ATIS STANDARD

**ATIS-1000014**

# VoIP Network-to-Network Interface Testing Framework

**Technical Report**

The Alliance for Telecommunication Industry Solutions (ATIS) is a technical planning and standards development organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. Over 1,100 participants from over 300 communications companies are active in ATIS' 22 industry committees and its Incubator Solutions Program.

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

## Notice of Disclaimer & Limitation of Liability



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.

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

Is an ATIS Standard developed by the **Interoperability (IOP)** Subcommittee under the **Packet Technologies and Systems Committee (PTSC)**.

*Published by*

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



Printed in the United States of America.

**ATIS-1000014**

ATIS Standard on

# VoIP Network-to-Network Interface Testing Framework

Secretariat

**Alliance for Telecommunications Industry Solutions**

Approved October 2006


**Abstract**

This Technical Report describes a framework for testing interoperability of an IP Network-Network interconnection for VoIP services. The framework is for such an interconnection as specified in ATIS-1000009.2006, *IP Network-to-Network Interface (NNI) Standard for VoIP*.

# FOREWORD

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between carriers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) -- formerly T1S1 -- develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

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

The Interoperability (IOP) Subcommittee of PTSC was responsible for the development of this document.

# TABLE OF CONTENTS



# TABLE OF TABLES

Technical Report on –

# VoIP Network-to-Network Interface Testing Framework

## 1 INTRODUCTION

This Technical Report (TR) describes a framework for testing IP-IP Network interconnection.

The testing framework described herein is for IP network-network interconnection (IP NNI) as specified in the ATIS American National Standard IP Network-To-Network Interface (NNI) Standard for VoIP. [1] That document is referred to in this TR as the *VoIP NNI ANS*.

A common testing framework has the benefits of:

1) Re-use, avoiding the inefficiency of pair-wise re-creation by network operators whenever any two particular networks are to be tested.
2) Industry-wide input.
3) Being a common reference for understanding test results (e.g., when network A tests with network B and then with network C).

This testing framework:

- Addresses pair-wise network interoperability, rather than equipment or vendor testing or certification, or protocol standards conformance.
- Is agnostic regarding the particulars of test environments and configurations – e.g., it could be with deployed networks or lab-lab; and does not assume any details about internal network architectures or systems.
- Describes the kinds of things to be tested, but does not provide explicit, enumerated test cases; also, it does not specify particular testing methods.
- Initially focuses on VoIP.

This testing framework does not address:

- Identification of the responsible organization performing the testing.
- Testing for services; however, services may be used as stimuli to invoke aspects of protocols that are to be tested.
- Load testing.
- Simultaneous testing of multiple NNIs between two networks. This TR addresses testing of a single NNI at a time.
- Failure scenarios.
- Test cases that intentionally result in a protocol timeout.

Successful network interoperability testing should be verifiable strictly by observing what happens at the network-network interface. Test generation and some verification methods may pragmatically involve the placement of actual telephone calls and observing results from that user point of view.

Before defining specific test plans, the network operators involved must agree on what subset of the VoIP NNI ANS they are implementing, according to the SLA. Testing could follow various models. For example:

a. Conduct a full suite of tests exercising the entire interface as defined in the VoIP NNI ANS, and verify which pass and whether that set is consistent with the aspects of the VoIP NNI ANS that are in the SLA agreed to by the network operators. An advantage of this approach is that it can discover capabilities supported across the interface that may not otherwise have been known to or agreed to by the network operators.

b. Conduct a test suite that exercises a *subset* of the entire interface in the VoIP NNI ANS, where that subset is limited to aspects of the VoIP NNI ANS that are in the SLA agreed to by the network operators. An advantage of this approach is that it may involve less testing. The subset may depend to some degree, for example, on the nature of the two IP networks, ('LEC' - 'interexchange', or peer-to-peer, or wireless versus wireline) and/or the services being supported.

The exercise of the testing guidelines and call stimulus scenarios contained in this document are intended to have no impact on the integrity or reliability of existing services being supported in a live network.

# 2 DEFINITIONS

For protocol-specific terminology, the reader should consult the corresponding protocol specifications.

