PSTN Transition Focus Group
Assessment and Recommendations

January 2013

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

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

The *ATIS PSTN Transition (PSTNTran-FG), Assessment and Recommendations* is an **ATIS Work Plan** developed for the **Technical and Operations (TOPS) Council**.

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

Printed in the United States of America.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

1 Problem Statement

The infrastructure of the Public Switched Telecommunications Network (PSTN) has been transitioning from TDM (time division multiplex) technology to IP (Internet Protocol). The TDM network that consists of a telecommunications service provider providing a single-purpose voice connection to the consumer is being replaced by an IP network where a voice application (Voice over IP, or VoIP) is transported over a multi-purpose broadband connection.

IP is significantly different from TDM. The existing processes and regulations associated with the PSTN are based on a TDM network. As the network transitions to IP, it is important for the industry to evaluate the impact of this transition and make changes and recommendations where necessary. The ATIS PSTN Transition Focus Group was formed to examine this issue.

2 Scope of Effort

The PSTN Transition to an IP-based network will impact many facets of the current network. For this reason, it was decided to assess this transition across four areas of network evolution: *application services, access, transport, and numbering*. The subsequent analysis will provide conclusions and recommendations around each of these topics.

3 Current State of the PSTN in Transition

The PSTN is in transition as more and more consumers each year decide to forego PSTN fixed voice in favor of alternative communications technologies. The PSTN is a voice-centric network that no longer satisfies all of the interactive communication needs and demands of the broad base of consumers. The transition opens many opportunities for new and richer communication capabilities. Interoperability between existing PSTN services and these newer IP-based services will need to continue for a number of years. Thus, PSTN transition is an *evolutionary* process, not a network replacement event.

"Successor networks" will consist of multiple interconnected networks supporting a range of IP-based services and applications. Consumers will have access to a baseline set of voice and data communication services. To meet our national goals, these services will have to achieve certain targets with respect to reliability, emergency notification, accessibility, and other critical needs.

4 Implications of Social Policy & Regulation on PSTN Transition

The Focus Group also reviewed the various aspects of the PSTN transition in the context of existing social policies and regulations. The identification of the key social policy areas related to PSTN transition and the associated regulatory framework related to each policy (see Appendix E) provided a baseline for further examination of the application services, access, transport, and numbering issues impacting the network evolution.

5 Assessment & Conclusions

5.1 Application Services

To understand the impacts on the PSTN services in transition, each application was analyzed in multiple dimensions. Consideration was given to both the current and future states as well as any implications for

regulatory policy and/or standards. For most applications, business drivers will determine which applications migrate and how they do so.

As a first step, a broad range of PSTN services in transition were defined, including Core Voice Services, Advanced Communications Services, Media/CPE Dependent Services, and Accessibility/Assistance Services. In addition, new capabilities and functions related to the Successor Network (e.g., Presence, Location, and Video Calling/Conferencing) were identified to map a migration to the future network.

As a final part of the analysis, the current set of PSTN applications available today were analyzed and placed into categories:

- *Sunset Services:* This set of services leverage outdated technology and are being or have been replaced by alternate mechanisms that provide superior capability.
- *Transitional Services:* Due to market penetration, this set of services will require strategies for ongoing support until it makes commercial sense to transition.
- *Successor Network Services:* Services definitively supported in successor networks driven by regulatory, social policy, or market forces.

5.2 Access

As part of this investigation, various characteristics and limitations of the PSTN access network were investigated. The goal was to determine which of these characteristics might need to be carried forward as the PSTN is evolved. For each of these areas, an attempt was made to assess whether regulatory requirements related to these areas existed, and what customer premises equipment (CPE) would be impacted if that particular characteristic was no longer present.

It was determined via this analysis that the key concerns were:

- *Stranding of CPE:* Overall, it was concluded that the stranding of CPE is best treated as an economic issue, not a policy issue.
    - For most CPE, consumers are voluntarily making the transition away from analog devices for better features, to save money, etc. Consumers already have abundant choices.
    - For those choosing not to transition the CPE, it is possible to provide a converter box and substitute an alternate technology. Many cable/fiber providers already provide such capability.
    - Since such an alternative exists, carriers shall be allowed to migrate technology. How to incentivize or force the adoption of converter boxes is an economic issue.
- *Implications of loss of central office power:* Phasing out of CO line power should be an economic issue. Emergency powering is not required, but can be provided as a feature. It should be a consumer choice whether it is needed and how it is provided.
- *Robustness:* For this analysis, the term "robustness" was interpreted to mean "availability" (or "survivability" in the case of disasters). Although access can be engineered for different levels of availability depending upon specific requirements, current broadband access networks are not typically engineered for the same level of availability as the PSTN. The traditional need for high availability was primarily driven by the need to maintain communications, since PSTN was the “only” network. Many subscribers now have access to more than one access (broadband, wireless), which will give overall higher availability than any single access. High availability may also be viewed as a commercial differentiator between service offerings.

5.3 Transport

Key technical and business challenges were identified, as were observations during the review of both existing and developing interconnect models. Existing documented IP interconnect models are primarily focused on “voice” service, but more advanced “multiservice” models are accompanied by further technical and business requirements with the goal of improving security and quality of service.

It is reasonable to anticipate a gradual adoption of IP interworking for voice services in which TDM and IP technologies coexist to form a hybrid network. Each provider’s decision to implement network

modernization will be based upon their business and customer needs, recognizing that limited resources will influence modernization to areas of growth or high cost. To this end, it is expected that the decision as to when and where to perform a TDM to IP technical substitution will be based on many factors and best left to the decision of SPs and Carriers.

The following are the key observations and trends related to Transport:

- IP interconnect depends on the availability of an industry-wide address translation and routing solution (e.g., ENUM).
- There is an increasing need for authentication of users and/or service providers to minimize fraud and spam.
- The industry is moving from an established interconnection model to multiple models.
    - The models have varying requirements (QoS, security, etc.) and compensation arrangements.
    - Model diversity breeds innovation, but eventually a few dominant models must prevail.
- These unique QoS and security requirements will introduce new challenges and opportunities for managed communication services.
- The PSTN transition is best served by allowing a gradual evolution of services and interconnection models.
- The separation of service provider responsibility for communication services and IP access is a key driver for new interconnection models.
- Emerging technologies and services (e.g., OTT, cloud, WebRTC, OMR) will significantly influence the evolution of interconnection models.

5.4 Numbering

A broad range of Numbering issues were identified and analyzed, and specific issues impacting the PSTN transition path were highlighted for further study. These issues were primarily focused in the areas of Numbering Authentication, Addressing, and Administration.

In addition, an assessment of the PSTN-related Databases was conducted, for the purpose of identifying the key functionalities of each system and the relationship of each database to the needs of the future network.

6 Recommendations

6.1 Application Services

The following areas are recommended for further study:

- *CLASS^{SM} (Customized Local Area Signaling Service)* – CLASS Services are a group of network-provided enhanced services that leverage the capability of the signaling network to pass the calling party's number across the network. CLASS-enhanced service offerings include incoming-call identification, call trace, call blocking, automatic return of the most recent incoming call, call redial, and selective forwarding and programming to permit distinctive ringing for incoming calls. If there is sufficient market demand for equivalent functions in successor networks, further study is recommended to define SIP extensions to achieve a more comprehensive and interoperable set of IP Consumer Services. The work should take into account the functions that could be carried out more efficiently by devices rather than network entities (e.g., Visual Voicemail display and Selective List Editing features).

- *Privacy Regulations* – Clarification is required from the Federal Communications Commission (FCC) around applicability of privacy rules of 91-281 to Calling Number and Name Delivery in successor networks. If applicable, details of implementation require ubiquitous adoption in IP-based networks.

- *Portability* – Areas for further study covering Portability include:

- Portability functionality in general and specifically, portability boundaries, as well as the role of network elements, and number or address resource optimization related to any elimination of rate centers and LATAs.
- Portability functionality for customer-facing addresses, whether they are e.164 numbers (and their associated LRNs) or something else.
- Evolution and architecture of industry and carrier databases for portability in the successor network. For example, can the ENUM hierarchical registry architecture support Number Portability in the U.S. in the successor network, and if so, how?

6.2 Access

The key Recommendations related to Access include:

- Stranded CPE should be treated as an economic issue, not a policy issue.
- Removal of central office provided line power should be treated as an economic issue, not a policy issue.
- IP-based technology has the potential to be engineered as a more reliable solution than circuit switched technology. However, the ultimate robustness depends on the requirements to which the network is engineered.

6.3 Transport

To facilitate widespread deployment of IP interconnect, the industry needs to agree on a tiered routing architecture. The interconnect architecture should flatten with more direct connections between service providers since LATA routing is unnecessary.

Future interconnect models should support identity authentication of users and service providers to provide security, compensation support and fraud/spam control.

ATIS should perform the following actions (with the PTSC taking the lead and coordinating with other committees where appropriate):

- Analyze the IP interconnection issues described in Appendix C, section C.5, to make recommendations for applicability of existing options or development of new specifications. These aspects include Security, QoS, Signaling, Media, Fax over IP functions, as well as transport configuration options and routing.
- Analyze the impact of emerging technologies and services (e.g., OTT, cloud, WebRTC, OMR) on the evolution of interconnection models.
- Examine commercial issues related to the technical issues, including the potential enhancements for multiservice support.
- Evolve current IP interconnection models to incorporate the latest advances.
- Encourage the voluntary convergence of the industry on a minimal set of the most broadly adopted models.

6.4 Numbering

The following recommendations related to PSTN Transition Numbering were developed:

Addressing:

- Resolve open issues regarding TN-to-internet addressing solution to enable industry-wide IP-to-IP routing. Open issues that need to be resolved:
  - *Administrative information exchange* – Method of sharing the address of the route server associated with the TN.

    - *Discovery* – Method of mapping the TN to an address of a route server during call processing.
    - *Mutual authentication* – Authenticating the route server querying and queried party.
- Consider a TDM-to-IP addressing solution that conserves numbering resources.

Administration:

- Consider introducing expanded geographic area codes for traditional communications service.
- Consider breaking the linkage between geography of the TN and geography of the POI.
- Closely monitor number allocation and utilization.
- Assess the implications of direct consumer registration of TNs.
- Eliminate number allocation and assignment based on rate centers and LATAs.

Numbering Authentication:

- Ensure that telephone numbers on IP networks are secured against spoofing.

Appendix A

Application Services

Appendix A: Application Services

A.1 Introduction

A.1.1 Background

The market for broadband services continues to grow. Consumers are quickly embracing multi-modal communications (e.g., voice, video, text, chat, presence exchange, social networking). This trend is driving the transformation of the legacy PSTN to new IP packet-based successor networks.

A.1.2 Objective & Scope

This Appendix identifies the set of PSTN services in transition along with an analysis of the implications from both a technical and regulatory perspective. Also included is a view of some of the new services and capabilities that will exist in successor Networks.

A.1.3 Definitions

A.1.3.1 PSTN in Transition

The PSTN is in transition as more and more consumers each year decide to forego PSTN fixed voice in favor of alternative communications technologies. The PSTN is a voice-centric network that no longer satisfies all of the interactive communication needs and demands of the citizens of the United States. The transition opens many opportunities for new and richer communication capabilities. Interoperability between existing PSTN services and these newer IP-based services will need to continue for a number of years as there will never be the money to "flash cut" away from the existing services. PSTN transition is an *evolutionary* process, not a network replacement event. Solutions exist to support most TDM functions in next generation networks, and customers will have the choice to move to new services and devices.

A.1.3.2 Successor Networks

"Successor networks" will consist of *multiple* interconnected networks supporting a range of IP-based services and applications. Consumers will have access to a baseline set of voice and data communication services. To meet our national goals, these services will have to achieve certain targets with respect to reliability, emergency notification, accessibility, etc.

A.2 Key Interests

There exists a baseline set of services we need for the coming decades that are required to meet the economic, public safety, and national security interests of the US. We should define the new successor network services based on those needs.

A.2.1 Economic

With the PSTN, we had universal connectivity to help US economic interests. As we evolve to successor networks, it is clear that the additional capabilities provided by broadband services improve the economic situation of communities by spurring job creation and improving business efficiencies. New national-scale social and economic opportunities may be enabled through near universal adoption of reliable IP-based services.

A.2.2 Public Safety/Accessibility

Key public safety and accessibility goals remain in place for successor networks. These requirements include emergency services at the individual incident level, robustness and priority access at larger scales to deal with crisis and disasters, operator assistance in public safety, and accessibility.

A.2.3 National Security

New strategies and services are required for monitoring communications beyond voice in successor networks. As communication capabilities and options for the consumer grow, the Lawful Intercept capabilities will also expand to incorporate these additional capabilities and options.

A.3 Assessment Approach

To understand the impacts to the PSTN services in transition, each application is analyzed in multiple dimensions. Consideration is given to both the current and future states, as well as any implications to regulatory policy and/or standards. For most applications, business drivers will determine which applications migrate and how.

A.4 Defining PSTN Services in Transition

A.4.1 Core Voice Services/ Regulatory Services

A.4.1.1 Dual-Tone Multi-Frequency Signaling (DTMF)

A.4.1.1.1 Definition of Current State

DTMF is used to control the operations of Interactive voice response (IVR) equipment enabling a variety of interactive services. DTMF tones are sent when the user presses a telephone's touch keys. These tones are used to access voicemail, enter passcodes, retrieve information, and navigate Interactive Voice Response units (IVRs) or attendants for large companies such as banks. Other telephone systems used by the military may leverage DTMF for override functions or other actions.

Within VoIP networks, DTMF tones are delivered either in-band or out-of-band via Real-time Transport Protocol (RTP) or Session Initiation Protocol (SIP) signaling messages. Delivery options include:

- *In-band* – DTMF tones are sent as normal audio tones in the RTP stream with no special coding or markers. Compression Codecs such as G.729 and G.723 may make tones unintelligible so it generally is used with codecs like G.711.
- *Out-of-band* – There are two methods for out-of-band DTMF. The more common method is to include the DTMF signals in special packets in the regular RTP stream as defined in the IETF RFC 2833 standard[1]. An alternative method is to send DTMF signals as a SIP INFO packet. The implementation of the SIP Info approach for DTMF has evolved in the industry without the constraints of definitive standards; hence, a number of variants are in commercial use.

A.4.1.1.2 Future State

Given the financial impacts to enterprises that have IVR services deployed, DTMF will continue to be a key capability for the PSTN in transition. As we move to the successor network, we expect that there will be a baseline communication device that may still utilize DTMF signaling.

However with advances in speech technology, the use of DTMF signaling will become less prevalent. Today speech technology is being adapted into web applications that enable what may become the new "voice" – web chat.

[1] < http://datatracker.ietf.org/doc/rfc2833/ >

A.4.1.1.3 Regulatory Implications

As set forth in the Telecommunications Act of 1996[2], DTMF signaling or its equivalent was defined as one of the services included in Universal Service.

A.4.1.1.4 Standards Implications

The IETF RFC 4733[3] describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets. It supersedes RFC 2833.

With regard to the SIP INFO approach to DTMF, while this is a recognized approach, it is not fully standardized in the same way as the RTP approach in RFC 2833/RFC 4733. The big challenge with SIP INFO is understanding the context with which the information contained in the SIP INFO message has been sent. The *SIP INFO Method* (RFC 2976) was superseded by *Session Initiation Protocol (SIP) INFO Method and Package Framework* (RFC 6086), which creates a framework for registering "packages" with Internet Assigned Numbers Authority (IANA) to help remove the ambiguity and enable applications to understand the context in which SIP INFO is being used.

A.4.1.2 Emergency Services

A.4.1.2.1 Definition of Current State

Emergency Services are the citizen-to-authority communications that supports the ability of the citizen to request assistance from emergency services such as fire, police, and emergency medical services (EMS). Emergency Services are also commonly called 9-1-1 services.

When the citizen requires emergency services, they can dial 911 on their wired or wireless phone to place a voice call to the Public Safety Answering Point (PSAP) for their current location. When the citizen dials 911, the telecommunications network determines the location of the citizen and uses that location to determine which PSAP should receive the emergency call.

For wired devices, the location is determined from a database of the telephone's location that was populated by the telecommunication service provider when the service was activated.

For wireless devices, the determination of the citizen's location cannot be pre-provisioned and has to be determined. The initial location information that is available for the wireless device is the location of the cell tower that is serving the mobile device. The appropriate PSAP is selected based upon the location of the serving cell site and the wireless 911 emergency call is routed to that PSAP. If the PSAP call taker requires a more accurate location of the emergency caller, the PSAP call taker can perform a rebid function to request more accurate location information. When the wireless telecommunications service provider receives the rebid request from the PSAP call taker, the wireless telecommunications service provider will initiate various location determination techniques. The specific location determination technique to be used is dependent on the wireless technology and network configuration of the telecommunications service provider. There are FCC regulations which specify the location accuracy requirements and which specify the maximum time for determination of the mobile device's location.

The above description is for voice-based emergency services. For individuals with disabilities, the following services are available:

- *Telecommunications Relay Services (TRS)* – See Appendix A, Section A.4.4.2.
- *Video Relay Service (VRS)* – See Appendix A, Section A.4.4.3.
- *IP Relay Service* – See Appendix A, Section A.4.4.4.

---

[2] < http://law.justia.com/cfr/title47/47-3.0.1.1.6.2.html >

[3] IETF documents are available from the Internet Engineering Task Force (IETF).
< http://www.ietf.org >

A.4.1.2.2 Future State

The Next Generation 9-1-1 services are based upon an IP-based network architecture, called Emergency Service IP Network (ESInet), and have been defined by the National Emergency Number Association (NENA). The ESInet will support voice and multimedia emergency communications to PSAPs and other emergency services.

Determination of the location of the citizen who requires emergency services is critical to providing a rapid and effective response by the first responders. In the PSTN wireline environment, the location of the wired telephone is known and is available to the first responders. In the PSTN successor network, the location of any cabled or wired devices must be known and available to the first responders. Location determination must be supported for VoIP services provided by telecommunications service providers and by OTT services.

For wireless handsets, the automated determination of the citizen's location could be difficult or not possible for some environments such as indoor conditions. The FCC CSRIC Working Group 3 is evaluating alternatives and developing recommendations to the FCC for location determination outdoors and indoors, as well as the feasibility of commercial location determination methodologies for use in emergency services. The FCC TAC should defer any recommendations for wireless handset location determination for emergency services to the FCC CSRIC Working Group 3.

A.4.1.2.3 Regulatory Implications

Existing FCC regulations address voice-based emergency calls for cable, wired, and wireless technologies.

Individuals with disabilities want direct text-based communications with emergency services from their mobile phones. The FCC Emergency Access Advisory Committee (EAAC)[4], which was established as part of the "Twenty-First Century Communications and Video Accessibility Act of 2010"[5] is currently developing recommendations for the FCC on the support of text communications with emergency services. The recommendations being developed by the FCC EAAC will be applicable to the general public as well as to individuals with disabilities.

The FCC CSRIC III Working Group 3 has been tasked with evaluating location accuracy for wireless emergency calls. CSRIC III Working Group 3 is responding to a series of location accuracy questions posed by the FCC and will be generating three reports. The first report is on outdoor location accuracy for emergency calls, the second report is on indoor location accuracy for emergency calls, and the third report is an evaluation and feasibility of leveraging location determination methodologies of commercial Location Based Services (LBS) for emergency services.

A.4.1.2.4 Standards Implications

NENA continues to develop standards for additional capabilities for the ESInet.

The next generation IP-based communications network defined in 3GPP is based upon the IP Multimedia Subsystem (IMS). A standards development effort is currently underway in ATIS to define the interconnection standards between the IMS-based networks and the ESInet. Additionally, ATIS is developing standards for OTT applications to obtain mobile device location information so that the OTT applications can initiate emergency sessions to the ESInet.

The IETF has defined a set of RFC specifications for the support of emergency communications in the Internet-based, non-IMS-based environment. Some of the specifications developed by the IETF include the LoST protocol in RFC 5222, the HELD protocol in RFC 5985, and Phone BCP in RFC 6443.

---

[4] < http://www.fcc.gov/encyclopedia/emergency-access-advisory-committee-eaac >

[5] < http://www.govtrack.us/congress/bills/111/s3304 >

A.4.1.2.5 Recommendations

- Support for voice-based emergency services must remain in the successor network and there are no known modifications to FCC regulations required.
- The FCC TAC should defer any recommendations regarding text-based communications with emergency services to the FCC EAAC.
- The FCC TAC should defer any recommendations about location accuracy for wireless emergency calls to the FCC CSRIC III and its associated reports.
- The FCC TAC recommends that the FCC evaluate and develop appropriate regulations for the support of emergency services by OTT communications services.

A.4.1.3 Lawful Intercept

A.4.1.3.1 Definition of Current State

Lawful Intercept (LI) is obtaining communications network data pursuant to a court order for the purpose of analysis or evidence. Such data generally consist of signaling or network management information or the content of the communications. Lawful Intercept is also known as wiretapping.

The wiretapping law in the United States is the “Communications Assistance for Law Enforcement Act” (CALEA) which as enacted in 1994. CALEA's purpose is to enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, allowing federal agencies to monitor all telephone, broadband internet, and VoIP traffic in real-time. CALEA has been expanded to include all VoIP and broadband Internet traffic.

A.4.1.3.2 Future State

As communication capabilities and options for the consumer expand with the next generation networks, the Lawful Intercept capabilities will also expand to incorporate these additional capabilities and options. The Lawful Intercept capabilities will continue to cover wired, cabled, and wireless communications options. The PSTN successor network will need to support Lawful Intercept capabilities for all supported communications technologies.

A.4.1.3.3 Regulatory Implications

The existing FCC regulations covered the requirements of CALEA and also define the reporting requirements for the telecommunications service providers and telecommunication equipment manufacturers. Information about the FCC regulations is available at < http://transition.fcc.gov/calea/ >.

A.4.1.3.4 Standards Implications

Standards have been developed by CableLabs®, ATIS, and 3GPP. Some of these standards are designated as “safe harbors”. The “safe harbor” designation means that if a cable operator or telecommunications service provider is compliant with the designated “safe harbor” standards associated with their technology, then the cable operator or telecommunications service providers is deemed to be CALEA compliant.

For a complete list of standards that the FBI feels are important (including WiMax, cable, wireline, and wireless cellular), see < http://askcalea.net/standards.html >. This contains a comprehensive listing of potential safe harbor standards from multiple industry standards bodies and other fora.

The latest CableLabs standard for Lawful Intercept is the CableLabs Cable Broadband Intercept Specification (CBIS). CBIS is designated as a “safe harbor” standard under CALEA.

The ATIS “safe harbor” standards under CALEA are as follows:

- ATIS-1000678.2006, *LAES for Voice over Packet Technologies in Wireline Telecommunications Networks*.[6]
    - ATIS-1000678.a.2007, *Supplement*.
    - ATIS-1000678.b.2010, *Supplement*.
- ATIS-1000013.2007, *LAES for Internet Access & Services*.
    - ATIS-1000013.a.2009, *Supplement*.
- J-STD-025: *Lawfully Authorized Electronic Surveillance* (covers mainly circuit-switched wireline and wireless), first published in 4Q97. Note that this spec (and its subsequent revisions and addenda) is a joint spec between TIA and ATIS, with TIA as the lead Standards Development Organization (SDO).
    - J-STD-025-A: *Lawfully Authorized Electronic Surveillance* (covers mainly circuit-switched wireline and wireless, and added support for FCC report and order decisions regarding FBI punchlist items), published April 2003.
    - J-STD-025-B: *Lawfully Authorized Electronic Surveillance* (added cdma2000 packet data support plus references to 3GPP specs for GSM/UMTS packet data support), published July 2006.
        - J-STD-025-B-1 (Addendum), *Lawfully Authorized Electronic Surveillance Addendum 1, Addition of Mobile Equipment IDentifier (MEID)*.
        - J-STD-025-B-2 (Addendum), *Lawfully Authorized Electronic Surveillance Addendum 2, Support for Carrier Identity*.

The following are the international lawful intercept standards being developed in 3GPP:

- 3GPP TS 33.106, *Lawful Interception*[7].
- 3GPP TS 33.107, *Lawful Interception Architecture and Functions*.
- 3GPP TS 33.108: *Handover Interface for Lawful Interception*.

Standardization work continues on Lawful Intercept specifications for international alignment purposes, to support additional communications options, and to support additional capabilities requested by Law Enforcement. The ongoing standardization work for Lawful Intercept needs to include support for the additional communications methods of the PSTN successor network and the support for surveillance within an environment of dynamic identification (e.g., obtaining a new identifier or account for each communication session).

A.4.1.3.5 Recommendations

There are no recommendations for modifications to the existing FCC regulations for lawful intercept services.

[6] ATIS documents are available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005. < https://www.atis.org/docstore/default.aspx >

[7] 3GPP documents are available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

A.4.1.4 Priority Services

A.4.1.4.1 Definition of Current State

Priority services for National Security and Emergency Preparedness (NS/EP) personnel are essential in order to provide telecommunications services to NS/EP personnel during times of network congestion and network degradation due to widespread disasters (e.g., earthquakes, hurricanes).

The Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS) are White House-directed emergency phone services provided by the Department of Homeland Security Office of Emergency Communications (DHS OEC). GETS provides emergency access and priority processing in the local and long distance segments of the PSTN. GETS is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.

During emergencies, cellular networks can experience congestion due to increased call volumes and/or damage to network facilities, severely curtailing the ability of NS/EP personnel to make emergency calls. With an increasing number of NS/EP personnel relying on cell phones while performing their emergency duties, the NCS developed WPS to provide priority for emergency calls made from cellular telephones.

WPS does not pre-empt any existing communications. Instead, WPS will place the NS/EP users at the top of the queue for the next available radio channel. To have full end-to-end priority service, the NS/EP dial into the GETS network access numbers with an additional prefix of *272 to indicate WPS is also requested.

NS/EP personnel must request enrollment in GETS and WPS via the DHS OEC:
< http://www.dhs.gov/about-office-emergency-communications >.

A.4.1.4.2 Future State

As the PSTN and wireless networks evolve into IP-based next generation systems, the GETS service and WPS service must also evolve to support the IP-based connectivity and to support multimedia-based communications for both voice and data.

The evolution of GETS and WPS is referred to as NGN GETS. The DHS OEC Industry Requirements are in development for deployment of this service in broadband networks (wireless and fixed).

A.4.1.4.3 Regulatory Implications

GETS is managed by the DHS OEC and not regulated by the FCC.

WPS is also managed by the DHS OEC and the FCC has specified regulations about the behavior of the WPS services on the Commercial Mobile Radio Service (CMRS) systems.

A.4.1.4.4 Standards Implications

ATIS has developed and continues to develop several standards for the Emergency Telecommunication Service (ETS). For example, the ATIS specification ATIS-1000005, *Service Description of ETS*, provides a service description of ETS. ETS supports priority connectivity for any authorized user from any originating point in the public network and to any destination point in the public network across multiple networks types (e.g., circuit-switched networks, wireless network/mobile radio access, cable satellite, or packet-based multi-media networks). The following ETS documents have been produced or are work in progress in the ATIS PTSC:

Table A.1- ETS Documents Produced or in Progress in the ATIS PTSC

Support of ETS in IP Networks	ATIS-1000010.2006
ETS Phase 1 Network Element Requirements	ATIS-1000023.2008
Supplement to ATIS-1000023-2008, ETS Phase 1 Network Element Requirements	ATIS-1000023.a.2010
ETS Packet Priority for IP NNI Interfaces - Requirements for a Separate Expedited Forwarding Mechanism	ATIS-1000020
Packet Priority & Priority Call Processing	ATIS-1000011
ETS Core Network Security Requirements	PTSC-SAC-2012-008R1[8]
ETS Wireline Access Requirements	PTSC-SAC-2012-010R2
NGN GETS (ETS) End-to-End Call Flows	ATIS-1000049
ETS Network Element Requirements Phase II	PTSC-SAC-2012-032
Service Requirements for ETS	No baseline
ETS Roadmap	PTSC-SAC-2012-098
ETS EPC Network Element Requirements	No baseline

3GPP is defining the standards for the enhanced Multimedia Priority Service (eMPS). For example, 3GPP TS 22.153, *Multimedia Priority Services*, defines the service requirements for eMPS. The scope of this document is to specify those requirements of eMPS necessary to provide an end-to-end service and to interwork with external networks where needed. The relevant CT 1, 3 & 4 stage 2 and 3 documents have been updated to eMPS.

A.4.1.4.5 Recommendations

There are no recommendations for modifications to the existing FCC regulations for priority services.

A.4.1.5 Malicious Call Trace

A.4.1.5.1 Definition of Current State

The Malicious Call Trace supplementary service is a terminating call feature that allows the receiver of an obscene, harassing, or threatening call to request that a record of the last incoming call be generated and provided to the Local Exchange Carrier (LEC) and, potentially, to an authorized law enforcement agency. Also called Customer-Originated Trace (COT), this feature adds the capability of the offended party to invoke the trace using a feature activation code. After the offended party invokes the call trace procedure, information collected includes the calling number (even if privacy is set against the calling party), the called number, the time and date of call, the duration of the call, and whether the calling number is set to private. The information collected is not forwarded to the offended party, but is handled according to the best practices of the service provider, including being forwarded to law enforcement authorities where appropriate.

After receiving and ending the malicious call, the COT customer activates the feature by dialing the call trace activation code (usually *57) or pressing a special key on their phone. The COT customer needs to activate the feature immediately after receiving the offending call, and prior to accepting a new call. COT can be activated during the offending call or after the offending call, as long as the offended customer has not received or made another call. The only information that the offended customer will receive after initiation is a tone indicating whether or not the call trace was successful. Once the trace is completed

[8] This reference is a committee contribution. PTSC committee participants can access this document at < http://contributions.atis.org >. Copies of this contribution will be made available to all other interested parties upon request. Such request should be made to the ATIS Document Center Administrator at < doccenter@atis.org >.

successfully, a tone or "Trace successful" announcement is provided. A different tone or announcement is provided if the trace is unsuccessful.

Today, this capability requires that both the originating and terminating central offices be interconnected by Signaling System #7 (SS7).

In IP-based cable deployments where a subscriber has multiple pieces user equipment (UE) registered using the same public identity, and the COT feature is invoked from one of these UEs, the call that is traced is the last call answered and ended from any UE registered to the public identity from which the COT feature was invoked.

In IMS, the Malicious Communication Identification (MCID) service provides the capability of storing the session-related information of incoming communications independent of service requested. It allows the service provider to trace the identity information of the source of an incoming communication at the request of the called user. As with the COT service, the communication information is not available to the called user or originating user. The communication information is stored under the control of the network operator. MCID may be a network subscription option where MCID is automatically invoked for a specified user or as a user subscription option where MCID may be invoked during the active phase of the communication session or for a limited time after connection termination.

A.4.1.5.2 Future State

As we move to the successor network, users must continue to have the ability to activate call tracing for malicious voice communications leveraging either the E.164 or SIP URI identity carried in signaling for session establishment. As additional real time communication capabilities are enabled by IP networks, it is expected that call tracing may be extended (i.e., Malicious Communications Tracing) to enable tracing for malicious instant messaging, video calls, content sharing, etc. To enable the MCID service when interworking across networks, both networks need to be within the same trust domain for identity information transfer.

A.4.1.5.3 Regulatory Implications

Currently the procedures by which Malicious Call Trace is administered are determined by each state's Public Utility Commission (PUC). While today's public service communications are defined as voice, a broad range of alternate communication services are emerging: video, chat/IM, file sharing, etc. Tracing capabilities for malicious communications are important to protect the use of public communications services. If any of these additional forms of communications are identified and characterized as base public communication services, then it is expected that Malicious Communications Tracing will also be supported for those forms of communication. It is also expected that Communication Service Providers have the duty of care to self-police and report malicious abuse.

A.4.1.5.4 Standards Implications

The Call tracing functionality is defined for IP networks by the following standards:

- PacketCable™ Residential SIP Telephony Feature Definition Technical Report PKT-TR-RST-V03-071106[9] based on service definition defined in GR-216 LSSGR: CLASS[SM] Feature: Customer Originated Trace, FSD 01-02-1052 (A Module of LSSGR, FR-64), Issue 2, April 2002G.[10]

[9] < http://www.cablelabs.com/packetcable/specifications/packetcableapps.html >

[10] Telcordia documents are available from Telcordia, 1 Ericsson Drive, RRC 1B-180, Piscataway, NJ 08854-4157 or < http://telecom-info.telcordia.com >.

- Malicious Communication Identification (MCID) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.616 version 10.0.0 Release 10).[11]

Communications tracing capability depends upon reliable identity information and the ability to store session information for incoming communications. The current standards define both the trigger mechanism to activate tracing as well as the information capture required.

A.4.1.6 Portability

A.4.1.6.1 Definition of Current State

The Telecommunications Act of 1996 defined number portability as "the ability of users of telecommunications services to retain, at the same location, existing telecommunications numbers without impairment of quality, reliability, or convenience when switching from one telecommunications carrier to another."

In mandating the implementation of number portability, the FCC adopted the following eight minimum criteria to serve as requirements for any long-term number portability method:

(1) Support existing network services, features, and capabilities.

(2) Efficiently use numbering resources.

(3) Not require end users to change their telecommunications numbers.

(4) Not result in unreasonable degradation in service quality or network reliability when implemented.

(5) Not result in any degradation of service quality or network reliability when customers switch carriers.

(6) Not result in a carrier having a proprietary interest in any long-term method.

(7) Be able to accommodate location and service portability in the future.

(8) Have no significant adverse impact outside the areas where number portability is deployed.

In compliance with the FCC's number portability mandate and the eight required minimum criteria outlined above, the industry implemented a long-term method called Location Routing Number (LRN) in the PSTN.

An LRN is a 10-digit number, in the form of an E.164 telephone number (NPA-NXX-XXXX), that uniquely identifies the PSTN switch to which a customer's number has been ported and the carrier that serves that ported customer. LRN technology was designed to enable the PSTN network to continue to route on the first six digits (NPA-NXX) of an E.164 number (the LRN), as opposed to the first six digits of the dialed number, in the case of a call to a ported telephone number. Database queries on virtually every originating call in the PSTN determine if the call is to a ported number and, if so, to obtain the LRN of the serving PSTN switch for proper call routing and call completion.

A.4.1.6.2 Future State

During the transition from legacy PSTN to the successor network, E.164 telephone numbers will continue to be assigned to and associated with subscribers both in the legacy PSTN and with subscribers served by Interconnected VoIP providers in order to continue to enable call routing and completion across both networks and to both universes of subscribers.

[11] ETSI documents are available from the European Telecommunications Standards Institute (ETSI).
< http://www.etsi.org/getastandard/home.htm >

Also during the transition, LRN routing will continue in the PSTN on calls destined to those ported subscribers still served in the PSTN and destined to those served by an Interconnected VoIP provider. This is currently in place today as end users continue to migrate from the legacy PSTN to an IP network.

Number Portability, or perhaps better referred to as customer name portability depending on the end user naming scheme utilized, will in all likelihood be an expectation of consumers and a requirement of regulators in the fully transitioned successor network.

E.164 numbers, and possibly LRNs, can still have relevance in a fully transitioned successor network as SIP addressing can support both; however, the customer-facing and network addressing scheme that is deployed will determine if that will be the case.

In addition, whether rate centers and Local Access & Transport Areas (LATAs) remain or are eliminated in the successor network could have an influence on determining portability boundaries and call routing. For instance, in today's legacy PSTN, the boundary of number portability is considered to be the rate center boundary. Numbers are not ported across LATA boundaries due to legacy PSTN switch limitations that impact the ability to route the call. In addition, numbers are used as proxies for geographic jurisdiction for intercarrier compensation. Although Interconnected VoIP providers today offer their end users the ability to retain or obtain telephone numbers that are associated with a LATA that is different than their physical location, calls to those numbers that originate in the PSTN must still be delivered to the LATA that is associated with the dialed telephone number and then back-hauled to the end user's physical location, wherever that is, by the VoIP provider.

A.4.1.6.3 Regulatory Implications

FCC Order 07-188[12] further obligated Interconnected VoIP providers to comply with all rules and requirements pertaining to number portability.

FCC Orders 09-41[13] and 10-85[14] mandated next-day porting for simple ports.

A.4.1.6.4 Standards Implications

Portability standards could be influenced by the results of the areas for further study recommended in section A.4.1.6.5 below.

A.4.1.6.5 Recommendations

Areas for further study include:

- Portability functionality in general and specifically, portability boundaries, as well as the role of network elements, and number or address resource optimization related to any elimination of rate centers and LATAs.
- Portability functionality for customer-facing addresses, whether they are E.164 numbers (and their associated LRNs) or something else.
- Evolution and architecture of industry and carrier databases for portability in the successor network – e.g., can the ENUM hierarchical registry architecture support Number Portability in the U.S. in the successor network, and if so, how?

[12] < http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-188A1.pdf >

[13] < https://prodnet.www.neca.org/wawatch/wwpdf/fcc0941.pdf >

[14] < http://www.fcc.gov/document/local-number-portability-lnp-porting-interval-and-validation-requirements-telephone-number- >

A.4.2 Advanced Communication Services

A.4.2.1 CLASS[SM] Features

A.4.2.1.1 Definition of Current State

Customized Local Area Signaling Service (CLASS) features provide Custom Calling services, and are generally based on the transport of the Calling Party Number (CPN). Most of the CLASS features do not require the use of specialized CPE. The CLASS Calling Identity Delivery (CID) services that do require some form of specialized CPE are:

- Calling Number Delivery (CND);
- Calling Name Delivery (CNAM);
- Calling Identity Delivery on Call Waiting (CIDCW);
- Call Waiting Deluxe (CWD); and
- Bulk Calling Line Identification (BCLID).

The interface between the switch and the customer's CPE display device is described in GR-30-CORE, *Voiceband Data Transmission Interface Generic Requirements.*

CLASS features have been used by residence and small-business customers since 1987. The availability of the features varies among LECs. Some of the features, such as Automatic Callback (AC), require the customer to dial a vertical service code (for AC, the code is *66). Other CLASS features, such as the CID features, do not require any special dialing by the customer. Vertical service codes are administered by the North American Numbering Plan (NANP). CLASS features are available on a pay-per-use as well as a subscription basis.

The CLASS features are listed in alphabetical order and their respective Generic Requirements documents.

Table A.2 - CLASS Features and Generic Requirements Documents

CLASS Features	Generic Requirements Documents
• *Anonymous Call Rejection (ACR)*	Telcordia Technologies GR-567-CORE[2]
• *Automatic Callback (AC)*	GR-215-CORE
• *Automatic Recall (AR)*	GR-227-CORE
• *Bulk Calling Line Identification (BCLID)*	GR-32-CORE
• *Call Waiting Deluxe (CWD)*	GR-416-CORE
• *Calling Identity Delivery Blocking (CIDB)*	GR-391-CORE
• *Calling Identity Delivery On Call Waiting (CIDCW)*	GR-575- CORE
• *Calling Name Delivery (CNAM)*	GR-1188-CORE
• *Calling Number Delivery (CND)*	GR-31-CORE
• *Customer Originated Trace (COT)*	GR-216-CORE
• *Distinctive Ringing/Call Waiting (DRCW)*	GR-219-CORE
• *Numbering Plan Area Split Management*	GR-1251-CORE
• *Screening List Editing (SLE)*	GR-220-CORE
• *Selective Call Acceptance (SCA)*	TA-TSY-001034[15]
• *Selective Call Forwarding (SCF)*	GR-217-CORE
• *Selective Call Rejection (SCR)*	GR-218-CORE
• *Visual Message Waiting Indicator (VMWI)*	GR-1401-CORE
• *Visual Screening List Editing (VSLE)*	GR-1436-CORE

[15] < https://telecom-info.telcordia.com/site-cgi/ido/docs.cgi?ID=D000833&KEYWORDS=Operations%20Technology%20Generic%20Requirements%20OTGR&TITLE=&DOCUMENT=&DATE=&CLASS=PS41&COUNT=1000 >

CLASS feature interactions between the subscriber and the network are facilitated by one or more of the following:

- DTMF signaling.
- Voice activated control and recognition of human speech.
- Screen display of visual menus and soft-keys (specialized CPE).

CLASS features are deployed by almost all service providers in the United States and Canada on the CCS SS7 network. These features are popular among subscribers; some have reached 70% penetration rates in various areas. Subscription and usage fees constitute a significant source of revenue for all types of service providers.

A.4.2.1.1.1 Caller Identification Services

Caller identification services include:

- *Caller ID* – Allows a subscriber to identify a caller before answering an incoming call. The caller's number is displayed on the phone (if the phone has display capability). It is also possible to buy an external display unit, and some telecom and cable operators that provide phone service offer widgets that allow display of the caller ID on the TV, PC, and tablet.
- *Caller ID with Name* – Provides the name identification of the calling party (e.g., personal name, company name, "restricted", "not available") to the called subscriber. Unlike the CPN, the originating provider does not transmit the name associated with the CPN. Instead, the terminating provider offering the Caller ID service uses the CPN to retrieve the name associated with the CPN from a Caller Name (CNAM) database. CNAM databases link CPNs to the individuals and entities to which the numbers have been assigned. Some terminating providers maintain their own CNAM database, and others purchase CNAM database services from third-party providers that aggregate the listing information from a variety of sources.
- *Caller ID Block* – Prevents display of the name and telephone number identification of the calling party on the Caller ID equipment of the called party. A subscriber can activate Caller ID Block on a per-call basis for one call only or permanently for all calls.
- *Call Waiting ID* – Works in conjunction with Caller ID and presents the caller number and name with the call waiting notification.

Signaling System 7 (SS7) signaling is used to transmit the calling party number (CPN) associated with all PSTN Traffic in the SS7 ISUP (ISDN User Part) CPN field. Multi-frequency (MF) signaling is also used to transmit CPN, or CN if it differs from CPN, associated with all PSTN Traffic in the MF signaling automatic numbering information (ANI) field. When a carrier uses SS7 to set up a call, it must transmit CPN and its associated privacy indicator for that call to connecting carriers and the terminating carrier must act in accordance with the privacy indicator.

A.4.2.1.2 Future State

Continuing to offer the same capabilities in the IP network will depend on the market demand and technical feasibility of these features. Recognizing that Caller ID-based features benefit both enterprise and end users alike, SIP vendors have started emulating some of the more popular features – a selection of the Caller ID family of services – in their products. SIP support for Caller ID facilitates a smooth transition to packet-switched VoIP services. At this time, Caller ID, Calling Name, and Call Forwarding appear to be the features receiving more attention and support in SIP. However, no formal specifications are available.

IETF holds that SIP is designed such that implementations of the standard protocol are interoperable. Protocol translation is not recommended. SIP extensions are expected to be individually negotiated during a given session.

An example extension is RFC 3325, *the Network Asserted Identity and Trust Domain*. This RFC provides a network-asserted identity service using a very limited, simple mechanism, and relies on a new header field called “P-Asserted-Identity”. However, that mechanism is only applicable inside a “Trust Domain”. In other words, it does *not* offer a general privacy or identity model suitable for inter-domain use or use in the Internet at large – unlike privacy implementation in the PSTN.

