As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry’s most pressing business priorities. ATIS’ nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer & Limitation of Liability

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

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

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

ATIS-0100069, Voice over Internet Protocol (VoIP) Availability

Is an ATIS Standard developed by the NRSC IP Reliability (NRSC IP) Subcommittee under the ATIS Network Reliability Steering Committee (NRSC).
Voice over Internet Protocol (VoIP) Availability

Alliance for Telecommunications Industry Solutions

Approved October 30, 2020

Abstract

The PSTN transition from a TDM-based network to an IP-based network has and will continue to impact many facets of the networks. For this reason, it was decided to assess this transition with regards to network availability. This document covers reporting metrics, network design, topography, and network monitoring, relevant to Voice over Internet Protocol (VoIP) architecture (e.g., Internet Protocol Multimedia Subsystem (IMS), Session Initiation Protocol (SIP)). This document also goes into some detail explaining the difference between reliability versus availability and why the reporting metrics should focus more on availability. The purpose of this document is to outline and describe in detail how to detect and monitor VoIP network outages with select standards-based reporting metrics to track network availability as the industry transitions from the TDM network. The recommendations and Best Practices in this document will serve as the guide by which industry can monitor and track the overall performance of new and transitioning VoIP architectures.
The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Network Reliability Steering Committee (NRSC) strives to improve network reliability by providing timely consensus-based technical and operational expert guidance to all segments of the public communications industry. The NRSC IP Reliability Subcommittee was formed to identify outage reporting metrics/methodologies that can be used to consistently detect voice outages by all service providers with networks in various stages of PSTN transition.

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

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

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

**ATIS NRSC Leadership:**
Carolyn Brown (CenturyLink), NRSC Co-Chair
Andis Kalnins (Verizon), NRSC Co-Chair

**ATIS NRSC IP Reliability Leadership:**
Mark Peay (Cox Communications), NRSC IP Co-Chair
Chris Oberg (Verizon Wireless), NRSC IP Co-Chair

The ATIS NRSC IP Reliability Subcommittee was responsible for the development of this document.
Table of Contents

1 Scope, Purpose, & Application ........................................................................................................ 1
  1.1 Scope ........................................................................................................................................ 1
  1.2 Purpose ...................................................................................................................................... 1
  1.3 Application ............................................................................................................................. 1

2 Normative References .................................................................................................................. 1

3 Definitions, Acronyms, & Abbreviations ................................................................................... 2
  3.1 Definitions ................................................................................................................................ 2
  3.2 Acronyms & Abbreviations ........................................................................................................ 2

4 VoIP Availability ............................................................................................................................ 4
  4.1 Overview ................................................................................................................................... 4
  4.2 Availability, Reliability, Robustness, Resiliency, & Serviceability Defined .............................. 4
  4.3 VoIP Architecture and Deployment Strategies .......................................................................... 5
  4.4 Network Segmentation ............................................................................................................. 5
    4.4.1 Access Layer ......................................................................................................................... 6
    4.4.2 Metro and Core Layer .......................................................................................................... 7
    4.4.3 Peering ................................................................................................................................ 8
  4.5 End to End VoIP Monitoring ...................................................................................................... 9
    4.5.1 Reality-Based Reporting for IP-Based Core Network ......................................................... 10
    4.5.2 IETF/ITU Metrics ............................................................................................................. 10
    4.5.3 Percent of Registered Users ............................................................................................ 10
    4.5.4 3GPP Metrics .................................................................................................................. 11

5 FCC 47 Part 4 Disruption of Communication Regulations ....................................................... 11

A Best Practices ............................................................................................................................... 12

B Input from ATIS NRSC to 3GPP TSG SA WG5 Drop in Registered Users Metric .................... 15
  B.1 Decision/action requested ......................................................................................................... 15
  B.2 References ............................................................................................................................ 15
  B.3 Rationale .................................................................................................................................. 15
  B.4 Use case to determine service availability by monitoring a rise in the percentage of non-
      registered users ....................................................................................................................... 16
  B.5 Detailed proposal ..................................................................................................................... 16

Table of Figures

Figure 1: IP-Based Network Building Blocks (IMS Example) .......................................................... 5
Figure 2: Network Topology ............................................................................................................ 6
Figure 3: Access Layer .................................................................................................................... 7
Figure 4: Access, Metro, and Core Layer ....................................................................................... 8
Figure 5: Inter-IMS Network to Network Interface between two IM CN Subsystem Networks, based
  on [Ref 1] Service assurance monitoring systems along with robust element monitoring systems become requirements for monitoring transitioning
  IMS networks (i.e., Next Generation 9-1-1) ................................................................................. 9
Table of Tables

Table 1: Applicable Best Practices ................................................................. 12
1 Scope, Purpose, & Application

1.1 Scope
The Public Switching Telephone Network (PSTN) transition to IP-based networks has and will continue to impact many facets of the networks. For this reason, it was decided to assess this transition with regards to network reliability. This document covers relevant reporting metrics, network design, topography, and network monitoring. This document also goes into some detail explaining the difference between reliability versus availability and why the reporting metrics should focus more on availability.

