BITAG

Broadband Internet Technical Advisory Group

VoIP Impairment, Failure, and Restrictions

A BROADBAND INTERNET TECHNICAL ADVISORY GROUP
TECHNICAL WORKING GROUP REPORT

A Uniform Agreement Report

Issued:
May 2014

Copyright / Legal Notice

Copyright © Broadband Internet Technical Advisory Group, Inc. 2014. All rights reserved.

This document may be reproduced and distributed to others so long as such reproduction or distribution complies with Broadband Internet Technical Advisory Group, Inc.'s Intellectual Property Rights Policy, available at www.bitag.org, and any such reproduction contains the above copyright notice and the other notices contained in this section. This document may not be modified in any way without the express written consent of the Broadband Internet Technical Advisory Group, Inc.

This document and the information contained herein is provided on an "AS IS" basis and BITAG AND THE CONTRIBUTORS TO THIS REPORT MAKE NO (AND HEREBY EXPRESSLY DISCLAIM ANY) WARRANTIES (EXPRESS, IMPLIED OR OTHERWISE), INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, OR TITLE, RELATED TO THIS REPORT, AND THE ENTIRE RISK OF RELYING UPON THIS REPORT OR IMPLEMENTING OR USING THE TECHNOLOGY DESCRIBED IN THIS REPORT IS ASSUMED BY THE USER OR IMPLEMENTER.

The information contained in this Report was made available from contributions from various sources, including members of Broadband Internet Technical Advisory Group, Inc.'s Technical Working Group and others. Broadband Internet Technical Advisory Group, Inc. takes no position regarding the validity or scope of any intellectual property rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this Report or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights.

About the BITAG

The Broadband Internet Technical Advisory Group (BITAG) is a non-profit, multi-stakeholder organization focused on bringing together engineers and technologists in a Technical Working Group (TWG) to develop consensus on broadband network management practices and other related technical issues that can affect users' Internet experience, including the impact to and from applications, content and devices that utilize the Internet.

The BITAG's mission includes: (a) educating policymakers on such technical issues; (b) addressing specific technical matters in an effort to minimize related policy disputes; and (c) serving as a sounding board for new ideas and network management practices. Specific TWG functions also may include: (i) identifying "best practices" by broadband providers and other entities; (ii) interpreting and applying "safe harbor" practices; (iii) otherwise providing technical guidance to industry and to the public; and/or (iv) issuing advisory opinions on the technical issues germane to the TWG's mission that may underlie disputes concerning broadband network management practices.

The BITAG Technical Working Group and its individual Committees make decisions through a consensus process, with the corresponding levels of agreement represented on the cover of each report. Each TWG Representative works towards achieving consensus around recommendations their respective organizations support, although even at the highest level of agreement, BITAG consensus does not require that all TWG member organizations agree with each and every sentence of a document. The Chair of each TWG Committee determines if consensus has been reached. In the case there is disagreement within a Committee as to whether there is consensus, BITAG has a voting process with which various levels of agreement may be more formally achieved and indicated. For more information please see the BITAG Technical Working Group Manual, available on the BITAG website at www.bitag.org.

BITAG TWG reports focus primarily on technical issues, especially those with the potential to be construed as anti-competitive, discriminatory, or otherwise motivated by non-technical factors. While the reports may touch on a broad range of questions associated with a particular network management practice, the reports are not intended to address or analyze in a comprehensive fashion the economic, legal, regulatory or public policy issues that the practice may raise.

BITAG welcomes public comment. Please feel free to submit comments in writing via email at comments@bitag.org.

Executive Summary

IP networks have supported voice communications for some time. Voice over IP (VoIP) services allow users to make calls between IP-based endpoints and to interconnect with the traditional public switched telephone network. VoIP applications use a variety of methods and protocols to manage connections and exchange media (i.e., the content of voice or video communications) over IP-based networks such as the Internet. In the majority of VoIP applications, connections are managed or controlled using one protocol or set of protocols, and the media is exchanged among the parties involved in the connection using a different transport protocol or set of protocols. The purpose of these separate connection control and signaling protocols is to allow the parties involved in the communication to establish, control, and terminate connections. Many services that provide VoIP capability also support other forms of real-time media (video or screen sharing, for example).

This report uses the term *VoIP impairment* to refer to anything that prevents a VoIP application from being used in the manner desired by a user. An impairment affecting a VoIP service can occur anywhere along the data path, including in the end devices. For example, impairment may be the result of actions by a network operator, the VoIP provider itself, or the provider of a smartphone's operating system. Impairment could likewise be the result of a poorly implemented network device or application, or may occur as a result of a configuration or misconfiguration of a home network. VoIP services can be rendered unusable if their quality is sufficiently reduced to prevent meaningful audio exchange between the participants, even if some VoIP traffic is still exchanged.

VoIP failure, as defined in this report, encompasses particular kinds of VoIP impairments that arise when VoIP calls cannot be established at all, or when no media is capable of being exchanged between VoIP endpoints. When network operators, VoIP providers, operating system vendors, or application store providers take steps that cause VoIP failures or prevent VoIP from being used, those steps are considered *VoIP restrictions* for the purposes of this report. The term *VoIP impairments* (plural) is used as shorthand for *VoIP impairment, failure, or restrictions* in this report. Issues related to interoperability between different VoIP services are out of scope.

This report discusses: (1) how VoIP works; (2) how VoIP may be impaired or restricted; (3) methods for mitigating VoIP impairments; and (4) recommendations concerning VoIP impairment, failure, and restrictions. The report focuses on VoIP impairments that may occur in residential or mobile networks. This report makes no assumptions concerning the motivations behind actions that result in VoIP impairment, failure, or restrictions, or about the frequency or scale of such occurrences.

There are a variety of technical causes of VoIP impairment, failure, and restrictions:

Port blocking. In the architecture of the Internet, communication between two systems is identified by five fields: (1) the source IP address, (2) the destination IP address, (3) the transport protocol in use, (4) the source port, and (5) the destination port used by the transport protocol. The pair of IP addresses representing two systems identifies all of the communication sessions between them, whereas the port number pair characterizes an individual communication session between the two systems. If traffic is prevented from flowing to or from the particular ports used by VoIP applications, VoIP failure can occur. This practice is known as port blocking.

Application-Level Gateways (ALGs). Many endpoints on the Internet sit behind a Network Address Translation (NAT) device. NAT allows multiple end devices within a local network (the network in a single home, for example) to share a single public IP address. NAT is challenging for applications such as VoIP that require reachability from the Internet. A variety of mechanisms have been developed for overcoming these challenges, including the use of Application-Level Gateways (ALGs), which can automatically detect traffic associated with particular VoIP services and help that traffic pass through NAT devices. However, ALGs may also affect traffic handling in such a manner as to impair the correct operation of other VoIP services.

Other network-based causes. The use of some network-based techniques that attempt to identify VoIP requests or VoIP traffic may result in VoIP impairment. These techniques may leverage the Domain Name System (DNS) infrastructure, deep packet inspection, or network-based flow policing and filtering that attempt to identify patterns of likely VoIP traffic.

Restrictions based on device, application, or application store. Actions taken on a device, in a VoIP application, or in an application store may restrict the use or functionality of VoIP applications. These examples often reflect business arrangements or agreements between application store providers, operating system vendors, device manufacturers, and/or mobile carriers.