RFC 3323 describes further Privacy Mechanisms for SIP, whereby a user can request a “privacy service”. The functions listed in the RFC attempt alignment with the privacy guidelines in the PSTN by creating levels or tokens of privacy. However, providing privacy in a SIP network is more complicated than in the PSTN because the IP address in itself may reveal private information. Furthermore, without encryption in an IP network, more information could be obtained, violating the originator’s privacy. Therefore, a key capability required going forward is for the service provider to support the ability for a subscriber to conceal their identity. With IP-based networks this would encompass both the user-identity and IP addresses. A user must be able to enable user-identity blocking or prevent presentation on a per call/session basis.

In the legacy world, the network supplied the Caller ID. With SIP, identity management is conveyed in a number of SIP headers:

- *P-Preferred-Identity header field* – Identity which the user would like to use.
- *P-Asserted-Identity header field* – Network derived identity of the user.
- *Privacy header field* – Users privacy preferences.
- *From header field* – Source routing information.

The common IMS caller identification services include:

- *Originating Identification Presentation (OIP)* – Provides the terminating user with the possibility of receiving network-provided identity information in order to identify the originating user. In addition to the trusted identity information, the identity information from the originating user can include identity information generated by the originating user, and – in general – transparently transported by the network. In the case where the originating user provides no identity information, the network shall include identity information based on the default public user identity associated with the originating user.
- *Originating Identification Restriction (OIR)* – Enables the originating user to prevent presentation of its identity information to the terminating user and is a service offered to the originating user. If the presentation of the public user identity is restricted, then the terminating user shall receive an indication that the public user identity was not sent because of restriction.
- *Terminating Identification Presentation (TIP)* – Provides the originating party with the possibility of receiving identity information in order to identify the terminating party.
- *Terminating Identification Restriction (TIR)* – Service offered to the connected party which enables the connected party to prevent presentation of the terminating identity information to originating party.

Caller identification service interworking between existing PSTN-based and new IP-based networks (SIP/IMS) is supported through protocol mapping between ISUP and SIP Calling Line identification parameters. Caller ID services can be further enhanced once offered on all IP networks. For example, delivery of a photo of the caller as well as the session description can be easily implemented. Caller ID services could also be supplemented with voice biometrics where the display name would appear, and when the voice call is answered and the calling party speaks, a positive identification could be made.

As we look to advanced multimedia communications (Instant Messaging, voice chat, etc.), it is possible to also provide user identity blocking as an optional capability.

To ensure seamless transition to the IP versions of CLASS, equivalent analysis and guidelines are recommended. ATIS could potentially collaborate with other bodies, such as IETF, on the definition of more SIP extensions to achieve a more comprehensive and interoperable set of IP Consumer Services.

The work should take into account the functions that could be carried out more efficiently by devices rather than network entities (e.g., Visual Voicemail display and Selective List Editing features).

A.4.2.1.3 Regulatory Implications

The introduction of CND caused considerable controversy at both the state and federal levels. Commissions struggled with privacy issues and potential personal risk issues associated with revealing the calling number to the called party. Some groups and social services providers asserted that actual physical risk could occur to clients and staff if calling numbers were permitted to be displayed. In some states, law enforcement raised concerns about undercover operations. The FCC expanded the CND regulatory concerns from the state to the federal level in October of 1991 when it issued a Notice of Proposed Rulemaking (NPRM) – CC Docket 91-281 – "Rules and Policies Regarding Calling Number Identification Service"[16]. The FCC supported the range of capabilities and services enabled by the SS7 infrastructure and CND in particular.

The FCC's initial ruling on 91-281 (released in March, 1994) emphasized the importance of CPN availability for the range of CLASS services, including CND. Because CPN was necessary for other important new services, the 1994 order facilitated CPN transport by requiring that all capable carriers transport CPN without any additional consideration or compensation. For callers who wished to preserve their anonymity, the order further mandated what came to be known as "per-call blocking" by use of *67 as the only method for implementing presentation restriction. Subsequent orders mandated that *82 must be provided so that CPN can be "unblocked" on a call-by-call basis. Carriers are required to forward the blocking/unblocking information without modification, and terminating carriers must abide by the instructions of the caller regarding availability of number and name. In the 1995 order, the FCC ruled that name should be treated the same as number. That is, if number is blocked, name should also be blocked. If number is permitted, name should also be permitted. Further, the order recognized that Automatic Recall (AR) had the potential to reveal identifying information, so the order concluded that if the calling number was blocked, AR to the calling number should be prevented as well. Exceptions to the rules are 800/900 services, since the called party is paying for the call.

Additionally, if calling customers cannot be provided blocking/unblocking options, those networks are precluded from providing CPN *at all*. In such cases, CPN would not be available at the terminating office for any services (CND or other CLASS features).

In addition to privacy issues, Caller ID services have recently become the subject of further regulation in response to malicious caller ID spoofing. Congress passed and President Obama signed into law the Truth in Caller ID Act[17], which prohibited caller ID spoofing with harmful or fraudulent intent and directed the FCC to adopt rules implementing the Act.

Under the FCC's new rules:

- Violators are subject to up to $10,000 for each violation, or three times that amount for each day of continuing violation, to a maximum of $1 million for any continuing violation.
- The FCC may assess fines against entities it does not traditionally regulate without first issuing a citation.
- The FCC can impose penalties more readily than it can under other provisions of the
- Communications Act.

Under the Act, callers are still permitted to alter caller ID information if their purposes are not harmful or fraudulent. For example, domestic violence shelters may have important reasons for not revealing the actual number of the shelter, and doctors responding to after-hours messages from patients may choose to transmit their office numbers rather than their cell phone numbers.

In transitioning to SIP signaling, there are several unanswered questions that require guidance and clarification from the FCC, including:

---

[16] < http://epic.org/privacy/caller_id/fcc_final.html >

[17] < http://www.gpo.gov/fdsys/pkg/BILLS-111s30enr/pdf/BILLS-111s30enr.pdf >

- Do the privacy rules of 91-281 apply to CND and CNAM in the new IP network?

While the logical answer is "yes", the details of implementation require ubiquitous adoption in IP-based networks. SIP and other VoIP protocols must implement equivalent capabilities to:

  - Allow the session initiator (caller) to block their information.
  - Require IP network providers to abide by similar rules about relaying blocking information from end to end.
  - Develop the capabilities necessary in the proxy servers to enforce privacy policies for both name and number delivery.

- If not, will the obligations of the PSTN carriers regarding privacy be removed? Otherwise, how will consumers reconcile the different flavors and expectations between networks?
- Spoofing Caller ID is much more feasible in an all IP network. Will the FCC simply rely on the penalties connected to the "Truth in Caller ID Act" to be a sufficient deterrent or should they seek a more proactive role from the IP providers in: (1) verifying the outgoing CID data; and (2) preserving it across intermediate networks?

A.4.2.1.4 Standards Implications

In addition to the privacy issues discussed above for caller identity-based features, there is a need to outline at least a use case for each of the CLASS services and clearly define:

- Standard SIP functions that could be relied on for deploying the service.
- Applicable Extensions for each service.
- Example implementations providing insight into functionality that may be carried out by end devices in the IP network.

Specifications for future network implementations include:

- ITU-T Q.1912.5,[18] which defines the interworking between the Bearer Independent Call Control (BICC) or ISDN User Part (ISUP) protocols and SIP in order to support services that can be commonly supported by BICC or ISUP and SIP-based network domains.
- *RFC 3261 SIP, Session Initiation Protocol*.
- ATIS-1000051, *TCAP Gateway Functionality*, addresses the complementary interworking between SS7 TCAP and IP for the purposes of remote operations application-level messaging.
- ATIS-1000047, *Signaling System 7 (SS7) and Internet Protocol (IP) Transport Networks Signaling Interworking and Compatibility*, provides requirements and guidelines for signaling interworking and compatibility between traditional SS7 transport networks and IP-based transport networks.
- RFC 5876, *Updates to Asserted Identity in the Session Initiation Protocol* (SIP).
- RFC 3966, *The tel URI for Telephone Numbers*.
- RFC 3323, *A Privacy Mechanism for the Session Initiation Protocol (SIP)*.
- The 3GPP TS 24.607 V10.0.0 technical specification defines the Originating Identification Presentation (OIP) supplementary service and the Originating Identification Restriction (OIR) supplementary services, based on the ISDN CLIP and CLIR supplementary service. It provides the protocol details in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP) and the Session Description Protocol (SDP).

[18] ITU-T Recommendations are available from the International Telecommunications Union.
< http://www.itu.int/ITU-T/ >

- The 3GPP TS 24.608 V10.0.0 technical specification defines Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) services, based on the ISDN COLP and COLR supplementary services. It provides the protocol details in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP) and the Session Description Protocol (SDP).

The issue of spoofing is recognized and there are standards defined which make illegitimate spoofing harder. With the advent of newer technologies like WebRTC for voice and video communications on the web, the IETF is currently discussing methods to guard against identity spoofing.

A.4.2.2 Database Services

A.4.2.2.1 Definition of Current State

Line Information Database (LIDB) is a distributed database system containing information associated with working telephone numbers. Each LIDB contains a unique set of line numbers and associated data attributes. Collectively, LIDBs contain information on nearly all working telephone numbers in North America including listed, unlisted, Centrex/Private Branch Exchange (PBX), non-published, landline, wireless, and VoIP numbers. LIDB is used to support fraud reduction, identity management, and communications-related services. LIDB resides as an application on network nodes with interfaces to CCS/SS7 and TCP/IP networks. LIDBs are owned and operated by telecom and non-telecom providers. LIDBs are geographically independent. Companies that do not own a LIDB can store their end user records in any LIDB of their choice; they decide which LIDB owner they prefer to do business with.

LIDB is not an online Directory. Access is limited to authorized clients. LIDB is a transaction-based database. A LIDB transaction consists of a query from a network system to the LIDB, followed by an appropriate response from the LIDB to the querying entity. Network systems that query the LIDB may include Hub providers, operator services systems (OSS), end offices (EOs), advanced intelligent network (AIN) service control points (SCPs), and other network elements such as wireless services platforms, media gateway controllers (MGCs), or application servers.

LIDB is accessed to support services such as CNAM. LIDB data is sourced directly from service providers and updated in near real-time, collectively containing more than 500 million records. Data is audited regularly to ensure its accuracy. The LIDB line record contains data elements/attributes associated with the 10-digit line number (NPA-NXX-XXXX). The following are a few examples of LIDB line-level attributes:

- Identification of the customer's service provider/carrier for branding and billing.
- Billing name and address to verify a customer or to reduce billing inaccuracies and fraud.
- Preferred language of the customer for providing customized service.
- The name of the customer and the name presentation status for privacy purposes.
- The type of service or equipment for the line number -- e.g., hospital, prison, business, residential, etc.
- Indication of how long the telephone number has been in service to verify a customer or to reduce billing fraud.
- Information indicating whether or not third party charges can be included on the end user's bill.

A complete list of LIDB data elements can be found in Section 21, LIDB Data Catalog, of GR-1158-CORE.

In recent years, LIDB has expanded its benefits to a wider base of clients, assisting them in the battle against Identity Theft. LIDB's reliable data has proven effective in analytics used to prevent online retail fraud and is poised to continue a similar role in the healthcare field.

In accessing LIDB, the role of a "Hub provider" primarily provides interoperability and routing services, factoring in all Number Portability and network traffic updates. Hub providers have established relations with the LIDB and Calling Name database providers. A LIDB client can choose a hub provider to simplify

connectivity and billing matters – one-stop shopping. A Hub provider also performs the necessary protocol conversion and transports the query to the appropriate LIDB.

In addition, LIDB's reliability and fault-tolerant architecture exceeds most commercial requirements. Integrating LIDB in the new network would significantly reduce CAPEX and OPEX and minimize customer impacts.

A.4.2.2.2 Future State

LIDBs were first introduced in the mid-1980s as a validation database for calling card, collect, and third number charged calls. Following that, LIDBs started supporting CLASS Calling Name/Caller ID feature, originating billing authorization, Single Number Service, GetData, service provider identification (SPID) in a post-LNP world, and more. LIDB has evolved in concert with a rapidly changing industry by offering data solutions in response to rising industry needs.

As a result, new data and capabilities were added to LIDB to meet those needs. Most significantly, IP interfaces to LIDB were introduced in the early 2000s. GR-3103-CORE, *Lightweight Directory Access Protocol (LDAP) Interface Specification for Line Information Database (LIDB)*, details the first steps toward migrating LIDB to IP-capable networks.

To expand and facilitate more diverse IP access to LIDB, hub providers perform a plethora of protocol translations making LIDB access virtually protocol-agnostic. Examples of protocols supported by most hub providers today include (but are not limited to):

- LDAP
- SIP
- Signaling Transport (SIGTRAN)
- XML

Therefore, there are no major technical hurdles anticipated for LIDB to become an integral part of the new IP network. LIDB is already a valuable resource in the Identity Management sphere. With the growing role of hub providers, LIDB has proven it is a viable member of the IP network and will continue to be.

Given that LIDB records correlate the data to an E.164 10-digit telephone number, it is expected that any changes to the format of telephone numbers would require major modifications to both LIDB and its Administrative System. The size of the impact could only be assessed at that point in the future, as the platform is in continuous evolution and it is difficult to predict the capabilities such platform will possess in 10, 15, or 25 years from now.

One of the outstanding issues in an all-IP environment is interconnection. This issue has not been resolved thus far and is expected to have far reaching impacts beyond LIDB. In the absence of a well-defined routing scheme, it is difficult to assess the precise impacts on LIDB query routing.

However, if we assume that the eventual routing mechanism(s) assign unique network identifiers (e.g., a URL or IP-address) and that interconnection between networks is ubiquitous (not limited to private peering), then query routing to LIDB would continue to function properly in the new network.

For queries destined to a given LIDB to be directed to the appropriate network, there will be a need for routing tables that associate and translate telephone numbers to network addresses (e.g., a DNS-like translation or an IP version of LERG/LARG tables, etc.) Once at the applicable network, the query traffic would be routed internally by the operator of that network to the appropriate database.

A.4.2.2.3 Regulatory Implications

LIDB data is regulated and is expected to continue to be so in an IP environment. The data is available for restricted use on a per transaction basis. LIDB data is not mined or accessed for marketing purposes

and is subject to Customer Proprietary Network Information (CPNI) rules (Section 222 of the Act)[19]. Assuming no changes to these rules, LIDB owners would continue to maintain consumer privacy, independent of the technology used to access that data.

A.4.2.2.4 Standards Implications

The early Calling Card services are described at a high level in ATIS-0300230.2010, *Telecommunications Charge Card and Billing Number Screening Validation Message Components*, (2010).

Greater detail of the LIDB capabilities and related systems are specified in key generic requirements documents, mainly:

1. GR-1158-CORE, *OSSGR Section 22.3: Line Information Database (a module of OSSGR, FR-271), Issue 9*, April 2009.
2. GR-3103-CORE, *Lightweight Directory Access Protocol (LDAP) Interface Specification for Line Information Database (LIDB)*, April 2009.
3. GR-1188-CORE, *CLASS^{SM} Calling Name Delivery Generic Requirements (a module of LSSGR, FR-64), Issue 3*, April 2009.
4. GR-1149-CORE, *OSSGR Section 10: System Interfaces (a module of OSSGR, FR-271), Issue 7*, December 2008.
5. GR-2838-CORE, *Generic Requirements for GetData, Issue 6*, December 2008.
6. GR-446-CORE, *Generic Requirements for the Line Information Database (LIDB) Administrative System (AS)-LIDB Interface, Issue 9*, April 2009.
7. GR-3697-CORE, *Line Information Database (LIDB) Data Screening – Volume 1 (SS7 Interface) and Volume 2 (LDAP Interface), Issue 5*, June 2009.
8. GR-1173-CORE, *OSSGR: Common Functions (FSD 65-01-0100), Issue 4*, August 2005.

A use case example is included in ATIS-1000035.2009, *Next Generation Network (NGN) Identity Management (IdM) Framework*, May 2009.

No critical changes are expected in the above specifications for LIDB to continue its role in the future IP Network.

A.4.2.3 ACD

A.4.2.3.1 Definition of Current State

Automatic Call Distributor (ACD) has been in use for decades by many companies offering sales and service support. ACD service provides an equal distribution of a large volume of incoming calls to pre-designated groups of answering positions, known as agent positions. The ACD Service is a special facility of a PBX or Central Office (CO) switch that automatically routes incoming calls to the next available or longest idle agent or attendant in a line hunt group. ACD systems may work on either traditional circuit-switched or IP voice platforms. These systems also work in conjunction with computer telephony integration (CTI) software, which transfers data obtained from the caller to the agent's computer screen over the ACD link, as well as other contact center applications.

A.4.2.3.2 Future State

It is expected that ACD will continue to be supported in successor networks. With the emergence of VoIP in the last decade, ACD vendors have evolved their platforms to support IP and the standards-based SIP.

[19] Section 222 of the Communications Act Of 1934, as amended 47 U.S.C. 222.

SIP-based ACD solutions can interface with SIP-based IP PBXs to support call routing and the ability to sign in at any phone or workstation. These IP-based systems may also be used to route non-voice interactions, such as email, web chat, Short Message Service (SMS), faxes, voicemail, callback requests, work items, etc.

A.4.2.3.3 Regulatory Implications

Currently ACD services provided by the operator are tariffed by some state PUCs. As this is a market driven capability, there are no expected regulatory implications.

A.4.2.3.4 Standards Implications

Existing standards provide the ability to implement ACD. There is no need to further expand standards.

A.4.2.4 IVR-based Systems

A.4.2.4.1 Definition of Current State

IVR systems are widely deployed in the current PSTN network. When a user initiates a call, the call can be directed to an IVR system that interacts with the user through voice recognition or DTMF digit collections. The IVR systems can provide user directed supplemental services through the voice recognition or DTMF digit collection.

A.4.2.4.2 Future State

IVR solutions will persist in the transition and successor networks. The interfaces used to integrate IVR solutions with the communication networks will evolve. Current IVR systems are typically connected to the PSTN network through TDM interfaces such as PRI trunks. In the successor and transition networks, it is expected that these interfaces will evolve to direct packet interfaces. For voice-band signaling used with these solutions, DTMF digits must continue to be supported. DTMF digits can be transmitted in-band or they can be transmitted out of band using standards based solutions such as RFC 2833.

A.4.2.4.3 Regulatory Implications

IVR systems provide convenient supplemental services. No regulator implications are identified here that are specific to IVR support in the transition or successor network.

A.4.2.4.4 Standards Implications

There are existing standards defined to enable support for DTMF digits transport in packet networks as described in section A.4.1.1. There are no additional standards required to support IVR based solutions.

A.4.2.5 IN Services

A.4.2.5.1 Definition of Current State

Intelligent Network (IN)-based services (e.g., SMS/800 toll-free numbers) and AIN-based services, (e.g., Local Number Portability (LNP), customized call forwarding and call redirecting services, customized time-of-day calling services) in today's PSTN typically utilize a mechanism whereby call processing is very briefly and temporarily suspended to perform an external SS7 database lookup in order to obtain additional information to properly route and/or bill for the call in progress.

IN-based toll free services via the SMS/800 database allow calling parties to dial numbers within dedicated and assigned toll-free NPAs (800, 888, 877, 866, and 855) to reach the assignees of these numbers on a toll-free basis. On calls to these numbers, call processing is temporarily suspended and a lookup of the dialed toll-free number is performed in an external database in order to obtain the

associated geographic Plain Old Telephone Service (POTS) number for network routing to the assignee of the toll-free number.

AIN-based services are typically customized services offered by Services Providers to their end user customers. Service Providers offering AIN-based services develop the custom service-specific logic that resides in their Service Control Points (SCPs) for their PSTN switches to query and obtain the additional information needed to properly route and complete the call.

In support of the current ongoing transition from PSTN to an IP-based network, many IN-based and AIN-based databases can accept SIP-based queries from IP switches in addition to SS7-based queries.

A.4.2.5.2 Future State

As stated above, many databases and the IN services they support have been somewhat transitioned to function in the successor network by virtue of the fact that they can receive and respond to SIP-based queries. Enhancements to the SMS/800 toll-free database are being considered so that it may become a more integral part of the IP network.

A.4.2.5.3 Regulatory Implications

The FCC currently requires that toll-free numbers be made available to subscribers who need and want them. Relevant FCC Orders and citations[20] include:

- 800 Service Management System (SMS/800) Functions Tariff – FCC No. 1 (effective May 1, 1993).
- Toll Free Service Access Codes, CC Docket No. 95-155, FCC No. 96-18, (adopted January 24, 1996).
- Toll Free Service Access Codes, Notice of Proposed Rulemaking, CC Docket No. 95-155, FCC No. 95-419 (adopted October 4, 1995) ("NPRM").

With the exception of Local Number Portability (LNP), there is currently no regulatory mandate to offer AIN-based services. As is the case today in the PSTN, the marketplace and competition will determine which of these services will be migrated and offered in the successor network.

The availability of toll-free numbers (or customer-facing addresses), as well as number portability (or customer-facing address portability), may be influenced by consumer needs and regulatory requirements. See section A.6.1.1 for further information related to Number Portability.

A.4.2.5.4 Standards Implications

Industry groups that have developed standards for IN-based services include ATIS, ETSI TISPAN, ITU-T, 3GPP, and 3GPP2.

A.4.2.6 Voicemail

A.4.2.6.1 Definition of Current State

Voicemail systems allow users to convey recorded audio messages to one or more recipients. The system comprises a user interface (for recording, delivering, and retrieving messages), a delivery interface (to select delivery options and distribution), and a notification method (to alert the subscriber of messages waiting). Voicemail systems allow users to leave audio messages without first calling the recipient(s) and allow the recipients to save these messages for an extended period of time.

[20] < http://www.fcc.gov >

Traditional voicemail systems have four core elements:

1. A central processor that runs the software and operating system;
2. Disks for message storage;
3. System software that includes user profiles (name, extension, password, preferences, etc.); and
4. Telephone line interfaces.

The central processor manages the necessary forwarding (Call Forward Don't Answer or Call Forward Busy) and playing the pertinent announcement to the caller for each forwarding scenario. The processor also validates the password before accessing the messages and prompting the disk controller to play messages back to the subscriber.

Corporate PBXs communicate with the voicemail system via data links through the telephone interface. These data links serve the purpose of exchanging the necessary data to properly identify the target mailbox and ensure the call envelope information is captured correctly, as well as provide the subscriber with alert information after the message has been recorded. The line interface is also responsible for playing the audio stream to the subscriber.

Most of the interfaces in the traditional systems are proprietary and have typically been plagued with traffic engineering problems. On one hand, over provisioning to reduce message delivery failures is a costly solution. On the other hand, inadequate provisioning increases customer complaints and operator costs.

A.4.2.6.2 Future State

IP voicemail is already proliferating among both traditional (telco-hosted providers) and Internet based providers. IP voicemail offers the benefits of reducing hardware, maintenance and per-user costs, open standards interfaces, and the ability to offer advanced voice and data services. IP messaging also offers the advantage of multimedia message store – beyond just voicemail (fax, email, video). With hosted (in the Cloud) messaging, more differentiated services are simpler to offer and more cost effective.

IP voicemail allows users to exchange messages through the medium of their choice (wireline or wireless) with no geographic boundaries or the costs associated with distance billing and fixed trunks. Also, IP voicemail does not lock a user to a single network or limit them with point-to-point communications; an IP voicemail user is able to forward messages to someone on another network – anywhere in the world.

However, IP voicemail is not likely to continue its evolution as a separate offering. It is expected to be integrated with email as part of the greater Unified Communications infrastructure. Text-to-speech and, conversely, the ability to read voicemail messages will become more commonplace and the distinction between voice and text messages will further blur in the future.

Most VM offerings for wireless customers provide:

- On-screen access to voice mail message status.
- Access to voice mail with one button and instant playback.
- Multiple caller-ID based greetings.
- Choices to reply via call back, text, or even voice mail.

All of the above is possible due to advances in screen size and technology. More device-based features and interactive VM apps are to be expected in the future due to the widespread use of smartphones and tablets.

A.4.2.6.3 Regulatory Implications

Voicemail has traditionally been offered as an unregulated service. No changes are expected for IP Voicemail on the regulatory front.

A.4.2.6.4 Standards Implications

Related specifications and generic requirements on Voicemail and the interfaces serving it include:

Table A.3 - Specifications and Generic Requirements for Voicemail

Specifications and Generic Requirements for Voicemail	Relevant Interfaces
Visual Message Waiting Indicator (VMWI)	GR-1401-CORE
ISDN Message Service Generic Switching and Signaling Requirements	GR-866-CORE
Generic Requirements for a Dedicated Data Link Interface Between an End Office SPCS and CPE	GR-1193-CORE
Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)	RFC 4458
Message Waiting Indication (MWI) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification	TS 24.606

A.4.2.7 Voice Conferencing

A.4.2.7.1 Definition of Current State

Voice conferencing is widely utilized in today's PSTN by both business and residential customers in order to set up and conduct multi-party calls. Voice conferencing includes the switch-based feature for three-way calling, more commonly used by residential customers, and multi-party conference bridging more widely used by businesses.

A.4.2.7.2 Future State

Consumers are very likely expect all forms of voice conferencing that are available in today's PSTN to remain available during the transition and after the network is fully transitioned to IP.

A.4.2.7.3 Regulatory Implications

The consumer market and competition among providers will continue to drive the availability of voice conferencing in the fully transitioned network. There is no need for any further regulatory action.

A.4.2.7.4 Standards Implications

The Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP) and Session Initiation Protocol Investigation (SIPPING) Working Groups have produced a number of standards related to voice conferencing. These include:

- RFC 4245, *High-Level Requirements for Tightly Coupled SIP Conferencing*.
- RFC 4353, *A Framework for Conferencing with the Session Initiation Protocol (SIP)*.
- RFC 4575, *A Session Initiation Protocol (SIP) Event Package for Conference State*.
- RFC 4579 – *Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents*.

- RFC 5366, *Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)*.
- RFC 5850, *A Call Control and Multi-Party Usage Framework for the Session Initiation Protocol (SIP)*.

Both the SIP and SIPPING Working Groups have been concluded. The SIPCore Working Group has been chartered in the IETF to maintain and continue the development of the core SIP specifications.

A.4.3 Media Services/CPE Dependent Services

Any system that is dependent on the PTSN for transport needs a transition plan. Need to avoid an unplanned impact on businesses and consumers.

A.4.3.1 Fax

A.4.3.1.1 Definition of Current State

Digital Facsimile machines have been used to send important documents since the 1960s. By the 1970s, most electronics manufacturers had produced FAX machines and they have become part of the core communications kit that is used by businesses and consumers. With the emergence of the Internet, ubiquitous email service, and file sharing services, the volume of fax traffic has declined significantly over the last 7 years. However, there are businesses and agencies that still require FAX documents due to the sensitive nature of the subject matter being transmitted. Additionally, many countries do not recognize electronic signatures as legal signatures. As such, faxed contracts continue to require support of this technology. So, fax enjoys a specific legal status in law in that fax communications has third party confirmation of transmission and/or delivery in carrier billing records (non-repudiation). Not all local-access providers are ready with effective IP-fax support, and the backbone IP providers have only recently begun the move to provide for the transport of quality IP-based fax. International IP fax, peered between national carriers, has yet to get underway.

A.4.3.1.2 Future State

In many corporate environments, fax servers have become the accepted way of transmitting documents. In the consumer markets, multipurpose printer/copier/fax/scan devices have become prevalent for those needing to fax. Additionally, Fax over the internet services are broadly available, both paid and free, that are available and support the uploading of a document which is then delivered to the recipients fax address.

As service migrates away from the PSTN, the industry has developed standards for Fax over IP for those consumers and businesses that aren't able to use the above services. ITU-T T.38 is the standard for Faxing over IP, typically, using a VoIP Analog Terminal Adapter. ITU-T G.3 is the standard for Fax over wireless.

A.4.3.1.3 Regulatory Implications

Fax uses a widely adopted digital sending standard, and fax documents are accepted as valid legal documents. Fax services can be supported today with the alternative technologies that are broadly available.

A.4.3.1.4 Standards Implications

Generally, standards exist and are mature to establish connections between fax devices and adapters to process the documents over IP networks. However, since 2008, the SIP forum has been dealing with FoIP issues that have arisen as documents are being transcoded from IP to TDM to IP, etc. This has become more apparent on international faxes, which potentially have multiple transcodings involved in a

multinational call. This appears to be more of an issue with SIP-based services than H.248 VoIP services. The SIP Forum FoIP Task Group Charter, as listed on their website, requests the task group to investigate ongoing issues with the deployment of fax services, specifically ITU T.38, in SIP networks. SIP networks cannot adequately replace analog PSTN in enterprises unless essential services such as FAX are accommodated. Classic FAX (T.30) over G.711 has not proven to be reliable and SIP communications, in the future, may use other codecs that have been proven to break T.30, such as G.729 and other high compression codecs like SPEEDEX, etc. The SIP Forum FoIP task group is chartered to accomplish the following tasks:

1. Fully document what the current issues are surrounding ITU T.38 in SIP networks:
   a. What interoperability testing procedures currently exist?
   b. What are the common factors in T.38 failure such as page length or lack of ECM support in carrier gateways and ATA's?
   c. Network packet loss considerations.
2. Determine what solutions are currently available to address the problem.
3. Determine if the problem can be solved within the scope of existing IETF SIP and ITU T.38 Recommendations.
4. If the problems can be solved using existing standards by tightening requirements, document the procedures vendors and carriers need to implement in an appropriate SIP Forum Technical Recommendation.
5. If, in the judgment of the SIP Forum FoIP WG, existing IETF and or ITU standards need to be modified, develop a strongly worded recommendation to the appropriate Standards Development Organization (SDO) on what the SIP Forum FoIP WG has discovered and recommend appropriate action by the SDO to remedy the issue.

To date, the task group has identified issues around FoIP timing, packet loss and lingering T.38 handshaking problems. In testing between the SIP Forum and the International IP Interconnect Forum (i3 Forum), it was not possible to clarify all of these problems and their causes due to the opacity of the multiple carrier networks often involved in international calls. Nonetheless, the document contains several components intended to provide guidelines to deliver reliable FoIP call setup.

The SIP Forum and the I3 Forum have jointly published a specification available here:
< http://i3forum.org/wp-content/uploads/2012/05/i3F-Technical-FoIP-Rel-2-FINAL-2012-5-3.pdf>.

A.4.3.2 Alarm System

A.4.3.2.1 Definition of Current State

Personal Security is a rapid growth area in the US and globally. The Global Security Monitoring market is expected to generate over $43B. Security systems have become a lifestyle product for consumers, which is providing service providers opportunities to expand their services to the burgeoning home automation market, including CCTV, HVAC controls, remote door unlocks, etc.

With the slump in the home construction industry, demand for security related products initially dropped. However, as the economy was in recession, business and residential break-ins increased at a considerable pace. This in turn has triggered a resurgence in this market.

While alarm monitoring originally required a TDM telephone line to dial the monitoring center when an alarm triggered, this system was reactive and was easily defeated by cutting the telephone line. A typical system included motion sensors and glass break detectors. Services began to switch to wireless dial up, still in a reactive mode. With Internet-based monitoring systems, companies and consumers can monitor a range of activities and spaces in real time. Notifications are no longer limited to a phone call from the monitoring personnel, but now include automated notifications of issues and events through SMS and email. An example is a teen arriving home after school and opening the door, which could generate an

MMS message showing the door being opened, the alarm disengaged, and a photo of the teen entering the home. This is creating a corresponding increase in the demand for these services.

A.4.3.2.2 Future State

The industry has been rapidly moving away from TDM lines for reporting to wireless (interim) to full Internet based monitoring. In many cases, the state of the art is to rely on wireless and IP to provide redundancy in reporting. Dual signaling is a method of alarm transmission that uses a mobile phone network and a telephone and/or IP path to transmit intruder, fire, and personal attack signals at high speed from the protected premises to an Alarm Monitoring Center. A dual signaling communication device is attached to a control panel on a security installation, and is the component that transmits the alarm to the Monitoring Center. It can do this in a number of different ways: via the GPRS radio path, via the GSM radio path, or via the telephone line/or IP if that has been chosen. These multiple signaling paths are all present and live at the same time, backing each other up, to minimize exposure of the property to intruders. Should one fail, there is always one form of back up, and – depending on the manufacturer chosen – up to three paths working simultaneously at any one time. Prior to the availability of dual signaling systems, police and responsible parties were often called out to the premises because of an alarm signal on the telephone path, only to discover that it was a network fault and not a genuine alarm.

Dual paths allow distinction between hardware failures and a genuine attack on the alarm. This helps eliminate false alarms and unnecessary responses. Dual signaling has helped considerably with the restoration of police response in cases where a phone line is cut and the dual signaling device continues to send alarm calls via one of its alternative paths, either confirming or denying the alarm from the initial path.

A.4.3.2.3 Regulatory Implications

The industry and consumers are selecting alternatives that are broadly available. Two options are available to regulators: Regulators can institute controls to guarantee that in-band alarm reporting will be supported on analog ports in both the transition and successor networks; alternatively, regulators can adopt a policy requiring that communication service providers provide notification to consumers when in-band alarm reporting is no longer supported.

A.4.3.2.4 Standards Implications

None identified.

A.4.3.3 BRI Services

A.4.3.3.1 Definition of Current State

Basic Rate Interface (BRI) is an integrated voice and data service developed in the early 1980s. ISDN is based on a pair of B channels (64kbps) and a D channel (16kbps). The B channels can carry voice and/or data traffic. The B channel data can be switched data, or the B channels can be statically configured to provide a nailed up data connection. The D channel is used for call control and can also be used as a dedicated data channel.

Mainly enterprise customers and government entities deployed ISDN BRI. In addition to the voice services offered with the BRI lines, these users also leveraged the data services and deployed a range of applications based on BRI, including secure voice solutions and video calling solutions.

Broadband access has largely replaced the use of ISDN BRI as a fixed data service (nailed up B channel or D channel data). However, the switched voice and data services are still in use by many of the enterprises and government agencies.

A.4.3.3.2 Future State

ISDN BRI services can be delivered on an IP network using an H.248 or SIP gateway. It is expected that some vendors and operators will continue to support ISDN BRI switched voice/data services in the transition network. It is expected that this will be driven through market demand. Enterprises and government agencies that have large Centrex and communications contracts with the communications providers will drive the carriers to continue to offer BRI support on the transition network. It is not expected that BRI services will be carried forward on the successor network.

A.4.3.3.3 Regulatory Implications

The key considerations from a regulator perspective are the commercial and operational impacts it would have on enterprises and government agencies if carriers discontinued support for BRI service without sufficient notification to the dependent customers.

It is expected that the local agencies that define and regulate BRI service will require such a notification of discontinuation with sufficient time to allow the end users an opportunity to migrate to alternate technologies. Government agencies in particular may need significant advanced notice that would allow funding plans and approvals for migrating to alternate technologies.

A.4.3.3.4 Standards Implications

There are standards that define the interface between the ISDN BRI terminal and the PSTN switches. These standards are referred to NI-1, 2, and 3. These standards allowed any CPE terminal to receive a broad range of ISDN BRI services from multiple vendor switches. There is no need to define additional terminal interface standards. The existing interfaces will still be applicable as vendors deployed SIP and H.248 access solutions that host ISDN BRI terminals.

Existing SIP and H.248 standards can be used to support ISDN BRI switched services. It is not expected that additional standards are required to provide greater ISDN BRI services and transparency support on the transition network.

A.4.3.4 PRI Services

A.4.3.4.1 Definition of Current State

Primary Rate Interface (PRI) is an integrated voice and data service developed for carrying multiple DS0 voice and data transmissions between two physical locations. PRI was developed specifically for industrial or large quantity users. A PRI is made up of 23 B-channels and one 64 Kbps D-channel in a T-1 configuration and 30 B-channels and 1 D-channel using an E1 line.

Primary Rate Interface channels are typically used by medium to large enterprises with digital PBXs to provide them digital access to the Public Switched Telephone Network (PSTN). The advantage of PRI was that the 23 or 30 B channels could be used in various combinations for specific data transmission needs, such as a videoconferencing, allowing bulk data transfer to be achieved more flexibly. Typical services provided via PRI include Direct Inward Dialing (DID), Toll-Free Numbers, and voice calling features such as Caller ID, Call Forwarding, Call Blocking, Call Transfer, and Accounting codes.

PRI/T1 is still the most commonly used trunking service today; however, the use of SIP trunking is growing. SIP trunking has been making steady progress and is the third-most-deployed trunking service, growing to 42% by 2014 according to an Infonetics *SIP Trunking and Enterprise SBC Strategies: North American Enterprise Survey* (March 2012).[21]

[21] < http://www.infonetics.com/pr/2012/VoIP-UC-Services-Market-Forecast-and-SIP-Trunking-Survey-Highlights.asp >

A.4.3.4.2 Future State

ISDN PRI services can be delivered on an IP network using an H.248 or SIP gateway. It is expected that vendors and operators will continue to support ISDN PRI switched voice/data services in the transition network. The transition to SIP trunking will be driven through market demand as some enterprises wait to upgrade their infrastructure until their contracts come up for renewal and the business case for upgrading becomes favorable. It is not expected that PRI services will be carried forward on the successor network.

A.4.3.4.3 Regulatory Implications

The key considerations from a regulator perspective are the commercial and operational impacts it would have on enterprises if carriers discontinued support for PRI service without sufficient notification to the dependent customers.

It is expected that the local agencies that define and regulate PRI service will require such a notification of discontinuation with sufficient time to allow the end users an opportunity to migrate to alternate technologies.

A.4.3.4.4 Standards Implications

There are standards that define the interface between the ISDN PRI and the PSTN switches. These standards are referred to NI-1, 2, and 3. The existing interfaces will still be applicable as vendors deploy SIP and H.248 solutions that connect via PRI.

Existing SIP and H.248 standards can be used to support PRI services. It is not expected that additional standards be required to provide greater PRI services and transparency support on the transition network.

A.4.3.5 Channel Associated Signaling (CAS) Trunk Services

A.4.3.5.1 Definition of Current State

Channel Associated Signaling (CAS), also known as per-trunk signaling (PTS), is a method of signaling where the signaling information is transmitted within the voice channel. Before the introduction of Common Channel signaling (CCS), CAS signaling was used to support PBX interconnect, Operator interrupt services, and PSAP/9-1-1 Services.

A.4.3.5.2 Future State

Newer forms of CCS based signaling have largely replaced CAS. While solutions have been developed to map CAS signaling in VoIP-based networks, it is not expected that this signaling will transition to the successor network.

A.4.3.5.3 Regulatory Implications

While CAS as a signaling variant is not regulated, there are regulated services that utilize CAS signaling in the PSTN today. Some PSTN switches still utilize CAS trunks for routing emergency services calls. As noted previously, there are other forms of interconnect signaling that are available for routing the emergency services call. As carriers evolve their network to new technologies (transition and successor networks), it is not expected that the carriers will maintain the CAS interconnects for emergency services call routing. It is expected that the carriers will evolve to other forms of signaling to route all regulated services.

A.4.3.5.4 Standards Implications

None.

A.4.3.6 Analog Loop Signaling

A.4.3.6.1 Definition of Current State

A range of services were developed on legacy TDM voice switches that utilized independent analog signaling leads in conjunction with the voice loops. The following are example services:

- *Hotel Billing* – A dedicated loop provides pulses to a hotel/motel billing system to represent surcharges for a call.
- *Customer Group Busy Indicator* – An independent loop can provide a signal to the class 5 switch to mark a member of business group as busy for incoming calls. In this scenario, the line which has this signaling active can still originate outbound calls; however, the class 5 switch will consider the line as busy and will only offer calls to other lines in the business group.
- *Emergency Call Signal* – With this type of service, the class 5 switch provides a signal on a dedicated copper loop when a specified line originates or receives a call. An example of this service would be a fire station. When an incoming call is received on the telephone line serving the fire station, a signal on a dedicated loop can raise a visual and audible alarm at the fire station.
- *Night Service* – A dedicated signaling loop allows a customer site to indicate that an attendant is not present and that all offered calls should be directed to an alternative for answer.

A.4.3.6.2 Future State

Alternatives to the analog signaling loops have been developed over the years. While some vendors may choose to maintain some of these services for commercial reasons, it is not expected that these signaling services will be supported in the transition or the successor network.

A.4.3.6.3 Regulatory Implications

It is expected that the discontinuation of these services will not have a material economic or public communications impact. There are no identified regulatory implications.

A.4.3.6.4 Standards Implications

None.

A.4.4 Accessibility/Assistance Services

A.4.4.1 Public Service Functions

A.4.4.1.1 Emergency Hot Line (e.g., Campus Security Hotline)

A.4.4.1.1.1 Definition of Current State

Many legacy class 5 switches support an automatic dial service. This is normally a provisioned option that is assigned to a line. When an origination attempt is received by the class 5 switch, digits are not collected when this option is assigned. The line instead will be assigned with a predefined set of digits. When the origination attempt is received, the class 5 switch will immediately translate the call based on the preconfigured digits. Hotlines cannot be used to originate calls other than to preselected destinations.

This line feature is often used for a public safety line. Phones can be deployed in an environment such as a college campus and when a person needs assistance, he/she can simply pick up a public service phone. A call will be automatically directed to the public safety office.

This same service is common in the current VoIP network architectures. In VoIP architectures, the service can be implemented in the client or the softswitch/application server.

A.4.4.1.1.2 Future State

It is expected that this service will continue to be supported in the transition network and the successor networks.

A.4.4.1.1.3 Regulatory Implications

The ability to define a line as a “hot line” is not currently a regulatory requirement. This is a market driven capability. There are no expected regulatory implications.

A.4.4.1.1.4 Standards Implications

Existing standards provide the ability to implement a “hot line” service. There is no need to expand existing standards.

A.4.4.1.2 Coin (Public Interest Payphone)

A.4.4.1.2.1 Definition of Current State

A payphone is a public telephone, often located in a phone booth or a privacy hood, with pre-payment by inserting money (usually coins), a credit or debit card, or a telephone card.

The number of payphones has sharply declined in the last several years, dropping from approximately 1M payphones in service in 2008 to under 500,000 in 2012, largely due to the increased usage of mobile phones. Payphones process 1.7 billion calls per year, so clearly they are valued by many people in this country. Payphone providers have sometimes tried to reverse the decline in usage by offering additional services such as SMS and Internet access, thus making their phone booths into Internet kiosks. Service Providers have been abandoning payphones at a rapid rate, with some criticism being directed at them by advocates for the poor. Even worse, due to the declining revenues, financially strapped owners are leaving the business and often abandon phones in places contributing to the view that they work poorly.

Many remaining payphones have been installed to comply with state laws requiring accessible voice service at public swimming pools. In many jurisdictions, there are requirements for a payphone to be provided by car towing services. Some hospitals are still required to provide payphones. While wireless and VoIP represent alternatives, CPE continues to be analog today, requiring either CPE replacement or deployment of terminal adapters to accommodate the transition from analog.

A.4.4.1.2.2 Future State

There will likely be a market for public phone services going forward. Batteries die, phones are stolen, etc. There will always be those who can’t afford to own a cell phone, though lifeline services are available that provide landlines or cell phones to the needy. However, transient populations, undocumented workers, etc., will continue to rely on public options.

