE Access Class 14 for National Security and Emergency Preparedness (NS/EP) Communications.*

[47] FCC 00-242, *Second Report and Order, Establishment of Rules and Requirements for Priority Access Service, July 2000.*

[48] Ibid.

commercial cellular providers ensure AC 14 is provisioned only on WPS authorized user devices and accept all mobile phones properly provisioned with AC 14 to roam (when authorized) on their networks.

A new feature in WPS on VoLTE for the highest priority users is the ability, in coordination with the FCC, of preempting in-progress public voice sessions, not including public safety emergency (911) communications. This feature became necessary because 4th generation VoLTE does not support session-queueing, which allowed 2nd- and 3rd-generation cellular WPS calls to be queued until an in-progress call disconnected voluntarily.

LTE Priority Capabilities:

The LTE priority capabilities are used to address and mitigate the various potential LTE congestion points and facilitate the high probability of session admission, completion and retention. The LTE priority capabilities used to access, invoke and maintain NS/EP priority service can include Access Class (AC), High-Priority Access (HPA) Establishment Cause, Access Class Barring (ACB), Allocation Retention Priority (ARP), the Quality of Service Class Identifier (QCI), and the Diameter protocol's reservation priority Attribute/Value Pair (AVP). These priority mechanisms are being phased in as the NS/EP priority services are evolving from an initial operational capability to a full operational capability.

- Access Class is a number between 0 – 15 assigned to mobile handsets; classes 0 – 9 are assigned randomly to the general public, while classes 10 – 15 are assigned to special categories. VoLTE-capable WPS mobile phones are provisioned with Access Class 14.
- During the process of establishing a new wireless session, mobile handsets provisioned with any Access Class 11 - 15 send the HPA indicator as the establishment cause. The LTE network then prioritizes the connection establishment request during high load situations in the network.
- Access Class Barring (ACB) is an access control capability at the physical level that automatically slows or prevents connection requests from non-priority mobile handsets once a certain overload threshold is reached in the network.
- Allocation Retention Priority (ARP) operates at the bearer level to prioritize session requests. The ARP also indicates whether the session being established is authorized to preempt in-progress sessions [denoted by the Preemption Capability Indicator (PCI)] or is vulnerable to being preempted by higher-priority session requests [denoted by the Preemption Vulnerability Indicator (PVI)].
- Quality of Service (QoS) Class Identifier (QCI) indicates the required performance level and QoS.
- The Diameter Reservation Priority Attribute/Value Pair (AVP) indicates the priority level of the request.

Provisioning of Network Elements:

Radio Access Network (RAN), Evolved Packet Core (EPC) and IP Multimedia Subsystem (IMS) network elements need to be provisioned to support WPS on VoLTE. Below are examples of capabilities and parameters that may need to be provisioned for each element to support the NS/EP features.

A commercial cellular provider's network might include different parameters and network elements than the examples below. Commercial cellular providers should determine individually the exact parameters and priority indicators applicable for each provider's unique network traffic patterns.

<u>Radio Access Network (RAN):</u>

Evolved Node B (eNodeB):

- Automatic ACB
- Admission Controls based on HPA establishment cause and ARP parameter
- Priority Paging
- Exemption from overload controls

<u>Evolved Packet Core (EPC)</u>

Mobility Management Entity (MME):

- QoS Parameters (ARP, QCI, PCI, PVI)
- Priority Paging
- Exemption from overload controls

Serving Gateway (SGW):

- Priority processing for NGN Priority Service bearer requests
- Exemption from overload controls

Packet Network Gateway (PGW):

- Priority processing for NGN Priority Service bearer requests
- Exemption from overload controls

Internet Protocol Multimedia Subsystem (IMS):

Proxy Call Session Control Function/Session Border Controller (P-CSCF/SBC):

- WPS feature code (*272) and GETS access number recognition
- Setting and supporting (SIP) Resource Priority Header (RPH)
- Setting Diameter Reservation Priority AVP
- Exemption from overload controls

Serving Call Session Control Function/Interrogating Call Session Control Function (S-CSCF/I-CSCF):

- Support Session Initiation Protocol (SIP) Resource Priority Header (RPH)
- Exemption from overload controls

Telephony Application Server (TAS):

- Support Session Initiation Protocol (SIP) Resource Priority Header (RPH)
- Exemption from overload controls

Policy and Charging Rules Function (PCRF):

- QoS Parameters (ARP, QCI, PCI, PVI)
- Exemption from overload controls

Home Subscriber Server (HSS):

- WPS subscription information
- QoS Parameters (ARP, QCI, PCI, PVI)
- Exemption from overload controls

9.3 NGN Priority Services

NGN priority services will include voice, video, and data priority services.

NGN priority services are expected to operate under a broad range of circumstances, from widespread damage to the network resulting from natural or man-made disasters up to and including nuclear war. NGN Priority Services should be implemented so they are at least as survivable or endurable as the networks upon which they are implemented.

The telecommunications industry's transitioning to the packet-switched IP infrastructure of the NGN will enable it to provide high quality multimedia services, including voice, video, and data. Both GSM and some CDMA SPs are deploying a new generation of radio technology with a more efficient air interface to the packet-based switching infrastructure. Long Term Evolution (LTE) is the accepted evolution path for both the Third Generation Partnership Project (3GPP) (GSM, UMTS, High Speed Packet Access [HSPA], LTE, LTE Advanced) and 3GPP2 (CDMA2000, Evolution Data Optimized [EV-DO]). Its two defining technologies are orthogonal frequency division multiplexing (OFDM) and Multi-Input Multi-Output (MIMO) antenna arrays. An optimized combination of OFDM and MIMO enables wireless systems to support up to five times more subscribers than today's networks are capable of supporting (dependent on the bandwidth of deployed spectrum) in addition to a significant increase in data transfer speed. It is expected to be the most widely deployed wireless access technology interfacing with the IP Transport and IMS cores, delivering controlled end-to-end packet transport (via IP) to the application and service layers (IMS). The first domestic commercial trials and deployments of LTE occurred in 2010.