When VoIP impairments occur, it may be very difficult for a user to solve the problem, even for technically sophisticated users. Whether a mitigation or workaround solution exists, and how difficult it may be to implement, depends on the mechanism that is impairing the VoIP connection. If mitigation options are unavailable, or if users lack the knowledge or willingness to pursue such, those users may be prevented from using VoIP altogether, or may need to switch to a different VoIP application. Mitigations available to application providers for dealing with VoIP impairment also depend on how the impairments are effectuated.

VoIP impairment, failure, and restrictions can create difficulties for VoIP users and may deter adoption of over-the-top VoIP services. VoIP impairments can also create difficulties for the operators of VoIP services and providers of VoIP applications, who may need to troubleshoot or work around impairments (where possible) to enable or restore their users' connectivity.

BITAG's Technical Working Group recommends the following to minimize the occurrences and impact of VoIP impairment, failure, and restrictions:

- **Network operators should avoid impairing or restricting VoIP applications unless no reasonable alternatives are available to resolve technical issues.** Certain network management actions may have the effect of limiting or restricting VoIP traffic as a method of ensuring network integrity. Examples include port blocks or traffic limitations implemented when a customer uses a vulnerable VoIP service that can be exploited by attackers for the purpose of flooding the network with unwanted traffic. In adopting any approach that has the effect of limiting the use of VoIP, network operators should seek to minimize the impact of the approach on legitimate VoIP use.

- **VoIP-related ALGs in operator-supplied home routers should minimize their impact on traffic other than the operator's VoIP service where possible.** VoIP-related ALGs can interfere with some VoIP services while attempting to facilitate NAT traversal for other VoIP services. Because of these problems, BITAG recommends that VoIP-related ALGs in operator-supplied home routers should either allow the VoIP-related ALGs to be disabled for customers who do not subscribe to the operator's VoIP service or minimize or avoid impact to independent VoIP services and all other traffic not associated with the operator's own VoIP service. Where possible, VoIP-related ALGs in operator-supplied home routers should be disabled by default. ALGs for real-time applications (including VoIP) can be problematic for services other than VoIP, but recommendations concerning ALGs more broadly are outside the scope of this report.

- **Manufacturers of home routers should disable VoIP-related ALGs by default.** Some consumers purchase their home routers from retailers rather than from network operators. To limit the impact of VoIP-related ALGs on VoIP services, home routers sold to consumers should have VoIP-related ALGs disabled by default.

- **Port blocking rules in consumer equipment should be user-configurable.** The port blocking (or firewall) rules of consumers' home routers should be user-configurable, whether the routers are provided by the ISP or purchased separately by the consumer. By making these rules user-configurable, technically sophisticated users may be able to eliminate port blocks that prevent them from using VoIP services. It is recommended that the documentation provided with the consumer equipment inform the consumer that port blocking or firewall rules have been implemented, the default ports blocked, and how consumers can modify those rules.

- **If network operators intentionally use network policies or practices that impair or restrict VoIP, they should provide disclosures about those policies and practices and provide communications channels for feedback.** BITAG recommends that network operators disclose their policies and practices that may or could result in VoIP impairment, failure, or restrictions. The information should be readily available to both customers and non-customers alike. For example, such policies could be provided on the operator's public-facing web site or on a page dedicated to summarizing or describing the ISP's network management practices. If specific VoIP applications are impaired or restricted, those applications should be listed by name, along with a brief description of the reason for the impairment or restriction. BITAG also recommends that ISPs provide a communications channel or other clear method for application providers and consumers to discuss the impact of VoIP impairment, failure, and restrictions, and possible mitigations.

- **Application developers should design VoIP applications to be port-agile where possible.** BITAG recommends that VoIP application developers design VoIP applications and services to be port-agile where possible. Applications designed to tolerate random source ports or to allow port selection to be user-configurable are better able to avoid VoIP impairments that result from port blocking or contention between multiple services for the same port. Whether particular applications can be re-designed to be port agile may depend on whether re-designed versions of the application can be made compatible with existing versions or other existing applications.

Table of Contents

1. Issue Overview

The ability to support voice communications over IP networks has existed for over two decades. Voice over IP (VoIP) services allow users to make calls between IP-based endpoints and to interconnect with the traditional public switched telephone network. Most VoIP service architectures include two distinct components: signaling and media. Signaling is used to setup and manage calls and to connect callers with each other. The Session Initiation Protocol (SIP) is a commonly used signaling protocol within voice and video telephony products offered by telecommunications carriers, independent voice service providers, and over-the-top Internet applications. Media involves the exchange of the voice traffic itself and is provided by a variety of application-layer protocols that carry the actual content of calls. Many services that provide VoIP capability also support other forms of real-time media (video or screen sharing, for example).

This report uses the term *VoIP impairment* to refer to anything that prevents a VoIP application from being used in the manner desired by a user. An impairment affecting a VoIP service can occur anywhere along the data path, including in the end devices. For example, impairment may be the result of actions by a network operator, the VoIP provider itself, or the provider of a smartphone's operating system. Impairment could likewise be the result of a poorly implemented network device or application, or may occur as a result of a configuration or misconfiguration of a home network. VoIP services can be rendered unusable if their quality is sufficiently reduced to prevent meaningful audio exchange between the participants, even if some VoIP traffic is still exchanged.

VoIP failure, as defined in this report, encompasses particular kinds of VoIP impairments that arise when VoIP calls cannot be established at all, or when no media is capable of being exchanged between VoIP endpoints. When network operators, VoIP providers, operating system vendors, or application store providers take steps that cause VoIP failures or prevent VoIP from being used, those steps are considered *VoIP restrictions* for the purposes of this report. The term *VoIP impairments* (plural) is used as shorthand for *VoIP impairment, failure, or restrictions* in this report. Issues related to interoperability between different VoIP services are out of scope.

Many Internet users rely on over-the-top VoIP applications as a means of communication. VoIP impairment, failure, and restrictions can create difficulties for those users and may deter adoption of over-the-top VoIP services. VoIP impairments can also create difficulties for the operators of VoIP services, who may need to troubleshoot or work around impairments (if possible) to enable or restore their users' connectivity. VoIP services are sufficiently important that a thorough understanding of the causes and mechanisms of VoIP impairments is warranted.

This report discusses: (1) how VoIP works; (2) how VoIP may be impaired or restricted; (3) methods for mitigating VoIP impairments; and (4) recommendations concerning VoIP impairment, failure, and restrictions. The report focuses on VoIP impairments that may occur in residential or mobile networks; enterprise networks are out of scope. Some other networks, such as hotels and Wi-Fi hotspots, are touched upon but are not the focus. For the purposes of this report, an Internet Service Provider (ISP) is defined as a provider of broadband Internet access service, an Application Service Provider (ASP) is defined as a provider of applications used on broadband Internet access services, and a network operator is defined as an ISP, or an ASP that operates a network. Some ASPs operate networks that interconnect with ISPs, while other ASPs attach servers directly to ISPs.

This report makes no assumptions concerning the motivations behind actions that result in VoIP impairment, failure, or restrictions, or about the frequency or scale of such occurrences. Rather, the report identifies and recommends approaches to minimize occurrences of impairment, failure, and restrictions.