It seems clear that coin-operated phones will be phased out as network equipment moves to IP and analog capabilities such as decrementing coins will no longer be supported. Where there is a need for a usage based phone, calling cards, credit card CPE all the way to internet kiosks are available that will fill that need. Where payphones exist to support emergency service requirements, deployment options will include analog terminal adapters, VoIP Phones, and wireless phones. The former two options will require broadband availability and power that could be problematic. The latter is available now and is packaged in weather and theft resistant packaging. The good news is that it works outdoors without even having a wireless plan (assuming cellular availability) and generally meets requirements. The FCC rulings mandate that cellular phones without a monthly service contract be able to make free 9-1-1 calls. This “9-1-1 only” emergency phone does not allow incoming calls and lacks call-back capability from the 9-1-1 Public Safety Answering Point PSAP. However, E9-1-1 generally requires the ability to call back which would not be supported with this solution. It would also require power for charging the phone or a regular

maintenance routine to update batteries. This solution would be prohibited in at least 3 states unless there was a wireless subscription.

A.4.4.1.2.3 Regulatory Implications

None identified. Options are there, but it could be costly.

A.4.4.1.2.4 Standards Implications

None identified.

A.4.4.1.3 Emergency Alerts

A.4.4.1.3.1 Definition of Current State

Currently the methods used by Public Safety for authority-to-citizen emergency alerts are the Emergency Alert System (EAS), the Commercial Mobile Alert System (CMAS), and mass calling methods. EAS is the alert system for broadcasters (e.g., radio, TV) and is not associated with the PSTN. CMAS is the alert system for mobile phones and is not associated with the PSTN. The mass calling method is associated with the PSTN.

The mass calling method is the technique where Public Safety will place voice calls to telephone numbers within the desired alert area and these voice calls contain recorded messages informing the citizens of the emergency. There are several existing commercial products which perform this functionality and several municipalities have implemented this mass calling method. The database of PSTN telephone numbers and associated location (e.g., street address of the house) is populated from other databases such as utility databases or is populated by registration by the citizen.

Under the mass calling method, an individual voice call is placed by the automated system to every telephone number in the database which is located within the desired alert area. The automated system could generate a volume of voice calls such that the PSTN switches could become overloaded. When the PSTN switches become overloaded, any or all voice calls could be blocked including calls to 9-1-1.

A.4.4.1.3.2 Future State

With the PSTN successor network being IP-based, the potential exists for authority-to-citizen emergency alerts to be delivered to any communication device connected to the PSTN successor network (e.g., VoIP phone, PC, set-top box, game console). The PSTN successor network also has the potential capability to provide authority-to-citizen alerts in multimedia formats such as video, pictures, graphics, audio, and text.

FCC CSRIC III Working Group 2 on Next Generation Alerting is currently investigating the topic of next generation alerting systems.

A.4.4.1.3.3 Regulatory Implications

Current FCC regulations address the EAS and CMAS alerting systems.

A.4.4.1.3.4 Standards Implications

EAS and CMAS are currently supported by industry standards. If authority-to-citizen alerting is expanded beyond broadcasters and mobile devices to incorporate other communications devices on the PSTN successor network, additional standards may be required.

A.4.4.1.3.5 Recommendations

It is recommended that the TAC defer any recommendations about emergency alerts to the FCC CSRIC III and its associated reports.

A.4.4.1.4 Operator Assisted Communications

A.4.4.1.4.1 Definition of Current State

Operator Assisted communication services are traditional PSTN services where the calling party requires some form of assistance provided by either an operator or automated system. These services often require the specialized capabilities traditionally provided by an operator services switch. Some examples of such services include:

- *Operator Assistance* – This allows the caller to perform either "zero minus" or "zero plus" dialing to be connected to a live operator or automated system for assistance with the call.
- *Collect Calls* – This allows the caller to request that the called party accept the charges for the call. Typically an Operator Services provider utilizes a human operator or automated system to provide this service.
- *Third-party billed calls* – When a number is called and Operator Assistance asks a party, other than the two parties on the call, to accept the charge.
- *Busy Line Verification and Interrupt* – This allows a caller to have the Operator services provider determine whether a target line is in use, and if so, to "barge in" to the conversation and request whether the interrupted party is willing to accept a call from the caller. If the interrupted party is willing to establish conversation, the operator services system then connects the calling and called parties. If the interrupted party refuses to establish conversation, the call is not completed.

Other operator-assisted communications include Information Services such as Directory Assistance (DA). DA is generally identified with "411" or "NPA-555-1212" type services in North America. DA services provide a user with telephone number associated with a name and locality provided by the user, can complete the call for the user, and can send SMS text message with the listing to the user's wireless phone.

A.4.4.1.4.2 Future State

As multimedia capabilities are enabled by IP networks, operator and information services may be invoked and delivered to the user via any mode, including verbal announcements, chat (IM), email, Web (HTTP), MMS, or SMS. To offer such advanced services, Operator and Information Services providers are planning to migrate to SIP-based platforms. In this architecture, application servers act as the primary controller, performing third party call control to route incoming calls among media servers and operator workstations, etc. In transition to the successor network, PSTN gateways which interwork between ISUP or MF signaling and SIP may be deployed to continue to provide access to existing PSTN operator services that utilize MF trunks.

A.4.4.1.4.3 Regulatory Implications

Market and/or regulatory factors in some PUC jurisdictions dictate that some subset of Operator Services continue to be provided going forward in the successor network. This subset typically would include operator assistance for emergency calls, Busy Line Verification and Interrupt service, and Directory Assistance.

A.4.4.1.4.4 Standards Implications

Some of the existing operator services such as Busy Line Verification are based on existing POTS where there is a strong association between a physical POTS line and the address (phone number) used to reach it. With SIP, the same concept of "busy" does not carry directly from POTS access to SIP given a

SIP address is a logical address that can be registered with multiple endpoints simultaneously. PacketCable Residential SIP Telephony Feature Specification, PKT-TR-RST-V03-07110622 defines an approach using the Event dialog package23 to determine whether the device has an active call, and using the Join header in order to bridge onto the current conversation for monitoring and interrupting the user.

Additionally an IETF Internet Draft "Considerations for Information Services and Operator Services Using SIP"24 has been proposed that identifies several protocol gaps and issues with providing operator and information services. ATIS has also developed the following standards:

- ATIS-1000027, *Technical Report on Operator Services in a Next Generation Network (NGN) Environment*, describes the traditional set of operator services and considers how corresponding services could be supported in the IP environment of a Next Generation Network (NGN).
- ATIS-1000036, *Next Generation Network (NGN) Operator Services Standard*, describes signaling support for Operator Services when the application providing the services resides in the Next Generation Network (NGN).
- ATIS-1000050.2012, *Next Generation Network (NGN) Operator Regular Intercept Standard*, describes Next Generation Network (NGN) signaling support for Operator Regular Intercept.

A.4.4.1.4.5 Recommendations

As some subset of Operator Services will continue to be offered in successor networks due to market and regulatory factors, it is recommended that the IETF draft and ATIS technical reports referenced above be referenced for future SIP-based implementations of operator and information services.

A.4.4.2 Telecommunications Relay Services (TRS)

A.4.4.2.1 Definition of Current State

Telecommunications Relay Service (TRS) is a telephone service that allows persons with hearing or speech disabilities to place and receive telephone calls. TRS is available in all 50 states, the District of Columbia, Puerto Rico, and the U.S. territories for local and/or long distance calls. There is no cost to the TRS user. TRS is designed to be connected through a TDD (TTY) or other assistive telephone device.

The operator at the TRS service provider is called a communications assistant (CA). The CA facilitates telephone calls between individuals with hearing and/or speech disabilities and other individuals. The individual with disabilities places a telephone call with a TDD/TTY device to the TRS service provider by either dialing 711 or by dialing the specific 10 digit telephone number of the TRS service provider. The individual with disabilities then uses a TTD/TTY device to send character by character text to the CA including the number of the person that they want to call. The CA plays a voice call to the indicated number and relays the text from the TDD/TYY device to the person on the voice call. The CA then sends the person's verbal response to the TDD/TYY device via text. The following are two common variations on this general procedure:

- *Voice Carry Over (VCO)* is the type of TRS where the individual with a hearing disability wants to use their own voice to speak directly to the called person and to receive the responses in text from the CA. This is especially useful to people LIKE senior citizens who have impaired hearing abilities but who can still speak.
- *Hearing Carry Over (HCO)* is the type of TRS where the individual with a speech disability wants to listen to the called party and type their portion of the conversation to the CA, who translates into speech for the called party.

---

[22] < http://www.cablelabs.com/packetcable/specifications/packetcableapps.html >

[23] < https://tools.ietf.org/html/rfc4235 >

[24] < http://tools.ietf.org/html/draft-haluska-sipping-directory-assistance-11 >

Many companies have their own TDD/TTY telephone numbers which allow individuals with disabilities to contact these companies directly with their TDD/TTY devices.

A.4.4.2.2 Future State

The use of TDD/TTY devices for text communications can be slow, cumbersome, and error prone. Mobile devices sold in the US are required to support TTY services via a connection with an external TDD/TTY device (typically via a special cable). However, TDD/TTY devices are bulky and individuals with disabilities don't carry them as they go about their daily activities.

Therefore, individuals with disabilities are adopting other types of text based messaging methodologies such as Instant Messaging, Short Message System (SMS), Facebook, Twitter, web chat, etc. These other types of text based communications can be performed on a variety of equipment including PCs, tablets, and mobile phones.

However, emergency communications with 9-1-1 Emergency Services is very difficult or impossible for individuals with disabilities. The use of TRS for emergency calls has many issues which impact the ability and timeliness of emergency services for individuals with disabilities. The individuals with disabilities want the ability for direct text based communications with emergency services from their mobile phones. The FCC Emergency Access Advisory Committee (EAAC)[25] which was established as part of the "Twenty-First Century Communications and Video Accessibility Act of 2010"[26] is currently developing recommendations for the FCC on the support of text communications with emergency services.

A.4.4.2.3 Regulatory Implications

- The existing regulations define the support required for TDD/TTY devices.
- There is a large variety of various text based communications available in the marketplace for use by individuals with disabilities. No additional regulations are necessary.
- The regulatory implications and recommendations for text based communications with emergency services are being developed by the FCC EAAC.

A.4.4.2.4 Standards Implications

- Standards have been developed which define the next generation IP-based emergency services network.
- Standards have been developed which defines how Internet based services interact with the next generation IP-based emergency services network.
- Standards are currently under development to define the interconnection and interoperability between next generation LTE-based wireless networks and next generation IP-based emergency services networks.

A.4.4.2.5 Recommendations

- Support for TRS must remain in the successor network to facilitate communications by individuals with disabilities with other individuals who may only utilize voice communications.
- The FCC TAC should defer any recommendations regarding text based communications with emergency services to the FCC EAAC.

---

[25] < http://www.fcc.gov/encyclopedia/emergency-access-advisory-committee-eaac >

[26] See < http://thomas.loc.gov/cgi-bin/query/z?c111:S.3828: >

A.4.4.3 Video Relay Service (VRS)

A.4.4.3.1 Definition of Current State

Video Relay Service (VRS) is a form of Telecommunications Relay Service (TRS) that enables persons with hearing disabilities who use American Sign Language (ASL) to communicate with voice telephone users through video equipment, rather than through typed text. Video equipment links the VRS user with a TRS operator who is called a "communications assistant" (CA).

VRS has the following features and capabilities which are not available with the text-based forms of TRS:

- VRS allows those individuals whose primary language is ASL to communicate in ASL, instead of having to type what they want to say.
- Because individuals using VRS communicate visually in sign language, they are able to more fully express themselves through facial expressions and body language, which cannot be expressed in text messages.
- A VRS call flows back and forth just like a telephone voice conversation between two hearing persons. For example, the parties can interrupt each other, which they cannot do with a TRS call using a TTY device.
- Because the conversation flows more naturally back and forth between the parties, the conversation can take place much more quickly than with text-based TRS. As a result, the same conversation is much shorter through VRS than it would be through other forms of text-based TRS.

Since video communication is involved, a broadband connection such as cable or DSL is required.

A.4.4.3.2 Future State

A high video quality is required for VRS so that the sign language can be clearly viewed by the other party. High video quality generally implies that a broadband connection is required. These broadband connections have generally been achieved with wired connections such as cable or DSL and will continue to be supported by these types of wired connections. However, with the evolution of the wireless networks to LTE, broadband speeds and connectivity will become available to the individual's mobile device which will give them the freedom to using VRS based communications as they move about on their daily activities.

Research on the use of sign language on mobile devices is being conducted in universities and other research centers for individuals with disabilities. One example is the MobileASL[27] project at the University of Washington.

While the results of these research activities could produce results that would allow ASL fluent individuals to talk directly with each other, these results do not eliminate the need for VRS services. Since only a small percentage of the population understands ASL, VRS is still required to perform the translation between an ASL fluent individual and another individual who does not understand ASL.

A.4.4.3.3 Regulatory Implications

- The FCC has existing regulations for VRS based communications. No additional regulations are envisioned.
- The regulatory implications and recommendations for direct video based communications with emergency services are being developed by the FCC EAAC.

[27] See < http://mobileasl.cs.washington.edu/ > for more information on University of Washington MobileASL.

A.4.4.3.4 Standards Implications

- Standards have been developed to support video communications via broadband networks.
- Standards have been developed to support video communications via the 3GPP defined LTE wireless networks.

A.4.4.3.5 Recommendations

- Support for VRS must remain in the successor network to facilitate ASL based communications by individuals with disabilities with other individuals who may not understand ASL.
- The FCC TAC should defer any recommendations regarding video based communications with emergency services to the FCC EAAC.

A.4.4.4 IP Relay Service

A.4.4.4.1 Definition of Current State

IP Relay Service is a newer type of the Telecommunications Relay Service (TRS) and is accessed using a computer and the Internet or a mobile phone with IP capability, rather than a TTY and a telephone. The user can connect to IP Relay using any IP-enabled device.

As with TRS, the IP Relay Service operator is called a communications assistant (CA).The CA communicates with the individual with a hearing or speech disability via text and the individual without a hearing or speech disability via voice. A call from the individual with disabilities goes from the caller's computer or other Web-enabled device to the IP Relay Center via the Internet. The IP Relay Center is usually accessed via a web page using an application. There are multiple types of computer programs that can be used, including custom Java-based programs that run in the user's web browser and instant message based services.

A.4.4.4.2 Future State

With the advent of smart phones, tablets, and other advanced wireless communication devices, direct text communications between individuals is available. However, if the party who is being contacted by the individual with disabilities is not capable of supporting a direct text-based communications and can only support voice based communications, then the use of the IP Relay Service is needed.

IP Relay Service is one of the evolution paths for the eventual replacement of TDD/TTY devices. However, the IP Relay Service does require an Internet broadband connection or an advanced mobile device (e.g., smartphone, tablet) which could be a constraint for some individuals with disabilities.

A.4.4.4.3 Regulatory Implications

- The existing regulations for TRS also include the regulations for IP Relay Services.
- At some point, support of TDD/TYY devices will no longer be necessary since they have been replaced more advanced technologies. Regulations regarding the support of TDD/TYY devices will need to be re-examined.
- The regulatory implications and recommendations for text-based communications with emergency services are being developed by the FCC EAAC.

A.4.4.4.4 Standards Implications

- Standards have been developed which define the next generation IP-based emergency services network.

- Standards have been developed which defines how Internet-based services interact with the next generation IP-based emergency services network.
- Standards are currently under development to define the interconnection and interoperability between next generation LTE based wireless networks and next generation IP-based emergency services networks.
- Standards have been developed to support one-to-one and one-to-many text messaging communications such as instant messaging or chat sessions. There are also proprietary applications that support one-to-one and one-to-many text messaging communications.

A.4.4.4.5 Recommendations

- Support for IP Relay Service must remain in the successor network to facilitate communications by individuals with disabilities with other individuals who may only utilize voice communications.
- The FCC TAC should defer any recommendations regarding text based communications with emergency services to the FCC EAAC.

A.5 New Services & Capabilities in Successor Network

A.5.1 Presence

A.5.1.1 Definition of Current State

Presence services were initially associated with proprietary instant messaging applications and provided a mechanism by which end users could see whether people were logged into their client and therefore likely to be available to chat. Since then, Presence capabilities have evolved with more granular states of availability, user defined states, and "social presence" (where a user may broadcast a range of information such as geo-location, mood, web links, etc.). Presence has also been incorporated in a greater range of applications, and today is seen as a core element of many real time communication clients.

Due to the fact that the Presence service broadcasts real-time information about a user to an external audience, a key factor in making Presence acceptable to end users is to ensure they have control over privacy aspects. This typically is achieved by a two-way association handshake where each party agrees to the other party being allowed to receive Presence information about them. After establishment of this association, the end-user typically has the option to revoke privileges on a temporary or permanent basis.

A.5.1.2 Future State

Given the appeal of Presence in the market, as network providers move into the IP services realm, they are likely to consider making a Presence service an integral part of new service offerings. A Presence service limited to only the subscribers of a particular operator is likely to have less appeal than one which permits use of a range of clients and with subscriber of other operators. Operators will therefore want to look at ways to achieve interoperability of any Presence service.

In order for Presence information to remain relevant, the client needs to periodically update the network and pull Presence information about other users. This generates continuous background traffic. Devices running multiple applications with autonomous Presence clients compound this situation. The impact of Presence updates on device battery life and network resources was one of the reasons behind the development of the GSM Association (GSMA) *Rich Communication Suite--Enhanced (RCS-e)* standard[28], which enables service discovery and multimedia communication but specifically without the need for Presence. Operators may want to look at ways to optimize Presence related signaling.

[28] < http://www.gsma.com/rcs/ >

A.5.1.3 Regulatory Implications

The service provider's primary responsibility is to adhere to privacy requirements by respecting the user's right to privacy and data protection, and only sharing Presence information with parties with which the user has agreed to.

A.5.1.4 Standards Implications

The lead industry standards in this space are based on IETF work and include *Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE)* (RFC 3265, RFC 3856, RFC 3903) and *Extensible Messaging and Presence Protocol (XMPP)* (RFC 6120, RFC 6121, RFC 6122, RFC 3922, RFC 3923). These solutions have then been further advanced by organizations like OMA and XMPP Standards Foundation to facilitate greater interworking and the creation of modular network functions. There however remains significant technical variety between Presence solutions in deployment, with many solutions remaining closed implementations.

Operators have options to deploy Presence as a component capability for a range of multi-media services. This is the case, for example, for the GSMA Rich Communication Suite (RCS), which builds on the Presence capabilities defined in OMA.

A.5.1.5 Recommendations

It is recommended to the FCC TAC that no specific action is required in relation to the Presence service.

A.5.2 Location

A.5.2.1 Definition of Current State

Location services come in many forms with different degrees of accuracy and reliability. The user can report their location manually to an application; the device can make its location known to authorized applications; or the network can determine the device's location based on its MAC address, IP address, or radio infrastructure serving the device.

The device may be provisioned with its location, have access to an internal GPS device, or – if it is a mobile device – have access to the Cell ID or other identifying information about the radio network in which it is being served. Various applications might access and use this information, with the end user's permission. For privacy reasons, this information would not be universally accessible. Location information provided by the device has limited applicability due to the potential for the user and/or device to misrepresent their location. Where legal or charging aspects come into play, a network solution is usually necessary. Most applications will use device provided location information to allow the end user maximum control over the sharing of this information.

Network location services come roughly in two flavors: IP geolocation and access network specific location services.

Many IP geolocation services are available today to help identify information about a particular IP address to varying degrees of accuracy, based on databases of publicly available information. These services can typically determine the country of origin, the domain of the address, the ISP, city of origin, and geographic coordinates. Even for information from the most reputable sources (e.g., well known ISPs), due to privacy reasons and dynamic address allocation policies, the information is rarely more accurate than the city of origin. Information from IP geolocation services is typically insufficient for legal or charging purposes, but can reliably identify the ISP providing most end user IP addresses. With this information it may be possible to get more accurate information directly from the access network provider (i.e., ISP). It should be noted that even the IP address can be spoofed by using forwarding or anonymization services such as Tor, but these come at a cost in convenience and performance that most legitimate users will avoid.

A.5.2.2 Future State

Broadband and wireless access network providers have information about the location of their customers. Broadband providers can associate a street address with an assigned IP address. Wireless providers can identify at least the current serving cell for a device, and methods are available to provide more accurate information using various radio techniques. This location information is typically available to satisfy various internal operational, service, or application needs.

A.5.2.3 Regulatory Implications

The location technologies described above may or may not comply with the existing FCC accuracy regulations for emergency voice calls (e.g., voice calls to 9-1-1). Wireless operators may use a variety of standardized device-based and/or network-based methodologies to determine the location of mobile devices within the constraints defined by FCC regulations. The existing FCC regulations only specify accuracy requirements for voice calls to 9-1-1. However, as part of the transition to NG9-1-1, emergency services will evolve to Multimedia Emergency Services (MMES), which will include text and video capabilities as well as voice for communications with emergency services. The location accuracy requirements for the non-voice capabilities for MMES are still to be defined by the FCC.

The FCC CSRIC III Working Group 3[29] has been tasked with the assignment to evaluate location accuracy for wireless emergency calls. FCC CSRIC III Working Group 3 is responding to a series of location accuracy questions posed by the FCC and will be generating three reports. The first report is on outdoor location accuracy for emergency calls, the second report is on indoor location accuracy for emergency calls, and the third report is an evaluation and feasibility of leveraging location determination methodologies of commercial Location Based Services (LBS) for emergency services.

With the rapid adoption of mobile location-based services, a number of privacy issues are raised by the use of such services. As mobile devices regularly transmit their location to a network, they are enabling the creation of a precise record of a user's locations over time. This can allow the creation of a very accurate and highly personal user profile, which raises questions of how, when and by whom this information can and should be used. The FCC in a report issued in May 2012, *Location-Based Services: An Overview Of Opportunities And Other Considerations*[30] has started to look at these privacy issues with the intent to ensure that LBS providers provide consumers with appropriate notice and choice with respect to the use of the data generated by LBS. Location privacy protection legislation is also being introduced in the U.S. Senate.

A.5.2.5 Standards Implications

There are various impediments to sharing location information with third-parties due to privacy and other security concerns, so work is still in progress to identify ways of making more accurate location information available to authorized third-parties if and when it is necessary.

A.5.2.5 Recommendations

It is recommended that the FCC TAC defer any recommendations about location accuracy to the FCC CSRIC III and its associated reports.

[29] < http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii >

[30] < http://www.fcc.gov/document/location-based-services-report >

A.5.3 Messaging

A.5.3.1 Definition of Current State

Messaging is generally considered to be text based messaging between two or more individuals. The earliest forms of messaging were the instant messaging services that were available via PCs over dial-up connections on the PSTN.

Messaging has expanded greatly beyond the earliest versions to now include mobile devices and high-speed PC connections. Due the availability of low cost mobile device and cellular rate plans, the use of SMS for messaging on mobile devices has been extremely popular, with billions of SMS messages exchanged on a daily basis.

A.5.3.2 Future State

For the younger generations, messaging has surpassed voice calls as the preferred method of communications. Messaging is also expanded to be more than just text messages and to include other multimedia types such as video clips, audio clips, pictures, and graphics.

Due to the large and growing popularity of messaging, the PSTN successor network will need to support the capabilities to support multimedia messaging among two or more individuals using a wide range of communications devices (e.g., PCs, tablets, mobile phones, game consoles).

A.5.3.3 Regulatory Implications

Messaging is an unregulated service.

The FCC Emergency Access Advisory Committee (EAAC)[31], which was established as part of the "Twenty-First Century Communications and Video Accessibility Act of 2010"[32], is currently developing recommendations for the FCC on the support of text and multimedia communications with emergency services.

A.5.3.4 Standards Implications

Some messaging services are proprietary. Other messaging services are based upon various standards defined in IETF, 3GPP, 3GPP2, and OMA.

See section A.4.1.2 for a discussion of the emergency services and multimedia communications including messaging.

A.5.3.5 Recommendations

- Support for messaging capabilities must be included in the successor network.
- There are no known modifications to FCC regulations required.
- The FCC TAC should defer any recommendations regarding text- and multimedia-based communications with emergency services to the FCC EAAC.

[31] See < http://www.fcc.gov/encyclopedia/emergency-access-advisory-committee-eaac >

[32] See < http://thomas.loc.gov/cgi-bin/query/z?c111:S.3828: >

A.5.4 HD Voice

A.5.4.1 Definition of Current State

The audio range of traditional (narrow band) telephony systems is 300-3400 Hz, which covers the key audio frequency range to enable comprehensible speech, and the communication industry has used this for many years. High Definition (HD) Voice takes this to the next level by extending the audio range to 50-7000 Hz. The result is a noticeable more natural-sounding speech with improved clarity and perception of closeness, all factors which have been shown to improve the user experience in human trials. HD Voice has yet to see widespread deployment in the PSTN. HD Voice is in the early phases of commercial launch in cellular networks.

To gain the most benefit and the best user experience from HD voice, both ends of the communication need to support a wideband codec, preferably the same one to avoid the need for transcoding. In end-to-end IP networks, session negotiation can be used to facilitate this. In existing networks, support of Tandem Free Operation (TFO) and Transcoder Free Operation (TrFO) provide mechanisms for the removal of unnecessary transcoding. The type of operator interconnect, therefore, has a bearing on the ability to offer HD voice.

In an attempt to limit technical fragmentation of the HD Voice market, the GSMA is actively engaged in a establishing a trademarked “HD Voice” logo (< www.gsma.com/technicalprojects/hd-voice/ >) with associated minimum requirements for its use.

HD Voice services are starting to be rolled out in fixed (and more so the cellular networks), while a number of Internet VoIP providers make widespread use of wideband audio.

A.5.4.2 Future State

The positive user experience of HD Voice will drive demand for the service; however, the size of the installed base that is not capable of delivering HD Voice, particularly in the PSTN, will remain a challenge for some time.

A.5.4.3 Regulatory Implications

Currently there are no regulatory requirements which mandate a service provider to offer HD Voice services.

A.5.4.4 Standards Implications

Key standardized wideband codecs include: ITU G.722, G.722.2 (also known as AMR-WB – Adaptive Multi-rate Wideband), EVRC-NW (Enhanced Variable Rate Narrowband-Wideband), and IETF Opus[33]. With many additional wideband codecs in commercial use, industry convergence towards mandating a single codec is extremely unlikely. It is hoped that a core subset of wideband codecs will achieve general market adoption and this will help facilitate interworking and reduce the need for transcoding.

The support of wideband codecs in fixed network devices has been addressed by the DECT Forum through the CAT-iq initiative[34]. The CAT-iq addresses wireless broadband home connectivity in the protected frequencies used by DECT. In turn, there has been collaboration between CAT-iq and the Home Gateway Initiative (HGI)[35], which is evolving the building blocks for Broadband Service Providers to deliver digital services to the home

[33] < http://www.opus-codec.org/ >

[34] < http://www.cat-iq.org/ >

[35] < http://www.homegatewayinitiative.org/ >

A.5.4.5 Recommendations

It is recommended that market forces be allowed to drive the deployment of HD Voice services without additional regulatory involvement.

A.5.5 Video Calling/Conferencing

A.5.5.1 Definition of Current State

Video communication services can be point-to-point or involve more than two parties. Today such services address a broad range of requirements including: business oriented systems; solutions to assist persons with hearing disabilities (see section A.4.4.3); cellular video communication services; systems to enable experts to see real time images from remote sites; and, more recently, high definition video services (TelePresence), which provide a virtual face to face meeting experience.

Interoperability between video communication service systems is typically only possible where the end points have been implemented to open standards. Many legacy video services have been deployed based on the ITU ISDN and H.323 video conferencing standards.

A.5.5.2 Future State

The greater bandwidth, system flexibility, and lower cost of Broadband IP-based video communication delivery has been drawing video services away from the PSTN for some time, and this trend is set to continue.

IETF SIP-based architectures such as 3GPP IP Multimedia Subsystem (IMS) are now seeing increased interest as the base architecture for video communication delivery. The key advantage of such solutions is the flexibility by which end points can negotiate their video capabilities, easing interoperability challenges, as well as the fact that these architectures create a common platform on which operators can provide many different services.

Greater affordability and availability of video communication services is driving user adoption, which in turn is leading to younger generations growing up with improved ease and expectations for video services, enhancing long term demand.

A.5.5.3 Regulatory Implications

The FCC has existing regulations for video services to assist persons with disabilities (see section A.4.4.3).

A.5.5.4 Standards Implications

There is an abundance of standards relating to video services, which in itself creates a challenge for interworking. The ITU has developed video services standards for POTS (H.324), ISDN (H.320), and IP networks (H.323). 3GPP has extended ITU H.324M to create 3G-324M for 3G mobile phone video services. GSMA has created IR.94[36] and RCS 5.0 standards containing profiles for video communication services based on IMS. GSMA is also working on a profile for High Definition Video Conferencing (HDVC).

Internet browser based video communication services are now emerging, and a framework of standards known as WebRTC is being jointly developed by the IETF and W3C (see RFC 3264).

Since IP video services are built out of many component standards which undergo frequent innovation, there is a process of continual standards evolution in organization such as the IETF, 3GPP, ITU, etc.

[36] < http://www.gsma.com/newsroom/ir-94-1-0-ims-profile-for-conversational-video-service >

A.5.5.5 Recommendations

The broad availability of video services provided directly by existing operators and available from alternative sources on the Internet has created a competitive eco-system in which video service innovation can flourish. No additional regulator involvement is believed necessary.

Where existing video communication service regulations already exist, these will need to be carried forward to the successor network (see recommendation in section A.4.4.3.5).

A.5.6 Content Sharing

A.5.6.1 Definition of Current State

Content sharing is the ability for users to exchange different types of content while in a session, such as a voice call, or as a standalone activity. Features may include

- "See What I See" – a live-streaming, real time video feature.
- File Transfer.
- Sharing of photos, music, contacts, and maps.
- Any other tasks that offers benefit to parties who need to share information.

The Multimedia Message Service (MMS) was the first standardized solution for content sharing, enabling images, video clips, text files, and ringtones to be transferred. This solution was developed by 3GPP, WAP, and OMA.

Initial video share implementations use current circuit-switched technology to connect speech-based calls with the use of packet-switched technology (IP) to establish a point-to-point real-time video connection. These video share capabilities are based on specifications of both the 3GPP and GSMA.

Implementations to negotiate the transfer of one or more files between two endpoints leveraged the Session Description Protocol (SDP) offer/answer model specified in IETF RFC 3264. The Message Session Relay Protocol (MSRP) is defined as the default mechanism to actually carry the files between the endpoints.

In addition to solutions offered by network operators, alternative mechanisms such as email and over the top applications are commonly used for content sharing.

A.5.6.2 Future State

Users are increasingly distributing and sharing content. Mobile phone users in particular are increasingly using their devices to take pictures and videos. Content sharing applications, many linked to popular social networks, will continue to grow in popularity as subscribers look for ways to share experiences. These solutions will be offered by both network operators and over the top service providers.

A.5.6.3 Regulatory Implications

Content Sharing is currently an unregulated service.

A.5.6.4 Standards Implications

Current standards covering Image Sharing and File transfer capabilities include:

- GSMA PRD IR.79, *Image Share Interoperability Specification 1.0*.[37]
- GSMA PRD IR.84, *Video Share Phase 2 Interoperability Specification*.[38]

[37] < http://www.gsma.com/newsroom/wp-content/uploads/2012/03/ir.79.pdf >

- IETF RFC 4145, *TCP-Based Media Transport in the Session Description Protocol (SDP)*.
- IETF RFC 4575, *A Session Initiation Protocol (SIP) Event Package for Conference State*.
- IETF RFC 4975, *The Message Session Relay Protocol (MSRP)*.
- IETF RFC 5547, *A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer*.
- OMA-TS-SIMPLE_IM-V1_0-20080903-C, *Instant Messaging using SIMPLE*.[39]
- GSMA Rich Communication Suite 5.1, *Advanced Communications Services and Client Specification 1.0*.[28]

The GSMA Rich Communication Suite (RCS) program is an effort of a group of industry players for the rapid adoption of applications and services providing an interoperable, convergent, rich communication experience both in mobile and fixed environments. RCS (Rich Communication Suite) 5.1 provides a framework for discoverable and interoperable advanced communication services and detailed specifications for a set of advanced communication services including content sharing.

A.5.6.5 Recommendations

Photo, Video, Music, etc., sharing applications provided directly by existing operators and available from alternative sources on the Internet has created a competitive eco-system in which content sharing innovation can flourish. No additional regulator involvement is believed necessary.

A.5.7 Social Networking

A.5.7.1 Definition of Current State

Social networking is one of the newest vehicles for communications and exchange of information between individuals. Social networking is currently performed via PCs, tablets, or mobile devices. The PCs could be connected to the social networking services via dial-up connections on the PSTN.

Social networking incorporates other capabilities discussed in this document including Presence (see section A.5.1), Location (see section A.5.2), and Messaging (see section A.5.3).

A.5.7.2 Future State

Social networking continues to expand in both the capabilities provided and the types of communications devices supported. Social networking is expanding to include capabilities such as information exchange (e.g., file transfers) and video conferencing.

The IP capabilities of the PSTN successor network will be the major enabler for social networking and its future evolution.

A.5.7.3 Regulatory Implications

Social networking is an unregulated service. There are no known modifications to FCC regulations required.

---

[38] < http://www.gsma.com/newsroom/wp-content/uploads/2012/03/ir.84.pdf >

[39] < http://technical.openmobilealliance.org/technical/release_program/docs/SIMPLE_IM/V1_0-20080903-C/OMA-TS-SIMPLE_IM-V1_0-20080903-C.pdf >

A.5.7.4 Standards Implications

Some of the social networking services are proprietary and use proprietary protocols. Other social networking services are open and use standardized protocols. The set of standardized protocols utilized varies among the various social network services.

A.5.7.5 Recommendations

- Support for enabling capabilities for social networking including presence, location, and messaging must be included in the successor network.
- There are no known modifications to FCC regulations required.

A.6 Conclusions & Recommendations

A.6.1 PSTN Services Summary

The following table summarizes the current set of PSTN applications available today and places them into categories defined as:

- *Sunset Services*: This set of services leverage outdated technology and are being/or have been replaced by alternate mechanisms that provide superior capability.
- *Transitional Services*: Due to market penetration, this set of services will require strategies for ongoing support until such time as it makes commercial sense to transition.
- *Successor Network Services*: Services definitively supported in successor networks driven by regulatory, social policy, or market.

Primary drivers are also highlighted that influence the disposition of each service. Drivers can include market, regulatory, and public safety.

Table A.4 - List of Services and Drivers

Service Category	Service	Successor Network Services	Transitional Services	Sunset Services	Comments
Core Voice Services/ Regulatory Services	Dual-tone multi-frequency signaling (DTMF)		✓		**Drivers: Market** Given the financial impacts to enterprises that have IVR services deployed, DTMF will continue to be a key capability for the PSTN in transition.
	Emergency Services	✓	✓		**Drivers: Regulatory** Emergency Services must evolve as new communications capabilities become available.
	Lawful Intercept	✓	✓		**Drivers: Regulatory** Lawful Intercept must evolve as new communications capabilities become available.

Service Category	Service	Successor Network Services	Transitional Services	Sunset Services	Comments
	Priority Services	✓	✓		**Drivers: Public Safety** Priority Services must evolve as new communications capabilities become available.
	Malicious Call Trace	✓	✓		**Drivers: Regulatory/Public Safety** Users must continue to have the ability to activate call tracing for malicious voice communications, As additional real time communication capabilities are enabled by IP networks, it is expected that call tracing may be extended (i.e., Malicious Communications Tracing) to enable tracing for malicious IM's, video calls, content sharing, etc.
	Portability	✓	✓		**Drivers: Regulatory** Customer identity portability depending on the end user naming scheme utilized will be an expectation of consumers and a requirement of regulators in the fully transitioned successor network.

Service Category	Service	Successor Network Services	Transitional Services	Sunset Services	Comments
Advanced Communication Services	CLASS^{SM}	✓ (partial)	✓		**Drivers: Regulatory, Market** Continuing to offer the same capabilities in the IP network will depend on the market demand. Further study is recommended to look at use cases for each of the CLASS services and clearly define: ●Standard SIP functions that could be relied on for deploying the service. ●Applicable Extensions for each service. ●Examination of functionality that may be carried out by end devices in the IP network. In transitioning to SIP signaling, there are unanswered questions around privacy rules that require guidance and clarification from the FCC.
	Database Services	✓	✓		**Drivers: Regulatory, Market** No major technical hurdles anticipated for LIDB to become an integral part of the new IP network. LIDB is already a valuable resource in the Identity Management sphere. LIDB and its administrative system would need to evolve in successor networks to support any changes away from telephone numbers as addressing and identity mechanisms.

Service Category	Service	Successor Network Services	Transitional Services	Sunset Services	Comments
	Automatic Call Distributor (ACD)	✓	✓		**Drivers: Market** It is expected that ACD will continue to be supported in successor networks and may also be used to route non-voice interactions, such as email, web chat, SMS, faxes, voicemail, callback requests, work items, etc.
	IVR (Interactive Voice Response)	✓	✓		**Drivers: Market** It is expected that IVR solutions in successor networks will take advantage of browser-based capabilities available on smart devices.
	Intelligent Network (IN) Services		✓		**Drivers: Market** Many databases and the IN services, including SMS/800 toll-free database, have been somewhat transitioned to function in the successor network by virtue of the fact that they can receive and respond to SIP-based queries. Enhancements to the SMS/800 toll-free database are being considered so that it may become a more integral part of the IP network. The marketplace and competition will determine which of these services will be offered in the successor network.

Service Category	Service	Successor Network Services	Transitional Services	Sunset Services	Comments
	Voicemail	✓	✓		**Drivers: Market** IP voicemail is expected to be integrated with email as part of the greater Unified Communications infrastructure. Text-to-speech and – conversely – the ability to read voicemail messages will become more commonplace and the distinction between voice and text messages will further blur in the future.
	Voice Conferencing	✓	✓		**Drivers: Market** Consumers will very likely expect all forms of voice conferencing that are available in today's PSTN to remain available during the transition and after the network is fully transitioned to IP.
Media Services/ CPE Dependent Services	Fax	✓	✓		**Drivers: Market/Legal** The industry has developed standards for Fax over IP (T.38) for those consumers and businesses that aren't able to use Fax servers or Fax over Internet services.
	Alarm System	✓	✓		**Drivers: Market** State of the art is to rely on wireless and IP to provide redundancy in reporting.
	BRI Services		✓		**Drivers: Market** Enterprises and government agencies that have large Centrex and communications contracts with the communications providers will drive the carriers to continue to offer BRI support on the transition network. It is not expected that BRI services will be carried forward on successor networks.

Service Category	Service	Successor Network Services	Transitional Services	Sunset Services	Comments
	PRI Services		✓		**Drivers: Market** It is expected that vendors and operators will continue to support ISDN PRI switched voice/data services in the transition network. The transition from PRI to SIP trunking in successor networks will be driven through market demand as some enterprises wait to upgrade their infrastructure until such time as the business case proves favorable.
	Channel Associated Signaling (CAS) Trunk Services			✓	**Drivers: Market** It is expected that CAS services will be phased out as enterprises replace their old PBX's and carriers upgrade their CAS interconnects for emergency services call routing.
	Analog Loop Signaling dependent Services			✓	**Drivers: Market** Alternatives to the analog signaling loops have been developed over the years. It is not expected that these signaling services will be supported in the transition or the successor networks.
Accessibility/ Assistance Services	Emergency Hot Line	✓	✓		**Drivers: Market** Often used for a public safety line, it is expected that this service will continue to be supported in the transition and successor networks.

Service Category	Service	Successor Network Services	Transitional Services	Sunset Services	Comments
	Coin (Public Interest Payphone)	✓ (alternate implementation)	✓		**Drivers: Regulatory, Market** Coin-operated phones will be phased out as network equipment moves to IP and analog capabilities such as decrementing coins will no longer be supported. Where there is a need for a usage based phone, calling cards, credit card CPE all the way to internet kiosks are available that will fill that need.
	Emergency Alerts	✓	✓		**Drivers: Regulatory** FCC CSRIC III Working Group 2 on Next Generation Alerting is currently investigating the topic of next generation alerting systems.
	Operator Assisted Communications	✓ (partial)	✓		**Drivers: Regulatory, Market** Some subset of Operator Services will continue to be offered in successor networks due to market and regulatory factors.
	Telecommunications Relay Services (TRS)	✓	✓		**Drivers: Regulatory** TRS must be available for individuals with disabilities for both the transitional and successor networks
	Video Relay Service (VRS)	✓	✓		**Drivers: Regulatory** VRS must be available for individuals with disabilities for both the transitional and successor networks
	IP Relay Service	✓	✓		**Drivers: Regulatory** IP Relay Services must be available for individuals with disabilities for both the transitional and successor networks

A.6.2 New Applications in Successor Networks

Consumers will have access to collections of application services (HD voice, video, messaging, content sharing, social networks, information services, etc.), which should meet national goals, such as

emergency notification, E9-1-1, accessibility, etc. A combination of market forces, standardization, self-regulation, and government oversight will ensure that the selected combinations of applications operate sufficiently well to meet specific national needs. It is important to realize that the new applications and combination of applications defined today will evolve over time as more broadband services become available and achieve market penetration.

A.6.3 Recommendations for Further Study

A.6.3.1 CLASS^{SM}

If there is sufficient market demand for CLASS service equivalence in successor networks, further study is recommended to define SIP extensions to achieve a more comprehensive and interoperable set of IP Consumer Services. The work should take into account the functions that could be carried out more efficiently by devices rather than network entities (e.g., Visual Voicemail display and Selective List Editing features).

A.6.3.2 Privacy Regulations

Clarification is required from the FCC around applicability of privacy rules of 91-281 to Calling Number and Name Delivery in successor networks. If applicable, details of implementation require ubiquitous adoption in IP-based networks. SIP and other VoIP protocols must implement equivalent capabilities to:

- Allow the session initiator (caller) to block their information.
- Require IP network providers to abide by similar rules about relaying blocking information from end-to-end.
- Develop the capabilities necessary in the proxy servers to enforce privacy policies for both name and number delivery.

Spoofing Caller ID is much more feasible in an all IP network. Will the FCC simply rely on the penalties connected to the “Truth in Caller ID Act” to be a sufficient deterrent or should they seek a more proactive role from the IP providers in: (1) verifying the outgoing CID data; and (2) preserving it across intermediate networks?

A.6.3.3 Portability

Portability standards could be influenced by the results of the areas for further study recommended below.

Areas for further study include:

- Portability functionality in general (and specifically, portability boundaries), as well as the role of network elements, and number or address resource optimization related to any elimination of rate centers and LATAs.
- Portability functionality for customer-facing addresses, whether they are e.164 numbers (and their associated LRNs) or something else.
- Evolution and architecture of industry and carrier databases for portability in the successor network – e.g., discuss if/how the ENUM hierarchical registry architecture can support Number Portability in the U.S. in the successor network.