The definitions of "layer" terms in this document – *physical*, *data link*, *network*, and *transport* -- are as per the OSI model. [2]

# 3 ABBREVIATIONS & ACRONYMS

| | |
|---|---|
| AIB | Authenticated Identity Body |
| ANS | American National Standard |
| APRI | Address Presentation Restricted Indicator |
| AS | Application Server |
| ATIS | Alliance for Telecommunications Industry Solutions |
| cpim | Common Presence and Instant Messaging |
| DiffServ | Differentiated Service |
| DTMF | Dual Tone Multi-Frequency |
| ETS | Emergency Telecommunications Service |
| GETS | Government ETS |
| IAM | Initial Address Message |

| | |
|---|---|
| IETF | Internet Engineering Task Force |
| IFP | Internet Fax Protocol |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| ISUP | ISDN User Part |
| ITU | International Telecommunication Union |
| LEC | Local Exchange Carrier |
| MIME | Multi-part Internet Mail Extensions |
| MS | Media Server |
| NI | Network Interconnect |
| NNI | Network-to-Network Interface |
| NP | Number Portability |
| OSI | Open Systems Interconnect |
| POTS | Plain Old Telephone Service |
| PSTN | Public Switched Telephone Network |
| RFC | Request For Comments |
| RTCP | Real-Time Control Protocol |
| RTP | Real-time Transport Protocol |
| SACK | Selective ACKknowledge |
| SCTP | Stream Control Transmission Protocol |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SIPS | SIP-Secure |
| SLA | Service Level Agreement |
| S/MIME | Secure MIME |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TR | Technical Report |
| UDP | User Datagram Protocol |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| VoIP | Voice over IP |
| XR | Extended Reports |

# 4 PHYSICAL AND DATA LINK LAYERS

At the physical and data link layers, there is no distinctive treatment of VoIP/multimedia versus data, or among VoIP/multimedia traffic types, and thus nothing specific to test in regard to VoIP/multimedia. Tests should be conducted to verify the satisfactory operation of those layers, but since there is no distinction from treatment of data traffic, testing at those layers is not addressed in this document.

# 5 NETWORK LAYER

Aspects of the network layer that may involve treatment of VoIP/multimedia different from data are addressed in this TR.

## 5.1 IP Addresses

The use of the IP addresses specified as per bi-lateral agreement should be verified. Note that IP addresses for different types of IP packet payload may be different; for example, IP addresses for UDP payload versus TCP payload, or IP addresses for SIP signaling payload over UDP versus RTP media payload over UDP.

## 5.2 Priority Differentiation

Traffic priority across the NNI may be differentiated at the IP packet level through the use of DiffServ code points. When employed, the use of such differentiation in DiffServ should be verified.

The VoIP NNI may more generally be an IP NNI that carries other kinds of traffic besides voice calls; for example, video, web-browsing, email, file transfer or presence information. Those other kinds of traffic may also receive differentiated treatment.

## 5.3 IP Payload Protocol Indication

Proper indication within IP of the payload protocol should be verified (i.e., use of the Protocol field in IPv4 or the Next Header field in IPv6).

# 6 SIGNALING TRANSPORT

The VoIP NNI ANS identifies the use of TCP, UDP, or SCTP for SIP signaling transport.

## 6.1 UDP

The use of UDP for SIP transport is the same as for other types of UDP payload. Therefore, there are no specific capabilities of UDP that need to be exercised for SIP payload. However, it should be verified that the intended UDP port numbers for SIP transport are actually used, if they differ from those for other types of UDP payload.

## 6.2 TCP

As with UDP, there is nothing special about the use of TCP for SIP signaling transport versus other kinds of TCP payload. However, unlike UDP, TCP involves the establishment of a connection. Therefore it should be verified that the specific TCP connection(s) for conveying SIP signaling are established, including the use of the intended TCP port numbers and the desired TCP connection characteristics of window size and maximum segment size.

### 6.3 SCTP

For SCTP, the following should be verified:

a. The establishment of associations between SCTP signaling endpoints (i.e., SCTP packets with INIT and INIT ACK chunks, etc.) and specific streams per association.

b. The passing of actual signaling content (SCTP packets with DATA and SACK chunks, the DATA chunks carrying SIP signaling).

c. The heartbeat mechanism (SCTP packets using HEARTBEAT and HEARTBEAT ACK chunks).

d. Congestion control (using procedures with the Advertised Receiver Window Credit in a SACK chunk).

e. Path Maximum Transmission Unit (MTU) discovery.