The technologies will impact how NGN Priority Services will need to be implemented. To achieve priority for a connection-oriented service in an IP network, the signaling protocol used for setting up the connection (e.g., Session Initiation Protocol [SIP]) should use its priority parameters (e.g., SIP Resource Priority Header [RPH]) to assign priority to both signaling and transport packets. That is to say, the signaling protocol should mark the Differentiated Services (DiffServ) Code Point (DSCP) in the IP packet header and/or assign priority-reserved routes in a MPLS implementation. Facilities consolidation activities present the potential of adversely affecting the number of available diverse priority-reserved routes that can be assigned.

In a fiber network, QoS capabilities will likely be used to provide priority to NGN Priority Service connections. In these networks, the policy server will be an "NGN Priority Services-aware" device and it will need to set the appropriate priority flows using existing QoS capabilities. Similarly, to achieve priority within SP Ethernet technology solutions, the policy server will need to transmit policy to the appropriate Ethernet switches and gateways. These elements will need to be able to identify the NGN Priority Services traffic, assign the appropriate class of service (COS) or DSCP to the traffic, and handle the traffic with priority. Facilities consolidation activities will need to account for these policy functions and allow for sufficient diversity and robustness of the effected network elements (e.g., the policy servers) to meet the NGN Priority Services' needs.

Across all technologies, NGN Priority Service connections should be provided exemption from overload controls and given priority queuing for resources. Consolidation notwithstanding, sufficient resources need to be provided to allow for the proper functioning of NGN Priority Services without extensive and extended queuing.

SP interconnection/interoperability will need to support NGN Priority Services. For example, SPs will need to establish trust relationships with interconnected peer SPs to ensure NGN Priority Services calls maintain priority across networks. As the barriers to entry decline and the number of interconnected SPs increase, establishing and maintaining trust relationships with an ever-increasing number of peer networks will become a serious challenge. Additionally, NGN Priority Services-compliant SPs will be required to test the interoperability of service features and priority parameters (e.g., SIP RPH) with peer networks, and to ensure NGN Priority Services connections are exempt from procedures that throttle inter-network messaging (e.g., to control overload).

Priority Services may require the caller, after being prompted, to enter a personal identification number (PIN), generally via dual-tone multi-frequency (DTMF) signaling. Thus, the network must allow for follow-on dialing that passes this in-band signaling after the call is connected. This capability is known as "early media cut-through."[49]

Session Border Controllers (SBCs), as well as certain other IP network elements such as IP Private Branch Exchanges (IP PBXs) may have early media cut-through disabled as the default (due to possible network-security and theft-of-services concerns). Not enabling this feature will prevent GETS calls from being processed.

It is recommended that early media cut-through be enabled in IP PBXs and other relevant IP components in SP next-generation networks to ensure that GETS calls made by NS/EP users can be authenticated and completed.

Current circuit-based priority telecommunications features and services will gradually disappear as industry phases out segments of the networks. NGN Priority Services' efforts will focus first on migrating GETS and WPS voice telephony features into the new infrastructure. Future efforts, however, will take advantage of the high bandwidths offered by the NGN to define additional priority telecommunications services such as video teleconferencing, and support data services such as Internet access and e-mail. During the transition, a hybrid circuit-switched/packet-switched communications environment will require the interoperation of legacy GETS and WPS with the new NGN

[49] Also referred to as "early answer voice cut-through" or "cut-through in both directions".

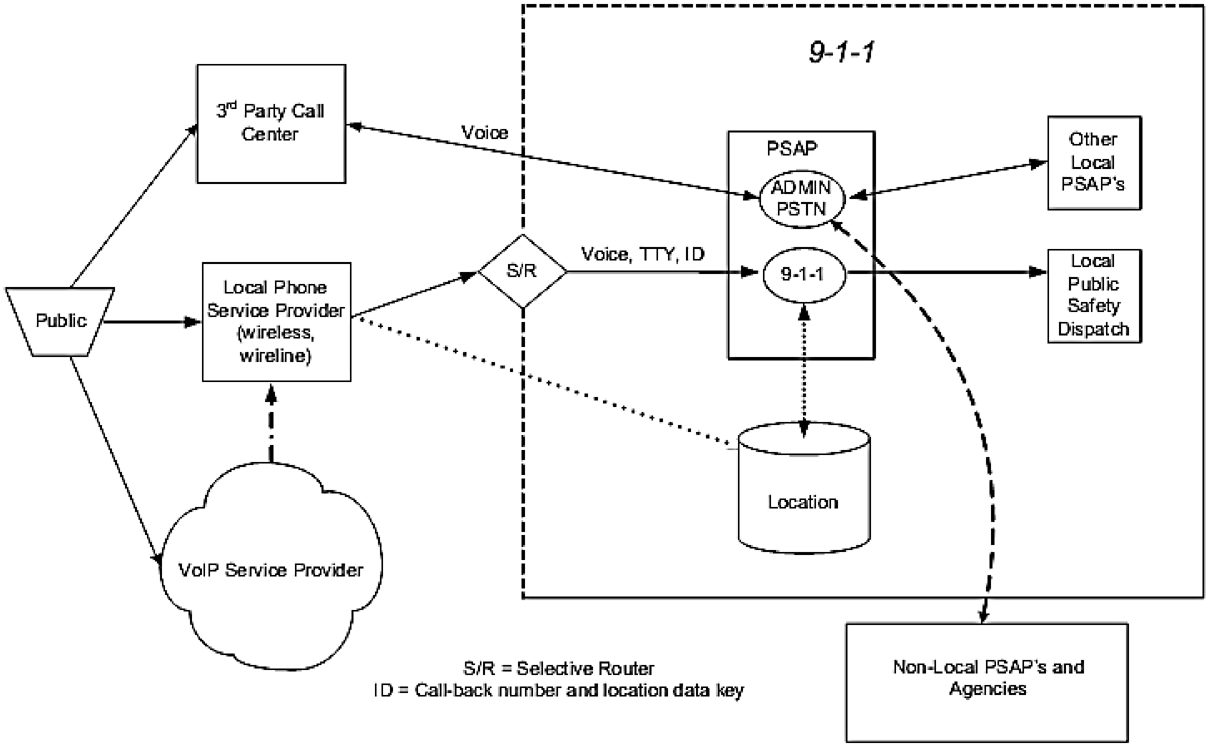
Priority Services, permitting NS/EP users to use these services interchangeably and transparently. In the long-term, legacy services may eventually be replaced completely by the new NGN Priority Services capabilities.