A.7 Acronyms

3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2

AC	Automatic Callback
ACD	Automatic Call Distributor
ACR	Anonymous Call Rejection
AIN	Advanced Intelligent Network
AMR-WB	Adaptive Multi-rate Wideband
ANI	Automatic Number Information
ANSI	American National Standards Institute
AR	Automatic Recall
ASL	American Sign Language
ATA	Advanced Technology Attachment
ATIS	Alliance for Telecommunications Industry Solutions
BCLID	Bulk Calling Line Identification
BCP	Best Current Practice
BRI	Basic Rate Interface
CA	Communications Assistant
CALEA	Communications Assistance for Law Enforcement Act
CAPEX	Capital Expenses
CAS	Channel Associated Signaling
CAT	Cordless Advanced Technology
CBIS	Cable Broadband Intercept Specification
CCS	Common Channel Signaling
CID	Calling Identity Delivery
CIDB	Calling Identity Delivery Blocking
CIDCW	Calling Identity Delivery on Call Waiting
CLASS	Customized Local Area Signaling Service
CMAS	Commercial Mobile Alert System
CMRS	Commercial Mobile Radio Service
CN	Core Network
CNAM	Calling Name Delivery
CND	Calling Number Delivery
CO	Central Office
COT	Customer-Originated Trace
CPE	Customer Premises Equipment
CPN	Calling Party Number
CPNI	Customer Proprietary Network Information
CSRIC	Communications Security, Reliability and Interoperability Council
CTI	Computer Telephony Integration
CWD	Call Waiting Deluxe
DA	Directory Assistance
DECT	Digital Enhanced Cordless Telecommunications
DHS	Department of Homeland Security
DID	Direct Inward Dialing
DNS	Domain Name Service
DRCW	Distinctive Ringing/Call Waiting
DSL	Digital Subscriber Line

DTMF	Dual-tone multi-frequency
EAAC	Emergency Access Advisory Committee
EAS	Emergency Alert System
ECM	Error Correction Mode
EMS	Emergency Medical Services
ENUM	Electronic Numbering
EO	End Office
ESInet	Emergency Services IP Network
ETS	Emergency Telecommunication Service
ETSI	European Telecommunications Standards Institute
EVRC-NW	Enhanced Variable Rate Narrowband-Wideband
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FoIP	FAX over IP
GETS	Government Emergency Telecommunications Service
GSM	Global System for Mobile communications
GSMA	GSM Association
HCO	Hearing Carry Over
HD	High Definition
HELD	HTTP-Enabled Location Delivery
HGI	Home Gateway Initiative
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IdM	Identity Management
IETF	Internet Engineering Task Force
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol
ISDN	Integrated Services Digital Number
ISP	Internet Service Provider
ISUP	ISDN User Part
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
IVR	Interactive Voice Response
LAES	Lawfully Authorized Electronic Surveillance
LARG	LIDB Access Routing Guide
LATA	Local Access & Transport Area
LBS	Location Based Services
LDAP	Lightweight Directory Access Protocol
LEC	Local Exchange Carrier
LERG	Local Exchange Routing Guide
LI	Lawful Intercept
LIDB	Line Information Database

LNP	Local Number Portability
LoST	Location-to-Service Translation
LRN	Location Routing Number
LSSGR	LATA Switching System Generic Requirements
LTE	Long Term Evolution
MCID	Malicious Communication Identification
MEID	Mobile Equipment IDentifier
MF	Multi-Frequency
MGC	Media Gateway Controller
MMES	Multimedia Emergency Services
MMS	Multimedia Messaging Service
MPS	Multimedia Priority Service
MSRP	Message Session Relay Protocol
NANP	North American Numbering Plan
NCS	National Communications System
NENA	National Emergency Numbering Association
NGN	Next Generation Network
NPA	Numbering Plan Area
NS/EP	National Security and Emergency Preparedness
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
OMA	Open Mobile Alliance
OPEX	Operating Expenses
OSS	Operator Services Systems
OSSGR	Operator Service System Generic Requirements
OTT	Over-The-Top
PBX	Private Branch Exchange
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Number
PUC	Public Utility Commission
RCS	Rich Communication Suite
RFC	Request for Comment
RTP	Real-time Transport Protocol
SCA	Selective Call Acceptance
SCF	Selective Call Forwarding
SCP	Service Control Point
SCR	Selective Call Rejection
SDO	Standards Development Organization
SDP	Session Description Protocol
SIGTRAN	Signaling Transport
SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol

SLE	Screening List Editing
SMS	Short Message Service
SPCS	Stored Program Controlled Switching system
SPID	Service Provider ID
SS7	Signaling System #7
TAC	Technology Advisory Council
TCP	Transmission Control Protocol
TDD	Telecommunication Device for the Deaf
TDM	Time Division Multiplexing
TFO	Tandem Free Operation
TIA	Telecommunications Industry Association
TIP	Terminating Identification Presentation
TIR	Terminating Identification Restriction
TrFO	Transcoder Free Operation
TRS	Telecommunications Relay Services
TS	Technical Specification
TTY	Teletypewriter
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
VCO	Voice Carry Over
VMWI	Visual Message Waiting Indicator
VoIP	Voice over IP
VRS	Video Relay Service
VSLE	Visual Screening List Editing
WAP	Wireless Application Protocol
WiMAX	Worldwide Interoperability for Microwave Access
WPS	Wireless Priority Service
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol

Appendix B

Access

Appendix B: Access

B.1 Introduction

B.1.1 Background

Consumers are demanding greater functionality and flexibility in the telephony market. This includes capabilities such as more media choices, mobility, and greater integration that cannot be provided by the traditional PSTN. This section of the report looks at the implications of migrating away from the PSTN accesses. Note that since there was not necessarily a clear distinction in the PSTN between access and the applications provided over these accesses, some of these aspects are covered in the applications part of this report.

B.1.2 Objective & Scope – Access Networks

The goal of this section of the report is to assess the implications of retiring the current PSTN access network. Most of the services that users actually expect from the PSTN are better viewed as applications, and are thus addressed under the applications section of this report. However, due to the ubiquity of the PSTN access network, there is a huge ecosystem of CPE devices in use that depend of the PSTN access that currently exists. This section of the report therefore focuses on:

- *Stranding of CPE*: Types of devices and migration strategies for those devices.
- *Central Office Power*: Implications and alternatives for not having power transmitted from the central office.
- *Robustness of the Access Network*.

B.1.3 Definitions

B.1.3.1 Stranded CPE: *Stranded CPE* refers to customer based equipment that will no longer function (or lose functionality) if the access network is migrated to a newer technology. These devices may, for example, depend on loop start signaling, use of the G.711 codec, or 48v power.

B.2 Assessment Approach

As part of this investigation, various characteristics and limitations of the PSTN access network were investigated. The goal was to determine which of these characteristics might need to be carried forward as the PSTN is evolved.

- *The access network limitation to voicegrade channels*: The PSTN assumes the use of the G.711 codec which transmits audio in the range of approximately 300-3400Hz, providing a voice-centric network that also supports voice-band data.
- *Carrier-provided line power for CPE connected to voice lines*: Local loops used with voice services provide line power independent of the commercial power provided to the customer's premises via the power grid. This means that some CPE connected to voice lines will work even during a commercial power outage at the customer's premises.
- *Network limited to fixed lines (no mobility)*: PSTN access is provided via a fixed infrastructure. This has made it possible to know the caller's location (e.g., for 911) and authorization to use the services (e.g., for long distance). In mobile or nomadic accesses, these assumptions no longer hold. Some facilities-based VoIP services have techniques designed to deal with this (e.g., by controlling the network segment, or by forcing the user to input their location), but these approaches have limitations.
- *Analog subscriber side signaling*: There is a large amount of signaling that is defined for communicating with CPEs and callers. These include signals that the user can perceive such as dial tone, DTMF, call progress signals, announcement tones, etc. It also includes signaling that is not perceived, such as loop start, operator services, or controlling coin telephones.

- *Digital subscriber side signaling*: ISDN BRI and PRI interfaces are deployed in the network. EKTS phones are also deployed.
- *Access provider is equivalent to voice service provider*: In PSTN, the access provider and the voice provider were the same company. It was clear who was responsible for providing telephony services. In the future network, this linkage cannot be assumed.
- *Availability*: Subscribers have come to expect that the PSTN is dependable.
- *Circuit switched voice service*: The PSTN mostly provided a single type of voice services. The PSTN in transition and the target network will likely provide many levels of voice services (from low rate codecs to high quality audio). In addition, many non-voice services, such as text or video, will be provided.
- *Assumed analog technology*: Some state, local, or PUC authorities may have imposed regulations that are tied to the technology traditionally used in the PSTN (e.g, existence of Cos or dB loss on a loop).

For each of these areas, an attempt was made to assess whether there were regulatory requirements related to these areas and what CPE would be impacted if that particular characteristic was no longer present.

It was determined via this analysis that the key concerns were:

- Stranding of CPE.
- Implications of loss of central office power.
- Robustness.

In general, there were few regulatory requirements that mandated the presence of the above characteristics. For this reason, the report focuses on CPE stranding, loss of central office power, and robustness. Where there are regulatory implications for particular types of CPE, this is described in the report.

B.3 CPE Stranding

The implications and mitigation measures (associated with the removal of the PSTN accesses) for different types of CPE are described below.

Overall, it was concluded that the stranding of CPE is best treated as an economic issue, not a policy issue

- For most CPE, consumers are voluntarily making the transition away from analog devices for better features, to save money, etc. Consumers already have abundant choices.
- For those choosing not to migrate CPE, it is possible to provide a converter box and substitute an alternate technology. Many cable/fiber providers already provide such capability.
- Since such an alternative exists, carriers shall be allowed to migrate technology. How to incentivize/force the adoption of converter boxes is an economic issue.

B.3.1 Stranding of Analog Phones

Millions of analog phones are still in use in North America. For daily use, many consumers have already migrated to wireless or VoIP and given up their landlines. Statistics on this migration can be found at: < http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-301823A1.pdf >. The particular case of keeping an analog phone around in case of a power outage is handled under the section on CO powered local loops.

Converter boxes for providing analog service inside the house while utilizing alternatives to copper loop outside the house (e.g., cable, fiber, wireless) are already widely deployed.

Conclusion: Stranding does not seem to be an issue. Most subscribers will migrate voluntarily. The remainder can be transitioned to converter boxes when it is no longer economical to maintain the local loops.

B.3.2 Stranding of Fax machines

Alternative mechanisms for sending documents are widespread. However, faxes have legal significance so in many cases, it is not possible to accept alternate distribution means such as email or ftp.

However Faxing is not necessarily tied to the access network. Faxing is possible using alternative mechanisms. These still are considered fax:

- Faxing over the internet (T.38).
- Faxing over wireless (G.3).
- Faxing services.

Converter boxes, if used, will support analog fax.

Conclusion: Stranding does not seem to be an issue. Most subscribers will migrate voluntarily. The remainder can be transitioned to converter boxes when it is no longer economical to maintain the local loops.

B.3.3 Stranding of Alarm Systems

Many alarm systems use an analog modem to communicate with the alarm center. However, alternative alarm systems are available using:

- Internet.
- Wireless.

These new alarm systems typically provide additional functionality such as surveillance, remote control, and home automation. Consumers and alarm companies are migrating to these richer types of alarm systems.

Converter boxes if used will analog signaling to the alarm center.

Conclusion: Stranding does not seem to be an issue. Many subscribers or alarm services will migrate voluntarily. The voluntary migration speed will be slower than for typical consumer devices. Converter boxes when it is no longer economical to maintain the local loops, although it may be cheaper to work with the alarm companies to incentivize new alarm systems.

B.3.4 Stranding of Public Payphones

Payphones are being phased out due to the ubiquity of wireless. They are simply no longer economical to maintain.

State regulations often require the presence of a payphone at specific locations for emergency purposes.[40]

The regulations do not mandate that these be analog devices, only that they can make emergency calls, Alternatives to analog payphones exist and are deployed. They are often replaced by internet kiosks.

Conclusion: Stranding does not seem to be an issue. Alternative technology can be used to provide required payphone services when local loops are phased out

B.3.5 Stranding of TTY Devices

TTY devices are an old technology (from WWII) that uses low rate analog signaling (baudot) to enable bi-directional communications for the hard of hearing.

[40] < http://www.payphone.com/State-Law-911-Requirements.html >

The FCC currently mandates support of TTY devices over both wireline and wireless systems for the purposes of emergency calls.

- PSAPs are capable of receiving TTY calls.
- Relays exist for converting TTY signaling to voice (TRS).

Converter boxes can be used to support analog signaling for TTY towards the user. In addition, mobile devices and networks already natively support TTY.

The regulatory implications and recommendations for text-based communications with emergency services are being developed by the FCC EAAC. Alternatives to TTY exist and are being deployed. In general, the subscribers wish to migrate to newer technologies that provide more functionality.

Conclusion: Stranding does not seem to be an issue. Most subscribers will migrate to newer technologies voluntarily. For those not wishing to migrate, converters can be used. Various committees have advised the FCC to loosen regulations requiring support of TTY in favor of newer technologies.

B.3.6 Stranding of Analog PBXes

A range of specialized analog signaling has been developed for support of analog PBXs. Customers are voluntarily transitioning to more modern PBX technologies due to the richer diversity of services. Many of these analog signaling services are not frequently deployed and are being phased out.

Converter boxes exist for supporting analog PBXs. They may either emulate analog signaling or may tunnel the signaling to a remote switch.

Conclusion: Stranding does not seem to be an issue. Many businesses will migrate voluntarily. Converter boxes can be used to support analog PBXs when the customer is unwilling to migrate. This is a business-to-business relationship.

B.3.7 Stranding of Other Types of CPE

There are various types of analog modems that are embedded in various types of CPE. These includes devices such as:

- Modems in Point of Sale devices (e.g., credit card verification).
- Data modems in computers.
- Modems used for various M2M applications (telemetry, vending machines, etc.).

In general, these devices are already transitioning to alternative access methods such as wireless or broadband which provide improvements in performance and functionality.

Technology and services specific to M2M is being developed with the goal of handling M2M communications effectively and efficiently.

Converter boxes for providing analog service inside the premises while utilizing alternatives to copper loop outside the premises (e.g., cable, fiber, wireless) are widely deployed.

Conclusion: Stranding does not seem to be an issue. Most devices will be transitioned voluntarily. The remainder can be transitioned to converter boxes when it is no longer economical to maintain the local loops.

B.3.8 CPE or Services Not Included in this Analysis

BRI/PRI (ISDN) was not addressed. BRI/PRI is used mainly by business customers and these are migrating to broadband interfaces. Digital interfaces were excluded since it is a relatively small population of users and is being addressed through business relationships.

Multiparty – Multiparty lines were not analyzed because the population of multiparty lines is small. Multiparty is also a service as opposed to a specific type of CPE.

B.4 Central Office Provided Power

The consumer reliance on central office provided power seems to be diminishing. Many consumers already have UPSs for critical electronics or have transitioned to cordless phones which require house power in any case. Many have transitioned to mobile devices which have their own battery.

Fiber/Cable/Wireless companies already provide converter boxes which provide battery backup for several hours.

There does not seem to be a mandate to requiring independent power:

- No regulations found mandating CO power.
- No regulations on availability of consumer devices during electrical outages.

It was noted that some consumers keep analog phones as a backup in case of power outages. Companies may want to address this desire as a marketing issue and provide solutions such as backup batteries that continue to function in the case of a power outage.

Conclusion: Stranding does not seem to be an issue. Phasing out of CO line power should be an economic issue. Emergency powering is not required, but can be provided as a feature. It should be a consumer choice on whether it is needed and the mechanism used to provide it.

B.5 Robustness

One of the characteristics of the PSTN is that it is dependable. Consumers have come to expect a high level of availability for the PSTN Access network. It should be noted that the Access Network is only part of the issue since end-to-end connectivity also involves applications and interconnection.

For this analysis, the term "robustness" was interpreted to mean "availability" (or "survivability" in the case of disasters).

It should be noted that any type of access can be engineered for different levels of availability depending on what the requirements are. However, current broadband access networks are not typically engineered for the same level of availability as the PSTN access.

The previous need for high availability was primarily driven by the need to communicate since PSTN was the only network. Many subscribers will now have to the availability of more than one access (broadband, wireless), which will give overall higher availability than any single access.

High availability may also be viewed as a commercial differentiator between service offerings.

B.5.1 Robustness During the PSTN Transition

This addresses availability of the network during the transition.

As always, access and transport availability will be based on the level of availability the system is engineered for. It is expected that interconnect availability may decrease during the transition, but it is not possible to quantify what that availability will be. This is primarily because the interconnection in the IP environment is more complex with many more commercial and technical possibilities.

- More interconnect design choices.
- More media types and bandwidth requirements.

Conclusion: During the transition, it is expected that end-user service availability will likely be driven by commercial factors and competition.

B.5.2 Robustness After the PSTN Transition

This addresses availability of the network after the transition.

Some components of broadband and wireless access technologies are not necessarily engineered to the same level of reliability as central office switches. However, the existence of multiple access options (wireless and broadband) may provide greater overall availability since they are largely independent.

Application, transport, and interconnect issues are also important in accessing end-to-end availability.

- Transport availability may be similar since it may be mostly the same transport infrastructure as today.
- End-user service availability is unknown, but may be driven by commercial factors and competition.
- Interconnect availability is evolving and is an area of active study in the industry.

Conclusion: After the transition, it is expected that end-user service availability will likely be driven by commercial factors and competition.

B.5.3 Technologies to Improve Robustness

It should be noted that IP technology is inherently more survivable than circuit-switched technology.

Redundancy and geographic distribution can in many cases increase availability. Application of these methods depends on the engineering requirements.

The above capabilities can be used to make accesses as available (or more available) as the PSTN.

Whether backup power is provided and the duration of provided backup power depends on the engineering decisions. This applies to both wireless and wireline.

Unlike PSTN, network backup power will also need to be supplemented by backup power on the customer premises.

Conclusion: No additional technologies are needed to provide highly reliable systems.

B.6 Conclusions & Recommendations

It is recommended that stranded CPE should be treated as an economic issue, not a policy issue.

- For most CPE, consumers are voluntarily making the transition away from analog devices for better features, to save money, etc. Consumers already have abundant choices.
- For those choosing not to migrate CPE, it is possible to provide a converter box and substitute an alternate technology. Many cable/fiber providers already provide such capability.
- Since such an alternative exists, carriers shall be allowed to migrate technology. How to incentivize/force the adoption of converter boxes is an economic issue.

It is recommended that the removal of central office provided line power be treated as an economic issue, not a policy issue.

- Many consumers have already migrated to devices that are not dependent on CO power (cordless phones, VoIP phones, cellular phones). Customers are employing UPSs to protect these devices.
- There does not seem to be regulation in place requiring CO provided power (for either normal or emergency calling).
- Many service providers already provide battery backup as part of converter boxes. Providing this is best treated as an marketing differentiator.

IP-based technology is technologically a more reliable solution than circuit switched technology. However, the ultimate robustness depends on the requirements to which the network is engineered. It is difficult to predict the robustness of the future PSTN since:

- End-to-end reliability depends not only on the access network, but also on application, transport, and interconnection aspects.
- Engineering a network for high reliability is more challenging in the new environment due to:
    - More interconnect design choices.
    - More media types and bandwidth requirements.
    - More and different types of providers.

It is expected that end-user service availability will likely be driven by commercial factors and competition.

No additional technologies are needed to provide highly reliable systems.

It should also be noted that the high availability of the PSTN network was due to the fact it was the only mechanism people had to communicate peer-to-peer. Consumers now have many more alternatives for communication, so may not need to depend so heavily on the PSTN as the sole source of communicating.

Appendix C

Transport

Appendix C: Transport

C.1 Introduction

C.1.1 Purpose

The infrastructure of the PSTN has been transitioning from TDM (time division multiplex) technology to IP (Internet Protocol). This transition has been transparent to most consumers because:

- Much of the transition has focused on the core networks.
- When IP has been introduced into the access network, the TDM customer interface has been maintained to a large extent.

However, direct access between the consumer and the PSTN has also been transitioning to IP and will accelerate in the near future.

The TDM network that consists of a telecommunications service provider providing a single purpose voice connection to the consumer is being replaced by an IP network where a voice application (VoIP) is transported over a multi-purpose broadband connection. In some cases, the VoIP provider and the broadband provider will be the same entity, but in other cases they will be different entities. Initially, the majority of VoIP will be transported over managed-service-based IP networks, utilizing service engineered virtual networks. Some of the traffic will be transported over the public Internet. As a new technology called web real-time communications (WebRTC, which enables voice, video, and other real-time applications over the public internet without plugins) becomes mature, we could see a large amount of VoIP traffic evolving to the public Internet.

IP is significantly different from TDM. The existing processes and regulations associated with the PSTN are based on a TDM network. As the network transitions to IP, it is important for the industry to evaluate the impact of this transition and make changes and recommendations where necessary. The FCC has already started evaluating the transition in its Universal Service Fund – Intercarrier Compensation Reforms (USF-ICC Reforms) issued at the end of 2011, by moving the PSTN to a billing environment more like the Internet and encouraging PSTN providers to interconnect using IP technology.

In its reform, the FCC is aligning “access charges/reciprocal compensation” for VoIP with the compensation levels for non-VoIP (i.e., PSTN) traffic. Access charges for VoIP and non-VoIP voice traffic will be replaced, and a bill and keep mechanism will be put in place instead.[41] This new intercarrier compensation regime includes VoIP-PSTN traffic.

In addition, the commission recognizes the importance of IP-to-IP interconnection (for voice traffic) and has initiated a FNPRM (Further Notice of Proposed Rulemaking) to seek comment on the rules that should apply to IP-to-IP interconnection. The commission has made it clear that “even while our FNPRM is pending, we expect all carriers to negotiate in good faith in response to requests for IP-to-IP interconnection for the exchange of voice traffic”.

This report will identify the areas impacted by the transition of the PSTN and will recommend further evaluation to address concerns and un-resolved issues that have been identified.

C.1.2 Definitions

This report will use the following definitions. These definitions apply to the PSTN before, during and after the transition. Of specific interest is a definition of the PSTN itself.

> **PSTN**: The global series of interconnected networks that enables a voice-grade call to any device/application with an E.164 TN

[41] < http://www.gvnw.com/Portals/0/seminars/fcc_icc_usf_order_2011.pdf >

In the above definition, the term “call” refers to an interactive communication session. This definition will be used to help us determine whether we consider certain aspects of the work as part of the PSTN or not. This is not to imply that those aspects identified as not part of the PSTN are not or could not be regulated in a manner similar to traditional voice communication services. Other relevant definitions applicable to this report include:

Advanced communications services: Means: (A) interconnected VoIP service; (B) non-interconnected VoIP service; (C) electronic messaging service; and (D) interoperable video conferencing service.

Bill and Keep: A charging mechanism for the two-way interconnection of two networks where each network agrees to terminate calls from the other network at no charge. This is in contrast to Sending Party Pays arrangements.

Broadband Internet access provider: A provider of mass market retail service by wire or radio that is able to support interconnected VoIP service. This is what we generally call an ISP.

Broadband backbone ISP: Provides long-haul transmission for one or more Internet broadband access provider.

Bundled signaling and media: When signaling and media flows are forced to traverse the same path between networks at an NNI by anchoring of both the signaling and media at network border functions.

Carrier: A business entity such as an “IP Carrier” offering IP interconnect capabilities

to Service Providers and/or Enterprise customers based upon commercial agreement. A Carrier providing such services in the PSTN is referred to as Interexchange Carrier.

Carrier NNI: Identifies the interworking facility of networks (i.e., the Network to Network Interface – NNI) between Carriers.

Controlled and Managed Public IP Network (Internet) Interconnection: A form of interworking where reliability, performance, and reporting is possible, given voice packets are transmitted onto public IP networks which are controlled and managed by the two parties establishing the voice bilateral NNI interconnection.

Direct IP Link: A dedicated physical or logical Carrier-to-Carrier or Carrier-to-SP link made up of facility segments under lease/ownership and control of the two parties involved in a bilateral interconnection. This form of interconnection provides transport with monitored levels of quality and security, allowing carriers to control the final voice quality characteristics to match those of the TDM environment.

End-to-End (SP-to-SP): End-to-End means from Service Provider premises to Service Provider premises.

ENUM: A system providing E.164 number mapping to Uniform Resource Identifiers (URI).

Indirect (Uncontrolled non-managed) Public IP Network (Internet) Interconnection: A form of interworking where reliability, performance, and reporting is not controlled nor managed by the carriers implementing the bilateral interconnection, given a third (or multiple) internet service providers to establish the voice bilateral NNI interconnection.

Interconnected VoIP service: Has the following characteristics: (1) the service enables real-time, two-way voice communications; (2) the service requires a broadband connection from the user’s location; (3) the service requires IP-compatible CPE; and (4) the service offering permits users generally to receive calls that originate on the PSTN and to terminate calls to the PSTN.

IP Multimedia Subsystem (IMS): The SIP-based multimedia communications architecture specified by 3GPP.

IPX (IP Packet eXchange): A private managed backbone providing guaranteed QoS, security, and cascading payments. The IPX is a network of networks provided by the whole group of interconnected IPX Providers.

IPX Provider (IPX P): A business entity (such as an IP Carrier) offering IP interconnect capabilities to Service Providers, possibly through interconnection with other IPX Providers for one or many IPX services compliant with the IPX operation criteria and compliant with the defined SLA and interconnect agreement for that end-to-end service.

Managed private Interconnection: A type of interconnection where only multi-media communications packets (and no other internet traffic) is exchanged across the interconnection. Although the IP addresses involved can be private or public, they shall not be announced onto or reachable from the Public Internet. Managed private IP networks provide transport, control, security (i.e., isolated from the Internet), and service layers with controlled and monitored levels of quality and security.

Managed-service-based transport (aka managed transport): The transport of traffic within a network, across an interconnection point, or across a transport provider's network using managed-service-type constructs such as dedicated or virtually dedicated facilities, separated from public Internet traffic. Such transport is managed in the sense that it is engineered, controlled, and monitored for security, reliability, performance, and QoS metrics to satisfy service needs and conform to any specific transport service SLA (service level agreement).

Multi-lateral Interconnection (Agreement): An IPX-SP agreement that covers the capability to interconnect to multiple SPs.

Network Link: Identifies the interworking facility of networks between two Carriers.

One-way VoIP service: Allows end users to place calls to or receive calls from the PSTN, but not both.

Optimal Media Routing (OMR): A mechanism specified by 3GPP for use in IMS to bypass unnecessary media gateways allocated for a multimedia session (typically at network boundaries) to provide the most direct media path routing. When OMR is used, signaling and media may traverse different networks.

Service Provider (SP): A business entity which offers services to end users. Thus, "service provider" includes mobile network operators and fixed network operators (for example, fixed broadband operators and NGNs), ISPs, ASPs, and similar entities.

Service Provider NNI: Identifies the interworking facility of networks (i.e., the Network to Network Interface – NNI) between an SP and another entity, such as a Carrier, an Enterprise, or another SP.

Sending Party Pays (SPP): A type of business model used for remuneration of services rendered where the party sending the traffic pays the party receiving the traffic. Services rendered may be measured in time, capacity, quantity, duration or any combination based upon business agreement. A common form of measurement is "minutes-based".

Transit Service: A Transit Service is provided by a Transit Carrier serving two Carriers needing to interwork their domains, but lack the physical connectivity necessary to interconnect on their own.

Transport Carrier: Refers to a Carrier providing "service unaware" bandwidth capacity necessary to move traffic between two domains – e.g., from Carrier A to Carrier B.

VoIPX: Identifies a specific logical subset of IPX devoted to managed voice service in terms of interfaces, features, and capabilities.

C.1.3 Background

C.1.3.1 Current US Telephony PSTN Interconnect Model

The figure below depicts the current US Telephony PSTN architecture and interconnect model. This architecture is characterized by:

- One or more end office local switching systems interconnected within a Local Access and Transport Area (LATA).
- One or more Inter-exchange carrier networks providing interconnect services between these LATA based local networks.

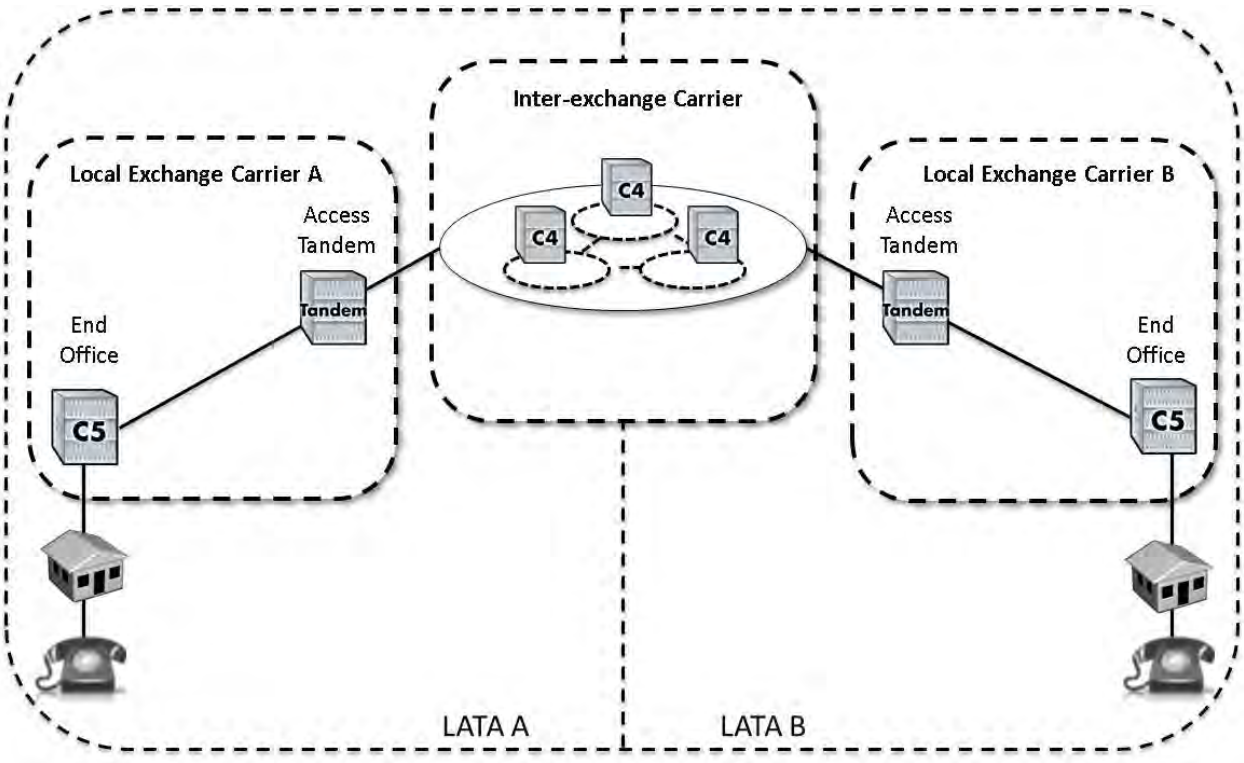

Figure C.1 - Current US Telephony PSTN Interconnect Model

The end office switches within the LATA are known as Class 5 (C5) switches. Within the LATA, Class 5 switches interconnect through a Tandem switch or through direct connections between the switches. Class 5 switches connect directly to customer premises equipment such as telephones and FAX machines, and provide local telephony services to this equipment.

Interconnectivity between LATAs is provided by Inter-exchange Carrier networks. These networks are comprised of Class 4 (C4) switches that provide interconnect services between other Class 4, Class 5, and tandem switches. The inter-exchange carrier's class 4 switch may connect to an access tandem and/or directly to the class 5 switches within a LATA.

C.1.3.2 VoIP Interconnection Basic Configuration

VoIP in this context will coexist with SMS, MMS, Multimedia features, video calling, and other Real Time Communications features that may come available.

VoIP has been introduced into the traditional PSTN network architecture in a variety of places, forming islands of VoIP that must interconnect. For example VoIP could be used in:

- Enterprise PBX networks.
- Local networks.
- Tandem and inter-exchange networks.

The figure below illustrates one example of a bilateral carrier VoIP interconnection wherein VoIP signaling and media are exchanged between carriers. More detail relating to interconnect models is provided in section C.2 of this document.

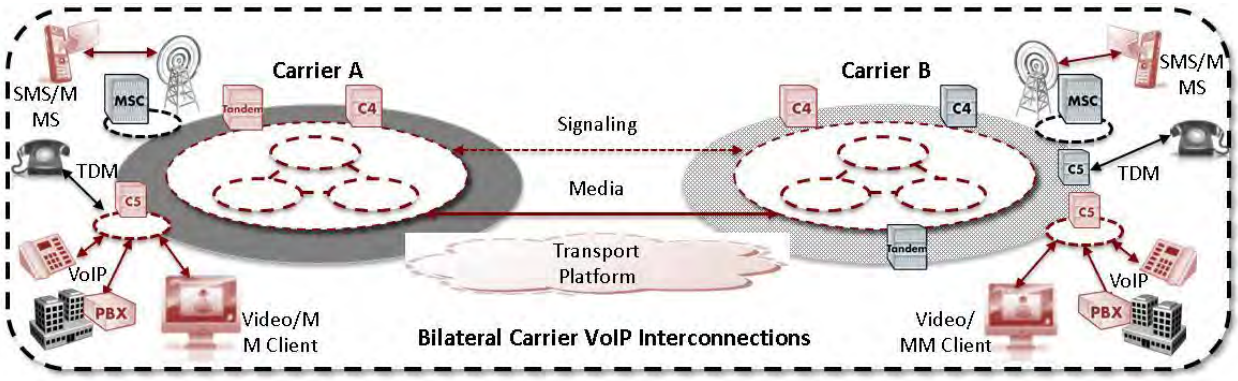

Figure C.2 - Bilateral Carrier VoIP Interconnections

C.2 Interconnect Reference Models

C.2.1 ATIS NGN Architecture

C.2.1.1 Reference Architecture

The figure below illustrates the interconnection reference model for IP NNI supporting VoIP, video, and data. It illustrates Border Elements (BEs) to enable IP interconnection between Service Providers. A BE includes an Interconnect Session Border Controller and Data Border Function. Details of the Interconnect Session Border Controller and Data Border Function are described in the ATIS-1000018, *NGN Architecture*, and ATIS-1000046, *Data Border Functions and Requirements*, respectively.

An Interconnect Session Border Controller is composed of an Interconnection Border Control Function (IBCF) and a Transition Gateway (TrGW). An Interconnect Session Border Controller provides the following functions:

- Performs SIP-based call/session control signaling functions with its counterpart in the peering network.
- Performs bearer/media-path-related functions with its counterpart in the peering network.
- Performs routing and control with its counterpart in the peering network.

The scope of the IP NNI work is illustrated in the figure below with a shaded box around the interfaces between the BEs. It includes Signaling, Media (RTP/IP), and Routing and Translation.

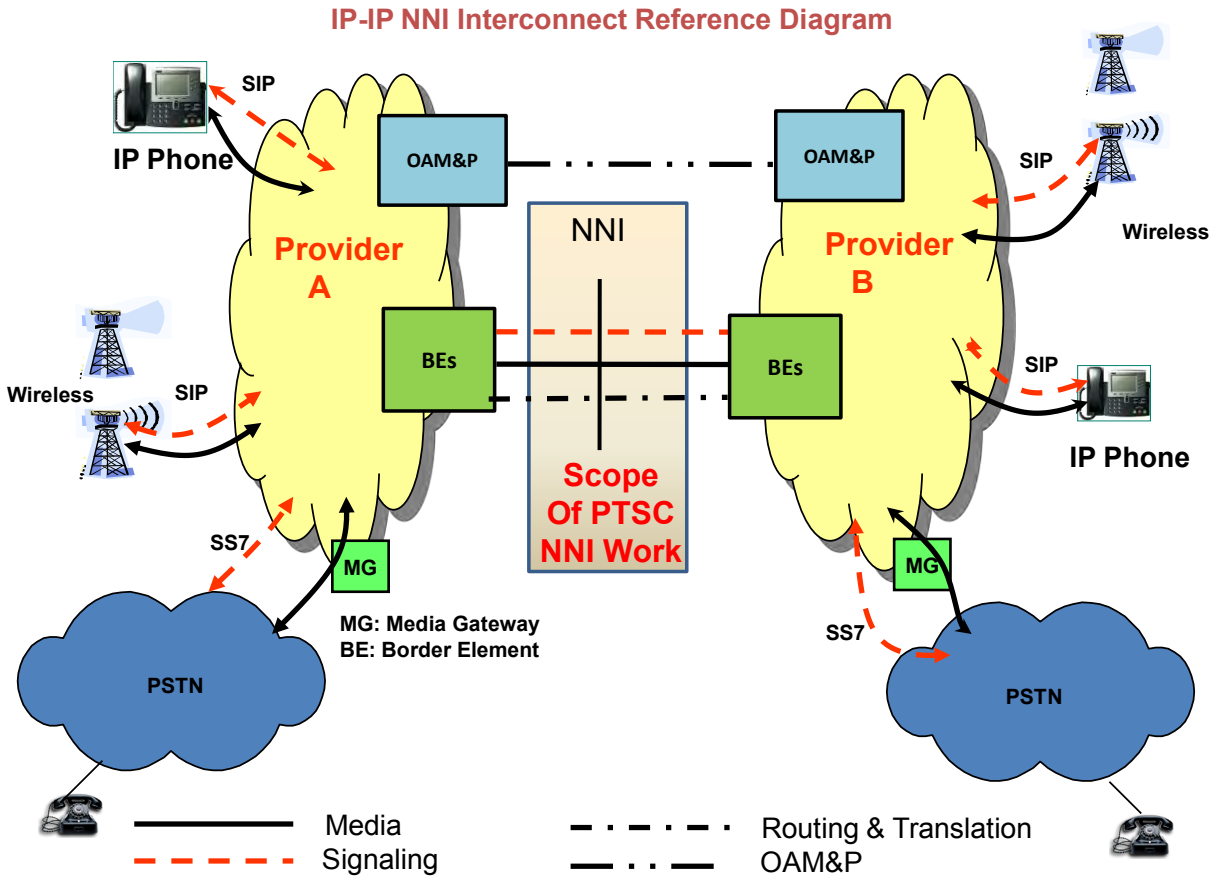

Figure C.3 - Interconnection Reference Model

The NNI Phase 1 NNI standard[42] defines the IP Network-to-Network Interface (NNI) for VoIP between carriers. It addresses the need for a standard interface as telecom networks migrate the NNI from TDM circuit switched to IP. The focus of this standard is to support VoIP. This standard defines:

- Interconnection architecture;
- SIP call/session control signaling;
- Signaling and media transport;
- Quality of Service (QoS);
- Association between call control and media control; and
- Mandatory SIP URIs to be Supported.

There is also an informative annex on items for consideration in SLAs.

The NNI Phase 1 NNI standard has a parallel recommendation published in the ITU[43].

---

[42] ATIS-1000009.2006 (R2011), *IP Network – To Network Interface Standard for VoIP*.

[43] Q.1912.5, *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part*.

The NNI Phase 2 NNI document[44] contains an IMS to IMS interconnection profile, and an IMS to non-IMS interconnection profile. The IMS to IMS interconnection profile section will define the ATIS deltas to 3GPP TS 29.165[45].

C.2.1.2 Access Networks Architecture

The current ATIS Access Network Architecture baseline (PTSC-SAC-2012-009) documents the following for various wireline and wireless technologies:

- Reference Architectures;
- Illustrative Call/Session Flows;
- Interfaces; and
- QoS and Policy Mechanisms.

The wireline technologies include:

- Digital Subscriber Line (DSL);
- Fiber to the Home (FTTH);
- Fiber to the Curb (FTTC); and
- PacketCable.

The wireless technologies include:

- EV-DO;
- UMTS; and
- LTE.

WiFi is not addressed in the current baseline.

C.2.2 IMS Architecture

C.2.2.1 Inter-IMS NNI

3GPP TS 29.165 defines the inter-IMS network-to-network interface (NNI). The reference model for the inter-IMS NNI is shown in the following figure. There are two sets of protocols associated with the NNI for SIP signaling at the Ici reference point and media transport at the Izi reference point.

The Interconnection Border Control Function (IBCF) provides application-specific functions at the SIP/SDP protocol layer for interconnection between IMS networks. It can act as either an entry point or an exit point for a network and can include the following functions: topology hiding, application level gateway, control of user plane functions, protocol screening, routing, generation of charging records, privacy protection, and other security functions. Network domain security at the Ici reference point is normally provided using IPSec.

The Transition Gateway (TrGW) forwards media streams using RTP/UDP and RTCP/UDP between IMS networks while providing network type/address/port translation and optional functions like transcoding and media security based on SRTP with keying schemes that include SDES and MIKEY-TICKET.

---

[44] ATIS PTSC Issue S0040. < http://www.atis.org/0191/issues.asp >

[45] 3GPP TS 29.165, *Inter-IMS Network to Network Interface (NNI)*.

The NNI network is normally comprised of dedicated or managed-service-based transit network (IPX) facilities between the IMS networks that can provide acceptable QoS and service guarantees for the signaling and media flows. It is usually understood that the signaling and media plane traffic for a "call" flow together through a selected transit network to facilitate charging. IMS assumes that a global ENUM is in place to facilitate translation of foreign tel URIs, which may be provided by the transit network or through other means.

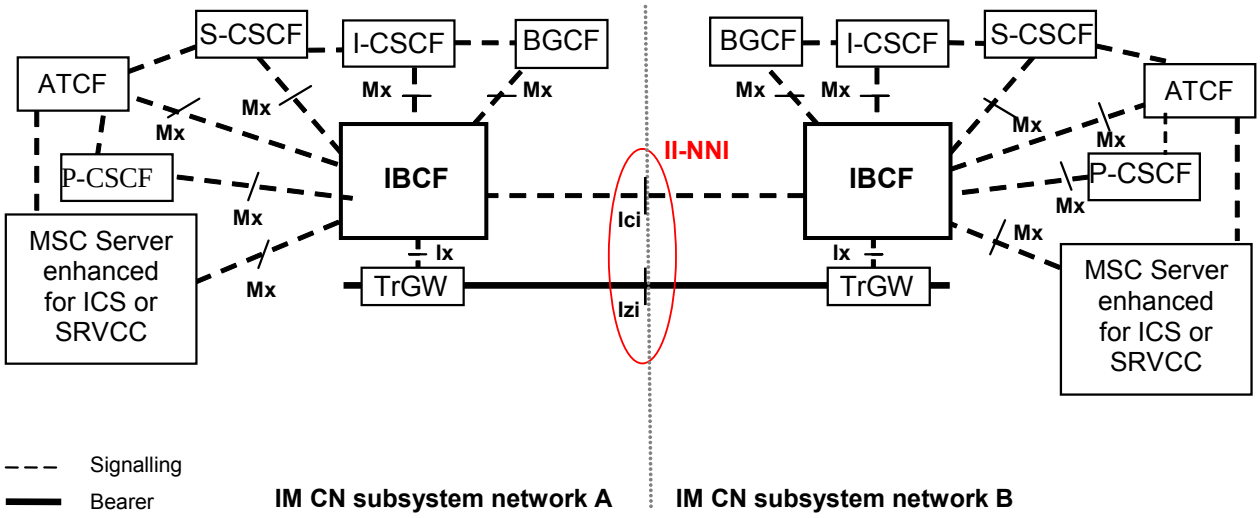

Figure C.4 - Inter-IMS Network to Network Interface between two IM CN subsystem networks

As an example of the most common NNI models, this model shows how the bundling of signaling with media at the point of interconnection is forced by the anchoring of media at TrGWs. The IBCF and TrGW together provide functions similar to the session border controller (SBC) in other models.