## 7 CALL CONTROL

### 7.1 SIP - Call Stimulus Scenarios

This subsection contains a set of call scenarios that could be used as stimuli to test aspects of the SIP protocol that it would be especially desirable to verify. The set below does *not*:

- Exhaustively exercise all possible facets of SIP use allowed according to the VoIP NNI ANS.
- In particular, error scenarios eliciting 4XX, 5XX, and 6XX SIP responses are absent.

Some of the scenarios below could be combined into a single stimulus call. The reason to separate out into different scenarios here is to focus on the different aspects of the protocol to be tested, which are in the third column of Table 1.

**Table 1. Call Stimulus Scenarios for SIP**

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 1. | Simple voice call; destination address types | Address formats in INVITE Request-URI and To header:<br>▪ sip:x…x@hostname;user=phone<br>▪ tel:+x…x<br>▪ sip:username@hostname | *RFC 3261,*<br>*RFC 3966,*<br>*RFC 2806*<br><br>The "x…x" string represents telephone number information.<br><br>The destination address could be domestic or international, POTS, Toll-Free or 911, etc. |
| 2. | Simple call; answered and cleared | Normal SIP messaging sequence with final response of 200 OK to the INVITE, including:<br>▪ 183 Session Progress with SDP content<br>▪ 180 Ringing<br>▪ the use of PRACK messages | *RFC 3261,*<br>*RFC 3262* |
| 3. | Simple call; called party busy | Final response of 486 Busy Here to the INVITE | *RFC 3261* |
| 4. | Simple voice call between SIP end-devices; answered | Use of a MIME-encoded message body with SDP offer content in the SIP INVITE and SDP answer content in one or more of the 183 Session Progress, 180 Alerting and 200 OK responses; with the Content-Type header containing "application/sdp"; and with the Content-Disposition header, if present, containing "session". | *RFC 3261,*<br>*RFC 3264*<br><br>Only the 200 OK response is required to be returned in this scenario, whereas the provisional responses 183 Session Progress and 180 Alerting are optional.<br><br>Because the use of the SIP PRACK procedure is mandatory in the VoIP NNI ANS (making provisional responses reliable), the SDP answer content is not required to be carried in a 200 OK response. |
| 5. | Audio + video multimedia call between SIP end-devices. | Use of a MIME-encoded SDP body in the SIP INVITE and one or more of the 180 Alerting, 183 Session Progress or 200 OK response messages, characterizing the single multimedia offer. | *RFC 3264* |
| 6. | Simple call; ring no answer for X seconds | The call and its SIP dialog attempt should remain in progress until cleared after X seconds by one of the networks, with either a CANCEL request from the caller-side network or a 480 Temporarily Unavailable final response to the INVITE from the called-side network. | *RFC 3261*<br><br>The value of X is equivalent to a PTSN network going to lockout; i.e., the call attempt should not be left up indefinitely |
| 7. | Simple call to a non-working address | Final response of either 404 Not Found or 410 Gone to the INVITE | *RFC 3261* |
| 8. | Simple call, but with multiple SDP offers in the INVITE | 183 Session Progress or 200 OK response, with a single SDP entry that is one of those offered in the INVITE | *RFC 3261,*<br>*RFC 3262,*<br>*RFC 3264* |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 9. | Simple call, PSTN-originated and terminated | SIP messages carry MIME-encoded ISUP messages *and* the correct corresponding SIP-ISUP mappings.<br><br>It should also be verified that the MIME-encoded ISUP does not include parameters, such as network-proprietary parameters, that are *not* intended to be passed across the network-network interface. | *RFC 3372*<br>*RFC 3204*<br>*T1.679-2004* |
| 10. | Call to a toll-free number; the upstream network has already performed the toll-free translation to a routing number | Routing number passed in the INVITE Req-URI, original dialed toll-free number in the To header | *RFC 3261* |
| 11. | Call to a ported number; the upstream network has done the LNP lookup | The INVITE Request URI addressing information is appropriately populated.<br>For example, for ported number 7324201234 with location routing number 7326719998,<br>the userinfo portion of the Request-URI would be +17324201234;npdi;rn=+17326719998 | *T1.679-2004*<br>*RFC 4694*<br><br>Alternatively, the ported number information could be embedded in a tel: URI.<br><br>The userinfo portion of the SIP URI in the To header may also contain the location routing number and npdi information. |