1.1. Relationship to Past BITAG Reports

BITAG has published a number of past reports that are related to the topic of VoIP impairments, including reports on Port Blocking [1], Large Scale Network Address Translation [2], and Real-Time Network Management of Internet Congestion [3]. This report will reference rather than repeat the analysis and recommendations from those reports, where they apply to the topic of VoIP impairments.

2. Understanding VoIP and Real-Time Applications

VoIP applications use a variety of methods and protocols to manage connections and exchange media – the actual voice, video, or any related communications content – over IP-based networks such as the Internet. In the majority of VoIP applications, connections are managed using one protocol (or set of protocols), and the media is exchanged among the parties involved in the connection using a different protocol (or set of protocols). Each party involved in the connection uses software that includes a VoIP client. These clients transmit and receive the media. The purpose of the connection control and signaling protocols is to allow the parties involved in the communication to establish, control, and terminate connections. This involves not only the VoIP clients but also the assistance of VoIP server(s). A VoIP server may be integrated with a VoIP client, or it may be managed by a service provider.

A number of signaling protocols have been standardized, including Session Initiation Protocol (SIP) [4], H.323 [5], and the Media Gateway Control Protocol (MGCP) [6]. Similarly, protocols for carrying media have been standardized, including Real-time Transport Protocol (RTP) [7]. A number of proprietary signaling and media transport protocols exist, including those used by Skype [8].

The media, e.g. voice and video, is carried over paths connecting the parties involved in the communication. In contrast, the signaling and control information is exchanged between VoIP clients and VoIP servers, and sometimes between multiple VoIP servers. As illustrated in Figure 1, the path through the network taken by the media need not be the same as the path taken by the signaling and control information.

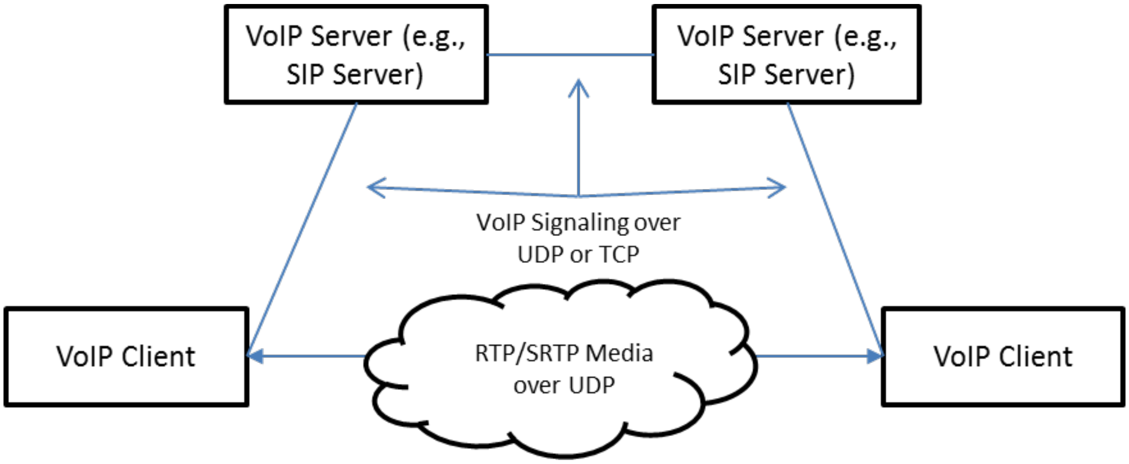
VoIP Server (e.g., SIP Server)
VoIP Server (e.g., SIP Server)
VoIP Signaling over UDP or TCP
VoIP Client
RTP/SRTP Media over UDP
VoIP Client

Figure 1. VoIP Protocols – Signaling vs. Media

A VoIP call is started by the initiator of the call. If SIP is used for control and signaling, for example, then the initiator's VoIP client transmits a SIP INVITE message to a VoIP server, which routes the message to the VoIP client of the party or parties being called. The SIP INVITE message includes the identity of the called party and parameters that must be agreed upon (e.g. port numbers, protocols, and compression algorithms). The called party's VoIP client responds by either accepting or rejecting the connection. At the end of the call, either side can terminate the connection by transmitting a SIP BYE message.

2.1. VoIP Ports

In the architecture of the Internet, communication between two systems is identified by five fields: (1) the source IP address, (2) the destination IP address, (3) the transport protocol in use, (4) the source port, and (5) the destination port used by the transport protocol [9] [1]. The pair of IP addresses representing two systems identifies all of the communication sessions between them, whereas the port number pair characterizes an individual communication session between the two systems.

Transport protocols, most often Transmission Control Protocol (TCP) or User Datagram Protocol (UDP), include in their header fields the "destination port" and the "source port" [10] [1]. When an application on one device wants to communicate with an application on another device, it directs the local operating system to open a connection between itself and the remote end point, and specifies the IP address, transport protocol, and port number that the service will use. For further reference, throughout the remainder of this report TCP and UDP ports will be denoted with the name of the transport protocol followed by a slash and the port number: TCP/5060, for example.

SIP servers often use ports TCP/5060, UDP/5060, TCP/5061, or UDP/5061 to listen for SIP requests, because these port numbers were specifically assigned for use by SIP. VoIP services that use proprietary signaling and media protocols may choose their own port numbers from those that have not already been assigned to standardized protocols. Port-agile SIP servers can listen for SIP on a variety of ports. RTP uses a wide range of non-standardized ports. The ports used for RTP during any particular conversation are agreed upon by the endpoints through the signaling messages used to set up the call. RTP uses UDP in almost all cases.

2.2. Network Address Translation (NAT)

Many endpoints on the Internet sit behind a Network Address Translation (NAT) device. NAT allows multiple end devices within a local network (the network within a single home, for example) to share a single public IP address [2]. NAT was originally designed to alleviate the scarcity of IPv4 addresses by separating the local network into a space of private IP addresses that maps to a single public IP address. To accomplish this, a NAT device maps private IP address/port combinations within the local private network to external ports associated with the public IP address. That is, the NAT's device map associates an external UDP or TCP port number for the public IP address to a UDP or TCP port number associated with the private IP address of a single device inside the local network. NAT creates challenges for VoIP service delivery and some VoIP failures are NAT-related.

NAT is challenging for applications such as VoIP that require reachability from the Internet for three main reasons: (1) port mappings in a NAT expire after a timeout period, (2) many VoIP servers expect the IP address in the signaling payload to be the IP address of the VoIP client (in order to receive incoming calls), and (3) some VoIP services do not tolerate arbitrary source port numbers, which causes problems when a NAT device changes the source port number (multiple devices that use the same port number internal to the local network must map to different external-facing port numbers). The following sections discuss these in turn.

2.2.1. NAT Port Expiration Management

To help ensure that a single NAT device has sufficient external-facing port numbers for the potentially large number of devices behind it, the NAT device's port mappings expire after a period of time, unless some mechanism is used to explicitly keep these mappings open. Once a port mapping expires, when the NAT device receives traffic on the expired external port, the NAT device will no longer send that traffic on to the internal device that previously corresponded to that mapping. The duration of a mapping depends on the transport protocol; TCP port mappings generally expire after a few hours, and UDP port mappings expire after a couple minutes or less. The exact expiration values vary among routers. Most VoIP traffic (both signaling and media transport) uses UDP, corresponding to very short port expirations.