As the PSTN and wireless networks transition to all-IP communications, many aspects of the way networks are managed must also transition, presenting new challenges. One such challenge is how outages are measured and reported in IP networks, and how faults that cause outages can be identified for reporting and restoration activity.

Interoperability between existing PSTN services and the newer IP-based services will need to continue for a number of years; thus, PSTN transition will continue to be an evolutionary process. During the transition process, successor networks will be used to lessen the strain on the existing infrastructure while supporting a range of IP-based services and applications. To meet our National goals, these services will have to achieve certain targets with respect to availability, emergency notification, accessibility, and other critical needs.

1.2 Purpose
To outline and describe in detail the reporting metrics, monitoring standards, development, and deployment of the IP infrastructure as the industry transitions from the existing TDM network.

1.3 Application
The recommendations and Best Practices in this document will serve as a guide by which new VoIP infrastructure or transitioning PSTN networks should be monitored and maintained.

2 Normative References
The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[Ref 1] ATIS-I-0000034, PSTN Transition, Assessment and Recommendations.¹

¹ This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at <https://www.atis.org>
² This document is available from the Institute of Electrical and Electronics Engineers (IEEE) at <https://www.ieee.org>
3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at <https://glossary.atis.org/>.

### 3.1 Definitions

**FTTx:** Fiber To The “x” where “x” = home (“H”), premise (“P”), or curb (“C”).

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

**Ici:** Name for interface that exchange messages between an IBCF and another IBCF belonging to a different IMS network.

**Inter-IMS Network-to-Network Interface:** defined in 3GPP TS 29.165 [Ref 5] as an interworking between the IMS CN Subsystem and IP Networks

**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

**Ix:** Interface between IBCF and TrGW or CS-IBCF and CS-TrGW

**Izi:** Interface that forwards media streams from a TrGW to another TrGW belonging to a different IMS network.

**Mx:** Interface used for the interworking with another IMS network, when the BGCF has determined that a breakout should occur in the other IMS network to send SIP message from BGCF to the IBCF in the other network.

### 3.2 Acronyms & Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd generation Partnership Project</td>
</tr>
<tr>
<td>ATCF</td>
<td>Access Transfer Control Function</td>
</tr>
<tr>
<td>ATIS</td>
<td>Alliance for Telecommunications Industry Solutions</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BGCF</td>
<td>Breakout Gateway Control Function</td>
</tr>
</tbody>
</table>