| 12. | Simple call, PSTN-originated, IAM Calling party number parameter APRI = *Presentation restricted*, no Generic Address parameter | INVITE P-Asserted Identity header includes the calling party number, and priv-value=; "id"; From header carries "anonymous" display name and 'Anonymous URI' | *T1.679-2004,*<br>*RFC 3325* |
| 13. | Simple call, PSTN-originated, IAM Calling party number parameter with APRI = *Presentation allowed*, no Generic Address parameter | INVITE P-Asserted Identity header includes the calling party number; From header also includes the calling party number | *T1.679-2004,*<br>*RFC 3325* |
| 14. | Simple call attempt, caller hangs up before called party answers | Originating network sends a CANCEL message after the INVITE. | *RFC 3261* |
| 15. | Simple fax call, fax passed as voiceband (aka "pass-through") | Address format in INVITE To header:<br>▪ fax:+12234567890<br>and SDP content indicates audio G.711 with silence suppression *off* | *RFC 2806*<br><br>There is a variety of additional information that can be conveyed as parameters with this kind of URL that is not identified here |
| 16. | Simple modem call, data passed as voiceband | Address format in INVITE To header:<br>▪ modem:+12234567890;type=*type info*<br>and SDP content indicates audio G.711 with silence suppression *off* | *RFC 2806*<br><br>There is a variety of additional information that can be conveyed as parameters with this kind of URL that is not identified here |
| 17. | Call from a wireline phone to a Government Emergency Telecommunications Service (GETS) destination number | SIP INVITE contains a Resource Priority header with namespace.value ets.X with an appropriate value for X; SIP OK message confirms that the receiving network supports that namespace.value | *RFC 4412*<br>*ATIS-1000010.2006* |
| 18. | Call from a wireless phone to a Wireless Priority Service (WPS) access code + destination number | SIP INVITE contains a Resource Priority header with a pair of namespace.values ets.X, wps.Y; SIP OK message confirms that the receiving network supports those namespace.values | *RFC 4412*<br>*ATIS-1000010.2006* |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 19. | Call involving an Application Server, such as a prepaid card service, during which a called party may be put on hold<br><br>Or, *alternatively*, a SIP phone-originated call answered by a called party, and the calling SIP phone at some point puts the called party on hold in such a way that the phone itself initiates a re-INVITE without an SDP offer. | Sending a second INVITE (re-INVITE) without an SDP offer, and receiving a 200 OK response confirming the SDP offer | *RFC 3261*<br><br>Caller may be able to input DTMF or a card balance timer may expire, causing the AS to return the caller to a MS and putting the called party temporarily on hold. |
| 20. | Same as above, but now the called party is reconnected after being on hold | Sending a second INVITE (re-INVITE) with an SDP offer, and receiving a 200 OK response confirming the SDP offer | *RFC 3261*<br><br>AS is reconnecting the called party to the calling party. |
| 21. | A VoIP connection exists between SIP end-devices A and B. Device A invokes a call transfer from itself to Device C. The connections A-B and B-C are across the NNI. | Between A and B: Use of the REFER method, including passing of REFER, 202 Accepted and NOTIFY messages. The REFER message includes the Refer-To and Referred-By headers as well as the escaped Replaces header.<br><br>The "triggered INVITE" from B to C contains the Referred-By and Replaces headers.<br><br>The REFER message may also include use of the message/sipfrag technique to carry the status of referenced requests. | *RFC 3515*<br>*RFC 3891*<br>*RFC 3892*<br>*RFC 3420*<br>*draft-ietf-sip-referredby* |
| 22. | One SIP end-device delivers an instant message to another SIP end-device. | Use of the MESSAGE method, involving sending a MESSAGE request with a 200 OK response. The instant message is carried in the MESSAGE request as MIME payload, type message/cpim. | *RFC 3428* |