10 9-1-1

10.1 Legacy 9-1-1 Service

Emergency 9-1-1 calls placed by the public on the public telephone network are permitted certain special treatments by the network. Figure 10.1 below presents the general call flows and system elements of a legacy 9-1-1 system.

9-1-1 calls are routed from the local phone SP's end office or MSC, or by a third-party emergency call center, to a Selective Router (SR) (also known as a "9-1-1 Tandem") switch which distributes these calls to a local Public-Safety Answering Point (PSAP). This routing is typically accomplished over dedicated SS7 trunk groups.



9-1-1
3rd Party Call Center
Voice
PSAP
ADMIN PSTN
Other Local PSAP's
Public
Local Phone Service Provider (wireless, wireline)
S/R
Voice, TTY, ID
9-1-1
Local Public Safety Dispatch
Location
VoIP Service Provider
S/R = Selective Router
ID = Call-back number and location data key
Non-Local PSAP's and Agencies

Figure 10.1 - 9-1-1 Call Flow 1

The PSAP has access to information about the caller's location and call-back number. The PSAP also has access to local public safety dispatch, (i.e., calls may be transferred to a dispatch center when that function and organization is different from the PSAP) to dispatch police, fire, medical, or other emergency services, or to other PSAPs.

Call routing by the SR of landline-originated 9-1-1 calls is based on local exchange SP subscriber data, which is also the source of the caller's location information. The Calling Party Category (CPC) parameter in the SS7 ISUP/IAM message establishing a 9-1-1 call is set to 11100000 (decimal 224), for "emergency service call". It is up to each local exchange SP to specify the appropriate treatment for calls marked by this CPC. The message transfer priority (MTP) level of 9-1-1 call-associated SS7 messages is set to "1," providing 9-1-1 call-associated signaling messages with priority in the SS7 network over normal public calls (MTP=0).

Wireless originated 9-1-1 calls are processed by each mobile SP regardless of whether the handset is subscribed to the SP. Apart from this feature, 9-1-1 wireless calls are not currently provided with priority over public calls by mobile SPs. Because of the mobile nature of wireless handsets, 9-1-1 call routing by mobile networks to the appropriate PSAP is based on cellular tower location and/or mobile positioning equipment. The specific processing of mobile 9-1-1 calls depends on the technology employed by each mobile SP.

10.2 Next Generation 9-1-1 Service

Dramatic improvements and changes in the public's use of communications technology, the saturation of the cellular phone market, and the adoption of digital, IP-based devices have rendered the analog, circuit-switched system obsolete. There is consensus within the 9-1-1 community on the need to take advantage of advances in information and communications technologies, to implement the next generation of the 9-1-1 system.

The use of IP-based technology allows for the transformation of the current legacy 9-1-1 system to an NG9-1-1 system, comprised of software and database components that equal and exceed legacy system capabilities. NG9-1-1 systems allow for more complete support of current and future telecommunications services used for access 9-1-1 systems, 9-1-1 PSAPs, and other entities that process emergency calls. The new structure of 9-1-1 systems, both in the call delivery network and within the PSAP, provides more flexibility and more direct control of how 9-1-1 calls are processed. Some of the new capabilities include:

- Enhanced location acquisition: new techniques for location acquisition enhance the capabilities of 9-1-1.
- Multimedia messaging: as SPs deploy new media types (e.g., text, video, etc.), they may provide those services to the users of the NG9-1-1 service as well as to emergency entities, including PSAPs.

10.2.1 Operational Issues

The transition from legacy to NG9-1-1 is expected to present its own challenges, including the coexistence of legacy 9-1-1 and NG9-1-1. SPs may have to interconnect to both services simultaneously within their service area, thus facing both technical and operational issues. Operational issues in transitioning to the NG9-1-1 environment are divided into those that are specific to the operations within the PSAP and those involving operation of the 9-1-1 system.