---

3 This document is available from the Federal Communications Commission (FCC) at <https://www.fcc.gov>

4 This document is available from the 3rd Generation Partnership Project (3GPP) at <https://www.3gpp.org>

5 This document is available from the Internet Engineering Task Force (IETF) at <https://www.ietf.org>

6 This document is available from the International Telecommunications Union (ITU) at <https://www.itu.int>

7 This document is included in the white paper as Annex B. It is also available from the 3rd Generation Partnership Project (3GPP) at <https://www.3gpp.org>
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>Core Network</td>
</tr>
<tr>
<td>CPE</td>
<td>Customer Premises Equipment</td>
</tr>
<tr>
<td>CS-IBCF</td>
<td>Call Session-Interconnect Border Control Function</td>
</tr>
<tr>
<td>CS-TrGW</td>
<td>Call Session-Transition GateWay</td>
</tr>
<tr>
<td>CSCF</td>
<td>Call Session Control Function</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>E-CSCF</td>
<td>Emergency-Call Session Control Function</td>
</tr>
<tr>
<td>EMS</td>
<td>Element Management Systems</td>
</tr>
<tr>
<td>ENUM</td>
<td>E.164 NUmber Mapping</td>
</tr>
<tr>
<td>FCC</td>
<td>Federal Communications Commission</td>
</tr>
<tr>
<td>FTTH</td>
<td>Fiber-to-the-Home</td>
</tr>
<tr>
<td>HSS</td>
<td>Home Subscriber Server</td>
</tr>
<tr>
<td>IBCF</td>
<td>Interconnect Border Control Function</td>
</tr>
<tr>
<td>ICS</td>
<td>IMS Centralized Services</td>
</tr>
<tr>
<td>I-CSCF</td>
<td>Interrogating-Call Session Control Function</td>
</tr>
<tr>
<td>IEEEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IM CN</td>
<td>IP Multimedia Core Network</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPX</td>
<td>IP packet eXchange</td>
</tr>
<tr>
<td>ISUP</td>
<td>Integrated Services (Digital Network) User Part</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunications Union</td>
</tr>
<tr>
<td>MSC</td>
<td>Mobile Switching Center</td>
</tr>
<tr>
<td>NNI</td>
<td>Network-to-Network Interface</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>NRSC</td>
<td>Network Reliability Steering Committee</td>
</tr>
<tr>
<td>NRSC IP</td>
<td>NRSC IP Reliability Subcommittee</td>
</tr>
<tr>
<td>OSP</td>
<td>Originating Service Provider</td>
</tr>
<tr>
<td>P-CSCF</td>
<td>Proxy Call Session Control Function</td>
</tr>
<tr>
<td>PSAP</td>
<td>Public Safety Answering Point</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>SAM</td>
<td>Service Assurance Monitoring</td>
</tr>
<tr>
<td>S-CSCF</td>
<td>Serving-Call Session Control Function</td>
</tr>
<tr>
<td>SDP</td>
<td>Session Description Protocol</td>
</tr>
<tr>
<td>SEER</td>
<td>Session Establishment Effectiveness Ratio</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SIP URI</td>
<td>SIP Uniform Resource Identifier</td>
</tr>
<tr>
<td>SRVCC</td>
<td>Also SRV-CC, Single Radio Voice Call Continuity</td>
</tr>
<tr>
<td>SS7</td>
<td>Signaling System no. 7</td>
</tr>
<tr>
<td>SSP</td>
<td>System Service Provider</td>
</tr>
<tr>
<td>TDM</td>
<td>Time-Division Multiplex</td>
</tr>
<tr>
<td>TEL URI</td>
<td>TELephone Uniform Resource Identifier</td>
</tr>
</tbody>
</table>
4 VoIP Availability

The ATIS NRSC IP Reliability Subcommittee was formed to identify outage reporting metrics/methodologies that can be used to consistently detect voice outages by all service providers with networks in various stages of PSTN transition. This white paper provides aid for determining availability in the evolving PSTN network.

4.1 Overview

The ATIS NRSC IP Reliability Subcommittee is supportive of the new and transitioning VoIP architecture work conducted under ATIS-I-0000034, *PSTN Transition, Assessment and Recommendations* [Ref 1]. To model a diverse communications industry covering cable, satellite, wireless, and wireline deployment strategies network architecture is displayed in functional blocks of functionality. Where and how these are physically deployed across the various networks will depend on individual company’s business models, implementation, and migration strategies.

In the TDM network, discrete voice switches and voice lines and trunks of deterministic voice call capacity make the determination of the number of lines impacted by any given fault (e.g., a switch port card failure, or TDM trunk failure) fairly straightforward. In contrast, IP networks are converged service networks where voice traffic typically represents a small proportion of the aggregate traffic through any given link or switch, and the throughput per voice connection varies significantly and continuously over time. In addition, IP congestion control mechanisms, depending on how the network is engineered, may not fully restore impacted voice connections. So, the question arises: How does one achieve the level of visibility and control needed to both accurately measure and minimize network outages in IP networks?

4.2 Availability, Reliability, Robustness, Resiliency, & Serviceability Defined

New terms associated with network performance, such as robustness and resiliency, all relate to industry defined terms such as availability and reliability. According to the International Telecommunications Union (ITU), availability and reliability are defined as follows:

- **Availability**: [ability] of an item to be in a state to perform a required function at a given instant of time or at any instant of time within a given time interval, assuming that the external resources, if required, are provided [Ref 7].
- **Reliability**: The probability that an item can perform a required function under stated conditions for a given time interval [Ref 1] [Ref 7].

According to the Institute of Electrical and Electronics Engineers (IEEE), robustness and resiliency are defined as follows:

- **Robustness**: Relating to the capability of a system to handle internal and external negative situations and disturbances [Ref 2].
- **Resiliency**: The ability of resistance from disturbance that is caused by sudden changes of system configuration [Ref 3].

Serviceability, as referenced by the FCC, is defined for the purposes of this white paper as follows:

- **Serviceability**: Also known as maintainability or supportability, this relates to the ease with which system faults can be identified and resolved, including early detection of faults, debugging, replacing hardware and software within the network, and identifying root causes in order to resolve faults with minimal interruption.
While the FCC is requesting metrics for network reliability and serviceability, given the definitions and metrics provided by ITU, it is recommended that the reporting metrics focus more on network availability. The goal of this white paper is to help define outage reporting metrics that can be consistently and reliably reported across the industry. These same metrics may also be utilized to help industry more accurately report events meeting NORS Outage Reporting regulations under Title 47, Part 4: Disruptions to Communications for a VoIP network [Ref 4].