SIP servers, which handle the signaling component of SIP-based VoIP, will often request clients to re-register with the server every hour, in order to update network information the SIP server needs to begin, maintain, and end VoIP sessions. If the VoIP client is relatively inactive, this re-registration message may be the *only* message the client sends to the SIP server within an hour. If the port mapping on the NAT device for a UDP VoIP client expires after only one minute, the server may be unable to reach the client (because any external traffic to an expired port mapping will not reach the internal device). Outside of signaling, the media transport itself can at times be impaired by short UDP port expirations as well. For example, if the VoIP client employs silence suppression – i.e., the client sends no messages when that party is not speaking – and that party is silent for more than a minute (or whatever the duration of the port expiration window is), the port mapping may expire, which will result in non-delivery of future VoIP messages to that client.

Various mechanisms exist to mitigate port mapping expirations:

- *Short re-registration intervals:* Given that port mappings expire and that VoIP-relevant UDP port mappings expire quickly (as mentioned, about one minute), the frequency of re-registration messages can be increased to prevent the port mapping from expiring. This is generally accomplished by the VoIP provider inserting a device called a Session Border Controller (SBC) in the networkbetween the VoIP client and the SIP server. The SBC device allows for short re-registration intervals on the order of 60 seconds to keep the port mapping alive, but also ensures that the critical SIP server itself is not required to handle the significantly increased number of registration requests it would otherwise receive if the re-registration interval is modified from every hour to each minute. More precisely, the SBC allows the VoIP client to send the SBC re-registration messages frequently through the NAT device to keep the associated NAT port alive and the SBC also then proxies the client registration to the SIP server, which only expects to see hourly re-registration.
- *Use of the Session Traversal Utilities for NAT (STUN) protocol* [11]. STUN involves a set of techniques and a STUN server is designed to, among other things, allow applications like VoIP clients to send messages through a NAT device to keep particular ports alive. STUN can be used by a VoIP client to send frequent messages on the port used for signaling, ensuring that the client and server do not encounter expired UDP port mappings. This requires the VoIP provider to maintain a STUN server to receive these messages.
- *SIP-specific keep-alive mechanisms* [12]. The SIP protocol itself has mechanisms for sending messages that serve the purpose of testing if a connection is alive and, if so, maintaining NAT port-mappings (as the act of testing the connection itself, if successful, extends the port mapping expiration time period). These mechanisms also allow a SIP device to register multiple connections with the SIP server at the

same time, so at any given moment an open connection is highly likely to be active through the NAT to reach the SIP device.

- *Application-Level Gateway (ALG) (generically described in* [13]*):* A router or NAT device may include mechanisms itself that can recognize certain protocols and modify port mapping expirations to avoid problematic session expiration. For VoIP, an ALG can automatically detect VoIP traffic passing through the NAT device and instructs the NAT device not to expire the associated VoIP port mappings.
- *Dynamic mechanisms:* Some NAT devices include more dynamic mechanisms that can keep port mappings alive for VoIP. These include Universal Plug and Play Internet Gateway Device Protocol (UPnP IGD) [14] and Port Control Protocol (PCP) [15], which allow applications themselves to create specific, lasting port mappings within a NAT device – as opposed to the mitigations listed above, which require the application to send specific traffic to keep the mapping alive or require the NAT device to detect specific types of traffic to do this. These mechanisms must be installed on the same device as the NAT in order to work and are not universally implemented on home routers.
- *Static port mapping in a NAT.* NAT devices can be manually configured to reserve a given externally-facing port such that it maps onto a static internal (private) IP address and port. The user or network administrator can create a static port mapping in the NAT device for VoIP such that all traffic received at the reserved external port will be delivered to the internal device with no risk of expiration (unless the static mapping is manually reconfigured or destroyed). In the case of remotely-managed routers, static port mapping can also be accomplished by use of a remote management protocol (e.g., SNMP, TR-069).

In the case of silence suppression that impacts media transport, the VoIP client can send a media transport message periodically (in spite of silence suppression), to keep the port mapping open. Additional tools for establishing media connectivity in the presence of NAT include Interactive Connectivity Establishment (ICE), which allows devices to probe for multiple paths of communication by attempting to use different port numbers and STUN techniques, or to use a separate media relay server via Traversal Using Relays around NAT (TURN) [16].

2.2.2. VoIP Client Public/Private IP Address Mismatches

Another issue caused by NAT arises when a VoIP server encounters a mismatch between the IP address that a VoIP client uses inside the VoIP signaling payload – which may be a private IP address – and the IP address where the device can be reached (in order to receive incoming calls). VoIP clients generally will put the same IP address they use as their source IP address in the signaling payload. Where the VoIP client is behind a NAT device, that IP address will be an unreachable private IP address. (The NAT device changes the private source IP address in the IP header, but leaves all IP addresses in the payload untouched.)

Various mechanisms exist to mitigate network address mismatches:

- The VoIP server can be designed to recognize private IP addresses in VoIP signaling payloads and instead use the source IP address. This is done by some VoIP providers, although it prevents use of some of the more advanced VoIP features.
- The NAT device can have an Application-Level Gateway (ALG) that recognizes specific VoIP protocols and the ALG can replace any private IP addresses it sees with the corresponding public IP address. This approach can cause problems when the ALG is not designed to modify fields in a manner expected by a particular VoIP provider's service. (This is discussed further in Section 3.2.)
- The VoIP provider can use a Session Border Controller (SBC) between the VoIP client and server. The SBC has an SBC-resident ALG that replaces private addresses in the VoIP payload with the public source IP address. Since SBCs are specific to particular VoIP services, an SBC-resident ALG will be designed to work for the particular VoIP service in question and will be programmed to understand exactly which parts of the payload clients will populate (and how) and what the VoIP servers expect.

2.2.3. VoIP Server Intolerance for Arbitrary Ports

Some VoIP services do not tolerate random or arbitrary source UDP or TCP port numbers, and expect the source port number used by the client to be the same one seen by the server. Some NATs will change the source port number, in order to allow multiple devices to use the same port number internal to the local network.

Mechanisms to mitigate this issue include:

- The VoIP service or application can be modified to tolerate random source port numbers.
- It may be possible for the NAT device to be configured to leave the source port unchanged for certain ports, such as TCP/5060, UDP/5060, TCP/5061, or UDP/5061, and only modify the source IP address. When a NAT device is configured in this manner, that source UDP or TCP port number cannot be used by multiple VoIP clients in the local network.

Different VoIP providers architect their services differently. To assist with negotiating real-time signaling and media management in the presence of NAT (referred to as "NAT traversal"), some VoIP providers will use SBCs, some will place the additional burden directly on their servers and include STUN servers in their architecture, some will place the burden on the user to acquire a compatible home router or manually configure the home router, and some will require use of a particular home router with an ALG specialized for their service. Most VoIP providers will provide the end user with VoIP clients that are designed or configured to work with that provider's particular service; however, many (especially over-the-top providers that have no formal relationship with the user's network provider) have found it difficult to influence the users' home router or home router configuration.