PSAP operational issues include those that affect the day-to-day operations of 9-1-1 systems; and/or the PSAP related to the convergence of legacy 9-1-1 and NG9-1-1; and to the answering and processing of 9-1-1 calls and data. Data may include text messages, images, video, data from other emerging technologies, and data associated with the processing of the call. The NG9-1-1 environment will create significant changes in PSAP operations related to the variety of new data that must be processed, the basic changes in the 9-1-1 infrastructure, new flexibility and more direct control of how 9-1-1 calls are processed.

System operational issues include issues related to the roles and responsibilities of 9-1-1 Authorities in the operation of the NG9-1-1 system. Implementation of NG9-1-1 will result in increased responsibilities for 9-1-1 Authorities in directly managing the components of the NG9-1-1 system, including issues related to roles and responsibilities, education and training, standards, and contingency planning.

10.2.2 Service Access

Sustained mass calling events to 9-1-1 may cause a focused overload of the 9-1-1 system. Additionally, certain 9-1-1 SR platforms could remove 9-1-1 PSAP trunks from service during periods of heavy emergency call volume. To counter these, special 9-1-1 treatments are employed by the telephone network to enhance the availability and proper operations of the 9-1-1 service. The ATIS Network Reliability Steering Committee (NRSC) published ATIS-0100034, *9-1-1 CAMA Trunk Throughput Optimization Analysis*, which provides recommendations to maximize 9-1-1 call throughput to PSAPs during high call volume conditions.

With the recent dramatic increase in the usage of wireless communications, radio access from mobile handsets to the mobile network's receivers may be severely curtailed during mass calling events, limiting the availability of 9-1-1 service during such events. As an example, in August 2011, the FCC investigated the failures of cell phone service that occurred after an earthquake, when for as long as an hour after the quake wireless customers were unable to get calls through. The FCC was very concerned with the fact that 9-1-1 calls were also congested, as the Commission is charged with ensuring that people who need emergency help are able to get it.

In the NGN, signaling associated with 9-1-1 calls will be marked with an RPH value of “esnet” to distinguish it from normal signaling (analogous to the CPC value of 224 in the SS7 network); it is still up to each local exchange SP to specify the appropriate treatment for calls so marked. Additionally, 3GPP has assigned Access Class 10 exclusively to 9-1-1 calls in the NGN (as described in 3GPP TS 22.011 version 3.8.0, *Technical Specification Group Services and System Aspects; Service Accessibility*), enabling these calls to be given priority access to the radio channel during congestion (similar to the EOP feature described elsewhere in this document). The use of this capability by each mobile SP is optional, however.

10.2.3 FCC Recommendations

The FCC’s Communications Security, Reliability, and Interoperability Council (CSRIC) regularly publishes reports of relevance to Next Generation 9-1-1 Service. CSRIC reports can be found on the FCC’s website.[50]

10.2.4 Other Organizations

Other organizations also address public safety standards and best practices. The following is a non-comprehensive list of organizations that address these issues:

- National Emergency Number Association (NENA)
- Association of Public-Safety Communications Officials (APCO)
- National Association of State 911 Administrators (NASNA)
- 3GPP

11 Telecommunications Service Priority (TSP)

The TSP system provides for the priority treatment of NS/EP telecommunication services in order to prioritize their installation and maintenance.

This section provides TSP installation and maintenance guidelines for access services and generic administrative procedures and interfaces between Access Service Customer (ASCs) and the Access Service Provider (ASPs).

In order for the TSP system to be effective, it must be incorporated into the day-to-day operating procedures for all ASPs and ASCs. All communications providers are expected to cooperate in the installation and restoration of services with TSP that involve the facilities of more than one SP.

11.1 Domestic NS/EP Services

The NS/EP TSP system and procedures provide priority treatment to the following domestic telecommunication services (including portions of U.S. international telecommunication services provided by U.S. providers) for which provisioning or restoration priority levels are requested, assigned, and approved:

- Commercially provided private services and public switched services

NOTE: Initially, the NS/EP TSP system’s applicability to public switched services is limited to provisioning of such services [e.g., business, centrex, cellular, foreign exchange, Wide Area Telecommunication Service (WATS) and other services that the selected provider is able to provision] and restoration of services that the selected provider is able to restore. For example, services that are provided by Government and/or non-common SPs and are interconnected to common SP services are assigned a priority level pursuant to Section 9 of the FCC's TSP system rules.

11.2 Control Services & Orderwires

The NS/EP TSP system and procedures are not applicable to authorize priority treatment to control services or orderwires owned by a SP and needed for provisioning, restoration, or maintenance of other services owned by

[50] https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council

that SP. Such control services and orderwires shall have priority of provisioning and restoration over all other telecommunications services (including NS/EP services) and shall be exempt from preemption. However, the NS/EP TSP system and procedures are applicable to control services or orderwires leased by a SP or user from another SP.

11.3 Other Services

The NS/EP TSP system may apply, at the discretion of and upon special arrangements by the entities involved, to authorize priority treatment to the following telecommunications services:

1. Government or non-common SP services which are not connected to common SP-provided services assigned a priority level.
2. Portions of U.S. international services which are provided by foreign correspondents.

11.4 TSP Code Identification

The TSP Authorization Code is composed of twelve characters and is divided into two parts. The first nine characters comprise the TSP Control ID, a computer-generated number, which is for the government's tracking purposes. A hyphen is always the tenth character and it separates the TSP Control ID from the TSP Code. The final two characters are the TSP Code. The first character of the TSP Code (the eleventh character of the entire series) indicates the provisioning priority. Acceptable values are: E (Emergency), 1, 2, 3, 4, 5, or 0. A value of "0" indicates no provisioning priority is assigned. The second character of the TSP Code (the twelfth character of the entire series) indicates the restoration priority. Acceptable values are 1, 2, 3, 4, 5, or 0. A value of "0" indicates no restoration priority is assigned.