| 23. | A SIP end-device that can include caller preferences originates a call to another SIP end-device | Passing of the Request-Disposition, Accept-Contact and Reject-Contact headers in the INVITE; the particular response to the INVITE is not specified here | *RFC 3841*<br><br>The response of the network receiving the INVITE will depend on what it does or doesn't do with the information in any of those 'caller preferences' headers |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 24. | Group 3 fax call between PSTN endpoints.<br><br>Across the NNI, the call starts as audio, then changes to fax, then changes back to audio.<br><br>IP/PSTN Gateways use the IFP protocol to transmit the fax.<br><br>Inband fax tones from the fax endpoints will be detected by the IP/PSTN Gateways and will trigger them to know when to perform re-INVITEs to switch between voice/audio and IFP transmission. | A first SIP INVITE is coded for voice/audio.<br><br>A subsequent re-INVITE is coded for fax transmission using IFP. – The SDP details will vary depending on whether transport is UDPTL/UDP, TPKT/TCP, or RTP over UDP.<br><br>A subsequent re-INVITE is coded for voice/audio. | *ITU-T T.30,*<br>*ITU-T T.38,*<br>draft-ietf-sipping-realtimefax,<br>draft-jones-avt-audio-t38 |
| 25. | Fax call between IP fax devices. (No PSTN involved.) | The SIP INVITE is coded for fax transmission using IFP. – The SDP details will vary depending on whether transport is UDPTL/UDP, TPKT/TCP, or RTP over UDP. | *ITU-T T.38,*<br>draft-ietf-sipping-realtimefax,<br>draft-jones-avt-audio-t38 |
| 26. | Voice call from a SIP phone to a called party; the called party deliberately does not answer, and the caller hangs up upon hearing ringing. | After the SIP INVITE from the caller side network and 1XX a provisional response from the called side network, a SIP CANCEL request should appear from the caller-side network, with a 200 OK response to the CANCEL *and* with a 487 Request Terminated final response to the INVITE. | *RFC 3261* |
| 27. | Call to an unassigned number in the terminating PTSN network. | A final response of 404 Not Found is received in response to the SIP INVITE. | *RFC 3261,*<br>*T1.679-2004*<br><br>Note: the terminating PSTN network is responding with an ISUP Release message with Cause 1 (unallocated(unassigned number)) |
| 28. | Call to a number in the terminating PSTN that is recently changed and unassigned. | A final response of 410 Gone is received in response to the SIP INVITE. | *RFC 3261,*<br>*T1.679-2004*<br><br>Note: the terminating PSTN network is responding with an ISUP Release message with Cause 22 (number changed) |
| 29. | Call to a PSTN-connected phone that is busy (and that does not have call waiting, call forwarding, etc). | A final response of 486 Busy is received in response to the SIP INVITE. | *RFC 3261,*<br>*T1.679-2004*<br><br>Note: the terminating PSTN network is responding with an ISUP Release message with Cause 17 (user busy) |
| 30. | Call to a SIP phone that can be set to temporarily refuse calls (e.g., a SIP phone 'do not disturb' feature) | A final response of 480 Temporarily Unavailable is received in response to the SIP INVITE. | *RFC 3261* |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 31. | Call established between PSTN-connected phones. After answering (off-hook), the called party briefly goes on-hook then off-hook again, causing the terminating PSTN to generate ISUP Suspend and Resume messages.<br><br>Here, “briefly” means for a few seconds – long enough to trigger an ISUP Suspend message (that starts ISUP timer T6, whose range is 10-32 seconds), but not long enough to trigger clearing of the call. | After the call is established across the IP NNI, a SIP INFO containing an ISUP Suspend message is passed and receives a 200 OK response. A subsequent SIP INFO containing an ISUP Resume message is passed and receives a 200 OK response. | *RFC 2976,*<br>*T1.679* |
| 32. | Toll Free-originated call, where the IP network *across* the IP NNI is the carrier responsible for the number translation. | INVITE message contains a cic= fragment with the SIP or tel address in the Request-URI and To header identifying the appropriate carrier | *draft-ietf-iptel-tel-np*<br><br>(CIC=Carrier Identification Code) |
| 33. | IP end-devices capable of treating early media separately from regular media as per RFC 3959; calling IP device offers regular media in the INVITE, the called IP device accepts it in a 183 Session Progress but also offers early media, which the calling IP device accepts in the 200 OK to the 183 Session Progress.<br><br>The caller device may be a SIP phone. The called device may be SIP equipment performing a prompt & collect activity with the caller before deciding to actually accept the caller’s media offer.