2.3. IPv6 Firewall

Some routers may implement an IPv6 firewall that blocks unsolicited inbound traffic [17]. These firewalls will generally act in a manner similar to NAT port mappings and port mapping expirations. The same mitigation techniques described in Section 2.2 for preventing NAT port mapping expiration can be used to ensure inbound traffic to certain ports of certain IPv6 addresses are not blocked by such an IPv6 firewall.

3. Technical Causes of VoIP Impairment, Failure, and Restrictions

There are a variety of causes of VoIP impairment, failure, and restrictions. The causes often differ according to the location (e.g., application store, application, device, or network) and the technology involved (e.g., operating system, or type of network).

Section 3.1 discusses VoIP restrictions implemented in the network using port blocking. Section 3.2 discusses VoIP failures caused by the use of Application-Level Gateways in the network. Section 3.3 discusses other network-based causes of VoIP impairment, failure, and restrictions. Section 3.4 discusses restrictions on the use or functionality of VoIP applications that are caused by actions taken on a device, in a VoIP application, or in an application store.

In addition to these technical causes, terms of service may place restrictions on the use of VoIP, e.g. by prohibiting use of cellular data connections for VoIP [18][19].

Some of the sections below include references to user reports of impairments they have encountered with VoIP. These user reports are included for illustrative purposes only, as BITAG has not confirmed the specific causes of these impairments with those users or any other relevant parties.

3.1. Port Blocking

A detailed analysis of Port Blocking was provided in a previous BITAG Report [1]. The report refers to port blocking as "…the practice of an Internet Service Provider (ISP) identifying Internet traffic by the combination of port number and transport protocol, and blocking it entirely." The Port Blocking report analyzed the various ways and locations in the network that port blocking could be implemented, among other topics. This report looks at the use of port blocking specifically in the case of VoIP applications.

There have been specific instances where a network operator intentionally blocked ports commonly used by VoIP applications [20][19][21]. Such VoIP restrictions caused by port blocking can occur anywhere along the data path. Most VoIP services use at least two data paths, one for signaling and another for media, and these typically diverge at some point along the end-to-end path. This communication model is detailed in Section 2. A VoIP call may have its ports blocked either along the signaling or media data paths.

Section 3.5 of the BITAG Port Blocking Report provides the following list for common locations where port blocking may be implemented:

(1) Service Provider's Network Interconnection Links between Network Operators;
(2) Service Provider's Customer Facing Network Links; and
(3) Customer Premises Equipment (CPE).

One example of VoIP port blocking involves blocking SIP signaling data flow. As mentioned previously, SIP functions over TCP/5060, UDP/5060, TCP/5061, and UDP/5061. SIP-based VoIP applications that are designed only to use these ports will not work if these ports are blocked at any point in the network. Some applications may be able to circumvent port blocking depending on how they are designed (see Section 4.2).

The port blocking may also be the result of an unintentional or poorly implemented network device or application. For example, a network operator could decide to take explicit action to limit the use of TCP/5060, UDP/5060, TCP/5061, or UDP/5061 to prohibit another service from operating on this port, defend against a security vulnerability that targets end user devices operating on that port, or protect network resources from Denial of Service attacks using this port, and thereby impact all SIP applications and not just the targeted or ill-behaved SIP application. Unintentional impairment due to port blocking may result from misconfiguration of the network operators' network equipment, misconfiguration of end user managed equipment, or misconfiguration of policies between networks.

VoIP restrictions caused by port blocking may also occur within the home network. End user equipment supports many features for managing the home network. The firewall feature found in the majority of home network routers allows users to filter (block) traffic based on IP address, port and protocol. A user could restrict VoIP applications by accidentally misconfiguring the firewall or deliberately disabling the VoIP service. Another feature often found in home network routers is called port forwarding. This feature is implemented as part of the Network Address Translation (NAT) function and supports the ability to map an incoming connection destined to a port to a specific host behind the NAT device. Using SIP port TCP/5061 or UDP/5061 as an example, a user could forward all traffic destined for port TCP/5061 or UDP/5061 to a single host in the home network, thereby blocking any other device from receiving traffic on this port.

Port blocking is generally ineffective against port-agile VoIP applications that can manually or dynamically choose different ports for SIP signaling. The use of STUN to avoid NAT can facilitate this port agility (see Section 2.2).

3.2. Application-Level Gateways

Application-Level Gateways (ALGs, also known as Application Layer Gateways) are mechanisms within a NAT device or firewall that provide special treatment for certain application protocols. In the context of SIP, these ALGs are generally designed both to keep port mappings alive and to change IP addresses that the VoIP client may put in various SIP message fields. Why these functions are useful is described in more detail in Section 2.2. Due to the wide variation in VoIP architectures employed by different providers, it is prohibitively difficult to design a SIP ALG that allows *all* SIP services to work correctly through a NAT device.

There have been specific instances where certain over-the-top VoIP applications have failed due to the implementation by a network operator of an application-level gateway in the network, in cellular handsets, or in residential gateways [22][23].

In fact, in many cases, a SIP ALG may make changes that can cause failure of a VoIP service that already incorporates mechanisms to solve NAT traversal issues using other mechanisms (for example, an SBC-level ALG may “undo” the changes made to SIP traffic by a NAT device’s ALG). The presence of a SIP ALG focused on facilitating one particular VoIP service can prevent other VoIP services from functioning.

For example, early versions of Windows Messenger were designed to “assume” Universal Plug and Play Internet Gateway Device Protocol (UPnP IGD) implementations existed in the home router that would allow Windows Messenger to create a port mapping there. Some home router vendors, rather than implement UPnP IGD, implemented a SIP ALG specifically designed to allow for proper functioning of Windows Messenger [24]. Home router vendors focused on Windows Messenger because of this application’s ubiquity in Microsoft operating systems. Unfortunately, while both of these accomplished the goal of allowing Windows Messenger to create port mappings, most of these ALGs had the side effect of preventing the proper functioning of other SIP-based services that were not designed specifically for Windows Messenger. Largely as a result of the inability of home router vendors to implement universally functioning SIP ALGs, the IETF published best current practices that recommend disabling SIP ALGs by default [25].

To avoid the complexity and cost of installing STUN servers, SBCs, or more intelligent VoIP servers, many network operators that offer a VoIP service have chosen to place an ALG specific to the operator’s own VoIP service inside the home routers they provide to customers. Such an operator that wishes to allow for the use of independent VoIP services can design the ALG to only target VoIP traffic of the operator’s service and to allow all other VoIP traffic to proceed untouched through the NAT device or firewall.

In cases where an end user has multiple VoIP services attempting to use the same external ports (e.g. TCP/5060, UDP/5060, TCP/5061, or UDP/5061 for SIP), an ALG could be designed that would allow for this. However, designing applications to be port-agile may be a better and more reliable approach than placing the level of intelligence necessary to accomplish this in a home router. Where a network operator already has an ALG enabled in the operator-provided home router, the operator may choose to include such differentiation between the operator's service offering and another VoIP service. If any form of mediation between multiple VoIP services is performed, it must be done carefully, as it introduces additional complexity in the ALG, which in turn can result in impairment of one or more other VoIP services.

Although this section has focused on SIP ALGs, the use of other kinds of ALGs (to facilitate H.323 NAT traversal, for example) can result in similar problems for over-the-top VoIP services.