A TSP Authorization Code is illustrated below:

```
T S P 1 2 3 4 5 C - 1 2
      |         |
 Control ID    Code
```

Table 11.1 below depicts the codes (eleventh and twelfth digits) allowable in the TSP system.

Table 11.1 - TSP Codes Reference Table

TSP Provisioning/Restoration Priority Levels

	P-R	P-R	P-R	P-R	P-R	P-R	P-R	
	E-1	1-1	2-1	3-1	4-1	5-1	0-1	
	E-2	1-2	2-2	3-2	4-2	5-2	0-2	
HIGHER ↑	E-3	1-3	2-3	3-3	4-3	5-3	0-3	↓ LOWER
←	E-4	1-4	2-4	3-4	4-4	5-4	0-4	→
	E-5	1-5	2-5	3-5	4-5	5-5	0-5	
	E-0	1-0	2-0	3-0	4-0	5-0	0-0	

E = Emergency Priority Level

P = Provisioning Priority Level

R = Restoration Priority Level

A code of “0-0” indicates “Revocation”, the removal of a previously assigned TSP code.

11.5 TSP Installation

Circuits with an E (Emergency) provisioning priority have the highest priority and must be installed as soon as possible, dispatching outside of normal business hours when necessary. Circuits with TSP provisioning priorities 1 – 5 will be installed by the due date according to the TSP provisioning priority assigned (see reference table above). For example, a circuit with a provisioning priority of "1" would be installed before a circuit with a provisioning priority of "2" when they both carry the same due date.

11.6 TSP Maintenance

Available resources should be allocated to restore NS/EP services as quickly as practical, dispatching outside normal business hours to restore services assigned priority levels "1", "2", and "3" when necessary and services assigned priority levels "4" and "5" when the next business day is more than 24 hours away.

The day-to-day administration for repair and restoral of services assigned a TSP restoration priority is shown in the following examples:

Example 1: If there are several pending Trouble Reports for circuits that do not have TSP restoration codes and a Trouble Report is received for a circuit with a TSP code of 23, the TSP23 circuit Trouble Report moves to the next Trouble Report to be worked ahead of the other circuit Trouble Reports that have no TSP restoration codes. Upon completion of the repair/restoral of the TSP23 circuit, work continues on the Trouble Reports for the circuits that have no TSP restoration codes.

Example 2: If there are several Trouble Reports to be worked (which includes a circuit with a TSP23 code) and two additional Trouble Reports are received for circuits with higher TSP restoration codes (such as TSP21 and TSP22), the circuit Trouble Report with the TSP21 code will move to the next Trouble Report to be worked, followed by the TSP22 circuit Trouble Report. Then, the TSP23 circuit Trouble Report moves ahead of the other Trouble Reports for the circuits that have no TSP codes. Upon completion of the repair/restoral of the TSP21, TSP22 and TSP23 circuits, work then continues on the Trouble Reports for the circuits that have no TSP codes.

11.7 Competition for Resources between Provisioning & Restoration Priorities

In general, SPs should restore existing services assigned TSP priority before provisioning new service; an exception is the provisioning of services assigned emergency priority, which should always be done before the restoration of services assigned restoration priorities "2", "3", "4", or "5". Restoration of any service assigned restoration priority "1" takes precedence over any other service assigned any other provisioning and restoration priority.

When two or more TSP services are competing for resources, the priority sequence listed below will ensure proper handling of these circuits:

- Restore TSP services with restoration priority of “1”.
- Provision TSP services with provisioning priority of “E”.
- Restore TSP services with restoration priority of 2, 3, 4, 5.
- Provision TSP services with provisioning priority of 1, 2, 3, 4, 5.

Using the priority sequence listed above, the following examples of two TSP services competing for the same resources at the same time, the underlined TSP service has the higher priority and should be worked on first:

- TSP code 2-1 and E-2 both in trouble status. 2-1
- TSP code 2-1 in trouble and E-2 to be provisioned. 2-1
- TSP code 2-1 to be provisioned and E2 in trouble. E-2

- TSP code 2-1 and E-2 to be provisioned. E-2

11.8 TSP Installation Preemption

Where facilities and/or equipment are not available to install a service assigned a TSP priority, preemption (interruption of an existing service) of a non-priority or lower priority circuit may be required. User consent is NOT required to preempt any user's existing service to provision an NS/EP service assigned a provisioning priority level "E" (Emergency) or to provision an NS/EP service assigned a provisioning priority level "1" through "5".

11.9 TSP Maintenance Preemption

Facilities of message circuits may be used for restoral of services assigned a TSP restoration priority after ensuring that sufficient message circuits are available for public switched network use.

Where facilities and/or equipment are not available to restore a service assigned a TSP restoration priority preemption (interruption of an active service) may be required. Interruption of a non-priority or lower priority circuit is authorized for the purpose of restoring the service assigned a TSP restoration priority.

User consent is not required to preempt any user's existing service to restore any NS/EP service assigned a restoration priority level from "1" through "5".

If no suitable spare or non-NS/EP services are available, then existing NS/EP services may be preempted to restore NS/EP services with higher priority level assignments. When this is necessary, NS/EP services will be selected for preemption in the inverse order of priority level assignment.