C.2.2.2 Interworking between IMS & IP networks

3GPP TS 29.162[46] defines the NNI between an IMS and another IP network. The reference model for interworking between IMS and IP networks is shown in the following figure. There are two sets of protocols associated with the NNI for SIP signaling and media transport. No reference names are assigned since aspects of the interface may need to be customized for each peer network.

In addition to the IBCF and TrGW functions described for the inter-IMS NNI in section C.2.2.1, they have additional responsibilities when interworking with other IP networks. The SIP (or other signaling protocol) profile on the NNI may be SIP-I, XMPP or other SIP profile, TLS, or other means may be used to secure the signaling; various authentication schemes may be used; and the media may use incompatible codecs or security mechanisms. In practice, a network will be able to support connections to only a limited number of non-IMS network types.

The nature of the NNI (transit) network is subject to bilateral agreement between the interconnected networks. The transit network may be dedicated, managed-service-based, or unmanaged (internet) and the signaling and media may traverse independent networks. Whether QoS and service guarantees are available for the signaling and media flows is also subject to bilateral agreement and choice of transit network.

[46] 3GPP TS 29.162, *Interworking between the IM CN subsystem and IP networks*.

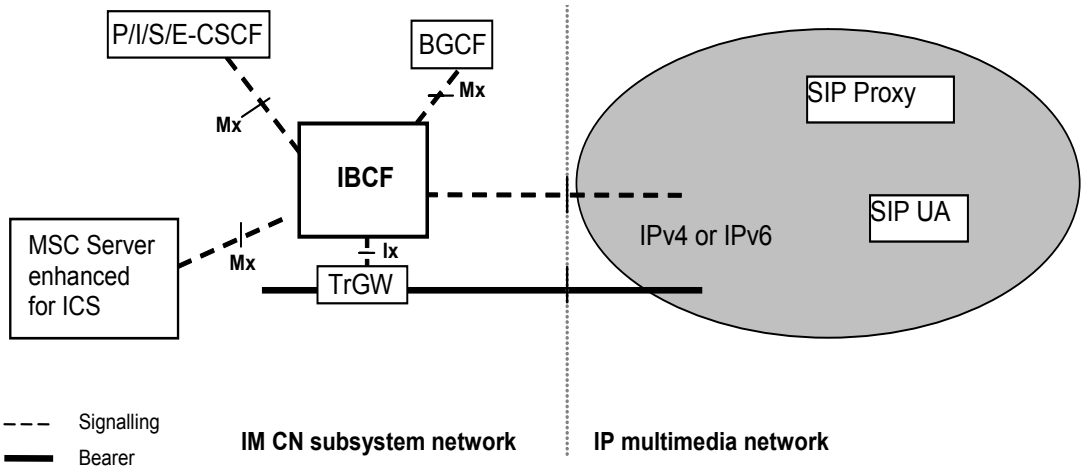

Figure C.5 - Interworking Model for IM CN Subsystem to IP Multimedia Network

C.2.2.3 RAVEL

RAVEL is the name of a study performed during 3GPP Release 11 to investigate solutions for the provision of voice over IMS in roaming scenarios that facilitate the realization of a charging model that replicates the principles of the CS model. The results of the RAVEL study are documented in 3GPP TR 23.850[47]. The resulting stage 2 specification is documented in annex M of 3GPP TS 23.228[48].

The figures below show the two roaming scenarios allowed within a RAVEL-constrained IMS deployment: the “loopback routing” case and the “home routing” case.

The loopback routing case in Figure C.6 modifies the normal IMS signaling flow depicted for the home routing case in Figure C.7 by forcing the signaling from the originating HPLMN back to the originating VPLMN (causing a “loopback” in the signaling flow). The sole purpose of the loopback routing case is to enable the originating VPLMN to control and mediate charging for the call placed to the destination HPLMN, thus duplicating the CS charging model for roaming.

In the loopback routing case, the interconnect between the originating VPLMN and terminating HPLMN follows all of the principles described for inter-IMS interconnect in section C.2.2.1, including the coincidence of the signaling and media in the corresponding transit network. The interconnect between the originating VPLMN and originating HPLMN is special in that only signaling flows are supported. Optimal Media Routing (OMR) procedures are used to avoiding hairpinning media through the originating HPLMN as long as the HPLMN allocates no media resources to a call. Another IMS feature called OSCAR complements RAVEL by enabling the originating HPLMN to allocate and control media resources within the originating VPLMN if necessary.

The home routing case follows standard IMS procedures for routing of signaling between networks with the additional constraint that media is forced to be coincident with signaling through every transit network, thus following the principles described for inter-IMS interconnect in section C.2.2.1 in cases.

[47] 3GPP TR 23.850, *Study on roaming architecture for voice over IP Multimedia Subsystem (IMS) with local breakout*.

[48] 3GPP TS 23.228, *IP Multimedia Subsystem (IMS); Stage 2*.

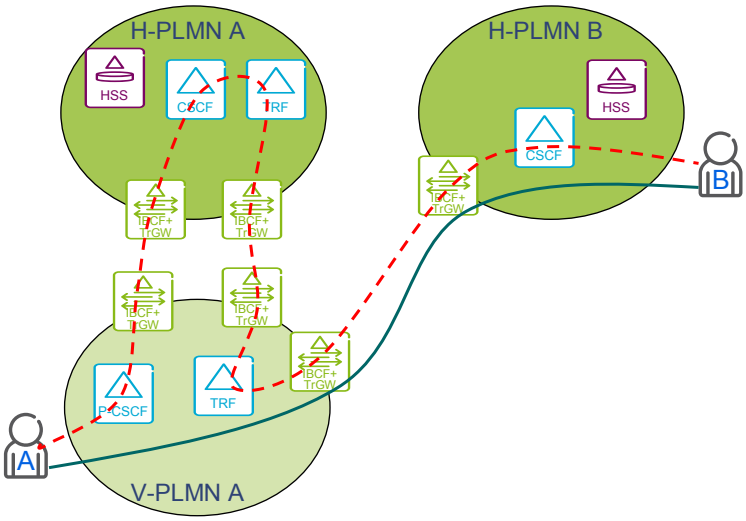

Figure C.6 - Transit routing via VPLMN after successful ENUM/DNS resolution - example use case

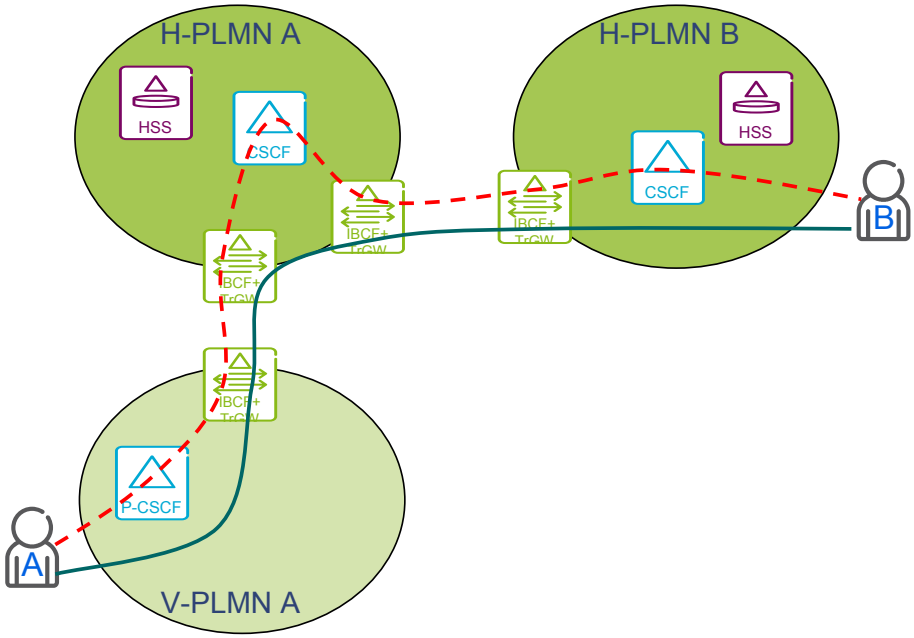

Figure C.7 - Forced home routing - example use case

By allowing IMS to emulate the signaling and media routing policies of the existing circuit-switched domain, RAVEL allows operators to deploy IMS without redesigning business agreements and charging policies to support the more efficient IMS model. There is limited support for RAVEL domestically.

C.2.2.4 OMR

3GPP TS 23.228, Annex Q, defines the stage 2 procedures for Optimal Media Routing (OMR). The stage 3 procedures are documented in 3GPP TS 29.079[49] and 3GPP TS 24.229[50]. The purpose of OMR is to identify and remove unnecessary media functions from the media path for each media stream associated with a session, to minimize end-to-end delay and to minimize the use of transport network resources. OMR also provides for NAT traversal at the access edge, but is not currently defined to interoperate with ICE (an alternative NAT traversal procedure described elsewhere in this document).

OMR applies to IMS deployments based on application level gateways (ALG) in the signaling path that control media gateways acting as media "anchors" in the media path. ALGs are normally deployed on network boundaries such as the IBCF on the NNI (shown in a previous section) and on the UNI in the P-CSCF to provide appropriate address translation and security functions at network borders. The result of the deployment of ALGs that anchor media at all network borders is that the media flows through the exact same sequence of networks as the signaling. There are many cases in which this is suboptimal since more direct media paths are available, for example, directly between the endpoints at the IP level. OMR provides SDP extension attributes to allow ALGs in the signaling path of an IMS session to examine alternative media paths to determine if any media anchor points can be removed to provide more direct media flow between the endpoints.

While the most direct path possible is usually directly between endpoints, there are some cases where this is not possible:

1. Media functions occasionally must be allocated within the network to perform unavoidable functions like transcoding between incompatible codec types, NAT traversal at the access edge, and media level support of conferencing. OMR in particular provides support for optimal transcoder allocation.
2. The available transport networks for direct connectivity may not support the desired level of QoS and service level agreements. ALGs are frequently used to steer the media to the appropriate managed-service-based networks when necessary. This can alternatively be accomplished via IP routing policies and appropriate transport level interconnect agreements, although there may be concerns related to call tracing, service accountability, and charging due to the separation of the media path from the signaling path that generates charging records.
3. Charging for transport of media between networks is typically per call rather than being based on the volume of IP packets with service level guarantees. For networks using this charging policy, it is necessary for media flow through a network to always have accompanying signaling that generates the appropriate charging records. This is a primary reason for the RAVEL features described in the previous section.

OMR can be selectively disabled to help implement operator policy with respect to these constraints. In some cases operators will need to realize compatible policies and OMR procedures, enforced by bilateral agreements, to realize these constraints.

To realize the full benefit of OMR to optimize the use of network resources for each call, operators need to agree to use the bulk transport of media supporting the desired QoS and service level guarantees without the availability of per call charging records.

If WebRTC based clients become important to IMS operators, and since WebRTC requires the use of ICE for NAT traversal, it may be necessary to consider how ICE can interoperate with operators networks based on the use of OMR.

---

[49] 3GPP TS 29.079, *Optimal media routeing within the IP Multimedia Subsystem (IMS); Stage 3*.

[50] 3GPP TS 24.229, *IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*.

C.2.3 i3 Forum Bi-Lateral Interconnect Model

NOTE: Industry practices are continuously evolving and therefore the following models may evolve over time.

C.2.3.1 Bilateral General Reference Architecture

The i3 forum general reference configuration[51] for voice interconnection based on IP protocol is given in the figure below. Service Providers (SPs) operate switching facilities that aggregate VoIP and TDM traffic from their domestic fixed and mobile networks serving their end user customers. The domains of Service Provider A and Service Provider B having VoIP and/or TDM distribution facility networks via wireless and wireline technologies are connected to each other via one or more Carriers. Shown below one can see Carrier A has a business relationship with SP A and Carrier B with SP B. Carrier A & B have a bi-lateral interconnection using signaling and media specifications agreed to under commercial agreement.

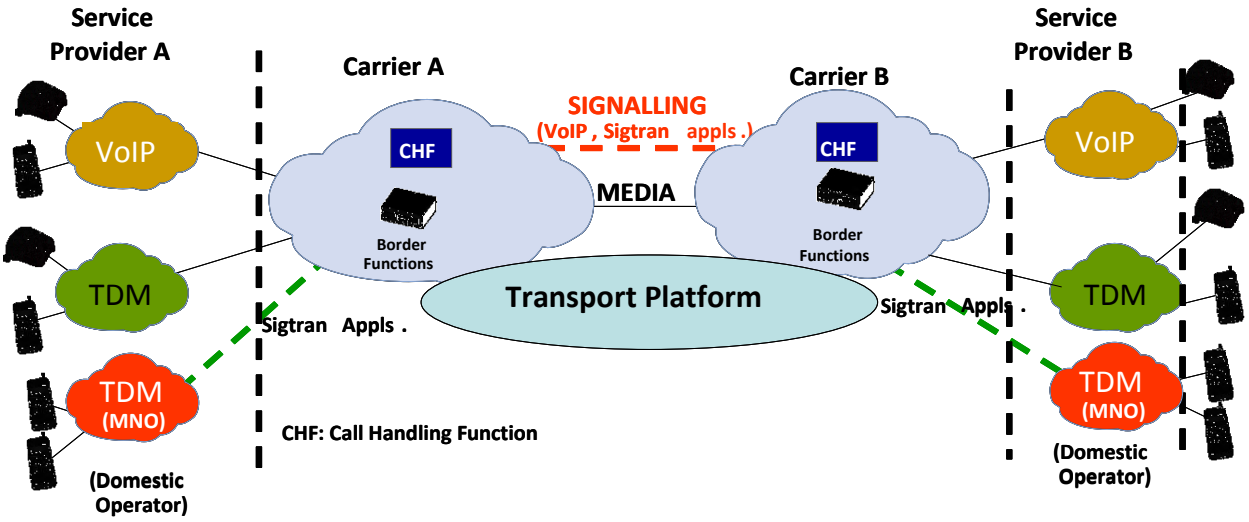

Figure C.8 - General Reference Configuration

The above general reference configuration also supports ISDN services and legacy SS7-based applications.

The carriers are free to connect at location(s) based upon mutual agreement, with the understanding of all terms of the agreement which may include but is not limited to:

1. Location and Means of Interconnection.
2. Technical specification for signaling and media handling.
3. Border Function Security Methods Required – e.g., use of IPSec for signaling if the public internet option is selected.
4. Quality of Service Settings/Parameters for Compliance to Service Level Agreements (SLA).
5. Ordering, Billing, and other BSS/OSS Charging Business Requirements/Contractual Clauses.
6. Payment Calculation, Method, and Amount (per minute or other measurement(s)).
7. Implementation Test, Service Initiation, and Soak timeframes.

[51] i3 Forum, *Technical Interconnect Model for International Voice Services*, Release 5.0, May 2012.

8. Fraud Detection Capabilities and Intercompany Responsibilities/Cooperation/Contacts.
9. Trouble Ticketing, Troubleshooting, and Escalation Process.

For illustrative purposes, a general reference configuration between Carriers is shown in the figure below. Note that SP networks are omitted for simplicity, recognizing the Carrier to SP bilateral commercial agreement is not the primary scope of this document. Although Carriers and SPs will interwork using TDM and IP technologies, the services provided by the Carrier and purchased by the SP will be unique.

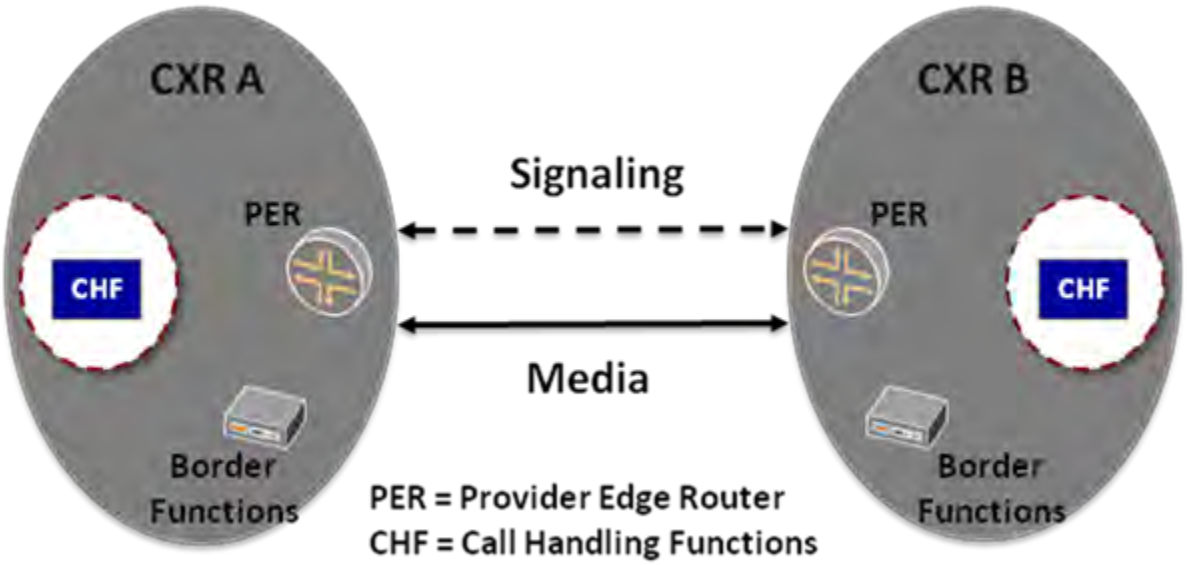

Figure C.9 - General Reference Architecture Between Carriers

Carrier A and B each have Provider Edge Routers (PER), Border Functions (for example, SBC), and Call Handling Functions (CHF) within their domains. Both Signaling and Media are shown to represent the Transport Platform. The business aspects as well as the physical and logical interworking of the transport platform are described in the following sections, for example:

1. Carrier-to-Service Provider (Cxr-SP) Link and Carrier-to-Carrier (Cxr-Cxr Link Nomenclature).
2. Service Reference Configuration (Logical).
3. Bilateral Voice Service Description.
4. Bilateral Sending Party Pays Business Model.
5. Bilateral Attributes and Assumptions for PSTN Replacement Service.
6. Transport Reference Configuration for both Private and Public Interconnection.

Carriers and Service Providers decide how (technically) and where (physically or logically) to interconnect their domains based upon customer and business needs. Given adding additional interconnection locations could involve significant cost it is expected that the financial and service attractiveness will influence when interconnects are viable and mutually beneficial.

C.2.3.2 Access and Network Links – Interconnection Nomenclature

A Cxr-SP “Access Link” refers to the interworking facility arrangement between a serving Carrier and a Service Provider (SP). In the figure below, the Cxr-SP access links are labeled.

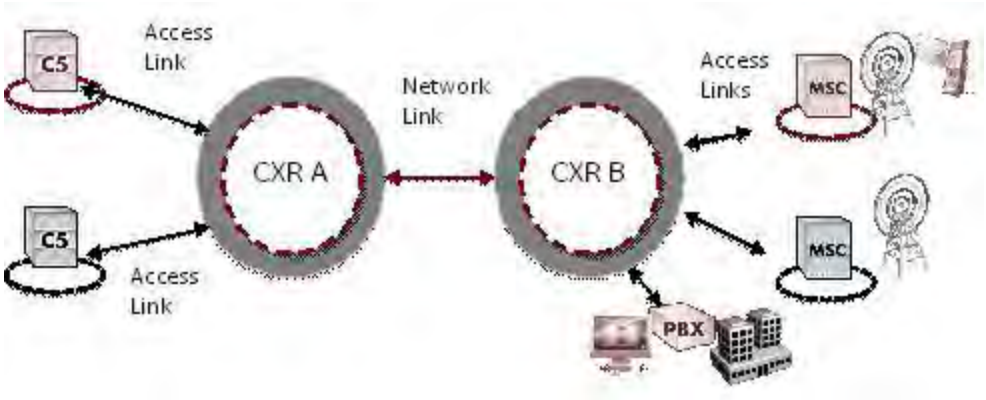

Figure C.10 - Access and Network Links

In the figure above we see that Carrier A and B established a Cxr-Crx "Network Link" to interwork their domains via a physical or virtual facility between the two Carriers. Note that Carriers may also act as and offer services as a SPs (not shown here for simplicity).

Please note, the use of the word "access" here is not to be confused with the usage in Appendix B.

The term Carrier and Service Provider are analogous to the PSTN definitions commonly referred to as the Interexchange Carrier (that carry LEC interstate or interlata traffic), and the retail SP business entity that is allocated telephone numbers for assignment to its customers and resellers.

C.2.3.3 Service Reference Configuration

The i3 Forum Service Reference Configuration[52] is depicted in the figure below. Although logical functions are not easily associated with physical placement in the network, we will reference the figure above for each of the four basic functional blocks in the figure below to assist the reader in understanding possible configurations.

Four basic functional blocks have been identified:

1. The *Call Handling Function* which performs the functions related to signaling management, call routing, control of the Media Gateways, and redirection of signaling and media to the Border Functions. For the sake of consistency with IMS TISPAN[53] terminology, in the Call Handling Function encompasses some capabilities of the functional blocks "Call Session Control Function" (CSCF), the Media Gateway Control Function (MGCF), and the Breakout Gateway Control Function (BGCF). In the figure above, these Call Handling Functions are placed within the trusted part of the Carrier's domain shown for each Carrier as the white oval shape.
2. The *Media Gateway Function (MGF)* which is devoted to the transcoding of the media flow from/to TDM domain and IP domain. In the figure above, the MGF Functions are placed within the un-trusted part of the Carrier's domain shown for each Carrier as the grey ring surrounding the white oval shap.
3. The *Signaling Gateway Function (SGF)* which is devoted to manage the SIGTRAN connections and to interwork SIGTRAN with MTP. In the figure above, the SGF Functions are placed within the un-trusted part of the Carrier's domain shown for each Carrier as the grey ring surrounding the white oval shape.
4. The *Border Function* which is devoted to separate the IP domain of the two carriers in order to implement trusted and secure VoIP interconnections. The border function applies to both the control plane and the user (media) plane. In the figure above, the Border Functions are placed

[52] *Technical Interconnect Model for International Voice Services*.

[53] < http://www.etsi.org/tispan/ >

within the un-trusted part the Carrier's domain shown for each Carrier as the grey ring surrounding the white oval shape. For the sake of consistency with IMS TISPAN terminology, in the figure below:

a. The control plane border function is identified with the Interconnection Border Control Function (IBCF).
b. The user (media) plane border function is identified with I-Border Gateway Function (I-BGF).

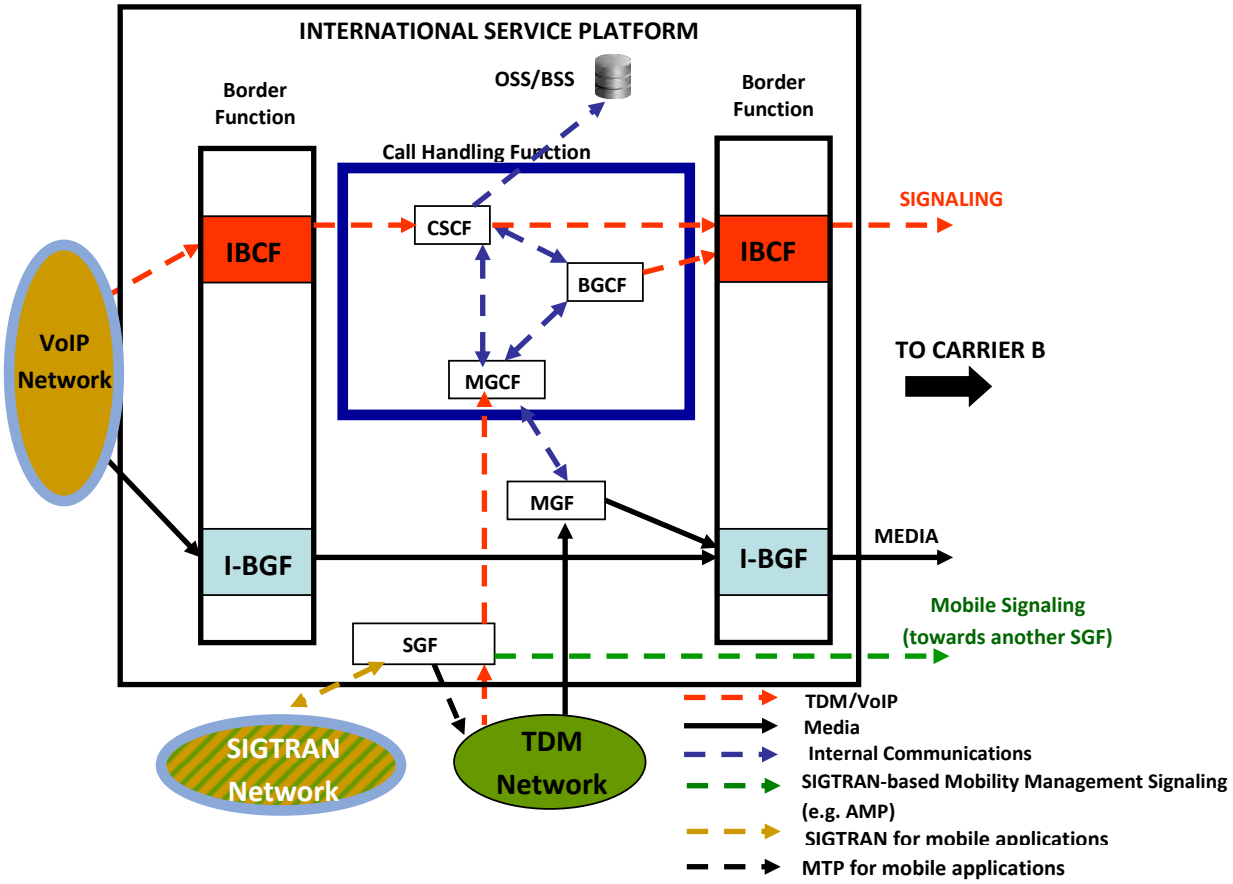

Figure C.11 - Service Reference Configuration

The implementation of integrated Border Function (i.e., co-located IBCF and I-BGF) versus distributed Border Function (i.e., IBCF geographically separated from I-BGF) depends on the specific carrier's implementation.

The IP transport layer can be IPv4 or IPv6; session interworking between separate voice interconnections using different versions of the IP protocols would be accomplished by the Border Functions of each carrier.

C.2.3.4 Bilateral Voice Service Description

The bilateral voice IP interconnect between two Carriers (Cxr-Cxr Network Link) may be provided by the direct interconnect of each Carriers IP domain at a common point – e.g., ColoATL, or via a third party referred to as a Transit Carrier. Another option is for one of the Carriers to build facilities to an agreed-upon location for IP interconnect purposes. Each Carrier also interworks with one or more SPs seeking to originate and/or terminate voice traffic between its own customers and other domestic SPs. These one-to-one relationships are call "bi-lats" or a bilateral agreement between (only) two parties.

The retail bases can be VoIP, TDM, or both. Service Providers can implement dedicated IP connections to Carriers (Cxr-SP Access Links) for a specific type of voice traffic (e.g., mobile traffic only), or use the same Access Link to transport any type of domestic retail traffic: mobile, fixed, TDM or VoIP. It is left to the bilateral negotiations (commercial agreement) between SPs and Carriers to decide on how (technology) and which combination of voice traffic (service) to carry through the Access Link IP interconnection. It is left to the bilateral negotiations between Carriers to decide on how (technology) and where they will implement (Network Link) TDM or IP interconnects to establish a Network-to-Network Interface (NNI).

In the figure below, SP A and D have individual commercial agreements with a common Carrier A specifying terms (location and type) of interconnection. Calls from SP A route to SP D use Carrier A only. Likewise, Carrier B has individual commercial agreements with SP B and C. Calls from SP B route to SP C using Carrier A only. For calls going from SP A or D to SP B or C, the calls would need to route over the bi-lateral established by commercial agreement between Carrier A and B.

SPs may connect via Cxr-SP Access Links to one or more Carriers at multiple locations using TDM and IP interconnect technologies. Carriers may connect via Cxr-Cxr Network Links to one of more Carriers at multiple locations using TDM and IP interconnect technologies. A hybrid of technologies and network topologies are expected to exist based upon customer and business needs and the decision as to when and where to perform a TDM to IP technical substitution is based upon many factors and best left to the decision of SPs and Carriers.

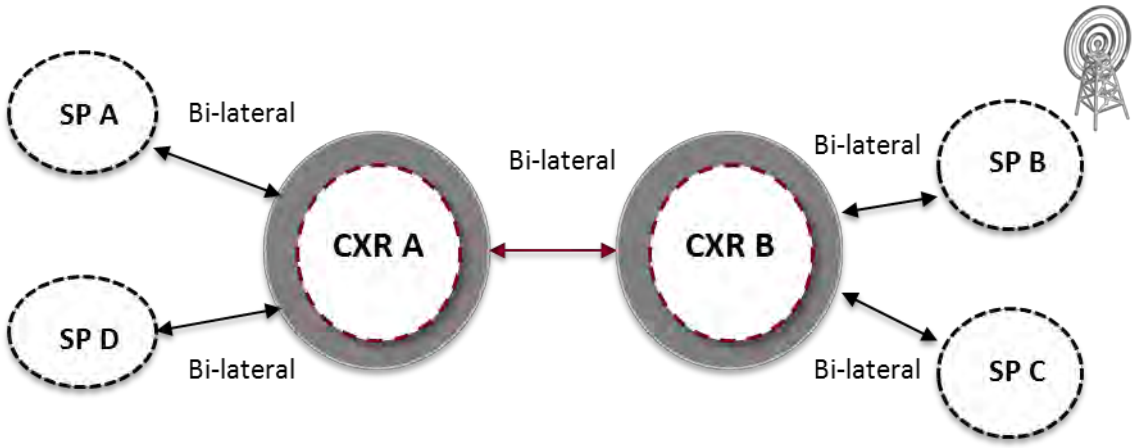

Figure C.12 - One-to-One Individual Bi-lateral Commercial Agreements

C.2.3.5 Bilateral Sending Party Pays Business Model

In order to facilitate and permit an unrestrained migration from TDM to IP of the thousands of existing TDM voice bi-laterals, the existing TDM Sending Party Pays (SSP) business model will remain fully applicable with Voice over IP (VoIP) interconnections. The use of this existing and widely implemented business model for voice bilateral interconnection will eliminate many commercial and billing issues, thereby facilitating migration to IP. However, Carriers and SPs are free to make arrangements under both the existing SPP business model as well as other business arrangements based upon commercial agreement. The approach employed will be decided by the Carriers and SPs during the commercial bilateral negotiation. Functions subject to negotiation include but are not limited to the accounting, billing, and customer service.

IP interworking using the Sending Party Pays business model simplifies the technical substitution process of migrating TDM to IP technology by eliminating many business and billing issues, with the understanding that companies are free to adopt other forms of commercial agreement based upon business and customer needs.

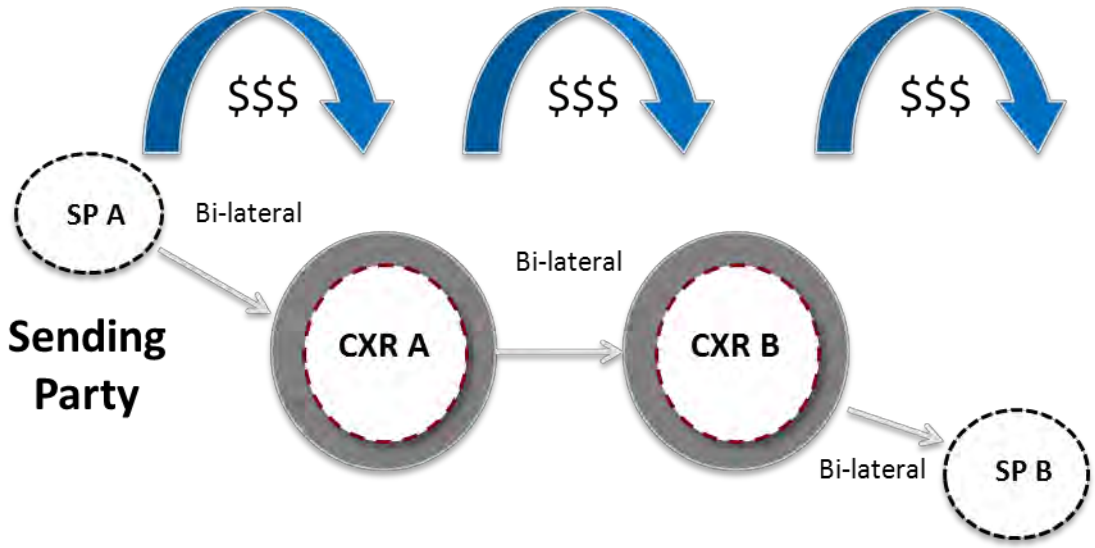

Figure C.13 - Sending Party Pays (SPP) Business Model

C.2.3.6 Bilateral Attributes & Assumptions for PSTN Replacement Service

To be a successful TDM replacement, IP interconnections should provide the same high quality service experienced by customers today when using the TDM technology. For domestic voice, TDM quality traversing a non-internet network interconnecting two SPs is relatively stable. Traffic which traverses the internet is "best effort", given varying infrastructure conditions and traffic priority that may be encountered. Voice quality and services specifications are described here after based on two categories of quality:

- *High quality:* This quality matches the characteristics of the best TDM bilateral interconnections in terms of voice quality, availability, privacy, and security.
- *Best effort quality:* This quality relies on Internet transport services provided by uncontrolled third party networks without any guarantee (SLAs) on the services provided. While in some cases the resulting voice quality could be adequate to implement voice over IP interconnections, this solution is not recommended as the first choice to be used to replace the high and consistent voice services quality found on high quality TDM bi-laterals.

SPs and Carriers can implement technical IP interconnection specifications that provide similar voice quality, availability, privacy and security as TDM interconnects. Although popular interconnect specifications may be documented offering high quality voice over IP (VoIP) interconnection, Carriers and SPs should be free to determine and agree what level of quality meets their business and customer needs.

C.2.3.7 Transport Configurations

The bilateral VoIP interconnect may be achieved using several transport configurations, most of which can be grouped together as either private- or public-oriented interconnection. Public-oriented interconnection allows VoIP traffic to be mixed at the Border Functions (BF) and PER with other IP traffic coming from the public internet, thereby allowing the BF – as well as the provider edge router – to be reached by unidentified third parties. This physical and/or logical exposure to internet traffic by unidentified third parties introduces the opportunity for security and quality risks. With private-oriented interconnection, both the CHF and Border Functions are either logically or physically separated from internet traffic.

The figure below shows the CHF (unlike the Border Functions and the PER) in a separate white oval indicating it is in the "trusted" portion of the Carrier's domain, whereas everything outside of the trusted domain (e.g., border functions) are in the "untrusted" domain given traffic from the internet and other carriers can reach these elements.

In the following subsections three private-oriented scenarios are described, namely via Layer 1 and via Layer 3 – without and with the use of a Transit Carrier.

C.2.3.8 Transport Reference Configuration – Access Link & Network Link

Different transport configurations for SP-to-Carrier and Carrier-to-Carrier exist for the two main categories[54]: Private IP Interconnection and Public IP Interconnection. Different options for each are described below. At the network layer IPv4 or IPv6 may be used and at the transmission layer either Synchronous Digital Hierarchy (SDH) transmission system or Ethernet-based systems are possible solutions.

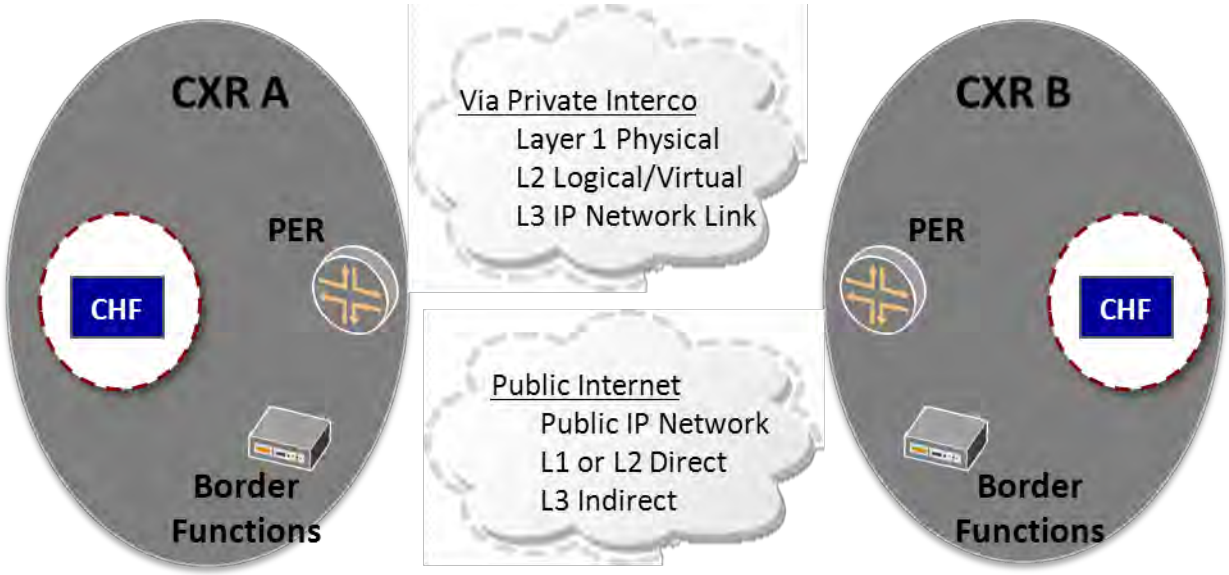

Figure C.14 - Transport Reference Configuration

C.2.3.9 Transport Configurations for Private-Oriented Interconnections

In the following subsections, three private-oriented scenarios are described, namely via Layer 1 and via Layer 3 without and with the use of a Transit Carrier. The Layer 1 physical interface of the interconnection can be either Dense Wavelength Division Multiplexing-based (DWDM-based or Plesiochronous Digital Hierarchy-based (PDH-based), Synchronous Digital Hierarchy Packet Over SDH/Sonet-based (SDH POS – based) or Ethernet-based (i.e., fast-Ethernet, gigabit-Ethernet or 10 gigabit-Ethernet).

In order to be a *"managed" private interconnection*, only voice packets (and no other internet traffic) are exchanged across the interconnection. Although the IP addresses involved can be private or public, they shall not be announced onto or reachable from the Public Internet. Managed-service-based private IP networks provide transport, control, security (i.e., isolated from the Internet), and service layers with controlled and monitored levels of quality and security.

> NOTE about Security: The VoIP traffic from the PE router to the Border Function in a carrier's domain shall be secured either physically or logically from Internet traffic. Security can be achieved physically by implementing separated and dedicated networks for the two types of traffic or logically by implementing mechanisms such as Virtual Private Networks (either layer 2 – e.g., VLANs – or layer 3 – e.g., MPLS-VPN) and tunneling (e.g., IP Sec).
>
> NOTE about Quality: The Carriers are responsible to handle the VOIP traffic (along the voice path) as agreed to ensure security and voice prioritization. Dedicated IP connections or *direct IP links* provide

[54] *Technical Interconnect Model for International Voice Services*.

transport with monitored levels of quality and security, allowing carriers to control the final voice quality characteristics to match those of the TDM environment.

C.2.3.9.1 Private & Dedicated IP link

The figure below describes four scenarios: one for each Layer 1 and Layer 2, and two for Layer 3 (owned and leased IP Link). Carriers can establish a bilateral interconnect implementing a dedicated (and direct) physical (Layer 1) connection between itself and an SP (Access Link), or with another Carrier (Network Link). This L1 interconnect can also be accomplished via a local loop or a leased line. A private interconnect can be implemented as a logical/virtual (Layer 2) link as well as a Layer 3 link (using owned or a third party's private IP network acting as a Transit Service Provider).

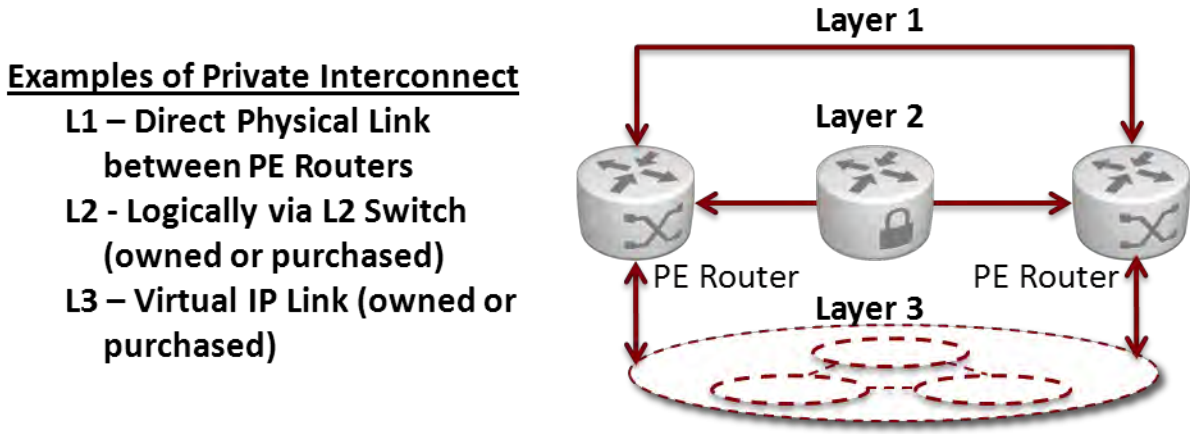

Figure C.15 - IP Interconnect Links – Private (Managed and Controlled)

The number of parties and the virtual and physical layers of interconnection involved will vary and although popular scenarios should be documented, parties are free to base their (Access and Network Link) interconnect method upon customer and business needs through commercial agreement.

C.2.3.10 Transport Configurations for Public-Oriented Interconnection

The figure below conveys examples of public interconnection, which includes two public-oriented scenarios of interconnection denoted Direct and Indirect. In order to retain the public interconnection feature, it is assumed that some IP addresses to be used in these configurations can be reached from unidentified third-parties via the Public Internet.