3.3. Other Network-Based Causes

Network-based causes of VoIP impairment, failure, or restrictions other than port blocking or the use of ALGs include:

- Filtering of relevant DNS resource records from user-facing DNS caches to prevent connectivity to VoIP services;
- Network flow filtering and policing that is designed to identify patterns of likely VoIP traffic and apply targeted treatment to this traffic; and
- Deep packet inspection (payload inspection) where specific VoIP protocol signatures are identified within IP packets.

Some methods for accomplishing each of these techniques are discussed briefly here.

3.3.1. Filtering of DNS resource records

The Domain Name System (DNS) is a distributed database used to map, most commonly, Internet hostnames (e.g., www.foo.com) to IP addresses (e.g., 192.168.1.1). Users and their systems typically query a DNS cache – a regularly updated mirror of DNS records – configured and maintained by their network operator. This DNS cache responds to requests on behalf of the user (or their systems) in the form of domain names and queries the distributed DNS database to return an answer in the form of an IP address.

Using features now available in popular DNS server software, an operator of a DNS cache can filter the results of user or system queries, answering incorrectly (or not answering at all) certain individual DNS requests. This feature is called 'Response Policy Zone' (RPZ) and was originally envisioned as a technique for a DNS cache operator to provide flexible filtering of DNS requests from clients for such things as malicious destinations (e.g., botnet command and control) and control server resource records. In the case of VoIP, RPZ can be used to block or modify relevant DNS records necessary for the use of VoIP applications.

Additionally, there are services sold to DNS cache operators which replace 'failed' DNS resource record lookups – e.g., when no such domain is associated with an IP address – with responses other than errors or failure notifications. These systems, similar to RPZ discussed above, can be configured to provide answers to any resource record lookup, not just in the case of replacing the results for failed lookups.

3.3.2. Network flow policing and filtering

A network operator could choose to deploy filters and policers – mechanisms designed to distinguish between various traffic flows and apply targeted treatment – on network devices that match and drop, degrade or improve flows of traffic typically associated with VoIP communications. For example, 50 small-sized packets per second often indicates an audio stream. This solution can impact other services not related to VoIP. Most deployed network equipment includes capabilities to implement these types of mechanisms.

3.3.3. Deep packet inspection

Outside the US, some nations ban the use of VoIP within their borders, and in some countries restricting use of VoIP is widespread [19] [21] [26]. In some of these cases network operators may be obligated to deploy payload inspection – examining the contents of the IP packet payload – in order to recognize packets relevant to VoIP communications and either degrade the performance of the network for those applications or simply not allow those flows.

3.4. VoIP Restrictions Implemented in Devices, Applications, and Application Stores

In addition to the network causes described above, actions taken on a device, in a VoIP application, or in an application store may restrict the use or functionality of VoIP applications. These examples often reflect business arrangements or agreements between application store providers, operating system vendors, device manufacturers, and/or mobile carriers.

Where an end-user device is supplied or controlled by a network operator, or by the manufacturer or operating system vendor, it is possible to place restrictions on the device that restrict the use or functionality of VoIP applications. The restrictions may be implemented by technically limiting use of cellular data connections by a particular application to customers subscribed to a particular pricing plan [27].

Agreements between a network operator and an application store have been used to limit the availability or functionality of VoIP applications that can be downloaded onto a specific wireless device or using a specific operating system [28][29]. Alternatively, the restriction may be placed by the application store itself [30].

A VoIP application provider may restrict the use or functionality of their VoIP application, e.g., it may restrict certain uses of their services or restrict calls to certain numbers or geographic areas [31].

Finally, in some cases users may be able to implement their own restrictions, e.g., parental controls.

4. Mitigations

4.1. End User Mitigations

When VoIP impairment, failure, or restrictions occur, it may be very difficult for a user to address the issue or solve the problem. Whether a workaround solution exists, and the difficulty of implementing it, depends on the cause. We consider here the causes discussed in the previous section.

If VoIP is restricted using port blocking, and if the VoIP service may be used on alternative ports, then technically sophisticated users may be able to reconfigure the VoIP service to use ports that are not blocked. If the VoIP service does not support use of alternative ports that are not blocked, then the availability of a workaround solution depends on the location at which the VoIP ports are blocked. If VoIP ports are blocked within customer premises equipment (CPE), e.g., cable or DSL modems and/or home routers or gateways, the availability of a workaround solution depends also on which party controls the equipment. BITAG's port blocking report considered two example scenarios: in scenario 1, CPE is managed by the customer, whereas in scenario 2, the network operator provides a device that is capable of port blocking and is solely managed by the operator [1]. Under scenario 1, technically sophisticated users may remove the port block by changing a configuration setting in the CPE. In contrast, under scenario 2, users cannot remove the port block themselves; they may be able to request an opt-out from the network operator, but not all operators honor such requests. In the port blocking report, BITAG recommended that the port blocking (or firewall) rules of consumers' home routers should be user-configurable – whether the routers are provided by the operator or purchased separately by the consumer. BITAG's port blocking report also recommended that the documentation provided with each unit inform the consumer that port blocking or firewall rules have been implemented, which default ports are blocked, and how consumers can modify those rules.

If VoIP ports are blocked in an ISP's network, the availability of workaround solutions is similar to that in scenario 2, i.e. users cannot remove the port block themselves, but they may be able to request an opt-out from the network operator.

If VoIP is restricted using port blocking, a workaround solution that may be available to users, and some application providers as well, involves the use of a Virtual Private Network (VPN). A VPN enables a computer to send and receive data across the Internet as if it were directly connected to a private network [32]. The VPN can avoid the port block by routing traffic through the VPN server's network to the intended destination, but requires availability of a VPN server. Some users have access to a VPN through their workplaces, in which case the VPN is typically intended for work use only. There are also commercial VPN services.

A VPN not provided in conjunction with a given VoIP service may not be designed with the needs of real-time traffic in mind and may degrade VoIP call quality if the VPN introduces too much delay or drops packets.

Additional mitigation tactics against port blocking are discussed in BITAG's port blocking report [1].

If VoIP failures occur due to an ALG in the user's home router, disabling or re-configuring the ALG may resolve the impairment. If the ALG is located in the operator's network, then configuration of the home router or the user's device will have no effect. As with VoIP restrictions using port blocking, use of a VPN may provide a workaround to some application providers and users.

If the cause of VoIP restrictions is the DNS, then technically sophisticated users may find a workaround solution by switching to a DNS server offered by a different organization. Some VoIP applications may offer users the option of turning on encryption or other obfuscation mechanisms to help them circumvent impairments that make use of network flow policing or deep packet inspection.

If the cause of VoIP restrictions are actions taken on a device, in a VoIP application, or in an application store, then users may be able to download versions of their preferred VoIP applications that are not approved by the operating system vendor, application store provider, or network operator. They may also switch devices to circumvent these restrictions.

In general, if the options discussed in this section are not available, or if users lack the knowledge or willingness to pursue such, users may be prevented from using the impaired application altogether.

4.2. Application Provider Mitigations

As with end users, the mitigations available to application providers for dealing with VoIP impairment, failure, and restrictions depend on the cause. In some cases, application providers may choose to develop user documentation or customer service expertise to assist their users in understanding the nature of the problem and potential workarounds, if available.