SPs who are preempting services will ensure their best effort to notify the end user of the preempted service and state the reason for and estimated duration of the preemption.

12 Testing Documentation

This section identifies common testing procedures/agreements between interconnection partners and the basic responsibilities of each.

12.1 ATIS Documentation Relevant for IP Network-to-Network Interconnection Testing

It should be noted that this list is not all inclusive and additional testing documentation may be available.

ATIS-1000038, *Technical Parameters for IP Network to Network Interconnection Release 1.0.*

This document was developed by the ATIS Next Generation Carrier Interconnection (NG-CI) Task Force under the ATIS PTSC. The document contains a technical report that specifies the “Interconnection Technical Parameters” that need to be collected and eventually exchanged between two SPs so that they can successfully interconnect IP-based facilities and VoIP services at an NNI.

The four ATIS NG-CI technical reports cover four aspects of interconnection and ATIS-1000038 has four companion technical reports that address VoIP service interconnection over IP-based links/networks. They are as follows:

ATIS-1000040, *Protocol Suite Profile for IP Network to Network Interconnection Release 1.0*

This document identifies a set of service specific protocol requirements needed to support service interoperability protocols, and specifies their profile so that signaling, media, and network related parameters can be uniformly and consistently utilized across the Interconnection interface. While the other documents in this release 1.0 set make reference to the specifications covered, this document identifies the specific details of protocol elements to be tested.

The objective is to support a service seamlessly across an IP Network to Network Interconnection as identified by the test scenarios defined in ATIS-1000041, *Test Suites for IP Network to Network Interconnection Release 1.0*.

ATIS-1000041, *Test Suites for IP Network to Network Interconnection Release 1.0*

This document provides the tests used for IP NNI interconnection testing in order to support service interoperability by specifying a set of call test scenarios involving SIP and other signaling messages which for various situations may be required to provide an expected reaction to an event or a sequence of events appropriate to the previously signaled message. This "expected reaction" is based upon the protocol profile established in the messages that flow across the NNI.

ATIS-1000039, *Testing Configuration for IP Network to Network Interconnection Release 1.0*

This document provides the network interface (i.e., Service Under test (SUT)) configuration in order to support service interoperability and verify conformance with the desired configuration and service interoperability.

Once the fixed and configuration profiles are established and specified, the variable or selectable parameters can be applied uniformly and consistently for interconnects. This will ensure a reliable level of conformance to the standards applicable at the NNI defined in ATIS-1000009, *IP Network-To Network Interface (NNI) Standard for VoIP*, thus supporting the establishment of successful interoperability. Note that the focus of these documents is on signaling passing between Session Border Controllers (described in ATIS-1000026, *Session Border Controller Functions and Requirements*) for voice traffic, only; data traffic, including database query/response signaling, is not included.

ATIS-1000053, *Emergency Telecommunications Service (ETS) Profile and Tests for IP Network to Network Interconnection*

This document provides an emergency telecommunications service (ETS) profile and tests for IP Network–to-Network Interconnection; ETS will be supported on IP Network to Network Interconnections. There is a need to test and verify the ETS requirements relevant to IP Network-to-Network interconnection. Additional information is provided in the Scope, Purpose, and Application section of ATIS-10000053.

ATIS-1000014, *VoIP Network-to-Network Interface Testing Framework*

This document describes a framework for testing interoperability of an IP Network-Network interconnection for VoIP services. The framework is for such an interconnection as specified in ATIS-1000009.2006, Additional information is provided in the Scope, Purpose, and Application section of ATIS-1000014.

ATIS-1000009, *IP Network-to-Network Interface (NNI) Standard for VoIP*

This standard defines the IP NNI for VoIP service between SPs. It also includes an informative annex on items for consideration in Service Level Agreements (SLAs).

ATIS-1000026, *Session Border Controller Functions and Requirements*

This standard defines the Session Border Controller (SBC) functions and requirements that reside within a SP's network, spanning interfaces from the SP's network to:

- Another SP.
- An enterprise network.
- A transit network.

- A residential customer network.
- An access network.
- An application network.

ATIS-1000018, *NGN Architecture*

This document describes the overall ATIS NGN Architecture based on the IMS architecture, its subsystems, and the relationships between them.

13 Testing Procedures & Responsibilities

There may be procedures and responsibilities listed in specific testing documents that may augment or supersede the following items. The following list includes basic testing responsibilities and should not be considered all inclusive:

- Develop a mutually acceptable testing agreement, including specific responsibilities, procedures, and test scripts (e.g., interoperability testing for different protocols, regression testing, etc.)
- Determine the testing schedule (dates/times)
- Provide trained personnel
- Provide a contact number for trouble reporting that is readily accessible 24 hours a day, 7 days a week
- Provide access to test lines where appropriate
- Provide billing authorization for any additional labor requested
- Ensure the test equipment used is compatible to other testing networks
- Test cooperatively as required to identify and clear a trouble, when the trouble has been sectionalized to another's network
- Perform cooperative analysis to determine if a trouble pattern exists
- Perform verification tests to ensure that trouble has been cleared

14 Disaster Considerations

During a disaster, the flow of traffic could be seriously impacted depending on the disaster scenario and businesses, increasing public reliance on communications and IT services. Disasters can also impact the availability of support staff for network operators. As a result, network operators may encounter decreased ability to respond to network problems. The combination of increased reliance on networks and decreased support could significantly impact customers' ability to communicate at a time when communication is critical.