<br><br>Alternatively, a calling SIP device may interact with a network AS and MS that supports early media (pre-answer interaction with the caller). | INVITE carries:<br>- an “early-session” option tag in the Supported header field,<br>- Content-Type “application/sdp”,<br>- Content-Disposition “session”,<br>- SDP description for a media session (e.g., for a voice call)<br><br>183 Session Progress with:<br>- Content-Type “application/sdp”<br>- Content-Disposition “session”<br>- SDP content<br>--- that accepts the regular media offer in the INVITE<br>and<br>- Content-Type “application/sdp”<br>- Content-Disposition “early-session”<br>- SDP description for another media session (e.g., for a voice call)<br>---- that offers the caller early media<br><br>200 OK to the 183 Session Progress with:<br>- Content-Type “application/sdp”<br>- Content-Disposition “early-session”<br>- SDP content<br>---- that accepts the called party’s early media offer<br><br>200 OK to the INVITE | *RFC 3959,*<br>*RFC 3960*<br><br>Typically the early media and regular media session IP addresses/port #s would not be the same; e.g., at least the port numbers would be different so the two IP end-devices can distinguish between the two media streams.<br><br>The early media stream can start as soon as the early media offer/answer exchange has occurred (the 183 and the 200 OK to it).<br><br>The early media stream ends and the regular media stream begins once the 200 OK to the INVITE has occurred (that transitions the SIP exchange status from early dialog to regular dialog). |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 34. | A call between SIP end- devices that support SIPS URIs and therefore also TLS and TCP or SCTP. | Use of a SIPS URI in the INVITE Request-URI; in which case the TLS method of encrypted transport must be employed to carry all the SIP messages for that SIP dialog.<br><br>The transport parameter of the SIPS Request URI must also indicate a reliable transport method (*tls* in the case of TCP, or *tls-sctp* in the case of SCTP).<br><br>The Contact header in the INVITE must contain a SIPS URI. Likewise, the Contact header in the 200 OK response must contain a SIPS URI. | *RFC 3261,*<br>*RFC 2246,*<br>*RFC 4168*<br><br>TLS must be used from the caller to the domain of the called party, which in this scenario would include going across the NNI.<br><br>Use of a SIPS URI and therefore TLS also means that a reliable transport must be in use (i.e., TCP or SCTP; not UDP). |
| 35. | Simple voice call between SIP end-devices that support the regular form of SIP header names. | Use of the regular form of SIP header names in SIP messages. | *RFC 3261*<br><br>If the networks happen to convert to compact form, then this scenario is not applicable. |
| 36. | Simple voice call between SIP end-devices that support the compact form of SIP header names. | Use of the compact form of SIP header names in SIP messages. | *RFC 3261*<br><br>Not all headers have a compact form for their names.<br><br>If the networks happen to convert to regular form, then this scenario is not applicable. |
| 37. | SIP end-devices that support the SIP OPTIONS request method.<br><br>The SIP device receiving the OPTIONS request is idle, i.e., able to receive an incoming call. | Passing of the OPTIONS request, possibly containing an Accept header indicating the type of message body (e.g., application/sdp) the originator would like to receive in the response.<br><br>Then a 200 OK response with: an Allow header listing SIP methods supported, an Accept header listing supported message body types, a Supported header with option tags for SIP extensions supported, an Accept Encoding header listing accepted encodings, an Accept-Language header listing languages supported, and potentially a message body (e.g., SDP) responding to what was indicated in the Allow header in the INVITE. | *RFC 3261* |
| 38. | SIP end-devices that support the SIP OPTIONS request method.<br><br>The SIP device receiving the OPTIONS request is currently incapable of receiving an incoming call, i.e., it may already be tied up in a call with another endpoint. | Passing of the OPTIONS request, possibly containing an Accept header indicating the type of message body (e.g., application/sdp) the originator would like to receive in the response.<br><br>Then a 486 Busy Here response with: an Allow header listing SIP methods supported, an Accept header listing supported message body types, a Supported header with option tags for SIP extensions supported, an Accept Encoding header listing accepted encodings, an Accept-Language header listing languages supported, and potentially a message body (e.g., SDP) responding to what was indicated in the Allow header in the INVITE. | *RFC 3261* |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 39. | A simple call between SIP end-devices that support S/MIME message content.