If VoIP is restricted via port blocking, it may be possible to redesign some applications to use different ports, to conduct connectivity testing before establishing connections, to be port-agile, or to make port selection user-configurable. Whether any of these options are available may depend on whether re-designed versions of the application can be made compatible with existing versions. For more discussion of port blocking mitigations, see the BITAG Port Blocking Report [1].

If VoIP is impaired via network flow policing, application developers may be able to redesign their application traffic so that it is less detectable or less likely to be impaired. For example, applications can be designed to fall back to using TCP if they encounter networks where UDP is impaired, applications may encrypt their packet payloads, or applications may "pad" their traffic flows with extra data so the flows are less likely to resemble a VoIP traffic flow.

To mitigate device-based restrictions, some application providers may redesign their applications to conform to the requirements of operating system vendors, application stores, or network operators.

5. Technical Working Group (TWG) Recommendations

This section of the report presents recommendations of the BITAG Technical Working Group (TWG).

5.1. Network operators should avoid impairing or restricting VoIP applications unless no reasonable alternatives are available to resolve technical issues.

Certain network management actions may have the effect of limiting or restricting VoIP traffic as a method of ensuring network integrity. Examples include port blocks or traffic limitations implemented when a customer uses a vulnerable VoIP service that can be exploited by attackers for the purpose of flooding the network with unwanted traffic. In adopting any approach that has the effect of limiting the use of VoIP, network operators should seek to minimize the impact of the approach on legitimate VoIP use.

5.2. VoIP-related ALGs in operator-supplied home routers should minimize their impact on traffic other than the operator's VoIP service where possible.

As discussed in Section 3.2, VoIP-related ALGs can interfere with some VoIP services while attempting to facilitate NAT traversal for other VoIP services. Because of these problems, BITAG recommends that VoIP-related ALGs in operator-supplied home routers should either allow the VoIP-related ALGs to be disabled for customers who do not subscribe to the operator's VoIP service or minimize or avoid impact to independent VoIP services and all other traffic not associated with the operator's own VoIP service. Where possible, VoIP-related ALGs in operator-supplied home routers should be disabled by default.

ALGs for real-time applications (including VoIP) can be problematic for services other than VoIP, but recommendations concerning ALGs more broadly are outside the scope of this report.

5.3. Manufacturers of home routers should disable VoIP-related ALGs by default.

Some consumers purchase their home routers from retailers rather than from network operators. To limit the impact of VoIP-related ALGs on VoIP services, home routers sold to consumers should have VoIP-related ALGs disabled by default.

5.4. Port blocking rules in consumer equipment should be user-configurable.

As BITAG previously recommended [1], the port blocking (or firewall) rules of consumers' home routers should be user-configurable whether the routers are provided by the ISP or purchased separately by the consumer. By making these rules user-configurable, technically sophisticated users may be able to eliminate port blocks that prevent them from using VoIP services. It is recommended that the documentation provided with the consumer equipment inform the consumer that port blocking or firewall rules have been implemented, the default ports blocked, and how consumers can modify those rules.

5.5. If network operators intentionally use network policies or practices that impair or restrict VoIP, they should provide disclosures about those policies and practices and provide communications channels for feedback.

BITAG recommends that network operators disclose their policies and practices that may or could result in VoIP impairment, failure, or restrictions. The information should be readily available to both customers and non-customers alike. For example, such policies could be provided on the operator's public-facing web site or on a page dedicated to summarizing or describing the ISP's network management practices. If specific VoIP applications are impaired or restricted, those applications should be listed by name, along with a brief description of the reason for the impairment or restriction.

BITAG also recommends that ISPs provide a communications channel or other clear method for application providers and consumers to discuss the impact of VoIP impairment, failure, and restrictions, and possible mitigations.

5.6. Application developers should design VoIP applications to be port-agile where possible.

BITAG recommends that VoIP application developers design VoIP applications and services to be port-agile where possible. Applications designed to tolerate random source ports or to allow port selection to be user-configurable are better able to avoid VoIP impairments that result from port blocking or contention between multiple services for the same port. Whether particular applications can be re-designed to be port agile may depend on whether re-designed versions of the application can be made compatible with existing versions or other existing applications.

6. References

[1] Broadband Internet Technical Advisory Group, “Port Blocking,” August 2013 <http://www.bitag.org/report-port-blocking.php>.

[2] Broadband Internet Technical Advisory Group, “Large-Scale Network Address Translation (NAT),” March 2012 <http://www.bitag.org/report-lsnat.php>.

[3] Broadband Internet Technical Advisory Group, “Real-time Network Management of Internet Congestion,” Oct. 2013 <http://www.bitag.org/documents/BITAG_-_Congestion_Management_Report.pdf>.

[4] Rosenberg, J., H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, “SIP: Session Initiation Protocol,” June 2002, <http://tools.ietf.org/html/rfc3261>.

[5] International Telecommunications Union (ITU), “Packet-based Multimedia Communications Systems,” 2009 <http://www.itu.int/rec/T-REC-H.323/en/>.

[6] Andreasen, F. and B. Foster, “Media Gateway Control Protocol (MGCP) Version 1.0,” Jan. 2003, <http://tools.ietf.org/html/rfc3435>.

[7] Schulzrinne, H., S. Casner, R. Frederick, and V. Jacobsen, “RTP: A Transport Protocol for Real-Time Applications,” July 2003, <http://tools.ietf.org/html/rfc3550>.

[8] Baset, Salman A. and Schulzrinne, Henning G., “An Analysis of the Skype Peer-to-Peer Telephony Protocol,” IEEE Infocom, 2006, <http://www1.cs.columbia.edu/~salman/publications/skype1_4.pdf>.

[9] Postel, J., “Transmission Control Protocol,” Sept. 1981, <http://tools.ietf.org/html/rfc793>.

[10] Cotton, M., L. Eggert, J. Touch, M. Westerlund, and S. Cheshire, “Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry,” Aug. 2011, <http://tools.ietf.org/html/rfc6335>.

[11] Rosenberg, J., R. Mahy, P. Mathews, and D. Wing, “Session Traversal Utilities for NAT (STUN),” Oct. 2008, <http://tools.ietf.org/html/rfc5389>.

[12] Jennings, C., R. Mahy, and F. Audet, “Managing Client-Initiated Connections in the Session Initiation Protocol (SIP),” Oct. 2009, <http://tools.ietf.org/html/rfc5626>.

[13] Srisuresh, P. and M. Holdrege, “IP Network Address Translator (NAT) Terminology and Considerations,” Aug. 1999, <http://tools.ietf.org/html/rfc2663>.

[14] UPnP Forum, “Internet Gateway Device (IGD) V 2.0”, September 2, 2010, <http://upnp.org/specs/gw/igd2/>.

[15] Wing, D., et al, “Port Control Protocol (PCP)” (work in progress), October 31, 2011, <http://tools.ietf.org/html/draft---ietf---pcp---base---17>.

[16] Mahy, R., P. Mathews, and J. Rosenberg, “Travel Using Relays aroung NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN),” Apr. 2010, <http://tools.ietf.org/html/rfc5766>.

[17] Woodyatt, J., “Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service,” Jan. 2011, <http://tools.ietf.org/html/rfc6092>.

[18] Tim Wu, “Wireless Carterfone”, International Journal of Communication, 2007, pp. 389-426, <https://www.eff.org/files/wu07wireless-carterfone.pdf>.