Therefore, there is a need for companies to coordinate network management actions consisting of preplanning, real-time surveillance, analysis, control of traffic flow, and system restoration in the communications networks. The objective is for companies to pre-plan and react to ensure the maximum utilization of the communications networks under stressful conditions due to traffic overload or network failure. When disaster conditions seriously impact traffic flow through interconnected network elements of interconnected network operators, the need for cooperative network management actions exists.

As noted in ATIS-0300100, *IP Network Disaster Recovery Framework,* and ATIS-0300202, *Internetwork Operations – Guidelines for Network Management of the Public Telecommunications Networks under Disaster Conditions*, companies and their network managers should consider the following phases in coordinating and addressing network management actions during disaster conditions:

- Planning of coordinated network management actions between interconnected Network Providers.
- Detection and identification of disaster conditions.
- Selection of system recovery and restoration strategies to be employed.

- Implementation of traffic network management actions.
- Evaluation and reporting of network management actions and responses.

14.1 Planning

A company should begin planning actions to be taken by its network operators, which should be initiated during disaster conditions. These actions should ensure that the most effective detection processes, control strategies, and communications with other network operators will be utilized. When forecasts, warnings, or experiences indicates the potential for impending disaster conditions, existing plans should be reviewed and updated and/or enhanced to ensure that they adequately address the specific type of disaster.

15 Network Management Control During High Level Congestion Events

Network managers will need to take action to minimize the intensity, spread, and duration of congestion. This section focuses on methods that could be used by network managers for congestion control during overload events.

15.1 Congestion & Overload

In general, a communications element can suffer from two types of overload. The first type of overload occurs when there is more traffic trying to get to the element than the pathways to that element can support. The second type of overload occurs when the demand on the components within the element exceed its capacity (such as processor or memory overload). These can be a physical limitation (e.g., 10 Gbps of traffic when only a 1 Gbps facility exists) or logical (e.g., attempting to support 1,000 sessions when the interface is only configured to support 500 simultaneous sessions).

Overload can occur due to network administration and control traffic and procedures, control signaling for customer sessions, or the bearer traffic of customer sessions. Network operators should understand the capacities and limitations of each network element, as well as how that element responds to congestion/overload, and the manual and automatic methods available to manage the element during congestion and overload events.

15.1.1 NGN Session Control & Congestion/Overload

SIP is currently the core signaling protocol for NGN implementation. As such, it is important to understand what can cause congestion and how to prioritize access during congestion. There are two types of SIP congestion that can cause overload. The SIP network can suffer an overload when packets are lost in the IP layer. SIP recognizes such a failure and attempts to retransmit the failed message. The other type of congestion is a server overload, which happens when the number of SIP messages a server receives exceeds the number of messages it can process. There are a number of triggers that could cause SIP server overload. These can include retransmission, capacity, emergency-induced call volume and flash/transient crowds, restarts, and Denial of Service (DoS) Attacks.

15.1.2 Retransmission

IETF RFC 3261, *SIP: Session Initiation Protocol*, defines retransmission procedures to improve the reliability of transmitting SIP messages. Although these retransmissions improve the message reliability, they can increase the load applied to a SIP server, which could impact SIP signaling performance during overload conditions.

15.1.3 Capacity

A SIP server can overload for many different reasons, for example, when it receives more traffic than it is designed to handle. A SIP network should be designed with proper capacity planning in mind so that it can meet the needs of the subscribers it anticipates serving. Without proper capacity planning, the network could have a difficult time processing predictable usage.

In addition, network equipment failures could cause a SIP server overload. It is difficult for the network to shed load due to the unpredictable nature of these types of failures. A SIP element can become overloaded when a resource it depends on fails, becomes overloaded, or when it is a member of a cluster of servers and there is a failure in the cluster.

15.1.4 Emergency-Induced Call Volume Flash/Transient Crowds

IETF RFC 5390, *Requirements for Management of Overload in the Session Initiation Protocol*, defines a flash crowd as follows: A flash crowd occurs when an extremely large number of users all attempt to simultaneously make a call. One example of how this can happen is a television commercial that advertises a number to call to receive a free gift. If the gift is compelling and many people see the ad, many calls can be simultaneously made to the same number. This can send the system into overload.

In addition to the example of the media stimulated event above, special dates and events, such as New Year's Eve, may stimulate a large rate of traffic to a large number of destinations. Even though the event may be known in advance, there may be no way to determine specific destinations that will be targeted.

Disasters could also stimulate overload, which could be focused to emergency services (9-1-1) and information lines, or could cause a load from the disaster location to a large number of destinations (similar to the special dates/events description above). Depending on the disaster, the network itself may be damaged which can cause an overload by the reduction in capacity due to network equipment failure.

15.1.5 Denial of Service (DoS) Attacks

The purpose of a DoS attack is to disrupt service in the network. The attack causes a large amount of traffic to be launched at a target server. The volume of traffic well exceeds the capacity of the server, sending the system into overload. A DoS attack can be disguised as legitimate traffic, so it may be difficult to distinguish the difference between a DoS attack and a sudden surge in traffic due to an event.