In simple terms, reliability is a measure of how often a device is working properly (i.e., performing its desired task known as uptime). A device may be out-of-service, affecting its reliability, however if the relevant network function is still being performed, then the network itself is still operational. Availability, on the other hand, is the measure of how often end users are able to access the network for their communications needs. A reliable network is often also a frequently available network; however, the two are not guaranteed. A network can be reliable in the sense that it is executing its defined objectives at a predetermined benchmark over a set period of time, but currently unavailable to customers in certain markets due to localized outages. For this reason, it is the recommendation of the IP Reliability Group that the VoIP Availability metrics be used for Part 4 FCC reporting as this focuses on end user access and end to end network interoperability of IP-based networks.

In summary, a highly available network must be engineered, deployed, and maintained.

4.3 VoIP Architecture and Deployment Strategies

Our industry has varying deployment strategies based on business needs. However, the basic building blocks for next generation IP-based networks are relatively similar. ATIS NRSC reviewed ITU E.425 [Ref 9], ATIS-I-0000034 [Ref 1], and 3GPP TS 29.165 [Ref 5] to identify the basic building blocks of an IP-based network. These building blocks are illustrated in Figure 1.

![Figure 1: IP-Based Network Building Blocks (IMS Example)](image)

Exactly where each of these components reside within a network and the number of each deployed across a network is dependent on a carrier’s geographic footprint and operational model. ATIS NRSC obtained consensus on four basic layers of a next generation network, consisting of an access, metro, core and peering layer as depicted below in Figure 2.

This exercise was important and drove ATIS NRSC’s conclusion that the availability metric was the most beneficial in tracking outage conditions as it is the measure of how often end users are able to access the network for their communications needs.

4.4 Network Segmentation

Cable, satellite, wireless, and wireline operators all reach their customers with varying technologies. This drives unique deployment and operational models across the communications landscape. To help drive consensus across these varying operating models and architectures ATIS NRSC derived four layers: access, metro, core, and peering.
Each of these layers has their own level of reliability and redundancy built in. This section will review each of the layers in more detail.

**4.4.1 Access Layer**

The Access layer remains relatively unchanged in the IP networks. Often known as the last mile access to customers, this segment of the network can be limited in the number of redundancy options it can offer. Since the deployment architectures remain relatively unchanged as networks migrate to IP, the existing alarming structure for the Access layer will continue to be used in identifying local outage conditions. Newer technologies being deployed in the last mile access space, such as FTTH / LTE / 4G / 5G / 6G, have alarm monitoring points that can be used in identifying localized outages. Edge devices such as Customer Premises Equipment (CPE) and last mile access components make up the Access layer.
4.4.2 Metro and Core Layer

The IP network core will vary across carriers as networks evolve and migrate to IP. The network resiliency afforded with IP networks adds a layer of complexity for monitoring alarms. A critical device alarm may not denote an outage condition as the metro or core networks re-converge and route around impairments.

These new conditions drive the need for reality-based reporting to effectively determine the health of a network’s core. ATIS NRSC has actively examined network monitoring solutions already in use during the PSTN transition, as well as standards-based performance metrics published by industry standards bodies (ATIS, IEEE, ITU, IETF, and 3GPP).
Within the Metro and Core layers will reside the basic building blocks of the IP network as shown in Figure 5. As shown in Figure 1, exactly where each of these components reside within the Metro and Core layers, and the number of each deployed across a network, is dependent on a carrier’s geographic footprint and operational model. These core functions are engineered across the network to add redundancy and resiliency. This adds a layer of complexity for monitoring alarms. A critical device alarm may not denote an outage condition as the core re-converges and routes around impairments. These new conditions drive the need for reality-based reporting to effectively determine the health of a network’s core and detect out of service conditions.

4.4.3 Peering
ATIS-I-0000034 defines the inter-IMS network-to-network interface (NNI). 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 [Ref 1].

The Interconnection Border Control Function (IBCF) provides application-specific functions at the SIP/SDP protocol layer for interconnection between IP networks. It can act as either an entry point or an exit point for a network and can include the following:

- Topology hiding
- Application level gateway
- Control of user plane functions
- Protocol screening
- Routing
- Generation of charging records
- Privacy protection and other security functions
The NNI network is normally comprised of dedicated or managed-service-based transit network (IPX) facilities between the IP 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. IP assumes that a global ENUM is in place to facilitate translation of foreign telecom URLs, which may be provided by the transit network or through other means [Ref 1]. NNI and SIP hand-off, depending on network deployment strategies, may have multiple peering protocols established in multiple locations throughout the network.