C.2.3.10.1 Via Public IP Networks

Carriers can establish a bilateral interconnection [both for Network (Cxr-Cxr) or Access (Cxr-SP) Links] via public IP networks or Internet. Based on this interconnection scheme, a range of network and voice performance, reliability, and reporting can be offered, depending on the type of public IP interconnection that is implemented. Two types of Layer 3 public IP interconnection are "direct" and "indirect". Direct uses public IP network(s) "controlled and managed by the Carriers implementing the bilateral interconnect". The form of public interconnect "indirect" uses public networks that are "not controlled nor managed by the carriers implementing the bilateral" interconnection (i.e., using third party Internet networks) which carry open internet traffic (voice and data packets). For Indirect interconnection, voice performance and reliability is "best effort" given the interconnecting parties have no management and control capabilities over the public internet portions provided by other entities.

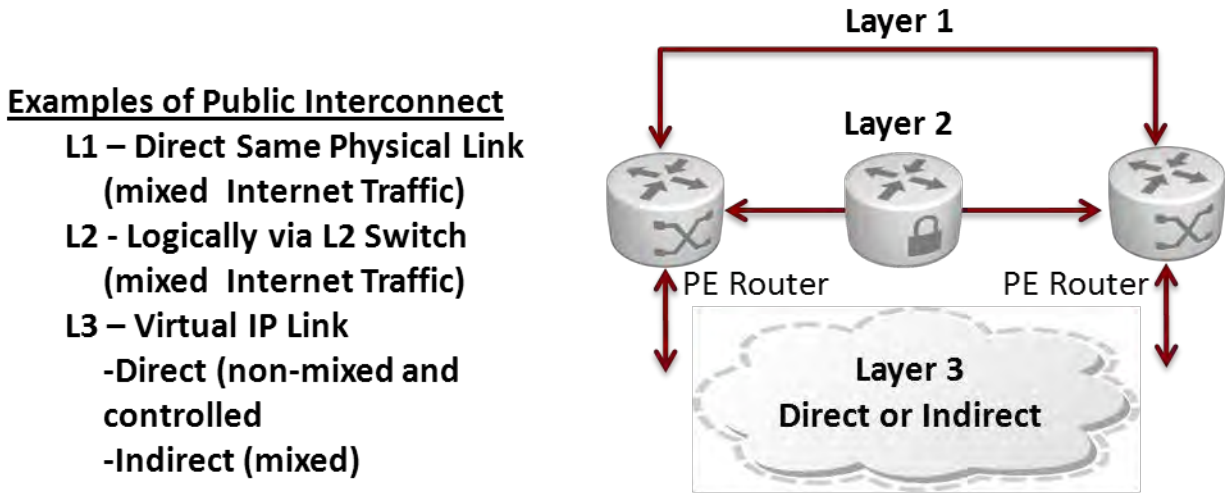

Figure C.16 - Examples of Public Interconnection

C.2.3.10.2 Via Layer 1/Layer 2 Interconnection Sharing Public Internet Traffic and VoIP

In this configuration, Internet traffic as well as VoIP traffic is exchanged either over the same physical link or via a Layer 2 switch. In both cases, logical Layer 2 traffic separation can be used by configuring VLAN based on the IEEE 802.1q standard[55]. QoS mechanisms (e.g., DiffServ) may be used to control and guarantee to some extent VoIP traffic performance over the interconnection. The IP addresses of the involved PE routers interfaces are public and can be announced over the Public Internet. Border Function IP addresses shall be exchanged only between the interconnecting parties using the no-export BGP community attribute or static routing.

C.2.3.10.3 Via *Indirect* Interconnection via the Public Internet

In this configuration, the VoIP traffic passes through the Public Internet – i.e., through a third (or multiple) Internet Transit Service Providers. The IP addresses of the PE Routers, as well as those of the Border Functions, are public and announced over and reachable from the Public Internet. Both Carrier and SP/Enterprise customer including all intermediary Transit Service Providers will be required to use the same version of the IP protocol, IPv4 or IPv6, for this logical interconnection. This configuration includes the case where PE routers are interconnected via an IPSec tunnel over the Public Internet. QoS mechanisms to deliver high quality TDM-like voice (quality, security, and availability) over the interconnection are not available due to the nature of an “indirect” and “public internet”.

C.2.3.10.4 Via *Direct* (Controlled and Managed) Public IP Networks

Within this solution, voice packets are transmitted onto public IP networks which are controlled and managed by the two parties establishing the voice bilateral NNI interconnection. Based on this method, adequate levels of network performance, reliability, and reporting can be controlled and offered to provide high voice quality voice service matching the TDM quality (expectations for QoE using QoS specifications). Note that the voice packets will always be routed to go directly between the Carrier’s IP network and the other Carrier/SPs IP network, without using any uncontrolled Internet network. In case of network congestion, voice packets might be prioritized over other Internet traffic, and both IP networks and the IP connection(s) between them should target high quality voice QoS with supporting SLAs.

[55] IEEE documents are available from the Institute of Electrical and Electronics Engineers (IEEE).
< http://shop.ieee.org/store/ >

C.2.3.10.5 Via *Indirect* Third Party Internet Networks

With this solution, voice packets are transported over the public Internet without any control from the bilateral carriers, neither on the routing nor on the quality of the transport given one or more uncontrolled third-parties are involved with the employed Internet networks. Based on this method, levels of network performance, reliability, security, and reporting can be offered only with a "best effort" quality, which at times can fluctuate and cannot be guaranteed to be sufficient to provide the high voice quality comparable to the one that is available in TDM.

Not all forms of Public (Internet) Oriented interconnection provide a comparable voice quality and security, and although SPs are free to purchase interconnection from a broad number of Carriers, both SPs and Carriers are free to determine what level of quality and security is necessary (to buy or offer) for their business and/or customer needs.

C.2.4 I3 Forum Implementation Practices of the GSMA IPX Model

Industry practices are continuously evolving and therefore the following models may evolve over time.

C.2.4.1 The Internet Protocol eXchange (IPX) Model

A solution requiring non-public interworking at the Network Link is a "managed private interconnection" for which two types are permitted; namely, the service unaware "transport only" service, and the service aware "transit service". All specifications endorsed by the i3 Forum and the GSMA must be respected for a service to be considered an "IPX". The transport only service is limited to the transport layer, whereas the service aware transit service option is defined by specific parts which include interface capabilities, protocol characteristics, and operational and commercial functionalities. Generally, the IPX key characteristics include Quality of Service (QoS), Transparency, Security, and Billing/Payment flexibility. These key characteristics are reflected in the Technical (network) Operational (processes) and Business (commercial) attributes, which (if achieved), only then constitutes a true IPX offering specified by the i3 Forum and the GSM Association. This Section summarizes the IPX model as described in the i3 Forum document *Technical Specification for Voice over IPX Service*, Release 3.0, May 2012.[56]

Specific key IPX characteristics reflected in the Technical (network) Operational (processes) and Business (commercial) attributes, if achieved, only then constitutes a true IPX offering specified by the i3 Forum and the GSM Association.

C.2.4.1.1 General IPX Reference Configuration for Voice Services

The general IPX reference configuration shown in the figure below reflects the architecture specific to a commercial and technical construct that embodies the design principals governing implementation of an IPX offering for Voice Services, with only two IPX Providers depicted.

[56] < http://i3forum.org/wp-content/uploads/2012/05/i3F-Technical-VoIPX-Release-3-FINAL-2012-5-3.pdf >

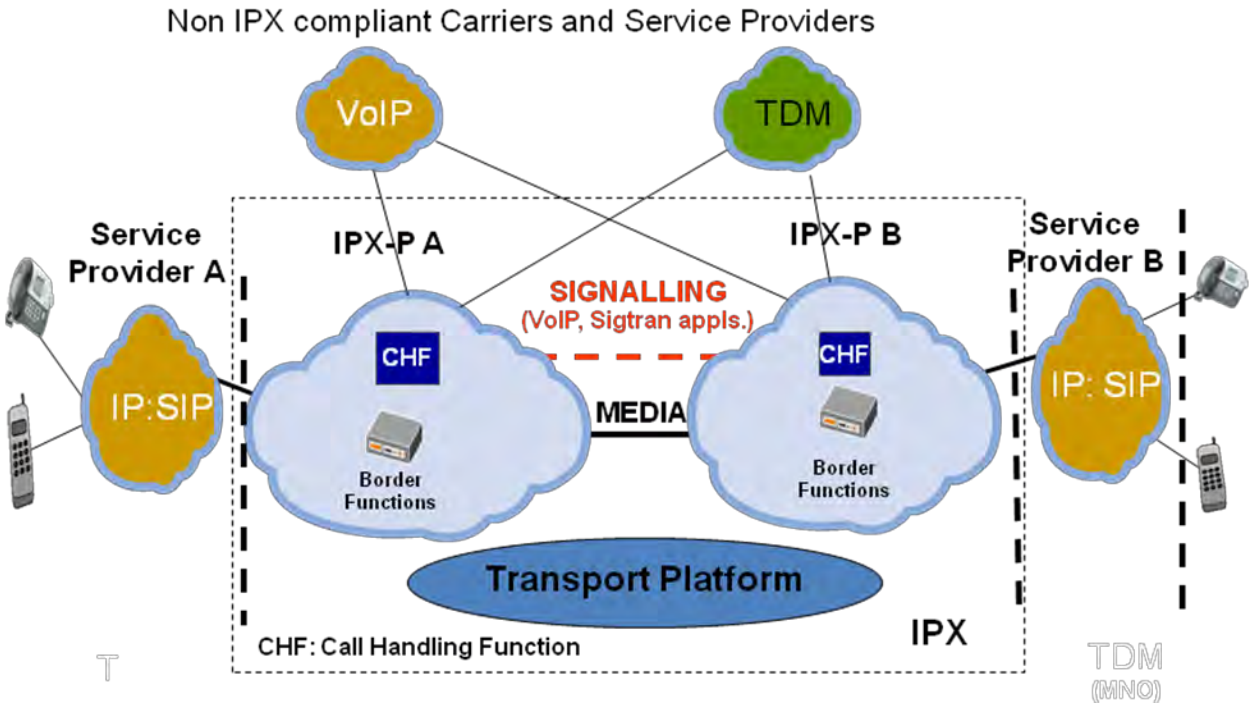

Figure C.17 - General IPX Reference Configuration for Voice Services

The IPX Provider (IPX-P) offers to a customer Service Provider (SP) having its own end users via fixed and/or wireless access technologies the ability to employ one IPX P-SP link (access link) connection for voice and multiple (optional and commercially negotiated) services. Outbound traffic is sent by the Customer SP and routed via the access link through the IPX-P network to another Customer SP, or possibly through another IPX-P to reach the target (and terminating) Customer SP. The Customer SP sending the traffic onto the IPX via its designated IPX-P is not obligated to receive traffic via the same IPX-P. Note that more than two IPX-P's may be involved in one path as long as requirements are maintained (e.g., QoS) and the Customer SP being provide the IPX service is aware of the need to utilize 2+ IPX-Ps for that particular destination.

The IPX P-SP Access Link interface between the IPX-P and the SP purchasing IPX features may be public with encryption or private. The Network exchange of traffic over the IPX-P NNI is wholly private, physically and virtually. In instances where traffic is only terminated by an IPX-P to an SP, this SP is not an IPX Customer. Traffic which routes entirely from one SP to another by traversing only one IPX-P is called "on-net" whereas traffic requiring two or more IPX-P's is called "off-net" routing.

The ability to employ one (access link) connection from the SP to an IPX Provider (IPX-P) for additional services beyond voice is a commercially available option, but is not mandatory to provider PSTN-like voice services.

The IPX IPX P-IPX P "network link" must be a non-public interconnect; however, the IPX P-SP "access link" may be public with encryption or private interconnection.

C.2.4.1.2 IPX Reference Technical Architecture

The commercial relationship in the form of a technical IPX Provider (IPX-P) network interconnection is referred to as the IPX-P NNI. IPX Customer SPs originate traffic destine for SPs reachable by the same IPX-P or via other IPX-Ps having among themselves commercial agreements and technical interconnect IPX-P NNIs. (See Figure C.18 below.) IPX Providers can connect to non-compliant Carriers or non-compliant Service Providers with the intent to either send traffic (break-out) to destinations not reachable via the IPX, or to accept traffic to be terminated on an IPX compliant Service Provider (break-in). Break

In/Out guidelines are very specific and as of this writing remain the focus of discussion between the i3 Forum and the GSMA.

Destinations will remain reachable only via TDM for some considerable time. Not allowing TDM and IP break-in/break-out would exclude many destinations from a direct communication via the IPX domain, and FNO/MNOs would have to keep TDM interconnects operational in parallel to IPX-based interconnects in order to have access to these IPX Providers.

C.2.4.1.3 Geographic Scope of IPX End-to-End Interconnection

The end-to-end interconnection responsibility is defined from egress port of the interconnecting element of the originating Service Provider network towards its own IPX Provider, to the ingress port of the interconnecting element of the terminating Service Provide. In this context, end-to-end corresponds to the above definition "from Service Provider premises to Service Provider premises"[57] and is defined by the dotted lines within the IPX boundary in Figure C.17 above.

The term "End-to-End" includes the IPX Provider domain(s) (including all network links), up to but not including the access link interface at the customer SP domain, given IPX-Ps cannot measure nor can they guarantee performance in the SP domain.

C.2.4.1.4 IPX Common Features

The IPX is isolated from the Internet and there are no IP addresses within the IPX domain reachable from any entity outside of the IPX domain. IPX-Ps can establish direct interconnects and shared interconnects in private or public locations, such as ColoATL at 55 Marietta Street. Note that Access Link connections to the IPX domain via an IPX-P can be a Layer 1 physical connection, a Layer 2 logical connection, or a Layer 3 private IP VPN connection via a third-party. Alternatively, a Customer SP may interconnect to its IPX-P via shared interconnections in public locations, usually owned by a third party for use by multiple IPX-Ps and SPs. Being an IPX domain separated by definition from the Public Internet, also in the case of shared interconnection at public locations, the involved IP addresses are not advertised onto the Internet.

The IPX is isolated from the internet and there are no IP addresses within the IPX domain reachable from any entity outside of the IPX domain.

C.2.4.1.5 Architecture of the IPX Domain for Voice Services

The figure below provides an overall sketch of the IPX domain together with compliant Service Providers and Non-Compliant Service Providers and Carriers.

Compliant Service Providers (to the left and right of the IPX Domain) generate IP traffic towards IPX providers. Each compliant SP can interconnect to one or more IPX Providers.

For each Access Link and Network Link interface there is a commercial agreement. A bi-lateral agreement covers the one-to-one exchange of traffic whereas an IPX-SP agreement covering multiple locations is referred to a "multi-lateral interconnection agreement".

IPX Providers can implement both direct (i.e., bilateral) interconnections and shared (i.e., multilateral) interconnections. A shared multilateral interconnection can be implemented in private and/or public locations where IPX Providers can meet.[58]

Although both IPX complaint and IPX non-compliant SPs can exchange traffic via an IPX Provider, the principles of routing transparency require the disclosure of break-in and break-out routes to each IPX compliant SP.

---

[57] *Technical Specification for Voice over IPX Service*.

[58] *Technical Specification for Voice over IPX Service*.

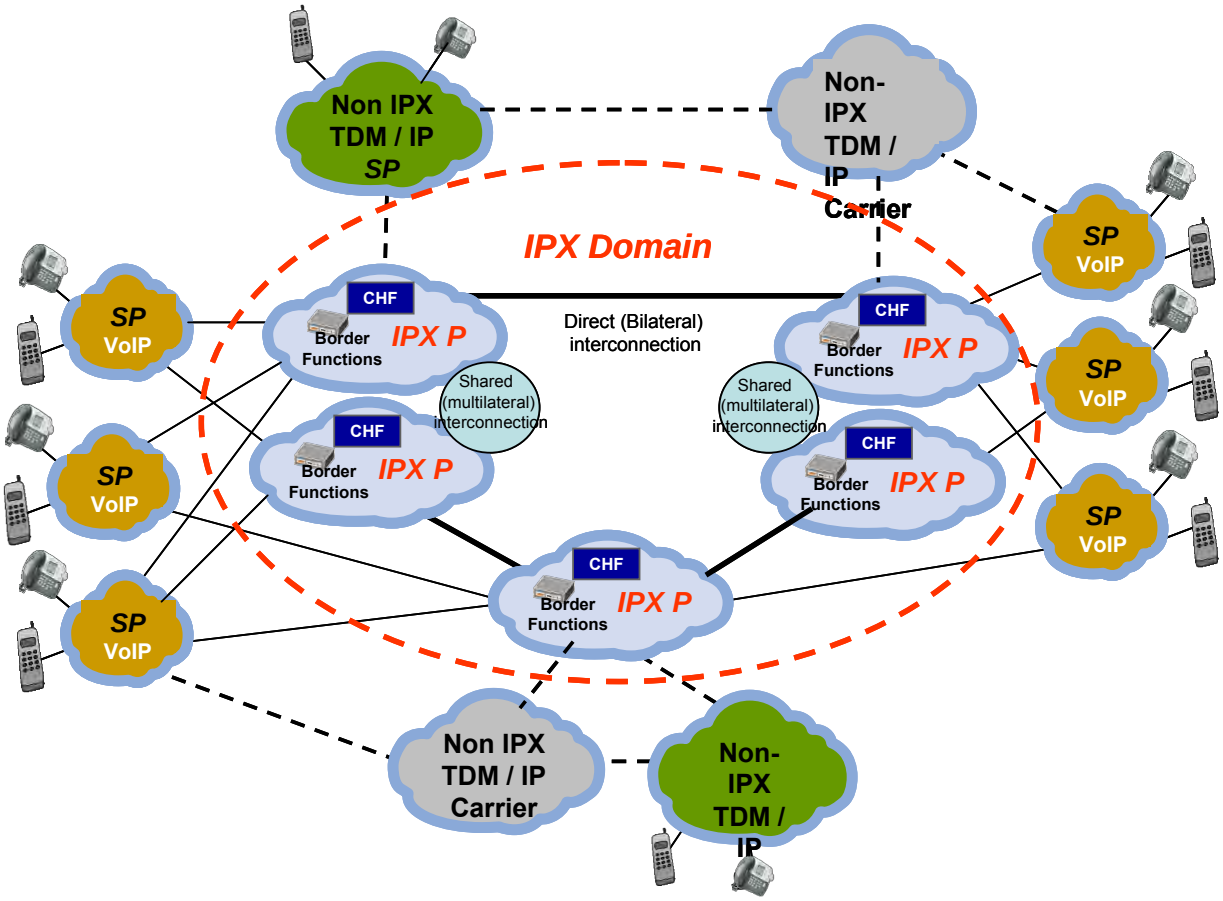

Figure C.18 - Example of IPX Domain

C.2.4.1.6 Computation of Service Level Agreement (SLA) Metrics

If only one IPX-P is involved in the end-to-end voice service, then that one IPX-P under commercial agreement is responsible to provide the customer SP with performance reports. Likewise, it is the responsibility of the IPX-P from which traffic is received directly from a Customer SP that is wholly responsible to aggregate each IPX-Ps performance data in the chain with that of other IPX-P provider data where more than one IPX-P provider is required to transmit traffic end-to-end. In other words, it is the serving IPX-P which commits to the IPX Customer SP the performance metrics for the services from IPX-P edge to IPX-P edge up to the border element facing the SPs.

It is the serving IPX-P which commits to the IPX Customer SP the performance metrics for voice services from IPX-P edge to IPX-P edge up to the border element facing the SP.

C.2.4.1.7 Cascading Method for Transport KPIs

If an SP customer raises a problem and requests information, it is the responsibility of this Customer SP to open a trouble ticket with its IPX-P. The IPX-P and the SP customer will then work together to verify if there is an end-to-end QoS fault. For instance, SP-A can open a trouble ticket to IPX-P X and complain that the commitment has been violated. In such a case, IPX-P X will start troubleshooting within its own network domain and with IPX-P Y if additional IPX-Ps are in the end-to-end voice service chain. Each IPX-P must at least offer this QoS cascading method. If the problem is proven, and if its duration until repair is above the limits set in the SLAs, then the IPX-P serving the customer must pay to the customer SP the penalties negotiated in each SLA. Likewise, if another IPX-P other than the IPX-P serving the customer SP (e.g., IPX-P Y) is at fault, then IPX-P Y must pay to IPX-P X the penalties negotiated in the SLA between IPX-P X and IPX-P Y.

Frequent monitoring (e.g., monthly) of QoS and SLA values experienced in all IPX domains is the responsibility of IPX-P X for reporting to the Customer SP based upon commercial agreement.

QoS Monitoring, Troubleshooting, Reporting, and payment of Penalties due to the Customer SP are the responsibility of the serving IPX Provider based upon negotiated commercial agreement commercial.

C.2.4.1.8 IPX-P – SP Commercial Construct

The SP can contract with and directly connect to multiple IPX-Ps to complete end-to-end (SP to SP, not user to user) voice path. In addition, the connected IPX-P that handles a particular call is only allowed to interconnect through at most one other IPX-P to establish the end-to-end (SP to SP) connection. An end user cannot directly contract with or connect to an IPX-P.

Each IPX-P can define for itself which products it will offer and may bundle services or groups of services so long as said offers IPX products in a way that complies with i3 Forum and GSMA requirements.

With limited exceptions made known to the customer SP, no more than two IPX-Ps can be in the end to end voice path.

C.2.4.1.9 Multilateral Hubbing

An SP can engage in a single agreement with an IPX-P, that in turn can directly reach other SPs – or indirectly via other IPX-Ps – by having agreements with one or more other IPX-Ps. This “hubbing” feature offered by IPX-Ps allows the SP to select multiple target SPs using only one interconnection agreement, to reach multiple SPs to which it wants to send traffic. As long as the traffic remains within the confines of the IPX domain, it is up to the IPX-P to determine the traffic path and the pricing to each destination.

Multilateral Hubbing feature allows IPX-Ps to offer the SP a single connection and commercial agreement to reach multiple SPs.

C.2.4.2 Other IPX Business Constructs

The IPX-Ps will agree upon in-service dates, trouble ticketing, Network Operations Center (NOC) contacts, escalation procedures, as well as the process for reporting/responding to performance issues and/or complaints. Likewise, dedicated contacts for technical, operational, business, and delivery issues will be identified in advance.

The relationship business model employed by the IPX-Ps for the IPX-P NNI is commercially negotiated. Two common IPX-P to IPX-P billing arrangements recognized by the i3 Forum and GSMA include “sending party pays” and “capacity charging”, respectively. Capacity charging is a GRX principle for “charging for volume of transmitted traffic”. As of this writing, the i3 Forum and GSMA are discussing these options, along with other principles for an IPX-Ps obligation to unbundle transit and termination pricing.

The IPX-P NNI interconnection agreement is negotiated under commercial agreement, with both the “sending party pays” and “charging for volume of transmitted traffic” being the most popular approaches.

C.2.4.3 Voice Over the IPX (VoIPX)

Voice over the IPX (VoIPX) is a specific subset of the IPX domain devoted to managed voice services in terms of interfaces, features, and capabilities including security, cascade billing, QoS accountability, and IPX-P/SP responsibility. The IPX domain includes all IPX-P networks and their interconnections in compliance with the i3 Forum Specification and the GSMA IPX model.

Service specific features for “voice” include the configuration and management features for the service. Features which are not required under the i3 Forum/GSMA IPX model are optional and may be different for the product offerings of the various IPX-Ps. Operational and technical implementation specifications represent solutions of issues addressed by the i3 Forum and the GSMA. These specifications involve both the interface between IPX-Ps and the Customer SPs.

Specifications include signaling with the support of SIP-I specified by ITU, and SIP specified by IETF signaling protocols, media codecs and features, security with support provided by border functions, Quality of Service (QoS) control and monitoring, and Service Routing (break in/out; number portability).

The GSMA model and I3 Forum Implementation Guidelines are stable, but are still evolving due to the discovery of new issues as early adopters begin to implement the IPX.

SIP and SIP-I are endorsed by the i3 Forum, with GSMA still considering whether SIP could be used for an alternative signaling solution.

C.2.4.3.1 Voice Commercial Framework

Voice services as a bi-lateral or multi-lateral hubbing service are expected to be the most common connectivity models. The business model is based on sending party pays and the charges are per minute per destination, but this does not preclude IPX-Ps from offering other commercial arrangements. Unlike the GSMA model, the i3 Forum proposes that termination and transit fees need not be segregated by the IPX-P for presentation to the Customer SP unless commercially negotiated. Under the GSMA IPX model, FNOs, MNOs, ISPs, and ASPs may have a commercial agreement among themselves and with their IPX-P. In all cases, IPX-Ps must be part of the negotiated service since they are the carriers forming the IPX domain.

Voice services as a bi-lateral or multi-lateral hubbing service are expected to be the most common connectivity models. The business model is based on sending party pays and the charges are per minute per destination, but this does not preclude IPX-Ps from offering other commercial arrangements.

C.2.4.3.2 Voice IPX Proxy

The VoIPX proxy functions are generally defined by i3Forum in section 5.3 of the "Technical Specification for Voice over IPX Service". The IPX proxy is a conceptual network element described in GSMA IR.34 Annex B[59]. Inside one IPX Provider's network, the IPX Proxy consists of all equipment and functions from the ingress Border Function (e.g., Session Border Controller, SBC) up to and inclusive of the egress Border Function. This includes the Call Handling Function, as well as also other functions (e.g., media or signaling protocol conversion, or IPv4/v6 translation, if required). The network between IPX Provider Edge routers and Border Functions are not part of the IPX Proxy.

Analysis of the VoIP Proxy Functions warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.3 VoIPX Common Transport Functions

The common transport functions are fully defined by i3Forum in section 6 of the "Technical Specification for Voice over IPX Service". The Voice over IPX specification by the i3 Forum for the transport functions include the internet protocol versions, physical interconnection alternatives, dimensioning requirements (packetization/Bandwidth for each codec), IP routing and addressing, IP packet marking by traffic type (media/signaling), and VLAN configuration.

Analysis of the VoIPX Common Transport Functions warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.4 VoIPX Signaling Functions

The VoIPX Signaling functions are fully defined by i3Forum in section 7 of the "Technical Specification for Voice over IPX Service". The signaling functions between IPX-Ps and their SPs may be SIP and SIP-I as specified by IETF RFC 3261 and ITU-T Rec. Q.1912.5, respectively. UDP is the default transport protocol for SIP and SIP-I.

---

[59] < http://www.gsma.com/technicalprojects/wp-content/uploads/2012/05/ir3449.pdf >

The i3 Forum is studying other protocols given voice over LTE services and the introduction of IMS (Integrated Multimedia System) will require the adoption of additional signaling systems – i.e., 3GPP TS 29.165 “Inter IMS Network to Network Interface”.

Analysis of the VoIPX Signaling Functions warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.5 VoIPX Media Functions

The VoIPX Media functions are fully defined by i3Forum in section 8 of the *Technical Specification for Voice over IPX Service*. Media functions supported include voice calls using different (mandatory and optional) codecs, DTMF support, Fax connections, and Modem connections. For voice calls, RTP and UDP protocols are used for real time media and at the transport layer, respectively. Both narrowband (e.g., G.711) and wideband (e.g., G.722) codecs are supported.

Table C.1 - Mandatory and Optional Narrow Band Codecs for Voice

Group 1. Mandatory Narrow band codecs	Group 2. Optional Narrow band codecs
G.711 A-law, μ-law 64 kbit/s	AMR-NB
G.729, G.729a, G.729b, G.729ab 8kbit/s	

Table C.2 - Mandatory and Optional Wideband Codecs for Voice

Group 1. Mandatory Wideband codecs (*)	Group 2. Optional Wideband codecs
G.722 (generally used by fixed network operators)	
AMR-WB (generally used by mobile network operators)	

The following general guidelines aim to provide default rules for codec choice and transcoding responsibility:

- Transcoding should be avoided whenever possible, due to the impact on speech quality and delay;
- The order of codec/packetization period preference is determined by the originating terminal, and should be honored wherever possible;
- If a G.711 encoded call is to be routed across the borders of either North America or Japan, then G.711 A-law/μ-law conversion is necessary and this companding conversion will be done by the IPX Provider/international carrier in the countries using the μ-law;
- If the call is to be routed to a TDM network, only one transcoding is recommended. If required, it should be performed during the voice over IP/TDM conversion;
- In case no common codec can be used between both end Service Providers, in the first instance it is the responsibility of Service Providers to support transcoding in order to ensure successful voice interoperability for their services;
- In the case of fixed-mobile interconnection, transcoding, if necessary, should always be performed by mobile service providers.

Analysis of the VoIPX Media Functions warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.6 Fax Over IP Functions

The Fax over IP functions are fully defined by i3Forum in section 8.6 of the *Specification for Voice over IPX Service*. Across the IPX domain, the ITU T.38 standard is implemented using implementation

guidelines are fully defined in the "*Specification for Voice over IPX Service*, which employs IFT protocol for T.30 media, UDPTL (Facsimile UDP Transport Layer), and UDP protocol in transport layer.

Analysis of the Fax over IP Functions warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.7 Modem Connections Functions

The Modem connection functions are fully defined by i3Forum in section 8.7 of the *Specification for Voice over IPX Service*.

To enable modem connections with IP in the middle the Voice Band Data (VBD) mode, as defined in ITU-T V.152, section 6, will be used with: G.711 A-law or μ-law codec, with the addition that it is also possible to use dynamic payload instead of static in SDP negotiation; RTP as the media protocol; UDP as the transport protocol; with VBD mode negotiated during call setup phase. Call discrimination procedure in case of modem TDM–IP–TDM connection should be performed according to V.150.1, Section 20. Interworking procedure between T.38 and V.150.1 should be as in T.38, Annex F.

Analysis of the Modem Connection Functions warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.8 VoIPX Security Functions

Security requirements are fully defined by i3 Forum in section 10 of the *Specification for Voice over IPX Service* and in i3 Forum "Technical White Paper on Security for IP Interconnection", Release 1.0, May 2011.[60]

Analysis of the VoIPX Security Functions warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.9 Voice over the IPX QoS Monitoring & KPIs

The VoIPX QoS Monitoring and KPIs are fully defined by i3Forum section 11 of "the *Specification for Voice over IPX Service*. The following KPIs at the Service Layer apply: ASR, NER, ALOC, PGRD, and MOSCQE/R-factor. The corresponding definitions and calculation methodologies may be found in the i3 Forum "Technical Interconnection Model, Release 5.0, May 2012.[61]

The path followed by the voice media and voice signaling may be different from the path followed at the IP layer using the OSPF/BGP routing protocols. Given this measuring, the IP parameters as an indication of QoS can yield misleading results. As a result, it is incumbent upon IPX-Ps to measure IP layer parameters using the various segments covered by the RTP packet in its own domain. Each IPX-P's results may then be aggregated and presented to the customer SP by the serving IPX-P. For the Voice KPIs, the call handling function up to the final user is to be used.

The SLA based on a bilateral commercial negotiation between SP and IPX Provider is accepted by the IPX-P with the understanding the relevant commercial risks penalties for failing to meet SLA commitments within its domain and that of subsequent downstream IPX-Ps.

It is incumbent upon IPX-Ps to measure IP layer parameters using the various segments covered by the RTP packet in its own domain. Each IPX-Ps results may then be aggregated and presented to the customer SP by the serving IPX-P.

The commitment and delivery of QoS performance data by each IPX-P in the chain (for cascading QoS assurance) is the responsibility of the IPX-P contracting and serving each of its customer SPs.

Analysis of the VoIPX QoS Monitoring and KPIs warrant further investigation by the appropriate ATIS Committee.

---

[60] i3 Forum, *Technical White Paper on Security for IP Interconnection*, Release 1.0, May 2011

[61] < http://i3forum.org/wp-content/uploads/2012/05/i3f-Technical-Interconnect-Model-Release-5-FINAL-2012-5-3.pdf >

C.2.4.3.10 VoIPX Routing & Traffic Management

The VoIPX Routing of traffic functions are fully defined by i3Forum in section 12 of the *Specification for Voice over IPX Service*. Routing confined within the IPX environment is a closed environment, but certain circumstances may be encountered warranting routing outside the IPX domain. Acceptable scenarios are: a called party can only be reached (resource restriction) via "break-out" using a carrier given there are no other resources to reach destination within the IPX domain, or the Customer SP has agreed to have traffic routed to its destination via a break-out route.

A routing confined within the IPX domain is always recommended unless:

- The call has to be routed towards a carrier in break-out in agreement with the contract signed between SP and IPX P.
- The call has to be routed towards a carrier in break-out since there are no available network resources which allow the call completion within the IPX domain.

i3 Forum recognizes the need to limit as much as possible the number of IPX Ps in the SP-SP communication to maximize the possibility of meeting quality requirements. However, the i3 Forum recognized that "Intercontinental calls" are an example where the limit of two IPX–Ps cannot be guaranteed and more than 2 IXP-P in the SP-SP communication may not be applicable in domestic environments.

The minimum set of information that the IPX Provider shall provide to the Service Provider consists of the type of connectivity used to reach each terminating SP, namely direct connectivity (i.e., there is only one IPX Provider from Originating Service Provider to terminating Service Provider), indirect connectivity (i.e., there is more than one IPX Provider from Originating Service Provider to terminating Service Provider),and break-out connectivity (or gateway connectivity) between the IPX Domain and the Non-IPX Domain.

The GSMA preference to limit the number of IPX-Ps in the SP-SP communication path to two IPX-Ps in order to maximize the possibility of meeting quality requirements is not fully adopted by the i3 Forum. The i3 Forum recognizes that "Intercontinental calls" are an example of where the limit of two IPX–Ps cannot be guaranteed (which may not be applicable in domestic environments).

Analysis of the VoIPX Routing and Traffic Management warrant further investigation by the appropriate ATIS Committee.

C.2.4.3.11 Break-in/break-out connectivity

Break-in and break-out can be implemented via three technology options: via TDM interconnection, via private IP interconnection, and via public IP interconnection. For Private IP interconnection break in/out, the IPX-P's border functions are secured either physically or logically from Internet traffic. For public IP Interconnections IPSec encryption is used for signaling information only, and all of the voice traffic entering the IPX-P network crosses the IPX-P's border functions.

The following basic assumptions apply[62]:

- Destinations will remain reachable only via TDM for some considerable time. Not allowing TDM and IP break-in/break-out would exclude many destinations from a direct communication via the IPX domain, and MNOs would have to keep TDM interconnects operational in parallel to IPX-based interconnects in order to have access to these providers.
- The IPX Provider may inject traffic from other non IPX-compliant trusted SPs, provided that the security of the IPX is not affected.

[62] *Technical Specification for Voice over IPX Service*.

- Break-out/break-in interconnections support a faster deployment of IPX services for voice as it breaks the dependency on all networks migrating to IP at the same time.
- More than one IPX Provider can be involved in the end-to-end (SP-to-SP) connection
- The interconnection functions are intended to provide a “private communication path” (i.e., separated and protected from the Public Internet).
- Security functions shall be implemented among interconnection functions.

The entity that provides the interconnecting physical line between SP and IPX Provider is responsible for ensuring the SLA’s for that physical line (as described in AA.80, Annex 8[63]).

Break-in and break-out can be implemented via three technology options: via TDM interconnection; via private IP interconnection and via public IP interconnection.

Analysis of the VoIPX Break-in/Break-out Connectivity warrants further investigation by the appropriate ATIS Committee.

C.2.4.3.12 DNS & ENUM Registry

Although each IPX-P can select their own solution, the GSMA IPX Model in GSMA IR.67[64] requires that DNS on the IPX backbone be completely separate from DNS on the internet. Although DNS/ENUM capabilities can be used for addressing and routing the termination of a voice call, there are many solutions available to IPX-Ps in the market today, including SS7/MAP protocol, SIP redirect protocol, and Diameter protocol.

C.2.4.3.13 Number Portability Resolution

Customer SPs of the DNS and ENUM Registry for IPX providers of Voice service are not expected nor will they be required to be capable of transiting a call to another SP for the purpose of number portability, unless NP is neither technically possible.

Analysis of the Number Portability Resolution warrants further investigation by the appropriate ATIS Committee.

C.2.5 IETF models

C.2.5.1 SIP

SIP is defined in IETF RFC 3261. In addition, there is a family of documents that define extensions to the base SIP protocol defined in RFC 3261.

The retired Session PEERing for Multimedia INTerconnect (SPEERMINT)65 WG focused on architectures to identify, signal, and route delay-sensitive (real-time) communication sessions. These sessions use the SIP signaling protocol to enable peering between two or more administrative domains over IP networks. Where these domains peer, or meet, the establishment of trust, security, and a resistance to abuse and attack were all important considerations.

Note that the term "peering" is used here to refer to the interconnection between application layer entities such as SIP servers, as opposed to interconnection at the IP network layer. However, in order to achieve real-time Session PEERing, both signaling and media flows must be taken into consideration. In addition, the working group recognized that there will be use cases that require SPEERMINT to focus on the

[63]< http://i3forum.org/wp-content/uploads/2012/05/i3F-Interconnection-Signalling-Profile-Rel-1-FINAL-2012-5-3.pdf >

[64] < http://www.gsma.com/technicalprojects/wp-content/uploads/2012/05/ir6741.pdf >

[65] < https://tools.ietf.org/wg/speermint/ >

interaction between the application layer and lower network layers, or the dependence of specific application layer use cases on lower layers.

The most focused deliverables of SPEERMINT were best current practices regarding exchange of real-time sessions among VoIP and other real-time application service providers and – in particular – how such calls are routed. SPEERMINT recognized that some of these providers also control underlying access networks (facilities-based), while others do not (not facilities-based), and this fact may present various additional requirements or use cases for consideration. The working group developed use case documents to record the varieties of the practices.

C.2.5.2 ENUM

C.2.5.2.1 Introduction

The heart of ENUM is the ability to translate an E.164 number into a SIP URI, and ultimately into an IP address. This makes ENUM, or equivalent functionality, an important capability to support IP interconnect for VoIP. IP-based interconnect provides important advantages over TDM interconnect. VoIP calls have lower cost and higher quality by eliminating the IP-TDM-IP translation necessary with TDM interconnect. Direct IP interconnect also achieve more efficient connectivity, especially for lower capacity routes. Finally, ENUM enables efficiency gains through the use of a centralized translation capability for all traffic.

There are various applications of ENUM for IP interconnect:

- *IP Interconnect via bilateral agreements*, where a Service Provider knows which Telephone Numbers (TNs), TN Ranges, or public identities are served by the peering partner and where the entry points are for the peering partner. Such sharing of the information is on bilateral agreement basis.
- *IP interconnect to a federation of service providers*, where a Service Provider joins a federation of Service Providers. Within the federation, each member has access to all the TNs, TN-ranges, and public identities of each federation member.
- *Local Number Portability*, where a centralized ENUM server is used to find out if the called party telephone number has been ported to a different switch/Service Provider.

ENUM utilizes a hierarchical tiered architecture. Tier 0 is the root directory for Tier 1 national level ENUM registries. The Tier 1 national ENUM registries delegate to operator level Tier 2 registries, which contain subscriber level information. This architecture enables scalability and manageability.

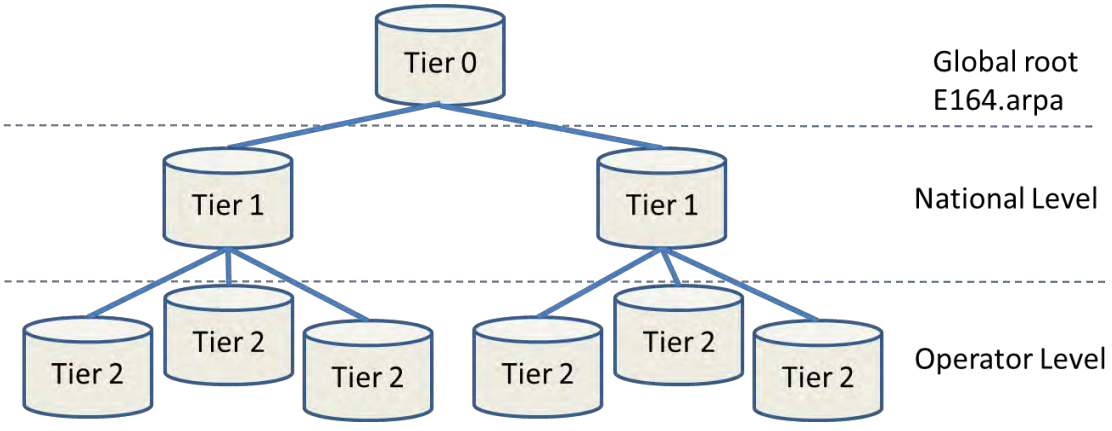

Figure C.19 - Hierarchical Tiered ENUM Architecture

C.2.5.2.2 IETF ENUM

The IETF defined the core set of specifications that describes ENUM functionality. The key specification defining ENUM, RFC 3761, was updated in 2011 by RFC 6116 and RFC 6117. From these specifications, additional RFCs related to ENUM can be located for ENUM services and attributes.

C.2.5.2.3 PacketCable ENUM

PacketCable has produced a set of IP Interconnect related specifications:

Table C.3 - PacketCable IP Interconnect Specifications and Document Control Numbers

PacketCable IP Interconnect Specification	Document Control Number
PacketCable™ ENUM Server Provisioning Specification[66]	PKT-SP-ENUM-PROV-I05-120412
PacketCable™ ENUM Server Address Resolution Specification[67]	PKT-SP-ENUM-SRV-I01-100630
PacketCable™ Interconnect Guidelines Specification[68]	PKT-SP-IGS-I01-110228

PacketCable ENUM is Tier 2.

C.2.5.2.4 GSMA & 3GPP-related ENUM

The current specifications for the 3GPP IP Multimedia System (IMS) rely on ENUM to convert an E.164 number to a globally routable SIP URI for use within IMS. However, the IMS specifications do not currently specify how Infrastructure ENUM functionality will be provided. This gap has been partially filled by the GSMA, which has launched an Infrastructure ENUM service. This service is now commercially available, and can be used to provide address resolution for global IP interconnect, based on the GSMA's IPX.

GSMA has a ENUM Tier 0 Root Directory that Operators and Carriers can query for free to find authoritative sources of Carrier ENUM routing information distributed around the world. GSMA's Tier 0 Root Directory contains pointers to Tier 1 Carrier ENUM registries around the world that contain authoritative and reliable ENUM data. The address of these registries is stored behind the relevant country code in PathFinder. PathFinder returns the Tier 1 registry address in the form of a NameServer address when a number with that country code is submitted in a query. In another words, this Tier 0 directory provides a starting point for resolving information about numbers and using standard DNS delegation techniques to provide referrals to another database where more information can be found.

GSMA also provides Tier 1 hosting solutions so that if a country does not have Tier 1 registry, GSMA offers a mechanism to host the Tier 1 directory on the GSMA PathFinder.