<br><br>The particular S/MIME content that is passed is not specified as part of this scenario. It could be, for example, an attachment file or some SIP message headers that could have significance to the end-devices but that the networks do not act upon. | Passing in the INVITE request, and possibly a 180 Alerting, 183 Session Progress or 200 OK response message, of S/MIME-encoded message body content, as indicated in the Content-Type (e.g. "application/x-pkcs7-mime") and Content-Disposition (e.g., "attachment; filename=smime.p7m") headers. | *RFC 3261,*<br>*RFC 2311*<br><br>With the use of S/MIME, the end-devices would also exchange key/certificate information to allow them to decrypt/authenticate.<br><br>The networks are not expected to decode or operate on the S/MIME content. Typically that information is intended for the SIP end-devices outside the network(s).. |
| 40. | A call between SIP end- devices, where the called device forwards the call to another endpoint, and employs the 181 Call Is Being Forwarded response to inform the originator of status | The INVITE receives a temporary response of 181 Call Is Being Forwarded | *RFC 3261* |
| 41. | Simple voice call between SIP end-devices, where the called device temporarily does not accept the call (e.g., it may be busy on another call or calls), and employs the 182 Queued response to inform the originator of status | The INVITE receives a temporary response of 182 Queued<br><br>The 182 Queued response may contain a reason phrase providing information about the queuing status. | *RFC 3261* |
| 42. | Any call where the originating-side network passes trunk group information across the NNI. | The INVITE includes the trunk-group and trunk-context parameters. These parameters may be in the Contact header or the Request-URI (in the case where the originating-side network is allowed to influence routing in the terminating-side network). | *draft-ietf-iptel-trunk-group* |
| 43. | Simple PSTN-originated call attempt, caller hangs up before called party answers | Originating network sends a CANCEL message after the INVITE with a Reason header containing a Q.850 cause value of 16 "Normal Call Clearing" | *RFC 3326* |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 44. | Call between SIP end-devices that support the SIP Authenticated Identity Body (AIB) capability for verifying user identity | INVITE request has a "multipart/mixed" MIME body that includes a body for the SDP offer *and* additional body content for the AIB information. The exact format can vary. An illustrative example is:<br><br>Content-Type: multipart/signed; protocol="application/pkcs7-signature";<br>micalg=sha1; boundary=boundary*XX*<br>Content length: *NNN*<br><br>--boundary*XX*<br><br>Content-Type: message/sipfrag<br>Content-Disposition: aib; handling=optional<br><br>*{SIP headers constituting the actual AIB body}*<br><br>--boundary*XX*<br><br>Content-Type: application/pkcs7-signature; name=smime.p7s<br>Content-Transfer-Encoding: base64<br><br>Content-Disposition: attachment; filename=smime.p7s;<br>handling=required<br><br>*{cryptographic signature}*<br><br>--boundary*XX*-- | *RFC 3893*<br><br>The AIB body may optionally be encrypted. |
| 45. | Call between SIP end-devices that support SIP content indirection, with content (e.g., a jpeg file) located elsewhere that will be identified by a URI from the calling device and retrieved by the called device | INVITE request contains a multi-part body with<br>▪ SDP offer content,<br>▪ content indirection information that will minimally consist of<br>Content-Type: message/external-body; access-type="URL";URL=" *address*"<br><br>The content indirection part may contain additional information such as content description, expiration date of the URL, or content size.<br><br>The INVITE may also carry "message/external-body" in the Accept header. | draft-ietf-sip-content-indirect-mech |
| 46. | SIP-based Instant Messaging from one SIP end-device to another | A MESSAGE request is passed forward, and responded to with a 200 OK.<br><br>The MESSAGE contains the user message in the body, with Content-Type: text/plain, or alternatively Content-Type: message/cpim . The 200 OK content must be what is appropriate as a response to a MESSAGE request (as opposed to, e.g., an INVITE); i.e., no body or Contact header is included. | *RFC 3428* |