![Diagram of Inter-IMS Network to Network Interface between two IM CN Subsystem Networks](image)

**Figure 5: Inter-IMS Network to Network Interface between two IM CN Subsystem Networks, based on [Ref 1]**

Service assurance monitoring systems along with robust element monitoring systems become requirements for monitoring transitioning IMS networks (i.e., Next Generation 9-1-1).

### 4.5 End to End VoIP Monitoring

A goal of ATIS NRSC is to identify network impairments and outage conditions that affect service availability. These same conditions may also be used to consistently and reliably across the industry report to the FCC in compliance with mandated NORS Reporting under Title 47, Part 4: *Disruption to Communications* for an IP network [Ref 4]. During ATIS NRSC’s review of standards a gap was identified in the monitoring of VoIP networks in the current reality-based reporting metrics. ATIS NRSC worked with 3GPP, receiving an endorsement on a contribution, *The Percentage of Non-Registered Users Metric* [Ref 8/Annex B]. This metric can be used as an additional means to determine VoIP user outages. For this reason, ATIS NRSC has developed a multi-plan approach to identify outages and impairments in an all-IP network. This approach incorporates a plan for monitoring VoIP outages and a second plan for drops in registered users. The plans are outlined in greater detail below. In order to accurately monitor a next generation IP network, a service assurance monitoring toolset is recommended. For VoIP monitoring to work, the assumptions will be as follows:

- Alarm monitoring (e.g., critical, major, minor) for all hardware components used in the end-to-end IP network configuration should be enabled to continue to deliver standard fault and performance monitoring
- Device alarms must provide geographic location information
  - Alarms associated with fixed devices must be named in a fashion providing basic geographic information such as city and state
  - Generated alarms may be interpreted manually or correlated with rules
- Affected users will be identified by a combination of reality-based reporting and/or various automated and manual methods
- Network monitors must be able to generate alarms
- Consider following Best Practices: https://bp.atis.org/, especially those listed in Annex A
4.5.1 Reality-Based Reporting for IP-Based Core Network

The core architecture will vary across carriers as networks evolve and migrate to IP. The network resiliency afforded with IP networks adds a layer of complexity for monitoring alarms. A critical device alarm may not denote an outage condition as the core re-converges and routes around impairments.

These new conditions drive the need for reality-based reporting to effectively determine the health of a network’s core. ATIS NRSC has actively examined network monitoring solutions already in use during the PSTN transition, as well as standards-based performance metrics published by international standards bodies (IETF and 3GPP).

Reality-based reporting metrics monitor a variety of factors to ensure the IMS packet core is performing within its engineering limits and design capabilities. Some of these same factors can be used to determine if an authorized user has accessed the network and established a session to the network’s edge and/or possibly the requested terminating end.

The goal of reality-based reporting metrics is to produce high quality, relevant technical and engineering metrics that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better.

Reality-based reporting metrics monitor the state of the network’s performance using Element Management Systems (EMS) and Service Assurance Monitoring (SAM) tool suites.

4.5.2 IETF/ITU Metrics

The work completed by IETF in RFC 6076 [Ref 6] and ITU in E.425 [Ref 9] has been found to be a good resource for determining network availability:

“Session Establishment Effectiveness Ratio (SEER) or other such metrics that monitor a ratio in the number of INVITE requests resulting in a 200 OK response and INVITE requests resulting in a 480, 486, 600, or 603; to the total number of attempted INVITE requests less INVITE requests resulting in a 3XX response. The response codes 480, 486, 600, and 603, were chosen because they clearly indicate the effect of an individual user of the UA (User Agent)."

\[
\text{SEER} = \frac{\text{# of INVITE Requests w/ associated 200, 480, 486, 600, or 603}}{(\text{Total # of INVITE Requests}) - (\text{# of INVITE Requests w/ 3XX Response})} \times 100
\]

The Network Effectiveness Ratio (NER), defined by the International Telecommunication Union (ITU), was also reviewed and was found acceptable for monitoring network issues resulting in mass call blocking event.

“NER expresses the relationship between the number of seizures and the sum of the number of seizures resulting in either an answer signal, or a user busy, or a ring no answer.”

\[
\text{NER} = \frac{\text{Seizures resulting in Answer Message or User Failure}}{\text{Total Seizures}} [\text{Ref 9}]
\]

It should be noted that a low SEER score may not be indicative of a problem within a given network. This is, however, an indication of a problem and will require further investigation to identify the source.

4.5.3 Percent of Registered Users

During ATIS NRSC’s review of standards a gap was identified in the monitoring of VoIP networks in the current reality-based reporting metrics.