C.2.5.2.5 ENUM & Carrier Interconnect

The following diagram of a deployment example illustrates how ENUM may be used to for Carrier Interconnect:

---

[66] < http://www.cablelabs.com/specifications/PKT-SP-ENUM-PROV-I05-120412.pdf >

[67] < http://www.cablelabs.com/specifications/PKT-SP-ENUM-SRV-I01-100630.pdf >

[68] < http://www.cablelabs.com/specifications/PKT-SP-IGS-I01-110228.pdf >

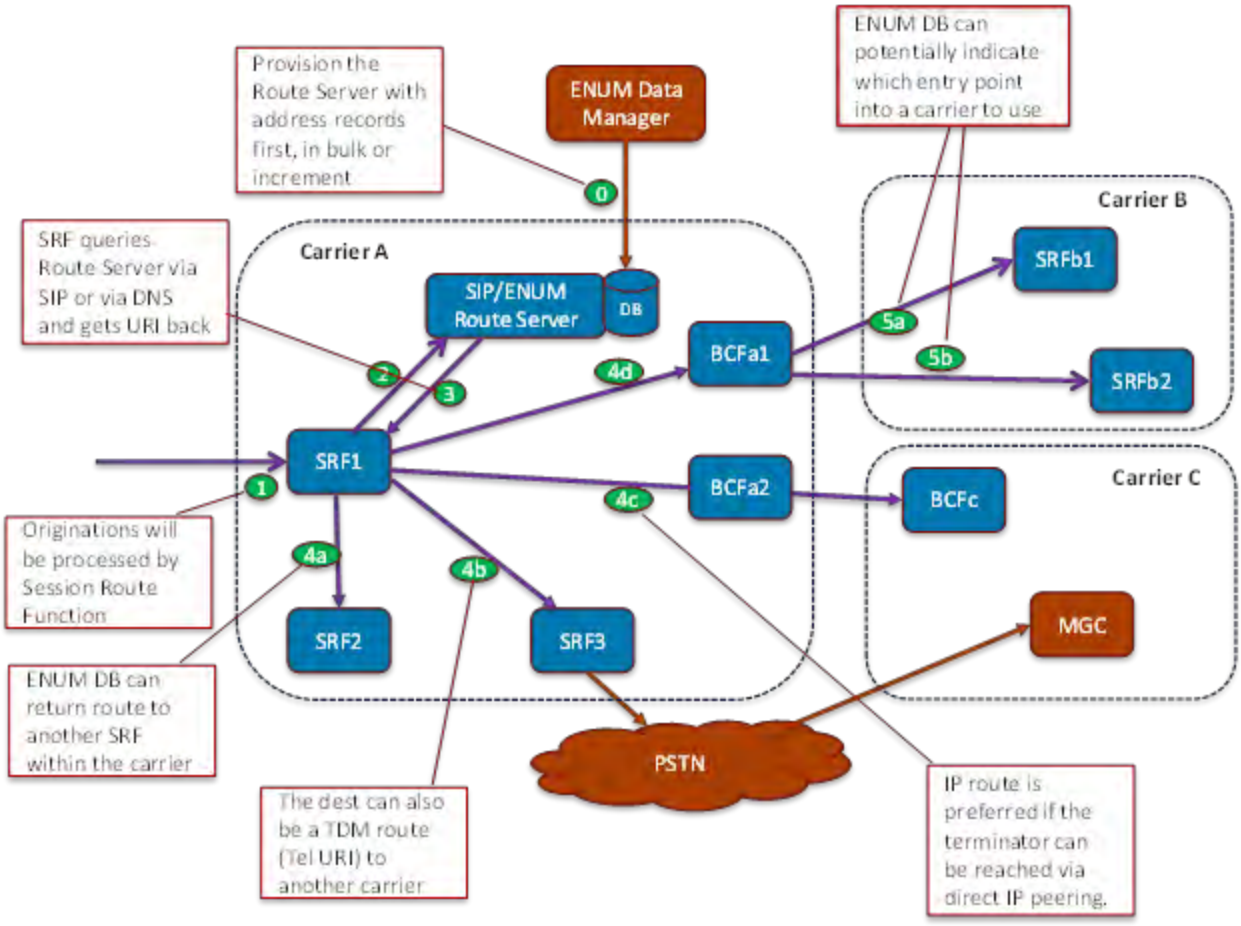

Figure C.20 - ENUM Intercarrier Interconnect Example

In this architecture, the following are the main components.

- *SRF* – Session Routing Function, which can be part of a soft switch, CMS, CSCF/BGCF, etc.
- *BCF* – Border Control Function, which can be an SBC, an I-BCF, etc.
- *SIP/ENUM Route Server* – This is a function that can receive a route query in either SIP (INVITE) or DNS (ENUM) format, looking for a route using the cached route database, and returns a destination route. This function receives route data from ENUM Data Manager.

Table C.4 - Legend for Diagram of ENUM Intercarrier Interconnect Example (Figure C.20)

Ref point	Protocol	Description
0	ENUM Server prov protocol	The SIP/ENUM Route servers must be provisioned with the mapping of TN, TN-range, or public identity to destination route. This interface must support bulk provisioning, where the large volume of route date can be transported in a file and loaded into the Route Server. This interface must also support incremental updates where deltas will be applied efficiently.
1	Call Origination	The origination can be from a line, an access trunk, or an incoming call from another carrier. For example, the protocols can be H.248, NCS, SIP, and ISUP. The SRF is configured to query the Route Server for destination routes.
2	SIP or DNS	The SRF queries the Route Server with the called party address and potentially with some context information, such as which SRF is originating the query.
3	SIP or DNS	The Route Server analyzes the called party address and potentially takes the context information provided in the query to come up with a destination route. This route is returned to SRF.
4a	SIP	The destination can be another SRF within the carrier's network, in which case the originating SRF will send the call to the terminating SRF via SIP.
4b	SIP	The destination can be a TDM trunk associated with another SRF in the network. In this case, the Route Server may return the destination SRF and the egress trunk group to use once the call reaches the egress SRF.
4c	SIP	If the called party belongs to a SIP peering partner, then the Route Server returns the egress BCF leading to the peering carrier.
4d, 5a, 5b	SIP	Sometimes, it's desirable to be able to specify which entry point into the peering partner's network should be used when the same egress BCF is used for these entry points. In this case, the Route Server is required to specify the egress BCF as well as the entry points into the peering carrier's network. This is similar to the reference point 4b, except that the entry point may be in a different form than trunk group.

A Session Route Function can locate an ENUM/SIP Route Server in a number ways – e.g., via statically configured list of Route Server IP addresses, or a (list of) FQDN that can be dynamically resolved into a list of Router Servers. The peering carriers can share the addresses (e.g., FQDN) of the Route Servers so that route info updates can be exchanged. Note that the Route Servers are typically protected by Border Control Functions just like any other signaling nodes. Secure transport mechanisms like TLS can be used to access Route Servers to provide route info update among peering partners. Authentication can be accomplished via a well- known mechanism such as HTTP Digest. Route data file exchange can be secured via Secure Copy (scp).

C.2.5.3 RTCweb

C.2.5.3.1 Introduction

RTCweb is currently being developed by the IETF to enable real time communication from a web browser[69]. IETF draft-ietf-rtcweb-overview[70] provides an overview of the RTCweb architecture. Significant flexibility is being incorporated in the overall design of RTCweb so that a "Telephony"-centric architecture is not forced upon the web ecosystem. The result is a focus on end point interworking, security, a framework for media handling, and the pragmatic adoption of an SDP based offer/answer model. The figure below shows the basic reference architecture for RTCweb communication.

[69] < http://tools.ietf.org/wg/rtcweb/ >

[70] < http://tools.ietf.org/html/draft-ietf-rtcweb-overview-05 >

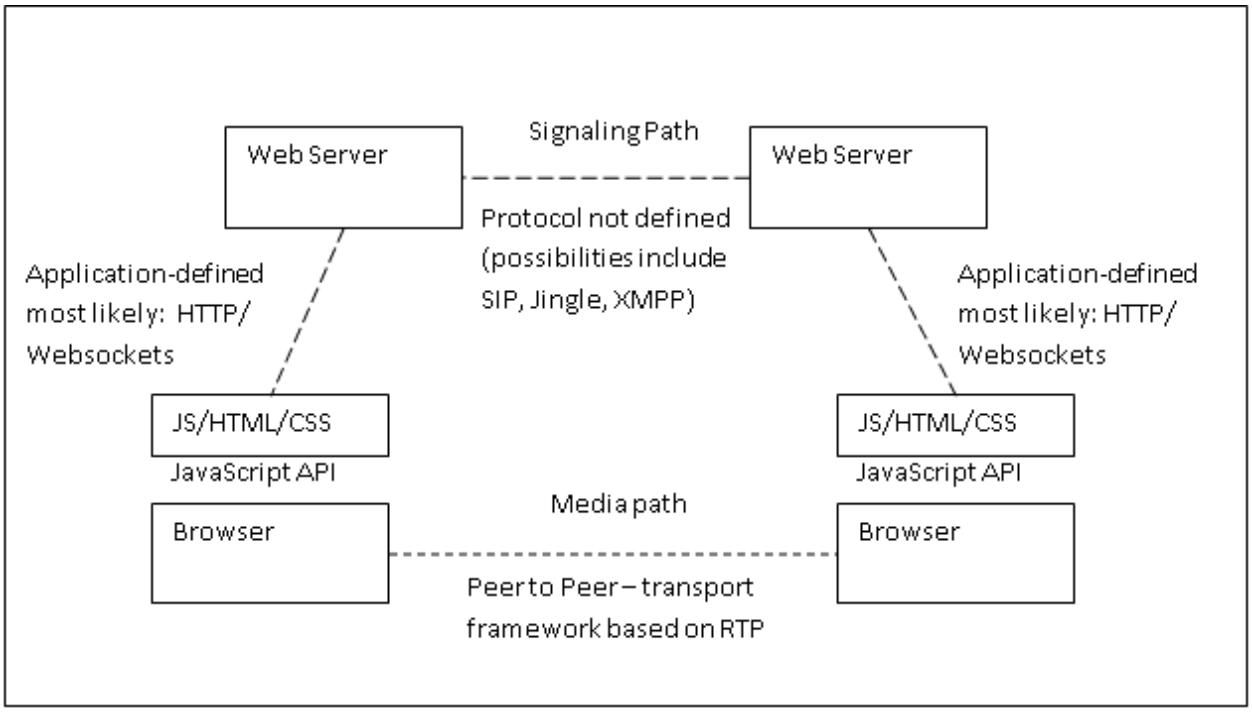

Figure C.21 - IETF RTCweb model

It should be noted that in the RTCweb a number of aspects such as the protocol used between for session signaling between web servers or another domain, addressing format, services such as forking, and a number of other areas have been left undefined. This creates requirements on interconnect which will be discussed in the following sections.

In conjunction with the IETF RTCweb activity, the browser API aspects of the solution are being developed by the W3C in specification “WebRTC 1.0: Real-time Communication Between Browsers”. More information on this activity can be found at < http://www.w3.org/TR/webrtc/ >.

C.2.5.3.2 Interconnection models to SIP, IMS, & PTSN domains

When the RTCweb interconnects to different technology domains, an interworking function will be required. The specific requirements of this function will depend on the technology domain into which interconnect is taking place and the signaling protocol used by the Web Server.

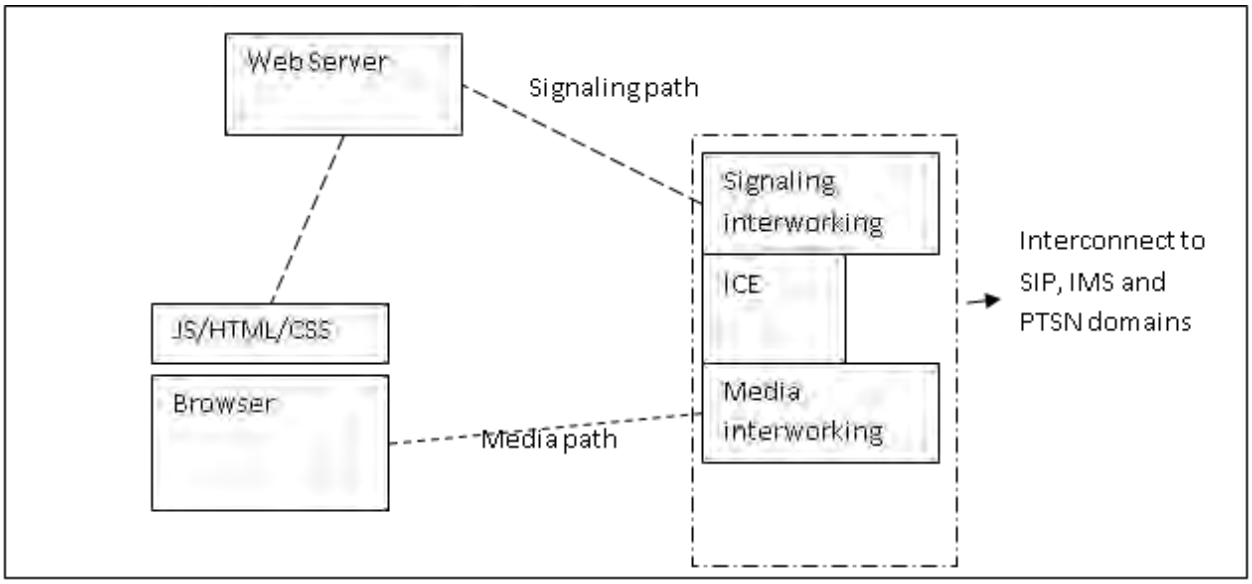

Figure C.22 - Simplified Inter-technology Interconnect RTCweb

C.2.5.3.3 RTCweb Interconnect Issues

RTCWeb does not specify the signaling protocol, although at this time it is considered quite likely that SIP (RFC 3261) will be used in many implementations. However, it will not be possible to assume that the signaling will be SIP in all cases. Therefore, the Interconnect border will need a signaling interworking function that can take the protocol being used by RTCweb and map it into the requirements of the transit or terminating network.

RTCWeb does not specify a specific user/client addressing scheme. Basic URI domain based routing can get interconnect traffic to the agreed interconnect point where additional address manipulation may be required. It can be anticipated that ENUM mapping between E.164/Tel URI formats and RTCWeb URI addresses will be required.

WebRTC is considering media encryption standards and SRTP has been agreed-to; however, there has been no consensus yet on the keying mechanism to be associated with it (e.g., DTLS-SRTP or SDES). This will require interworking with other domains.

RTCWeb makes use of ICE for hole-punching through NATs and to ensure consent from both parties. Hence, support of ICE will need to be required and this may be placed on the interworking function.

RTCWeb has not yet agreed on the mandatory baseline voice and video codecs; candidates include G.711 and Opus[71] for voice and VP8[72], H.261 and H.264 for video. Issues of contention around making a decision include the royalty framework around particular codecs and differing opinions on whether there needs to be a single mandatory codec for each service. The impact of this decision will affect the range of codecs required at interconnect for media transcoding.

Analysis of RTCweb warrants further investigation by the appropriate ATIS Committee as this standards framework evolves.

[71] < http://datatracker.ietf.org/doc/draft-ietf-codec-opus/ >

[72] < http://www.webmproject.org/tools/ >

C.2.5.4 ICE

C.2.5.4.1 Introduction

Network Address Translators (NATs) enable sharing of IP addresses, but with the drawback that clients sitting behind a NAT will not be aware of which IP address and port numbers will enable a media stream to reach it from beyond the NAT. This creates a problem for real time communication where an end client wishes to inform its peer of the IP address and Port numbers it should send media to.

ICE (RFC 5245) provides a mechanism to enable client end points to determine IP addresses and port numbers which will enable peer-to-peer communication through NATs. ICE endpoints use mechanisms such as STUN (RFC 5389) to discover potential candidate IP address and port pairings for each protocol. A multiplicity of these IP address and port pairings are included in SDP offers and answer, and then tested for connectivity by peer-to-peer connectivity checks. Once a successful IP address and port check has been achieved, and consent provided for communication, then media flow can begin.

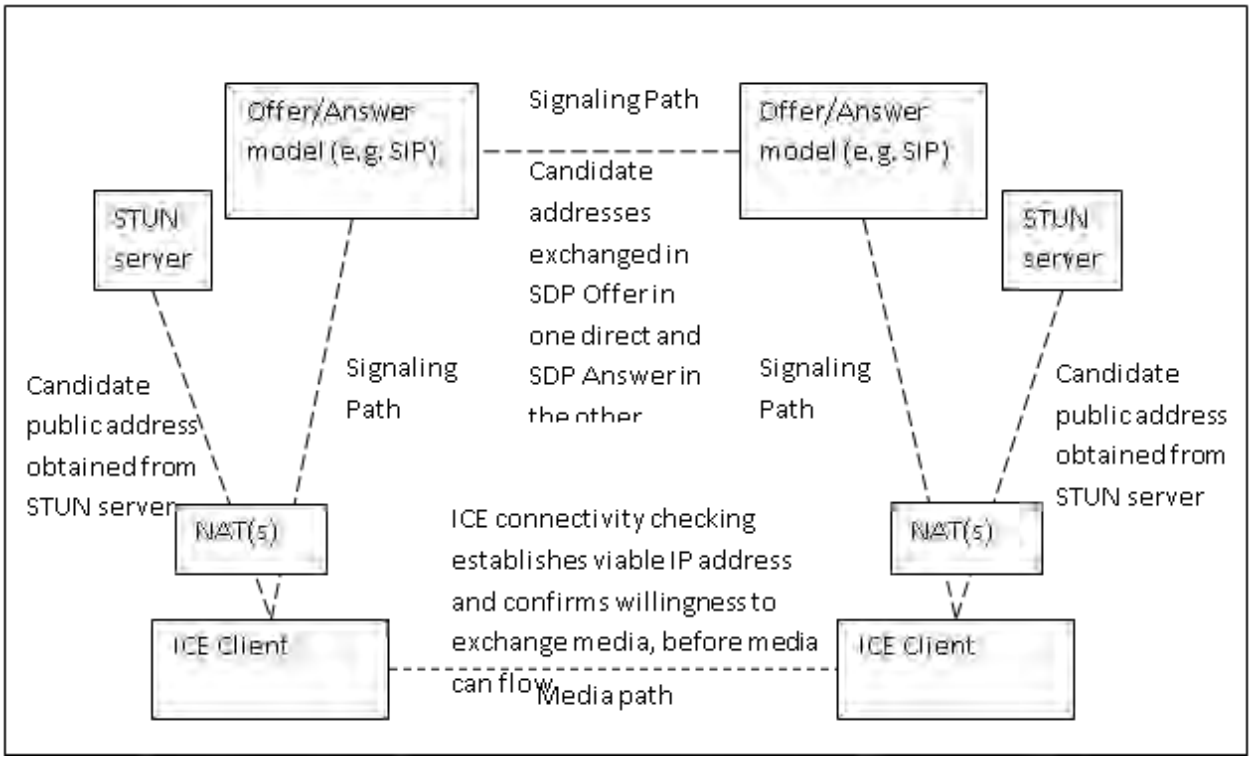

Figure C.23 - ICE establishment of peer to peer connection

C.2.5.4.2 ICE-Lite

In addition to the full implementation of ICE, RFC 5245 also defines a reduced functionality implementation known as ICE-Lite. The key differences being an ICE-Lite implementation:

- Only gathers candidate addresses from its own interfaces.
- Cannot be a controlling endpoint.
- Does not generate checks, but only responds to periodic checks from other endpoints.

Support of ICE-lite by network entities enables endpoints with full ICE implementations to perform ICE connectivity checking to establish a routable path for media. This is particularly useful when one of the endpoints does not support ICE (e.g., the PSTN).

The host IP address for an implementation supporting ICE-Lite will need to be routable and not a local address behind a NAT.

C.2.5.4.3 Interconnect Issues

When ICE is not supported on one side of the communication establishment dialogue, the default behaviour is to fall back to normal SDP offer/answer handling (RFC 3264). This creates a dependency on interim nodes to provide the necessary IP routing for the media. In the case of WebRTC, where support of ICE is mandatory, if interconnect is to occur to a network technology where ICE support is not guaranteed, then an interim node must provide the necessary support of the ICE functionality expected by the WebRTC client.

NATs remain a challenge to real time communication, and in response the industry continues to evolve solutions for enabling media connections through NATs. ICE is particularly suited to peer-to-peer media connection establishment. However, it is yet to be seen whether this becomes the dominant NAT traversal solution in this space. The wider applicability of ICE in carrier networks is still not well established.

C.2.6 Other Interconnect Models

C.2.6.1 Google Talk Federation & Jingle

The Google Talk infrastructure is based on the XMPP protocol with open protocol and interface specifications available at xmpp.org[73]. The Jingle spec allows for development of third-party clients that can work within Google Talk or other XMPP-based networks. The open interface specifications allow for XMPP-based networks to directly interconnect for interoperable services based on the available specifications.

Since most VoIP networks use a variant of SIP, the XMPP-based interconnect is an unlikely candidate for a universal interconnect model. Nevertheless, it is an example of an effective solution for unmanaged multilateral interconnect that addresses some key security issues while allowing for relatively simple addition of new federation members. Key functions like addressing and charging are not included in the model.

Google Talk Federation is an example of an unbundled multilateral interconnect model without use of managed-service-based transport (i.e., using the Internet).

C.2.6.2 SIP Connect

SIPconnect is a standards-based method of interconnection between IP PBXs and VoIP service provider networks, with an open specification available at www.sipforum.org[74]. It specifies a reference architecture, required protocols and features, and implementation rules necessary for seamless peering between IP PBXs and VoIP service providers.

It does not address general interconnect between SIP networks, but does address many of the same technical issues. As a bilateral interconnect model on the access side, it does not address key issues associated with multilateral interconnect on the NNI, including addressing, charging and QoS.

C.2.6.3 Interconnect with Proprietary Networks, such as Skype

While non-SIP, non-XMPP networks like Skype exist, interconnection to them must either be based on an open standard, probably SIP-based, or must be avoided altogether for use cases where the endpoints are able to interconnect natively using the proprietary network.

---

[73] xmpp.org, *XMPP Standards Foundation* background and specifications.

[74] www.sipforum.org, *SIP Forum* background and specifications.

C.2.6.4 WebRTC-based Interconnection

Some WebRTC advocates point out that WebRTC-enabled browsers enable networks to provide universal clients to both call originators and terminators, thus making interconnection between disparate networks unnecessary for some WebRTC use cases. While this may be possible for some use cases, network interconnection remains critical to enable universal reachability.

C.3 Interconnect Business Models

The following figures provide simplified models of the relationships between various providers involved in telecommunications sessions. In many cases, the same provider may account for access, transport, service and application functions, or any subset thereof.

In particular, the end user may have separate relationships with access, service, and application providers, but still need them to cooperate to the extent necessary to provide acceptable service.

For the most part, access and transport providers can be independent of service and application providers for services and applications using unmanaged (best effort) transport. For provision of emergency services, an emergency service will also require location information and priority access, although these functions are not critical for most sessions.

These figures also demonstrate the potential complexity of the NNI when separate providers are involved at the transit and transport levels. While allowing the flexibility to deploy much more efficient media transport based on OMR and/or ICE, these models require the development of new business arrangements to support managed-service-based transport with QoS and to support charging reconciliation between all providers.

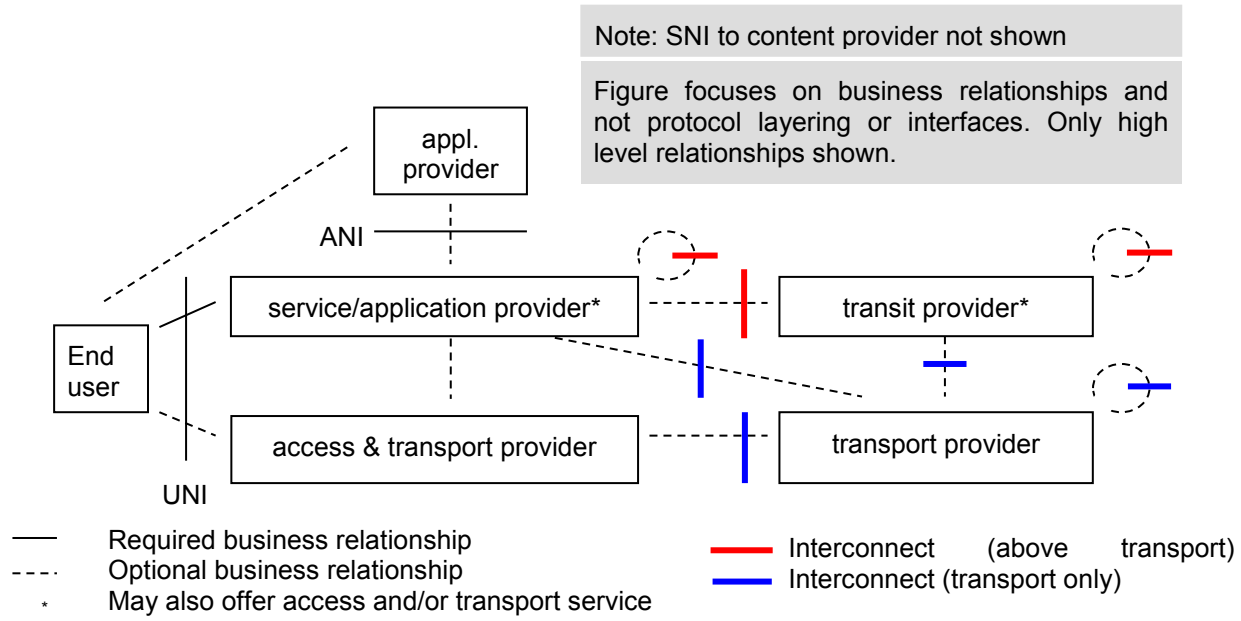

Figure C.24 - Simplified business model with no roaming or SNI

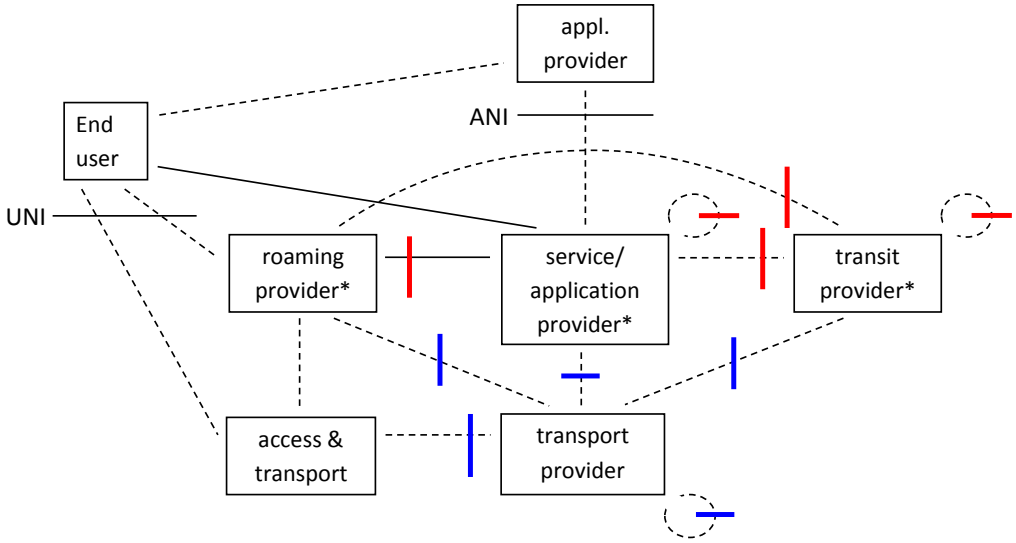

Figure C.25 - Simplified business model with roaming and no SNI

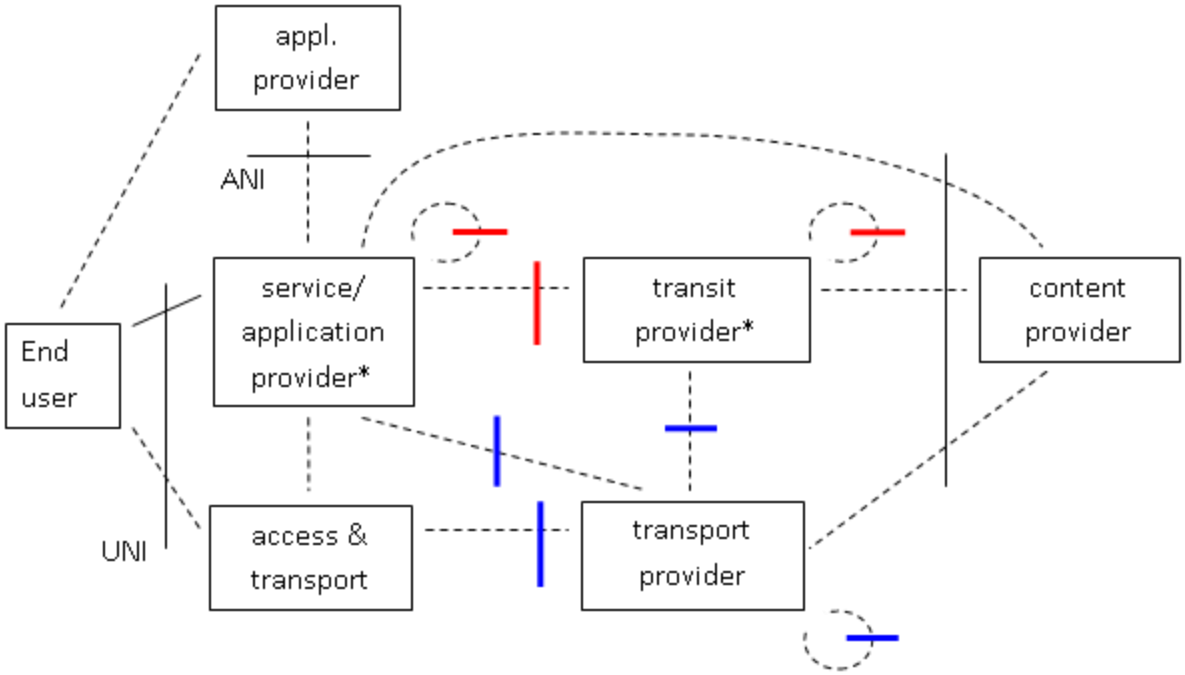

Figure C.26 - Simplified business model showing SNI without roaming

As users become more accustomed to establishing separate business relationships with access, service, and application providers, relationships between those providers and the corresponding transit, transport, and content providers can be expected to evolve to support new technical capabilities and business models.

C.4 Technical Considerations at Interconnect

C.4.1 Bundling of Signaling with Media

Inter-operator charging conventions normally require that call control signaling be present in any network handling media transport for a call to enable per-call charging for media transport. Per-call charging of media transport is the norm due to the special provisions associated with the managed-service-based transport of media that is usually used by transit operators for voice calls.

As discussed in earlier sections on OMR and RAVEL, it is possible to disassociate media transport from signaling transport to achieve more efficient use of available transport resources, but there are several issues with fully separating them:

1. In networks that transport media without associated signaling, it is not possible to use current signaling-based conventions to charge for the transport of the media. As an alternative, operators could charge for transport of media traffic on a bulk basis without regard to individual call details, but this requires a complete revision of inter-operator roaming and interconnection agreements.
2. IP level routing policies must ensure that routing paths are selected to ensure that existing service level agreements are enforced on an end-to-end basis. This requires the consistent partitioning of QoS-enabled traffic end-to-end via consistent packet marking policies and/or routing through appropriate managed-service-based networks. While technically feasible, such end-to-end IP routing policies are unavailable in today's networks for managed and/or QoS-enabled transport.
3. Per-call traceability is more difficult when media flow is uncorrelated to signaling. With redundant paths built into routing tables of necessity, it may be difficult to identify the networks involved in transporting media for a particular call. Per-call statistics are thus more difficult to correlate to specific networks. This issue is managed today by provisioning and monitoring the network based on aggregate traffic, although the statistics used and the basis for service level agreements may need to change.

The presence of multimedia traffic – i.e., mixed voice and video – introduces another issue in the transport networks, since voice usually takes priority over video, under congestion. In the bundled case, each media type is assigned clear priority at each interconnection point and may be assigned to transit separate portions of the network based on the associated service agreements. For unbundled media, the differentiation between different media types is assured by deploying consistent routing policies for each media type, usually based on appropriate packet markings.

Bundling of signaling with media for transport is assumed by some existing intercarrier business agreements, but could potentially be changed in the future with new agreements.

C.4.2 Addressing & Routing

See Appendix D of this report for the impact of the PSTN transition on addressing and routing within the context of numbering.

C.4.3 Media Routing & NAT Traversal

The default configuration at the NNI for most interconnect models is for signaling and media to be routed together between the interconnected networks. In many cases, this results in suboptimal routing of the media since signaling can traverse more provider networks than necessary to transport media. Signaling may flow through extra networks when roaming and to provide various originating and terminating services, and via transit networks for routing and interconnection when direct bilateral connections are unavailable.

On the other hand, when OMR and/or ICE are deployed to optimize media routing, IP packets can potentially flow directly between the endpoints based on IP level routing. This is consistent with services using unmanaged media transport since there are no additional charges associated with delivery of best effort IP packets anywhere in the internet once they are accepted for delivery at the access POI. In

particular, any forced routing of media at an NNI to route it together with signaling will be a waste of resources, since there can be no service guarantees associated with the media.

OMR and/or ICE can provide the same media optimization for managed-service-based transport, but this has the potential to unbundle the media from the signaling at the NNI, thus introducing the issues described in section C.4.1.

C.4.4 Security

Interconnection with dedicated facilities relies on the fact there is physical security, therefore other security techniques are not required. VPNs with dedicated traffic also typically do not require additional security.

C.4.4.1 Signaling Security at Interconnect

IP Security (IPsec) is the preferred method for securing signaling at the interconnect. TLS is used as an alternative in some cases.

C.4.4.2 Media Security at Interconnect

Media is typically not secured, but can be secured with either Secure Real-time Transport Protocol (SRTP) or IPsec.

C.4.4.3 End Party Identify Verification & SPam over Internet Telephony (SPIT) Considerations

This topic is addressed in Appendix D.

C.4.5 QoS in Support of Voice SLAs

C.4.5.1 Introduction

VoIP services' quality can be evaluated by measuring reliability and audio quality. Factors that contribute to the reliability are directly measured from the signaling protocol (SIP) performance, where audio quality is computed as an aggregate of the performance factors related to audio clarity and audio delay. There are some two dozen signaling and media delivery performance metrics, and understanding how the metrics are calculated and what they mean about the behavior of signaling and media is most important in determining which are "must haves".

Note that services provided with QoS assurances are sometimes referred to as "Managed Services" to distinguish these offerings from those that rely on public internet "best effort" quality. This generally requires the use of managed-service-based transport, such as layer 2 or 3 VPNs or dedicated layer 1 connections within a network, and dedicated layer 1 interconnection points between network operators, which can be engineered specifically to meet the security, reliability, performance, and QoS requirements of the services carried.

C.4.5.2 Description of QoS

There are numerous aspects of a network's architecture, protocols, customer behavior, measurement practices, etc., that impact call quality and the interpretation of QoS. First, it is necessary to understand which of these variables has a meaningful impact on QoS, and to what extent each of these impacts has upon QoE, thus warranting inclusion in the QoS model.[75] By analyzing various transport, service, and call

[75] PTSC- SAC-2010-042.doc, Verizon Contribution to Issue Number S0079 – NNI QoS Architecture (PTSC-SAC) Titled "Primer for a QoS Model" by James Castagna, dated February 15, 2010. This reference is a committee contribution. PTSC committee participants can access this document at < http://contributions.atis.org >. Copies of

attributes and determining which are most likely relevant to network and service performance, we can drive towards a QoS model that is practical, meaningful, and effective, thereby likely to experience widespread acceptance and use.

There are indicating symptoms of network or service difficulty experienced by customers and operators made available by various mechanisms. Customer equipment failure or network failure in any of the multiple network links may be the cause of voice quality degradation. The tell-tale signs of sub-standard quality and even explicit failures in service need to be accurately identified and defined by a corresponding indicator to recognize and measure changes in quality. The challenge is to effectively recognize changes in the network and service by filtering out misinformation by establishing common practices that make it easy to identify and counteract situations which will likely lead to unacceptable levels of QoS/QoE. Some changes can be made in real-time, whereas other factors need to be addressed during the specification of interconnect requirements that are known to have an impact on voice quality.

The ability to connect a call and provide sufficient voice quality is a general indication of QoS. The network reason why a call was not connected quickly, not connected at all, or was connected but provided poor voice quality is more complex to determine. Signaling, media, and equipment selection may predetermine the level of QoS capable for a particular network or link in a chain of networks. Having the tools to determine what, where, and how long a problem existed requires an understanding of the potential problems, how to recognize them, and how to quantify and identify them, so that the information is meaningful and useful.

C.4.5.3 QoS Factors & Indicators

Issues that may be due to network or customer factors must be segregated into those that are under the control of an Operator, and those that are only under the control of End Users. For those factors which have a meaningful impact, the identification of how to measure the effect of the impact needs to be identified. Once we understand how to measure the effect, we can see how to better engineer/configure the network to avoid these influences, and successfully detect occurrences that degrade voice quality.

The three following sections and table segregate the above approach to understanding quality issues:

A. Quality issues likely due to network characteristics and configuration:

1. Call is not connected, and a fast busy is returned (implying network congestion).
2. Silence due to call set-up delay or no ring-back tone when placing a call.
3. Poor speech quality due to network settings, equipment selection/configuration.

B. Quality issues likely due to network characteristics and configuration which contribute to End User behavior:

1. Call refusal since no Caller ID provided (by end user choice or network inability) .
2. Unacceptable call quality leading to short length-of-call hold times to certain affected destinations/routes.

C. Quality issues not due to network characteristics but likely due to End User behavior:

1. Poor or broken hand-sets with poor voice quality, broken ringers, etc.
2. Customer ambient background noise or other hearing difficulties.
3. Unavailable to receive calls, for whatever reason.

Defining these influences to determine which are meaningful representations of service and network quality issues “under the control of SPs” is necessary before a process of measurement and calculation “that accurately reflects an Operator’s ability to manage network and service variables” to deliver sufficient and consistent QoS/QoE is needed.

Table C.5 - Relationship of Symptoms, Network Influences and QoS Metrics

QoS/QoE Symptom(s)	Reflects SP QoS?	Likely Reasons	Indicating Metric	Configuration Influence(s)
A – Ntwk Characteristics				
1. Call is not connected	Yes	Congestion/Other (session failure)	Answer Seizure Ratio (ASR)	Accurate Signaling (Reason Cause)
2. Call Set-up Delay	Yes	Congestion/Other (session set-up delay)	Post Dial Delay (PDD)	Accurate Signaling (Reason Cause)
3. No ring-back Tone	Yes	Failed Execution	Part of ASR	Understanding Proper Handling
4. Poor Voice Quality	Yes	Multiple Issues	Mean Opinion Score (MOS)	Loss, Jitter, Delay (incl. Codec Type, Transcoding)
B – Ntwk Characteristics Contrib. To EU Behavior				
1. No Caller ID or CLI	Yes	Not offered/passed Signaling	Is Calling Line Identification	Loss of Header Information (e.g., TDM-SIP)
2. Short length-of-call hold times	Maybe	See A and B	Avg. Length of Call (ALOC)	See “Poor Voice Quality”
3. Other	TBD	NA	TBD	TBD
C - End User Contributing Issues				
1. Broken hand-sets	No	NA	None	None
2. Ambient background noise	No	NA	None	None
3. Unavailable to receive calls	No	NA	None	None

From this table, we can see that there are several network and service influences that impact end user QoE and an Operator's ability to manage QoS, contributing to the overall quality of experience (QoE) of the end user. Understanding and monitoring these influences after service is established, as well as establishing/selecting certain NNI network settings (see ATIS PTSC Issue S0075[76]), both can impact voice quality capability of the network, and the ability to adequately address and monitor quality with uniformity and consistency among Operators.

The primary indicators and network influences warranting consideration are identified as follows:

- **Network Selection and Configuration Factors**
    - Codec Selection, Transcoding Function Delay/Impairment
    - Handling/Interpretation of Signaling Message Response Cause (RC) Code (See resulting "Signaling Performance Factors" listed below)
    - Availability and interworking implementation of SIP, SIP-I and ISUP
- **"Signaling" Performance Factors**
    - Session Establishment/Completion [similar to Answer Seizure Ratio (ASR)]
    - Session Establishment/Effectiveness [similar to Network Efficiency Ratio (NER)]
    - Session Set-up Delay [similar to post-dial delay or Post-Gateway-Ring-Delay (PGRD)]
    - No Ring-back Tone
    - Passing of Calling Line Identification (CLI)
- **"Transport" Performance Indicators**
    - RTP/UDP Single Pass (ITU-T G.114) Packet Delay
    - RTP/UDP Packet Jitter
    - RTP/UDP Packet Loss
    - RTP/UDP Burst Duration
    - RTP/UDP Burst Density
- **"Service Performance" Indicators**
    - Average Length Of Call (ALOC)
    - Answer/Seizure Ratio (ASR)
    - Post Dial Delay or Post Gateway Ring Delay (PGRD)
    - Network Efficiency Ratio (NER)

The challenge remains to analyze and recommend an approach to establishing a uniform Network and Signaling Configuration, as well as how to define, measure, calculate, and report QoS Transport and Signaling influences upon QoS in the form of performance indicators. An analysis of this nature will yield a description of *Service Performance Factors* and Indicators describing a preferred network and signaling configuration, and establishing a uniform and standard approach to understanding network and signaling performance when exchanging QoS information among Operators. With a QoS model defined, a specification for the exchange of meaningful information across the NNI that sufficiently enables inter-provider QoS assurances and mechanisms for management and policy enforcement of SLAs will be available for use among Operators.

Before Operators can depend upon their interconnecting partners to support QoS beyond "best effort" to achieve a PSTN-like level of service to their end users, there needs to be a consistent understanding among the parties involved as to what is to be measured and how to measure it, before it is possible to

[76] http://www.atis.org/0191/issues.asp

monitor, troubleshoot, and report/share QoS information – for example, to be able to compare "with confidence" the QoS performance against an SLA.

Ideally, a definition of the terms and a general problem statement identifying performance factors and indicators are first established for analysis and recommendation as to the measurement methodology to begin defining a complete QoS model. Subsequently, the QoS model can then be defined in the context of a model that includes the exchange of meaningful QoS information across the NNI.

This study plan includes the following steps:

1. *Define "Indicators"* to measure Transport, Signaling and Service performance.
2. *Define "Factors"* associated with Network Configuration and Signaling Configuration.
3. Establish *Measurement Methodology and Calculation* of Indicators.
4. Study and Recommend a *Network Configuration and Signaling* QoS model.
5. For the QoS Model (Items 1 – 4) establish requirements for the *Exchange of QoS Data*.

One such analysis has been conducted by the i3 Forum, which is described in the following section.

C.4.5.4 I3 Forum QoS Study & Conclusions

The i3 Forum recognizes the need for the ability to measure QoS parameters for specific network segments for reporting and collecting data for presentation to the Customer/Service Provider. This expectation implies the need to measure identified parameters for the identified end-to-end domain across downstream network(s) for QoS reporting, and to analyze the call flow in order to locate and isolate faults. On the basis of a four year i3F study carried out jointly with other bodies and vendors, the i3F concluded there is only one protocol (RTP Control Protocol, RTCP) which reports back the quality information of the downstream networks.

However, the i3F and other bodies/vendors recognize that although the RTCP stream is generated by the RTP endpoint and it propagates back across all border functions in the path, there is no information available in the RTCP reports indicating where the actual RTCP end-point is located in the downstream networks, creating an uncertainty on the segment actually being measured77.