[19] Body of European Regulators for Electronic Communications (BEREC), “A View of Traffic Management and Other Practices Resulting in Restrictions to the Open Internet in Europe,” May 29, 2012, <http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf>.

[20] Federal Communications Commission (FCC), “In the Matter of Madison River Communications, LLC and Affiliated Companies”, Consent Decree, DA 05-543, March 2005, <http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A2.pdf>.

[21] Moskvitch, Katia, “Ethiopia Clamps Down on Skype and Other Internet Use on Tor,” BBC News Technology, June 15, 2012, <http://www.bbc.co.uk/news/technology-18461292>.

[22] AT&T Community Forums, “Using Third Party VoIP Service with ATT-Uverse Internet: Call Drops After Some Time,” Feb. 11, 2013, <http://forums.att.com/t5/Features-and-How-To/Using-Third-party-VOIP-service-with-ATT-Uverse-internet-Call/td-p/3426287#.Uv0RmfldXyQ>.

[23] “VoIP with AT&T U-Verse,” Broadband DSLReports.com, VoIP Tech Chat Forum, June 26, 2013, <http://www.dslreports.com/forum/r28413905-Equipment-VOIP-with-AT-T-U-Verse>.

[24] D-Link Advanced Support, Firewall Settings - Application-Level Gateway (ALG) Settings, March 19, 2014), http://support.dlink.com/emulators/dir635/109/Help_Advanced.html#Firewall.

[25] Audet, F. and C. Jennings, “Network Address Translation (NAT) Behavioral Requirements for Unicast UDP,” Jan. 2007, <http://tools.ietf.org/html/rfc4787>.

[26] Barnum, Tristan, "Interactive Infographic of Countries that Block VoIP," July 30, 2013, <http://blog.voxox.com/blog/bid/320731/Interactive-Infographic-of-Countries-That-Block-VoIP-DEFCON-VoIP>.

[27] Federal Communications Commission, Open Internet Advisory Committee, Mobile Broadband Working Group, "AT&T/FaceTime Case Study," Jan. 17, 2013, <http://transition.fcc.gov/cgb/events/ATT-FaceTimeReport.pdf>.

[28] Tessler, Joelle, "iPhone to Run on AT&T: Will Allow Google Voice, Skype on 3G Network," Huffington Post, Oct. 6, 2009, <http://www.huffingtonpost.com/2009/10/06/iphone-voip-to-run-on-att_n_311677.html>.

[29] O'Brien, Kevin J., "Skype in a Struggle to Be Heard on Mobile Phones," New York Times, Feb. 17, 2010, <http://www.nytimes.com/2010/02/18/technology/18voip.html?_r=0>.

[30] Fortt, Jon, "AT&T: We didn't ask Apple to block Google Voice," CNNMoney, Aug. 21, 2009, <http://tech.fortune.cnn.com/2009/08/21/att-we-didnt-ask-apple-to-block-google-voice/>.

[31] Stross, Randall, "Why Google Doesn't Like Its Phone Bill," New York Times, Oct. 31, 2009, <http://www.nytimes.com/2009/11/01/business/01digi.html>.

[32] Wikipedia, "Virtual Private Network," Last Visited on March 19, 2014, <http://en.wikipedia.org/wiki/Vpn>.

7. Additional References

Phipps, Eric, "In Depth: Verizon Blocks SIP Traffic Using ALG," ONSIP, July 2, 2013, <http://www.onsip.com/blog/2013/07/02/in-depth-verizon-blocks-sip-traffic-using-alg>.

"Verizon Wireless Blocking SIP Packets Going to Port 50," Broadband DSLReports.com, VoIP Tech Chat Forum, Dec. 29, 2012, <http://www.dslreports.com/forum/r27865722-General-Verizon-wireless-blocking-sip-packets-going-to-port-50>.

8. Glossary of terms

All definitions of terms are solely for the purposes of this report, and many are adapted from publications of the Internet Engineering Task Force (www.ietf.org). Readers should be aware that a number of terms have alternate definitions, particularly when used in different or non-networking contexts.

Application Layer Gateway (ALG)	An Application Layer Gateway (also known as an Application-Level Gateway or ALG) is a security component that augments a firewall or NAT employed in a computer network, to enable certain kinds of traffic that would not otherwise be enabled.
Interactive Connectivity Establishment (ICE)	A protocol for Network Address Translation (NAT) traversal for UDP-based multimedia sessions established with the offer/answer model. ICE can be used by any protocol utilizing the offer/answer model, such as the Session Initiation Protocol (SIP).
Network Flow Policers	Traffic policing, also known rate limiting, enables control of the maximum rate of IP traffic sent or received on an interface and also to partition network traffic into multiple priority levels, which can be used as classes of service.
Session Initiation Protocol (SIP)	An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.
Session Traversal Utilities for NAT (STUN)	A protocol used to permit NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. STUN can be used by applications operating behind a NAT to determine the IP address and port allocated to it by the NAT. It can also be used to check connectivity between two endpoints, and as a keep-alive protocol to maintain NAT bindings.
Signaling or Control Protocol	In VoIP communication, the signaling that controls the conversation – establishing, maintaining, and ceasing a call – is distinct from the actual stream of data carrying the voice content of the conversation. Session Initial Protocol (SIP) is one example of a signaling or control protocol.
SIP BYE Message	A Session Initiation Protocol (SIP) request code used for communication. A “BYE” message terminates a call and can be sent by either the caller or the callee of the VoIP call.
SIP INVITE Message	A Session Initiation Protocol (SIP) request code used for communication. An “INVITE” message indicates a client is

	being invited to participate in a call session.
Transport Protocol	The transport layer is responsible for delivering data to the appropriate application process on host computers. Transport protocols deliver packets to applications, and can provide additional functionality such as congestion control, reliable data delivery, duplicate data suppression, and flow control. Transmission Control Protocol (TCP) is one example of a transport protocol.
Traversal Using Relays around NAT (TURN)	A protocol that allows a host behind a NAT to request that another host act as a relay. The client can arrange for the server to relay packets to and from certain other hosts and can control aspects of how the relaying is done.
VoIP Failure	Particular kinds of VoIP impairments that arise when VoIP calls cannot be established at all, or when no media is capable of being exchanged between VoIP endpoints.
VoIP Impairment	Anything that prevents a VoIP application from being used in the manner desired by a user. An impairment affecting a VoIP service can occur anywhere along the data path, including in the end devices.
VoIP Restriction	When network operators, VoIP providers, operating system vendors, or application store providers take steps that cause VoIP failures or prevent VoIP from being used.

9. Document Contributors and Reviewers

- Fred Baker, *Cisco*
- Lily Chen, *Verizon*
- Alissa Cooper, *Cisco*
- Michael Fargano, *CenturyLink*
- Joseph Lorenzo Hall, *Center for Democracy & Technology*
- Trace Hollifield, *Bright House Networks*
- Jaime Jimenez, *Comcast*
- Scott Jordan
- Gary Langille, *Echostar*
- Chris Morrow, *Google*
- Jon Peha
- Tushar Saxena, *Verizon*
- Donald Smith, *CenturyLink*
- Barbara Stark, *AT&T*
- Sanjay Udani*, Verizon*
- Jason Weil, *Time Warner Cable*