Measurement of the percent of registered users will evaluate the network state and identify processes or subsystems that may have become unavailable to some quantity of previously registered UE(s). Near real-time measurements (polled by service providers at varying rate from 5, 10, 15, 30 minutes, etc.). ATIS NRSC worked with 3GPP, receiving an endorsement on a contribution, The Percentage of Non-Registered Users Metric [Ref 8/Annex B].
4.5.4 3GPP Metrics

End-to-end network availability metrics are critical for network service providers to gauge the health of their networks. ATIS NRSC notes that current reporting metrics monitor a variety of factors to ensure the IMS packet core is performing within its engineering limits and design capabilities. These same factors could be used to determine if users are successfully registering on the network and establishing sessions, or possibly failing to register and establish sessions due to a fault in the Service Provider’s network.

Monitoring a rise in the number of UE(s) not registered on the network can identify a systemic problem impacting network availability to the networks edge. Using IMS core statistics provides aggregation points in the network that can identify issues quicker. The need for this metric is two-fold—not only is it critical for all service providers to have insight into their networks when an event has occurred impacting network availability, service and/or customers, it also gives North American service providers additional data to help identify events that have the potential to be Federal Communications Commission (FCC) reportable under mandated Disruption of Communications Title: 47; Part: 4 rules [Ref 4].

At its simplest form the percentage of non-registered users would be comprised of:

\[
\text{Rs} = \text{Number of registered users} \\
\text{Pri} = \text{Number of provisioned users} \\
\% \text{ of non-registered users} = 100^* (1 - (\text{Rs}/\text{Pri})) \text{ [Ref 8/Annex B]}
\]

Registered users can be segmented by service type. Voice specific registrations can be identified using the information found in Annex B.

5 FCC 47 Part 4 Disruption of Communication Regulations

The current Telephony User Outage Conditions [Ref 4] state that an outage must last longer than thirty (30) minutes and exceed 900,000 user minutes. Solving for 900,000 user minutes currently involves monitoring critical and major network element alarms at the Access, Metro, and Core locations and identifying the geographic areas of potential impact by city and state.

ATIS NRSC has evaluated a host of standard based metrics relevant to IMS networks. Key focus has been on three areas that mimic current Title: 47, Part 4: Disruption of Communications mandates.

1. 90,000 Blocked Calls
2. 900,000 User minutes
3. 911 (Call Failures)
   - PSAP Isolation
   - Name and Number Information
   - Location Information

ATIS NRSC believes that end-to-end network monitoring is required to achieve a reliably sustainable outage reporting process in the new IP space that can be used to aid in FCC outage reporting as mentioned in clause 4.5. The continuously evolving nature of the networks necessitates end-to-end network monitoring. These same metrics can be used to track various aspects of network capabilities and performance, along with identifying potentially FCC reportable events.
A Best Practices

The industry Best Practices include responsibilities of various Network Operators and Service Providers to monitor alarms in an IP Network as outlined in Table 1 below. Best Practices are developed through collaborative efforts by members of the communications industry. Best Practices will be adjusted throughout the life of the IP infrastructure deployment and implementation. As the IP Infrastructure continues to develop, more specific Best Practices will be developed to increase network availability and network hardness.

Best Practices have a unique numbering methodology. The table associated with this document references only the last four digits of a Best Practice, because they are the only static digits of the Best Practice number.

A complete listing of Best Practices can be found online at <https://www.bp.atis.org>.

Table 1: Applicable Best Practices

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
<th>Keyword</th>
</tr>
</thead>
<tbody>
<tr>
<td>0400</td>
<td>Network Operators, Service Providers, and Public Safety should establish measurements to monitor their network performance.</td>
<td>Network Operations</td>
</tr>
<tr>
<td>0407</td>
<td>Network Operators and Service Providers should establish processes for NOC-to-NOC (Network Operations Center) peer communications for critical network activities (e.g., scheduled maintenance, upgrades and outages).</td>
<td>Facilities-Transport, Industry Cooperation, Network Interoperability, Network Operations, Network Provisioning, Procedures</td>
</tr>
<tr>
<td>0409</td>
<td>Service Providers should use virtual interfaces (i.e. a router loopback address) for routing protocols and network management to maintain connectivity to the network element in the presence of physical interface outages.</td>
<td>Network Elements</td>
</tr>
<tr>
<td>0416</td>
<td>Network Operators, Service Providers, and Public Safety should design and implement procedures for traffic monitoring, trending and forecasting so that capacity management issues may be addressed.</td>
<td>Network Operations, Pandemic, Procedures</td>
</tr>
<tr>
<td>0421</td>
<td>Equipment Suppliers should design network elements intended for critical hardware and software with recovery mechanisms to minimize restoration times.</td>
<td>Hardware, Network Elements, Software</td>
</tr>
<tr>
<td>0436</td>
<td>Network Operators, Service Providers, and Public Safety should have a process to ensure smooth handling and clear ownership of problems that transition work shifts or organizational boundaries.</td>
<td>Network Operations, Procedures</td>
</tr>
<tr>
<td>0454</td>
<td>Network Operators, Service Providers, Equipment Suppliers, and Public Safety should consider establishing technical and managerial escalation policies and procedures based on the service impact, restoration progress and duration of the issue.</td>
<td>Business Continuity, Disaster Recovery, Emergency Preparedness, Network Operations, Policy, Procedures</td>
</tr>
<tr>
<td>0484</td>
<td>Network Operators and Public Safety should have a program (e.g., automated drive test equipment, network probes) to monitor and detect network performance anomalies.</td>
<td>Network Operations, Procedures</td>
</tr>
<tr>
<td>0501</td>
<td>Network Operators, Service Providers, and Public Safety should report problems discovered from their operation of network equipment to the Equipment Supplier whose equipment was found to be the cause of problem.</td>
<td>Hardware, Network Elements, Network Operations, Policy, Procedures, Software, Technical Support</td>
</tr>
</tbody>
</table>
### ATIS-0100069