15.2 NGN Access Prioritization

According to ATIS-0300100, *IP Network Disaster Recovery Framework*, there are at least five (5) different resources in SIP applications that could become congested during emergencies. It may be necessary to prioritize access to these resources during an emergency in order to improve emergency response. These resources are as follows:

- Gateway resources: The number of channels (trunks) on a Circuit-Switched Network (CSN) gateway is finite. Resource prioritization may prioritize access to these channels, by priority queuing or preemption.
- CSN resources: Resources in the CSN itself, away from the access gateway, may be congested. This is the domain of traditional resource prioritization mechanisms such as Multilevel Precedence and Preemption (MLPP) and GETS, where circuits are granted to ETS communications based on queuing priority or preemption (if allowed by local telecommunication regulatory policy and local administrative procedures). A gateway may also use alternate routing to increase the probability of call completion.
- IP network resources: SIP may initiate voice and multimedia sessions. In many cases, audio and video streams are inelastic and have tight delay and loss requirements. Under conditions of IP network overload, emergency services applications may not be able to obtain sufficient bandwidth in any network. When there are insufficient network resources for all users and it is not practical to simply add more resources, QoS management is necessary to provide priority treatment for emergency services applications.
- Receiving end system resources: End systems may include Automatic Call Distribution (ACD) systems or Media Servers, as well as traditional telephone-like devices. Gateways are also end systems. Since the receiving end system can only manage a finite number of sessions, a prioritized call may indicate to the called party that a high-priority call is waiting. Such terminating services may be needed to avoid overloading, for example, an emergency coordination center. However, other approaches beyond

prioritization (e.g., random request dropping by geographic origin) need to be employed if the number of prioritized calls exceeds the terminating capacity.

- SIP proxy resources: While SIP proxies often have large request handling capacities, their capacity is likely to be smaller than their access network bandwidth. Therefore, some types of proxies may need to silently drop selected SIP requests under overload, reject requests, with overload indication or provide multiple queues with different drop and scheduling priorities for different types of SIP requests. Responses should naturally receive the same treatment as the corresponding request. Responses already have to be securely mapped to requests, so this requirement does not pose a significant burden. Since proxies often do not maintain call state, it is not generally feasible to assign elevated priority to requests originating from a lower privileged called party back to the higher-privileged calling party.

16 Disaster Recovery

When a disaster situation occurs, individual companies will activate their own disaster recovery plans as required. Mitigating some disasters may require mutual aid. Individual interconnect agreements may determine responsibilities and other aspects of mutual aid provided during an emergency disaster situation.

All communications providers should ensure that their respective departments and personnel are well versed in all aspects of disaster recovery and mutual aid procedures. Typically, companies internally perform table top exercises for business continuity plans in a disaster situation. Interconnection agreements may include mutual aid exercises between companies at their discretion.

Providers transitioning from a TDM environment to an All-IP environment should periodically review disaster plans for any changes or modifications required due to technological evolution.

16.1 Force Majeure

Force Majeure events, as applicable to interconnection, include any events beyond the reasonable control of the SP that results in a delay or failure in performance. Force Majeure events include, but are not limited to, adverse weather conditions, floods, fires, explosions, government requirements, acts of civil or military authorities, earthquakes, volcanic actions, power failures, embargoes, boycotts, wars, revolutions, civil commotions, acts of public enemies, labor unrest (including, but not limited to, strikes, work stoppages, slowdowns, picketing, or boycotts), inability to obtain equipment, parts, software or repairs thereof, acts or omissions of another party, and acts of God.

If a Force Majeure event occurs, prompt notification should be provided to impacted companies. These events may result in parties being temporarily excused from some contractual performance obligations as defined in interconnection agreements.

16.2 Governmental Disaster Plans

In addition to individual company plans, there are disaster plans available from various government agencies. Listed below are some of those agencies; however, this list may not be all inclusive. A search can be made to look for disaster plans on the respective agency website.

- FCC
- Department of Homeland Security (DHS)/ Federal Emergency Management Administration (FEMA)
- Department of Homeland Security (DHS) CISA ECD
- NS/EP
- State – refer to Emergency Operations Centers (EOCs) in each individual state

16.3 Standards Groups Disaster Plans

In addition to individual company plans, various standards bodies have created disaster plans including (not limited to):

- ATIS NRSC:
  - ATIS-0100019, *Emergency Preparedness and Response Checklist*
  - ATIS-0100018, *Pandemic Checklist*
- ITU-T: The International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) develop international standards critical to defining elements in global infrastructure of information and communication technologies, to ensure global communication for countries' ICT networks and devices are compatible with one another.
- CSRIC: The Communications Security, Reliability and Interoperability Council's (CSRIC) mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety. Information related to CSRIC can be found on the FCC's website, http://www.fcc.gov.

17 Disaster Reporting

In the event of a major disaster, the FCC and the Department of Homeland Security's National Communications system need to have accurate information regarding the status of communications services in the disaster area, particularly during restoration efforts. The following systems are used for reporting outage information to the FCC.

17.1 Network Outage Reporting System (NORS)

NORS is the web-based filing system through which communications providers covered by the Part 4 reporting rules[51] submit reports to the FCC. This system uses an electronic template to promote ease of reporting and encryption technology to ensure the security of the information filed. The Communications Systems Analysis Division of the FCC's Public Safety and Homeland Security Bureau administers NORS, monitors the outage reports submitted through NORS, and performs analyses and studies of the communications disruptions reported.[52]

17.2 Disaster Incident Reporting System (DIRS)

DIRS is a voluntary, web-based system that communications companies, including wireless, wireline, broadcast, and cable providers, can use to report communications infrastructure status and situational awareness information during times of crisis.[53]

[51] 47 C.F.R. Part 4: <https://www.federalregister.gov/>.

[52] FCC NORS Website: <http://transition.fcc.gov/pshs/services/cip/nors/nors.html>.

[53] FCC DIRS Website: <http://transition.fcc.gov/pshs/services/cip/dirs/dirs.html>.