Although this is the case, the i3F recommends that nonetheless, the industry needs methodologies and guidelines for practical measurement of transport KPIs in scenarios where there is one or more networks involved in the end-to-end domain – that is, a Single network domain and Multiple network domains.

The following section describes the QoS definitions and measurement methodologies recommended by the i3 Forum applicable to single and multiple network domains.

C.4.5.5 Quality of Service Measurements

GSMA for the voice service over an IPX platform in GSMA AA.8178 identifies the need to measure, in addition to the traditional voice parameters, transport-dependent parameters such as packet loss, delay, and jitter.

Specifically, GSMA states the need:

1. To measure and report the service dependent KPIs for ASR, ABR, NER, ALOC, and PGRD;
2. To measure and report transport-dependent parameter KPIs for packet loss, packet delay and packet jitter;
3. To carry out the above measures following the RTP path and not the shortest path driven by routing protocols OSPF[79], BGP[80], and other IP routing protocols; and

---

[77] *Technical Interconnect Model for International Voice Services.*

[78] GSMA AA.81, *Packet Voice Interconnection Service Schedule to AA.80*, and related approved change request.

[79] IETF RFC 2328, *OSPF Version 2*, April 1998.

4. To perform the measures of the transport-related parameters for the whole intercarrier domain end-to-end – i.e., from the last equipment in the Carriers network facing the originating Service Provider to the first equipment in the Carriers network facing the terminating Service Provider.

The figure below describes the i3 Forum reference configuration for QoS measurement.

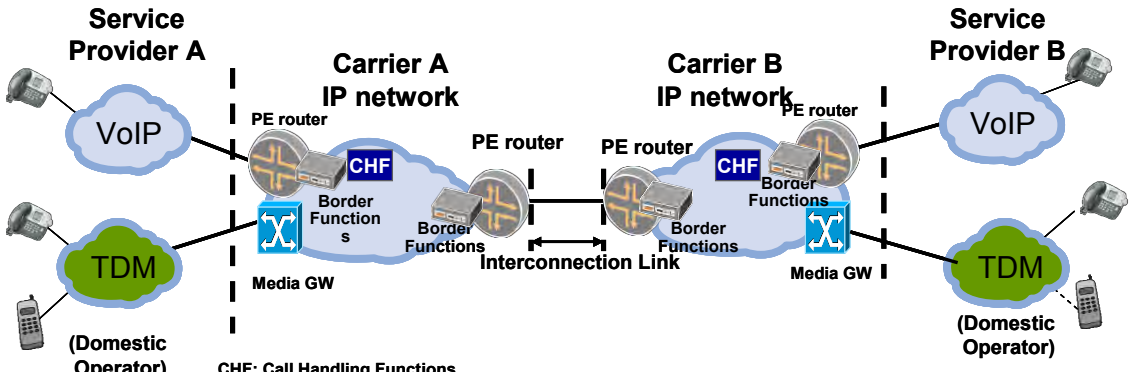

Figure C.27 - Reference Configuration for QoS Measurement

C.4.5.6 i3F QoS Transport & Service Parameter Definitions

The i3F considers the following QoS parameters most relevant, and they are divided in two sets pertaining to the transport layer, and the service layer, as follows:

1. ***Transport parameters***
   a. *Round-Trip Delay* – Time it takes for a packet to go from one point to another and return. The RTP control protocol RTCP is adopted by the i3F to measure round trip delay. This is a passive measurement performed on all live traffic and it calls for a full compliance of the RTP end-point to the existing standard, specifically IETF RFC 4855[81]. One way delay cannot be measured with RTCP, so with regard to the MOS measurement, since the ITU –T G.107 R FACTOR/G.107 E-model[82] requires one-way delay measurement, this is estimated by halving the round-trip delay[83].
   b. *Jitter* – The absolute value of differences between the delay of consecutive packets. For the same reasons as for the loss measurements, for jitter measurement, RTP is uniquely positioned to measure accurately live traffic[84].
   c. *Packet Loss* – Ratio of the total lost packets and the total sent packets for a time period. Measuring RTP, which is the real voice traffic, is the most accurate approach of measuring the performance of the voice application[85].

---

[80] IETF RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*, January 2006.

[81] IETF RFC 4855, *Media Type Registration of RTP Payload Formats*, February 2007.

[82] ITU-T Recommendation G.107, *The E model, a computational model for use in transmission planning*, March 2005.

[83] *Technical Interconnect Model for International Voice Services*.

[84] *Technical Interconnect Model for International Voice Services*.

[85] *Technical Interconnect Model for International Voice Services*.

2. Service parameters

a. *MOSCQE/R-factor*[86] – MOS is defined in ITU-T Rec. P.10. ITU-T Rec. G.107 defines an objective transmission rating model (the E-model) for representing voice and estimated or MOSCQE is defined in ITU-T Rec. P.10 using formula in ITU-T Rec. G 107 Annex B.

b. *ALOC* – Average Length of Conversation (ALOC) expresses the average time in seconds of conversations for all the calls successfully setup in a given period of time.
   i. SIP protocol: ALOC is measured from the time of SIP 200 OK (in response to an INVITE initiating a dialog) to the time of call release (SIP BYE).
   ii. SIP-I protocol: ALOC is measured from the time of a SIP 200 OK with an encapsulated ANM to the time of receiving a BYE message with encapsulated REL.

c. *ASR* – Expresses the ratio of the number of calls effectively answered in a given period of time against the number of call session requests in that time.

   i. SIP protocol: ASR is the ratio between the number of received 200 OK (in response to an INVITE initiating a dialog) and the number of sent INVITE initiating a dialog.

   ii. SIP-I protocol: ASR is the ratio of the number of received 200 OK with an encapsulated ANM (in response to an INVITE with an encapsulated IAM initiating a dialog) to the number of INVITE sent with an encapsulated IAM.

d. *NER* – Expresses the ability of a network to deliver a call without taking into account user interferences (measure of network performance) in a given period of time. In a TDM environment, NER has been defined in ITU-T E.425.

   i. SIP protocol: NER is the ratio of the number of received responses amongst the following responses, with the number of sent INVITE initiating a dialog:

      - A response 200 OK to an initial INVITE; or
      - A BYE response; or
      - A 3xx response; or
      - A 404, 406, 410, 433, 480, 483, 484, 485, 486, or 488 response; or

        NOTE: 403 is not included because it is categorized as both Network and User events and 403 is not sent to international networks.

      - A 600, 603, or 606 response; or
      - A CANCEL message (in forward direction i.e., from the calling party).

   ii. SIP-I protocol: NER is the ratio of the number of received responses amongst the following responses, to the number of sent INVITE with an encapsulated IAM:

      - A response with an ANM encapsulated or
      - A response with REL encapsulated and cause value 1, 17, 18, 19, 20, 21, 22, 28, 31, 50, 55, 57, 87, 88 or 90, or
      - A CANCEL message (in forward direction i.e., from the calling party)

        NOTE: It is recognized that cause value 53 (outgoing calls barred within CUG) has to be considered as a user failure. Being the scope of the i3F document is limited to international interconnection, they assumed that no SIP message related to this cause value 53 will be received.

e. *PGRD* (preferred over PGAD, because PGRD depends on the end-user behavior) -- Expresses the time elapsed between a request for a call setup and the alerting signal for that call. In a VoIP environment, and for the purpose of this document, PGRD is defined

[86] *Technical Interconnect Model for International Voice Services*.

as follows:
The PGRD is the elapsed time after INVITE unti media is available to the remote device. It can be calculated with the average time between sending an INVITE initiating a dialog and the first received message of the following SIP Responses:

i. 180 resulting in local ringing at the remote device.

ii. The first 200 OK without preceding 180 or 183, resulting in the call/session being answered.

iii. 183 with SDP and if there is no 180, resulting in media being available from the far end to the remote device.

C.4.5.7 Methodologies for QoS Measurements – Multiple Network Domains

Where there is more than one Carrier between the originating and the terminating Service Providers, two different approaches are recommended by the i3F:

- An available implementation called an aggregation scheme where individual carrier measurements are added or "aggregated" and reported to the Service Provider [2]; and
- A medium term implementation called the Media Loopback Approach under development by the IETF MMUSIC working group[87].

See the *Technical Interconnect Model for International Voice Services* for a description and calculation methodology for the Aggregation and Media Loopback methodologies.

C.4.5.8 KPI computation for SLA/QoS reporting

As a general principle, the i3 Forum recognizes each provider can offer KPIs of QoS parameters according to its own commercial policy[88]**.** KPIs are averaged values over a time period, the length of which is outside the scope of this document. Generally speaking, the reported KPI is obtained as a function of all the measured samples *KPI = f(KPI0, KPI1,..., KPIN)*. The following functions are suggested:

- *RTD*: 95/99 % percentile or average
- *LOSS*: 95/99 % percentile or average
- *JITTER*: 95/99 % percentile or average

- *MOS*: 95/99 % percentile
- *ALOC*: average (by definition)
- *NER*: average (by definition)
- *ASR*: average (by definition)
- *PGRD*: 95/99 % percentile.

C.4.6 Charging

The FCC has stated that for terminating calls the end goal is to bill and keep the call as the default charging treatment. With that said, carriers can negotiate alternative arrangements (e.g., session and message based charging as in the case for RCS). The FCC is still evaluating originating traffic.

International traffic is typically charged based on minutes of use, with a transit provider transporting the traffic.

---

[87] *Technical Interconnect Model for International Voice Services*.

[88] *Technical Specification for Voice over IPX Service*.

C.4.7 Roaming

Roaming may occur with either direct connection between the visiting and home networks, or via a third-party transport provider (e.g., GRX or IPX provider).

Wireless roaming is a special case of interconnection. Section C.2.2.3 describes RAVEL, which enable IMS deployments to emulate the interconnection model of circuit switched roaming.

C.5 Assessment of Key Interconnect Models

C.5.1 i3 forum

The i3 Forum is in its sixth year with many technical releases, including "Technical Interconnection Model, Release 5" describing Voice interconnect implementation specifications. This bilateral model established the QoS "carrier domain" to include both carrier domains, excluding the SP domain. Public interconnection for the Cxr-Cxr and Cxr-SP is supported but many security functions including IPSec for signaling is required. Signaling and media functions are specified and further detailed in separate i3 Forum technical recommendations. At the lower layers, interconnection may be accomplished via private, layer 2 ethernet or public internet. The most notable technical challenges are T.38 fax and QoS. Due to inconsistent vendor implementation, the mixture of TDM and IP technologies in the end-to-end path, and standards gaps, both QoS and T.38 fax are still be closely analyzed by the i3 Forum.

Like the bilateral model, the i3 Forum is now documenting the implementation specification for a multilateral model with specific technical and business constructs necessary to meet the GSMA IP Packet Exchange IPX model requirements. Although this model is still under development by the GSMA, the feat of implementation is already being trialed, and experience has triggered changes to the model and the i3 Forum's evolving technical specification. Unlike the "bi-lateral" model, the IPX is both bilateral or multi-lateral, delivering a single service over one interconnection or "multi-service". It is the multiservice functionality that sets this model apart, given that in addition to the service of Voice, GPRS Roaming and Transport for signaling services, etc., are also specified.

Beyond the technical highlights stated above, there are rigorous commercial constructs in the form of "schedules" for each service that, for example, cover the concept of transparency and QoS SLAs, as well as other detailed technical specifications (for example, covering security), but are out of scope for this summary. Most notable regarding the commercial constructs for the IPX model are the QoS SLA requirements in the concept of "cascading." Cascading SLAs requires each of the IPX Carriers in the chain of a service to commit to monthly reporting and troubleshooting of faults with the contractual commitment to do so under penalty of written service level agreements. This cascading of responsibility means each party in the service chain is responsible for monetary penalties, which is proving to be both a technical and commercial implementation challenge.

In summary, the IPX model requires further technical specificity from a QoS, Security, and Service (multiservice) perspective, and the "one connection" to the IPX carrier for all services with commercial commitments make this model a target implementation that is being embraced but not yet fully deployed.

C.5.2 ATIS NGN

ATIS-1000009.2006 (R2011), *IP Network-To-Network Interface Standard for VoIP* (NNI Phase1), is a generic signaling and media profile reflecting implementations at that time. The current ATIS NGN specifications build primarily on the relevant IETF and IMS specifications and are closely linked to the corresponding i3 forum specifications and 3GPP TS 29.165.

C.5.3 IMS

The i3 forum, ATIS NGN, and GSMA interconnect specifications are primarily profiles of 3GPP IMS, which builds further on the underlying IETF protocol specifications.

C.5.4 IETF

The IETF provides the base protocol specifications used by IMS without defining any aspect of the interconnect architecture or providing any profiles associated with the interconnect. All of the key protocols used over the interconnect were developed in the IETF, including SIP, SDP, RTP, and IPSec.

C.5.5 Other Models

Many other interconnect profiles exist, with most based on SIP or SIP-I. The most notable exception is Google Talk Federation, which is based on XMPP. Many of these other interconnect profiles use the Public Internet rather than managed facilities. They also use a variety of protocol options, different security models, and different addressing/routing solutions.

WebRTC suggests that use cases exist in which users can rendezvous using the same web server so that interconnect between service providers is not necessary. This scenario is generally limited to a subset of WebRTC endpoints.

C.5.6 Summary

The i3 forum and ATIS NGN specifications are the most mature profiles available but have limitations that need to be addressed in future work. Besides service limitations described elsewhere in this document, these models generally assume bundling of signaling with media at the interconnect point (by forcing the anchoring of media at the point of interconnection) and thus do not fully support business and charging models that separate responsibility for service layer functions from media transport.

C.6 Conclusions

C.6.1 Foreword

Key technical and business challenges were identified, as were observations during the review of both existing and developing interconnect models. Existing documented IP interconnect models are primarily focused on “voice” service, but more advanced “multiservice” models are accompanied by both further technical and business requirements with the goal of improving security and quality of service.

Interconnect practices necessary to realize a fully functional commercial implementation cannot overlook the operational and transition issue from TDM to IP. However, if one assumes a “technical substitution” and not a onetime “cut-over”, this not only simplifies the transition but represents what is being experienced in today’s marketplace.

C.6.2 Observations/Expectations

One of the challenges to wide-scale deployment of more efficient IP interconnect is the lack of availability of an industry-wide address translation and routing solution (e.g., ENUM). Its availability would allow fundamental changes in the interconnect architecture to flatten the routing hierarchy and to enable more direct interworking between service providers.

With wide deployment of IP interconnect, current problems with telemarketer calls, robo-calls, and fraud are likely to increase. Authentication of users and/or service providers might help to mitigate this threat.

The industry is moving from an established interconnection model to multiple models that have varying requirements for aspects including QoS and security, and also varying compensation arrangements. Negotiated commercial agreements allow early adopters to work out the technical details and choose the proper path for capacity expansion to meet their customer and business needs. This diversity breeds innovation to a point, but eventually a few dominant models must prevail.

The unique QoS and security requirements of these different models will introduce new challenges and opportunities for managed communication services.

It is reasonable to anticipate a gradual adoption of IP interworking for voice services, with both TDM and IP technologies coexisting to form a hybrid network. Each provider decision to implement network

modernization will be based upon their business and customer needs, recognizing that limited resources will influence modernization to areas of growth or high cost. To this end, it is expected that the decision as to when and where to perform a TDM to IP technical substitution is based upon many factors and best left to the decision of SPs and Carriers. Although this is not always the case, limiting migration to technical and operational constraints necessary for technical interconnect eliminates many business variables while retaining the commercial flexibility, allowing companies to adopt other forms of commercial agreement based upon business and customer needs.

Technical implementation of IP interworking is commonplace for data and voice, but it is recognized that when it is necessary to reproduce the voice quality of experience and security achieved by TDM infrastructure, certain engineering and operational conditions must be met.

Currently the primary method of interconnect with IP providers is PSTN TDM interconnect via TDM gateways. Many destinations will remain reachable only via TDM for some considerable time, so consideration must be given to maintaining this access as IP interconnect becomes the norm.

C.6.3 Key Issues

C.6.3.1 Bundling

Bundling of signaling with media for transport at the point of interconnect is assumed by some intercarrier business agreements, but could potentially be changed in the future with new agreements. This would potentially enable the unbundling of charging for the service and media transport functions, the use of more efficient media routing procedures like OMR, and the resulting improvement in quality of experience from shorter media routing and lower delay. This is particularly an issue for interconnection of communications service that is already unbundled from IP transport service at the point of user access – e.g., as is common with OTT providers.

C.6.3.2 Addressing & Routing

While technical solutions are available, no accepted industry-wide addressing and routing solution is deployed. Availability of an industry-wide solution (e.g., ENUM) would enable significant improvements in the interconnect architecture through flattening of the routing hierarchy and by enabling more direct interworking between service providers.

C.6.3.3 Media routing & NAT Traversal

NATs remain a challenge to real time communication and the industry continues to evolve solutions to enable media connection through NATs. ICE is the preferred IETF mechanism to establish peer-to-peer media connection in the presence of NATs, but its applicability in carrier networks remains to be established.

OMR overlaps to some extent with ICE in functionality, but is in some ways better suited to carrier networks since it optimizes the media path in the presence of both SBCs and NATs.

Since both ICE and OMR are likely to see significant deployment, procedures for coexistence and/or interworking between them are likely to be useful.

C.6.3.4 Security

While IPSec is the norm for signaling security at the point of interconnection between service providers, TLS is also used in many other networks. While IPSec is preferred to secure a small number of large bandwidth signaling connections, TLS may have some advantages when scaling to a large number of interconnections.

Identity assertion and authentication of users and service providers is also a growing issue when flattening the network and may require new approaches for scalability.

There are also numerous approaches to media security that complicate interconnection. Some use SRTP with varying key exchange procedures, while others use RTP over private facilities or over a larger IPSec pipe for security.

When using the public internet for transport of signaling or media, more stringent security procedures are usually, but not always, used.

C.6.3.5 QoS

There already are defined quality metrics in use today that allow operators to sufficiently manage and measure both transport & service QoS parameters.

Case in point: Phone service “reader score” as rated by Consumers Report (6/12) found that six (6) out of the seven (7) top-rated “phone service” providers were VoIP, and that all but one achieved a high score in “call quality”.

There are business, technical, and operational aspects of offering special QoS Service Level Agreements (SLAs), and the need today is determined by an SP or Carrier’s request during interconnect negotiations. In the IP realm, there is usually distributed responsibility for QoS, and special QoS SLAs only apply to certain situations.

From the end user perspective, each SP is responsible for only a portion of the end-to-end transport, so Quality of Experience issues are difficult to troubleshoot.

When end-to-end QoS SLAs are not available (e.g., OTTs), there is an undefined distribution of QoS responsibility across multiple operators.

The end user needs to understand the distributed responsibility for QoS and have a means for viewing quality of the access and interconnect provided by their SP so they can differentiate quality and price to understand value.

A combination of the following can help engineer a required level of QoS: Capacity Management (monitoring and planning); Admission Control (accept manageable call volume); and DiffServ (packet marking and prioritization). If higher levels of QoS enforced by SLAs are desired, specific engineering, technical, and operational guidelines need to be observed – e.g., GSMA’s IPX model.

QoS becomes more complex as you add providers in the end-to-end path. For example, if there is more than one provider, all would have to agree to what, how, where, and when to measure and exchange QoS data for SLA monitoring.

Even with exacting standards, varying architectures and network topologies make comparing QoS among two carrier networks between the same endpoints very difficult and sometimes misleading.

If we assume use of the public internet as the transport medium, QoS SLAs are not currently possible, but even so, “best effort” provides acceptable quality for most users.

Most user perceived problems are associated with unmanaged access networks

If we assume the use of privately managed dedicated facilities, then TDM-like levels of QoS SLAs are possible, but not guaranteed.

One “private networking” solution is the GSMA’s IP eXchange (IPX) model. The technical and business constructs specified by the GSMA IPX model address – for example, Security and QoS. However, even the GSMA recognizes true “end-to-end” QoS SLAs (from subscriber to subscriber) is a target architecture and although possible, not yet economically feasible.

The need to mark VoIP packets as priority traffic over the open public internet to allow the offering of quality voice service has yet TBD.

When we have multiple types of media, it raises the need to classify traffic types and treat them differently to deal with network congestion when it occurs – e.g., DiffServ can be used to give voice priority over video.

C.6.3.6 Other Aspects

The variety of signaling protocols, service variations, codecs, charging/business models, and interconnect architectures (bilateral versus multilateral, and flat/direct versus hierarchical Class 4/5) are additional sources of variance between interconnect models.

Other aspects mentioned throughout the document as worthy of further analysis include: VoIP Proxy, VoIPX Common Transport, VoIPX Signaling, VoIPX Media, Fax over IP, Modem Connection, VoIPX Security, VoIPX QoS Monitoring/KPIs, VoIPX Routing and Traffic Management, VoIPX Break-in/Break-out Connectivity, Number Portability, and WebRTC.

C.6.4 Recommendations & Next Steps

The industry needs to agree on a tiered routing architecture based on the carrier registering the user's TN. The interconnect architecture should flatten with more direct connections between service providers since LATA routing is unnecessary.

Future interconnect models should support identity authentication of users and service providers to provide security, compensation support and fraud/spam control.

ATIS should perform the following actions:

- Analyze the IP interconnection issues described in Appendix C, section C.5, to make recommendations for applicability of existing options or development of new specifications. These aspects include Security, QoS, Signaling, Media, Fax over IP functions, as well as transport configuration options and routing.
- Analyze the impact of emerging technologies and services (e.g., OTT, cloud, WebRTC, OMR) on the evolution of interconnection models.
- Examine commercial issues related to the technical issues, including the potential enhancements for multiservice support.
- Evolve current IP interconnection models to incorporate the latest advances.
- Encourage the voluntary convergence of the industry on a minimal set of the most broadly adopted models.

Appendix D

Numbering

Appendix D: Numbering

D.1 Background

The numbering report addresses only the North American Numbering Plan (NANP). Specifically it addresses the US portion of the NANP, although some background and recommendations could have relevance in other NANP countries.

D.2 Names & Addresses

Today, telephone numbers (TNs) are used independently as both addresses and names. Communications networks use them as addresses to make routing decisions. For example, 571-434 is the network address of the Verizon Herndon switch. Consumers use them as names – "if you want to reach me, dial 571-434-5400." Until the late-90s, each TN was used as both an address and a name, and its use as an address took precedence over its use as a name. The TN was a combination of the address of the switch, the first 6 digits, and of the specific line on that switch, the last 4 digits. The user would dial the TN and the telephone switches would use the digits to set up the connection. The TN was linked to the geographic location of the user and the telephone switch associated with the user. If a user moved to an area served by another switch they had to change their TN. The use of the TN as an address overrode its use as a name.

In the late-90s, the implementation of location routing number (LRN) call processing enabled the separation of the use of TNs as a name from its use as an address. LRN was a nationwide effort to change how telephone calls are routed. Instead of using the dialed TN to route a call, networks now use the LRN. LRNs look exactly like TNs, but they designate a specific switch in the network rather than a specific user. Today, over 90% of all telephone calls in the United States generate a query to a database to obtain the LRN. The dialed TN is replaced with the LRN in the call signaling. The switches use the LRN, not the TN, to route the call. The dialed TN is carried in another call parameter and is used to complete the call when the call reaches the terminating switch. The LRN identifies the switch and the dialed TN identifies the user on that switch. Thus, the LRN becomes the address while the dialed TN continues as the name.

The use of LRNs enabled the implementation of local number portability (LNP) which allowed service providers to move a TN from one switch to another and therefore one service provider to another. LNP also is used to conserve numbering resources by allowing the allocation of a smaller quantity of TNs to service providers than had previously been possible. Where TNs used to be issued in blocks of 10,000, the same block of TNs can now be divided into 10 blocks of 1,000 and shared among many service providers. This is called thousands block number pooling and was implemented in the early-00s.

D.3 Telephone Number Structure

The figure below shows the structure of the different numbering resources available for assignment;:area codes (aka number planning areas or NPAs, 3 digits), central office codes (CO codes, 6 digits), thousands blocks (1KBs, 7 digits), and TNs (10 digits). These four resources can be divided into two categories: 1) network resources - area codes and CO codes; and 2) consumer resources – 1KBs and TNs.

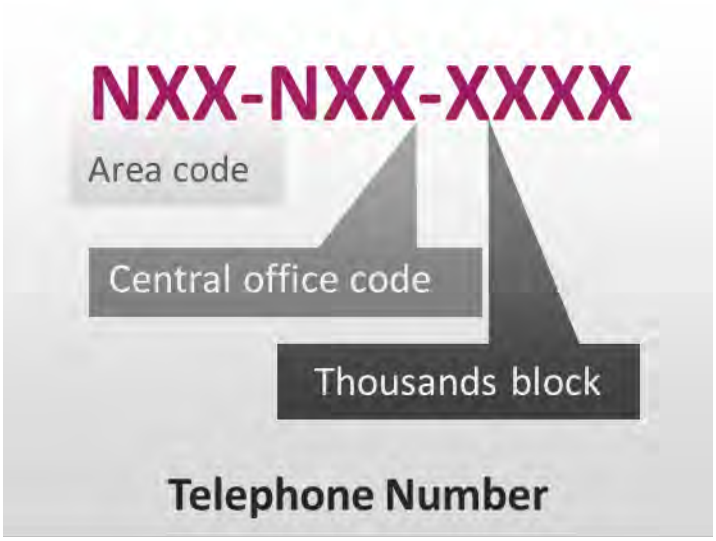

Figure D.1 - TN Structure

Table D.1 shows the quantity of resources available for each. It's important to note that there are eight hundred area codes in the entire North American Numbering Plan (NANP). Once these are all allocated, more digits will need to be added to our TNs. There are also eight hundred CO codes in an area code and once these are all allocated, a new area code must be added. This is the definition of area code exhaust.

Table D.1 - Quantity of Numbering Resources

Resource	Quantity
Area Code	800 in NANP 8M TNs/Area Code 6.4B TNs in NANP
CO Code	800/area Code 10K TNs/CO Code
1KB	10/CO code 1K TNs/1KB

There are geographic and non-geographic area codes. Geographic area codes are allocated to states and cover a specific geography within the state. Non-geographic area codes are typically used for a specific service such as toll free.

CO codes are allocated to a specific service provider and switch. TDM networks use CO codes to route calls – i.e., 6 digit routing. The implementation of LRN allowed networks to continue to route on 6 digits because the CO code of the LRN identified the terminating carrier's switch. At one time, CO codes were allocated as a block of 10,000 TNs of inventory in addition to identifying the switch for routing. Today, they are only allocated as an LRN, to identify switches, or to replenish 1KB number pools.

1KBs are allocated to service providers as blocks of 1,000 TNs for inventory to allocate to users.

TNs are allocated by service providers to end users.

D.4 Rate Centers & LATAs

In addition to being allocated to specific service providers and switches, CO codes are also allocated to rate centers. A rate center is a geographic area designated by an ILEC that can be used to generate distance based billing for phone calls. Historically, this often corresponded to the geographic area served by a switch. There are over 20,000 rate centers in the US. Since CO codes are associated with a rate center, the ten 1KBs associated with a specific CO code are also associated with that rate center.

LATAs are geographic areas set up at divestiture to differentiate between local and long distance calling. According to FCC rules, calls within a LATA are carried by a local telephone company and long distance calls are carried by an interexchange carrier. The Telecom Act of 1996 enabled long distance providers to provide local service and criteria that would allow local providers to provide long distance service. Local service providers have met these criteria since 1996 and LATAs are no longer relevant from a billing perspective. There are 197 LATAs in the US.

Rate centers and LATAs, while losing relevance from a consumer and billing perspective, are still quite relevant from a numbering perspective. Service providers are entitled to one CO code (as an LRN) per LATA per switch. That is, if there are three switches within a LATA, they get three CO codes to use as LRNs. Also, service providers are entitled to one 1KB in each rate center in which they plan to offer service.

D.5 Interconnection & Routing

In order to be eligible for the assignment of geographic numbering resources, service providers need to prove that they have an interconnection agreement with the ILEC in the region where they are requesting resources. For example, if a service provider wanted Washington, DC numbering resources, they would need to provide proof of interconnection with the ILEC (Verizon) in Washington, DC. This interconnection is typically a TDM trunk into the ILEC tandem switch that serves traffic in that area.

This interconnection to the ILEC tandem will be associated with a specific CO code. The North American Numbering Plan Administrator (NANPA) will assign a CO code to that switch for that service provider to use as an LRN. Other service providers that do o't directly connect to that service provider will route calls to the ILEC tandem. The tandem will route those calls to that service provider over that interface. Service providers that do have a direct connection to that service provider will route calls directly rather than go through the tandem.

The CO code that's assigned to the switch will also be assigned to a specific rate center. The ten 1KBs from that CO code will be used to populate the pool of numbers for that rate center. The service provider can also request numbering resources for inventory. They can request a 1KB associated with the CO code they were assigned. They can also request a 1KB in any rate center in that LATA. If there are ten rate centers in the LATA, they can request a 1KB in each of those rate centers. But all of those 1KBs can use the same CO code as an LRN for routing purposes.

D.6 Geography & Telephone Numbers

There is currently a tight linkage between geography and TNs.

- A service provider can only get numbering resources in a specific state if they interconnect to the ILEC in that state.
- A service provider can get a CO code in each LATA for each switch that they have deployed. The CO code is assigned to a specific rate center in that region.
- 1KBs from CO codes assigned to a rate center are used to populate the pool of numbers available for assignment.
- Service providers that provide service in a region are eligible for a 1KB in each rate center in that region.
- Many of the calls between service providers traverse points of interconnect (POI) physically located in that region, often at an ILEC tandem.

D.7 Impact of PSTN Transition

As the PSTN transitions to IP, networks will stop using TNs as routable addresses. That is they will no longer rely on the first 6 digits of the TN to route the call – i.e., the IP networks will no longer need LRNs. Instead, they will translate the TN to an address that is usable by IP networks, such as a URI. This is a profound change and will have a significant impact on addressing (and naming) and number administration.

Even though IP networks will no longer rely on TNs as addresses, TNs will still be used for the foreseeable future. They are still useful to consumers as names because they are familiar, globally unique, non-linguistic, easy to use on small keypads, internationally compatible, and provide a level of anonymity. More importantly, they will be required for backwards compatibility for nodes and regions that do not have IP infrastructure. TDM infrastructure will still exist both within the US and outside the US for many years. We can assume that the TDM infrastructure will still need TNs and existing capabilities for interoperability and routing.

In addition to impacting addressing and administration, the PSTN transition could also have an impact on number authentication.

D.8 Future of PSTN Names

As stated already TNs will be used as names on the PSTN for the foreseeable future. It's possible that they will be replaced by another naming resource in the future. While it is too early to determine whether there will be a successor to TNs on the PSTN, much less evaluate and make a recommendation for one, it is worth identifying desirable attributes of such a resource.

Attributes of a future PSTN name:

- Separation of the name and address.
- Method to map name to address.
- Globally unique.
- Portability – the ability to select service provider without changing name.
- Consumer selection of the name.
- Authentication.
- Policies that discourage speculation and squatting.
- Extensive inventory.

D.9 Addressing

D.9.1 IP Network Addressing

The current LRN process of querying the TN to obtain an LRN and using the first 6 digits of the LRN to route based on static routing tables will be replaced on IP networks by a process to query the TN to ultimately obtain an address usable on IP networks, such as a URI. Many companies already perform this same process using a version of ENUM within their own networks. ENUM, however, is hardly used today between networks in the manner necessary for the PSTN. Service providers will need to use a version of ENUM for this purpose if they plan to interconnect using IP within the next couple of years. While other solutions may evolve over time, such as those envisioned in the IETF effort called Telephone-Related Queries (TeRQ) or ATIS's effort called Trusted Information Exchange (TIE), ENUM is the only viable alternative for the near term.

The IP addressing process for TNs can be divided into three categories:

1. *Administrative information exchange* – Ability to share the address of a route server associated with the TN.
2. *Discovery* – Mapping the TN to a route server that contains addressing information.
3. *Mutual authentication* – Authenticating the querying party and the queried party.

Currently an inter-service provider ENUM solution would likely include the following with regard to these three categories:

1. *Administrative information exchange* – A central DB provider which maps TNs to a Tier 2 server address, a DNS name server address.
2. *Discovery* – A DNS query over the secure IP connection retrieves a DNS NAPTR record from the Tier 2 server, the NAPTR typically identifies a gateway.
3. *Mutual authentication* – A secure IP connection that allows a service provider to authorize each individual querying party for access to their Tier 2 server.

The industry needs to address these three issues to determine an ENUM-based solution for the US.

Having access to a service provider's Tier 2 implies that those service providers have an agreement and would also have an interface for exchanging traffic. For the purposes of evaluating addressing and routing, we will assume that IP interconnect arrangements will cover termination of traffic, but not transit of traffic to other service providers.

The interconnection point between networks is defined by the application layer interface (gateway), not the network or physical layer. The physical address of the gateway provided by the Tier 2 can be correlated to the geography associated with the geographic number, or not. And that association can be narrow or broad. For example, the address provided for a 212 number could be located in NYC, NY state, the Northeast or the East Coast. Or the Tier 2 could operate more like a mobile network and provide a gateway based on the location of the device and the interconnection points of the service providers.

Since IP enables mobility, it makes sense for the correlation between TN and gateway not to be narrow in geographic scope. To do so would drive inefficient network architectures. However, the industry is not at a stage yet where it could go to a completely mobile model. We should assume that there will be some broad correlation between the TN and the physical address of the gateway.

D.9.2 TDM Network Addressing

It has been suggested that the FCC could lift the requirement for ILECs to provide interconnection on a TDM basis. Presumabl,y companies that only had a TDM infrastructure would contract with a third-party to transport and transcode their TDM-to-IP calls. At this time, the industry cannot assume that that will be the case.

TDM-to-TDM routing will continue to work as it does today for the foreseeable future. CO codes will be associated with a specific interface to the PSTN. TDM calls will be routed to that interface based on the first 6 digits of either the LRN or the dialed digits.

TDM-to-IP routing will rely on TNs and existing TDM capabilities. For some period of time, there will be two interfaces for IP accessible TNs: the IP interface and the TDM interface. The most obvious solution would be to retain the existing TDM routing practices for IP-capable TNs. The IP network could get a TDM interface identified by an LRN.

The existing TDM routing practices, however, would create a new demand for CO codes for LRNs for the new IP interconnects. This new demand could advance the exhaust of many area codes. There are potential alternatives to this practice that use existing TDM capabilities, but have trunking and billing implications that would need to be addressed.

Alternatives to continuing to use existing practices are:

- *Decouple the geography of the LRN from the geography of the TN* – Allow the terminating service provider to choose the location of their interface, e.g., a call to a Virginia TN could go to a California interface. This would allow service providers to consolidate the TDM->IP traffic in a smaller number of interfaces.
- *Use non-geographic NPA-NXXs for LRNs which identify specific service providers*.
- *Route on 10 digits* – Use a non-geographic NPA.

The impact of changes to the LRN/location association on Intercarrier Compensation has yet to be evaluated.

The industry should evaluate TDM->IP addressing alternatives that would conserve numbering resources and not require IP providers to duplicate the TDM infrastructure – i.e., an LRN in every LATA for TDM terminations.

D.10 Administration

The transition to IP will create new demand for TNs but will also offer the ability to conserve TNs. Numbering administration can be divided into: 1) network resources, area codes, and CO codes; and 2) consumer resources, thousands-blocks (1KBs), and individual TNs. The industry should look at ways to conserve both categories.

D.10.1 Network Resources

Area codes are our most scarce and important resource. There are only eight hundred area codes available and when they are gone the numbering plan will need to be expanded beyond 10 digits. The good news is that with careful planning, the numbering plan will never need expansion. In fact, the transition to IP offers some opportunities to use area codes in new and innovative ways.

Area codes are divided into geographic and non-geographic numbers. Non-geographic codes are assigned to specific services such as toll free or Personal Communication Services (PCS), and geographic codes are assigned to traditional telephone service. But there's no need to maintain this distinction going forward. Geography is irrelevant to IP communications. Consumers that access their service online can do so from anywhere. IP offers the opportunity to start using non-geographic codes for traditional voice service. This would require the industry working together to develop solutions for interconnection, routing, and 911. The industry should consider expanding the geographic area served by area codes.

The evolution to IP interconnection will likely increase CO code demand, if CO codes continue to be managed as they are today. Service providers may need a CO code for an LRN for the new IP connection to the PSTN. Or they may need it for a TDM interface for TDM networks that corresponds to the IP interface. Certainly, without changes to the LRN Assignment Guidelines, they would be entitled to a CO code for each new IP interface.

The industry can use this transition as an opportunity to reduce the assignment of CO codes. CO codes are assigned to each service provider per switch per LATA. As people move their service to mobile and VoIP, LATAs will continue to become less relevant. There is no technical reason to have an IP POI in each LATA.

The industry should consider breaking the linkage of CO codes to LATAs for future assignments. To do so would conserve resources and allow service providers to be more creative and efficient in designing their networks.

D.10.1.1 Consumer Resources

In the early 2000s, the industry implemented multiple conservation measures. While these measures have conserved CO codes quite well, number utilization is still about 50% of allocated TNs. Service providers are entitled to one 1KB in every rate center where they provide service regardless of whether they have customers. Rate centers are even more irrelevant than LATAs. Not only are they irrelevant, they are problematic, because they create complexity in routing decisions and are inefficient for numbering. Rate centers are the primary reason that the industry can't improve beyond 50% utilization of allocated TNs.

The industry should consider decoupling rate centers from numbering. This creates inefficiencies for both number conservation and network engineering.

While there is no real risk of NANP exhaustion now, we know from the 1990s (as we went through the last major change in numbering) that demand can increase rapidly and making broad changes takes time.

The industry should closely monitor number allocation and utilization to look for any signs that increasing demand is causing premature area code exhaust and placing the NANP at risk.

As TNs stop being used as addresses by networks, they are going to be primarily used as names by consumers. It's possible that consumers could be allowed to register TNs directly, just like they can register domain names today. There would have to be measures put in place to discourage squatting and speculating, but there would be many benefits from this system. Consumers would get the TNs they prefer and service providers would be relieved from the tedious process of managing inventories of TNs across 22,000 rate centers. If the consumer controlled the TN – i.e., held the certificate as the assignee – porting would be much simpler. A complex pre-porting process would no longer be required. TNs could be ported in seconds at the consumer's request.

The industry should assess the implications of direct consumer registration of TNs.

D.11 Authentication

Unlike the current PSTN, the Internet is not a closed, trusted network. By design the Internet is an open network that facilitates the flow of information between computers. Unless specifically secured, it is relatively trivial to impersonate an entity on the Internet. This is called spoofing and it is already a problem with TNs. It is becoming quite common to spoof caller ID for spam text messages and telemarketer calls. Spoofing is only going to get worse as VoIP and IP interconnection become more common and as access charges are reduced. Email has become notorious for the difficulty of determining the actual sender of the email, a key enabler of spam. A means of determining who owns a number must therefore bring not just authority, but also a responsibility, to TNs on the Internet and on the managed IP networks that will carry much of the voice traffic.

The security of TNs on the Internet is the most significant issue that the industry will face. It is important to secure TNs to the proper authority – the assignee. Domain names and IP addresses were both secured only after the industry realized they could be spoofed and imitated.

The problem of authentication is easier to solve in an all IP environment than it is on the current TDM network. The TDM network has the problem of transitive trust. That is, each entity in the chain trusts the entity previous to them and therefore there's often no direct trust relationship between the originator and terminator of a call. On the Internet, a digital certificate can be associated with the TN that binds it to the assignee. The TN can be authenticated everywhere in the chain, including the end point.

One solution that is available as part of the transition to IP networks is the introduction of a certificate authority in the TN administration process. The administrator would provide a certificate for each TN or block to the assignee. The assignee could have the ability to delegate authority for that certificate to others such as reseller, enterprises, and even consumers. In addition to verifying caller ID, this certificate could be used for management of the TN including establishing services and applications, changing service providers, as well as verifying caller ID.

The industry should learn lessons from the past and secure TNs on the Internet before lack of authentication becomes a problem.

D.12 Recommendations

To enable industry-wide IP-IP interconnection the industry should resolve open issues regarding a TN-to-Internet addressing solution. These open issues concern:

- *Administrative information exchange* – Method of sharing address of the route server associated with the TN.
- *Discovery* – Method of mapping the TN to an address of a route server during call processing.
- *Mutual authentication* – Authenticating the route server querying and queried party.

To conserve numbering resources and take advantage of the non-geographic nature of Internet-based services, the industry should eliminate number allocation based on rate centers and LATAs and develop a new TDM-to-IP addressing solution that does not tie the geography of the TN to the physical geography

of the point of interconnect. In addition, the industry should consider expanding the geographic area covered by area codes.

As TNs move to IP the industry should secure them, as has already been done with domain names and IP addresses, to prevent spoofing.

IP interconnect should foster new services and service providers. The industry should monitor number allocation and utilization.

As TNs evolve away from their use as an address for networks, the industry should consider allocating them directly to consumers.

Appendix E

Social Policies & Regulations

Appendix E: Social Policies & Regulations

The Focus Group considered various aspects of the PSTN transition in the context of existing social policies and regulations, as described in the following table. In addition, key technical factors associated with access, transport and applications/services are listed.

Table E.1 - Existing Social Policies and Regulations

SOCIAL POLICY	REGULATION
Reachability - Networks should enable the ability for devices/applications to contact any device/application with an E.164 telephone number.	**Interconnection/Interoperability** • Operators must provide non-discriminatory IP-IP interconnection capabilities. • NNI signaling transparency to allow signaling information to pass transparently from access network to access network when not understood by the interconnect network. **Dialing Parity** **Numbering** **Number Portability** – Consumers can change their service provider and keep their existing telephone number.
Universal service – Advanced services should be accessible to the public with good quality at reasonable rates even in rural and high cost areas.	**Universal Service Fund**
Public Safety/Emergency Services – The public should have access to communications and emergency services for health, safety, and security reasons.	**E911** - Sufficient location information must be available to meet Emergency Services location determination requirements. **Emergency Notification Systems**
Homeland security • Governmental agencies need access to communications for the security of all. • Security Requirements to insure secure access control, authentication, Non-repudiation, data confidentiality, communication security, data integrity, availability, and privacy. • Address/Identity integrity requirements to insure that identity and addressing information passed to the interconnect network should not be deleted or altered.	**CALEA** – Legal intercept requirements. **Priority Access Services**
Reliability/Availability – The services provided to the public should be reliable in both availability and QoS, both as standalone services or when aggregated with other services.	**Outage Reporting**
Accessibility – Persons with disabilities should have access to communication services.	**Access for Persons with Disabilities**
Cost Effectiveness • Accounting and reporting requirements to insure that the network can keep track of call/session specific data.	**Resale** **Price Regulation** **Depreciation and Amortization** **Unbundling**
Privacy – Personal identifying information that service providers have access to as part of providing a service must be kept private.	**CPNI**
Stranded assets – As the network transitions and certain services are no longer supported alternative solutions should be identified (e.g., FAX).	
Carrier of Last Resort	**State by state**