<p>| 0514 | Network Operators, Service Providers should when available, utilize a device management architecture that provides a single interface with access to alarms and monitoring information from all critical network elements. | Human Resources, Network Elements, Security Systems, Intrusion Detection |
| 0515 | Network Operators, Service Providers should for easy communication with subscribers and other operators and providers, use specific role-based accounts (e.g., <a href="mailto:abuse@provider.net">abuse@provider.net</a>, <a href="mailto:ip-request@provider.net">ip-request@provider.net</a>) versus general accounts (e.g., <a href="mailto:noc@provider.net">noc@provider.net</a>) which will help improve organizational response time and also reduce the impact of Spam. | Cyber Security, Emergency Preparedness, Industry Cooperation, Network Operations, Policy, Procedures, Technical Support |
| 0516 | Route Flapping: Network Operators and Service Providers should manage the volatility of route advertisements in order to maintain stable IP service and transport. Procedures and systems to manage and control route flapping at the network edge should be implemented. | Cyber Security, Network Elements, Network Interoperability, Network Operations, Procedures |
| 0519 | Network Operators, Service Providers and Public Safety should engineer and monitor networks to ensure that operating parameters are within capacity limits of their network design (e.g., respect limitations of deployed packet switches, routers and interconnects, including &quot;managed networks&quot; and &quot;managed CPE&quot;). These resource requirements should be re-evaluated as services change or grow. This applies to Public Safety only in an NG9-1-1 environment. | Network Design, Network Elements, Network Interoperability, Network Operations, Network Provisioning, Policy, Procedures, Public Safety Service |
| 0574 | Network Operators, Service Providers, and Public Safety should actively monitor and manage the 9-1-1 network components using network management controls, where available, to quickly restore 9-1-1 service and provide priority repair during network failure events. When multiple interconnecting providers and vendors are involved, they will need to cooperate to provide end-to-end analysis of complex call-handling problems. | Essential Services, Network Operations, Pandemic, Procedures, Supervision |
| 0580 | Network Operators and Public Safety should apply redundancy and diversity where feasible, to all network links considered vital to a community's ability to respond to emergencies. | Essential Services, Facilities-Transport, Industry Cooperation, Liaison |
| 0588 | Network Operators, Service Providers, Equipment Suppliers and Public Safety should provide awareness training that stresses the services impact of network failure, the risks of various levels of threatening conditions and the roles components play in the overall architecture. | Contractors &amp; Vendors, Network Operations, Pandemic, Public Safety Service, Supervision, Training and Awareness |
| 0602 | Network Operators, Service Providers and Public Safety should establish procedures to reactivate alarms after provisioning or maintenance activities (when alarms are typically deactivated). | Facilities-Transport, Network Operations, Network Provisioning, Procedures, Public Safety Service, Training and Awareness |
| 0612 | Network Operators, Service Providers and Public Safety should verify both local and remote alarms and remote network element maintenance access on all new critical equipment installed in the network before it is placed into service. | Network Elements, Network Operations, Network Provisioning, Procedures, Public Safety Service |
| 0616 | Network Operators, Service Providers and Public Safety should design and implement procedures to evaluate failure and emergency conditions affecting network capacity. | Network Operations, Pandemic, Procedures, Public Safety Service |
| 0690 | Network Operators, Property Managers and Public Safety should consider providing power alarm redundancy so that no single point alarm system failure will lead to a network power outage. | Network Operations, Power |
| 0767 | Network Operators and Service Providers should consider using media gateway controllers to achieve interoperability with SS7/ISUP-signaled TDM voice networks. | Cyber Security, Network Interoperability, Software |</p>
<table>
<thead>
<tr>
<th>Code</th>
<th>Text</th>
<th>Related Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0818</td>
<td>Network Operators, Service Providers should deploy network equipment that report alarms if they deploy Internet Access Service.</td>
<td>Network Elements</td>
</tr>
<tr>
<td>5075</td>
<td>Network Operators, Service Providers, and Public Safety should ensure that networks built with redundancy are also built with geographic separation where feasible (e.g., avoid placing mated pairs in the same location and redundant logical facilities in the same physical path).</td>
<td>Essential Services, Facilities-Transport, Network Elements, Network Operations, Network Provisioning, Policy</td>
</tr>
<tr>
<td>5235</td>
<td>Network Operators and Service Providers should ensure that impacted alarms and monitors associated with critical utility vaults are operational after a disaster event.</td>
<td>Access Control, Disaster Recovery, Emergency Preparedness, Facilities-Transport, Network Operations, Physical Security Management, Security Systems</td>
</tr>
<tr>
<td>8725</td>
<td>Signaling DoS Protection: Network Operators should establish alarming thresholds for various message types to ensure that DoS conditions are recognized. Logs should be maintained and policies established to improve screening and alarming thresholds for differentiating legitimate traffic from DoS attacks.</td>
<td>Cyber Security, Network Elements, Network Operations, Intrusion Detection</td>
</tr>
</tbody>
</table>
Annex B  
(normative/informative)

B Input from ATIS NRSC to 3GPP TSG SA WG5 Drop in Registered Users Metric

3GPP TSG SA WG5 (Telecom Management) Meeting #116  
27 November - 1 December 2017, Reno, US  
Source: ATIS NRSC  
Title: The Percentage of Non-Registered Users Metric  
Document for: Endorsement  
Agenda Item: B.1 Decision/action requested

ATIS NRSC seeks endorsement from SA-5 on a metric to define a percentage of non-registered users for IP-based networks.

B.2 References
[1] TS 32.409, Telecommunication management ; Performance Management (PM); Performance measurements; IP Multimedia Subsystem (IMS).
[2] LS S5-176290, “LS reply to ATIS NRSC on ‘Establish a Metric to Determine a Drop in Registered Users in an IP-Based Network’” from 3GPP SA5.

B.3 Rationale
End-to-end network availability metrics are critical for network service providers to gauge the health of their networks, ATIS NRSC notes that current reporting metrics monitor a variety of factors to ensure the IMS packet core is performing within its engineering limits and design capabilities. These same factors could be used to determine if users are successfully registering on the network and establishing sessions, or possibly failing to register and establish sessions due to a fault in Service Provider’s network.

Monitoring a rise in the number of UE(s) not registered on the network can identify a systemic problem impacting network availability to the networks edge. Using IMS core statistics provides aggregation points in the network that can identify issues quicker. The need for this metric is two-fold—not only is it critical for all service providers to have insight into their networks when an event has occurred impacting network availability, service and/or customers, it also gives North American service providers additional data to help identify events that have the potential to be Federal Communications Commission (FCC) reportable under mandated Disruption of Communications Title: 47; Part: 4 rules.

At its simplest form the percentage of non-registered users would be comprised of:

\[ \text{Rs} = \text{Number of registered users} \]  
\[ \text{Pri} = \text{Number of provisioned users} \]  
\[ \% \text{ of non-registered users} = 100 \times (1 - (\text{Rs}/\text{Pri})) \]
B.4 Use case to determine service availability by monitoring a rise in the percentage of non-registered users

Service availability is basic to Service Providers to operate and maintain their networks. These measurements can help to evaluate the network state and identify processes or subsystems that may have become unavailable to some quantity of previously registered UEs. Near real-time measurements (polled by service providers at varying rate from 5, 10, 15, 30 Minutes, etc..) would make this a useful metric to also identify network impairments and alert operations teams of faults.

B.5 Detailed proposal

The percentage of non-registered users metric has the ability to monitor multiple data points depending on the service provider’s business model. This proposal states a simplified formula that can monitor a broad range of operational models.

% of non-registered users = 100*(1- (Rs/Pri))

Rs = Number of registered users
Pri = Number of provisioned users

Variables to be considered under TS 32.409:
Rs = Number of registered users
4.2.3.2 Successful S-CSCF registration/de-registration notifications

Pri = Number of provisioned users
4.2.1.6 Number of Public Service Identities with SIP URI format stored in a HSS
4.2.1.7 Number of Public Service Identities with TEL URI format stored in a HSS
4.2.1.1.1 Number of provisioned IMS subscriptions currently stored in a HSS
4.2.1.1.2 Number of provisioned Private User Identity stored in a HSS
4.2.1.1.3 Number of provisioned Public User Identities with SIP URI format stored in a HSS
4.2.1.1.4 Number of provisioned Public User Identities with TEL URI format stored in a HSS