| # | Scenario Name/Description | SIP aspect to be exercised & verified | Comments |
|---|---|---|---|
| 47. | A SIP end-device initiates a Registration, where the network or other entity *across* the VoIP NNI serves as Registrar. | REGISTER message with a 200 OK response. | *RFC 3261*<br><br>How registration works is dependent on what the particular network-network relationship is. The network serving the SIP end-device may be, for example, a featureless SIP access network and not perform registration itself. |
| 48. | A call between SIP end-devices A and B already exists. A third SIP end-device C, across the VoIP NNI from B, invites itself to join the A-B SIP call at device B, creating a 3-way call.<br><br>Both SIP end-devices B and C must support the SIP Join capability, and additionally the device B must have a 3-way bridging capability. | The SIP INVITE from device C addressed to device B includes a Join header with call ID, to-tag and from-tag information from the device A – device B SIP dialog.<br><br>That SIP INVITE should also include the option tag "join" in a Supported header, and may also include that option tag in a Required header.<br><br>The Contact header in the 200 OK response contains a conference URI corresponding to device B, and an "isfocus" parameter (that identifies which party is controlling the conference) | *RFC 3911*<br><br>How the device A – device B SIP dialog information is provided to device C is not specified here. Presumably the information can be identified at device B and somehow conveyed to and input into device C.<br><br>The dialog information must be as it is known to device B. |
| 49. | SIP end-devices A and B are engaged in a SIP dialog. Another SIP device C, across the VoIP IP NNI from device B, subscribes with device B for the dialog state of the device A – device B SIP dialog.<br><br>After the subscription has begun, device B ends its call with device A.<br><br>Devices B and C support the SIP Subscribe/Notify capability and the 'dialog' event package.<br><br>This scenario assumes that the subscription interval does not expire before the device A – device B dialog is ended. | SIP SUBSCRIBE request from the network serving device C, addressed to device B, with an Event header containing the event package name "dialog" with parameters: to-tag, from-tag, call-ID of the device A – device B dialog, and optionally an include-session-description parameter, and<br>optionally an Accept header indicating what kind of data format is acceptable to be returned in a NOTIFY<br><br>A response of either 200 OK or 202 Accepted is returned<br><br>A first NOTIFY request indicates a dialog state of "confirmed", and also provides the (media) session description information if it was requested<br><br>That first NOTIFY request receives a 200 OK response<br><br>A second NOTIFY request indicates a dialog state of "terminated"<br><br>That second NOTIFY request receives a 200 OK response.<br><br>(That second exchange of NOTIFY and 200 OK will implicitly end the SUBSCRIBE dialog, because the A-B dialog state was "terminated".) | *RFC 3265,*<br>*RFC 4235*<br><br>How the device A – device B SIP dialog information is provided to device C is not specified here. Presumably the information can be identified at device B and somehow conveyed to and input into device C.<br><br>The dialog information must be as it is known to device B.<br><br>Inclusion of the include-session-description parameter means device C wants to know the nature of the media session between A and B.<br><br>The default NOTIFY data format for the dialog event package is "application/dialog-info+xml" |
| 50. | VoIP call between SIP end-devices that support the RTCP Extended Reports (XR) capability | The SDP offer/answer exchange in the INVITE and response messages includes one or more "rtcp-xr" attributes with information on which XR blocks are supported | *RFC 3611* |

It is possible that a reader of this TR who is not intimately familiar with SIP might have expected additional scenarios to be included in the above list to exercise other aspects of SIP, but which are in fact not manifest in SIP. Examples may be priority treatment of 911 calls, passing of the calling party name, or passing information about called party preferences.[1]

Some information that a network needs for recording may be received from across the network-network interface. That set of information should be specified, and verified that it is passed. Note that not all of that information is necessarily used in call processing of a particular call (e.g., calling party number, or OLI digits from a PSTN network earlier in the call path.)

### *7.2 Media - Call Stimulus Scenarios*

This subsection contains a set of call scenarios that could be used as stimuli to test aspects of media support that it would be especially desirable to verify. Analogous to the SIP-related section above, the set below does *not*:

- Exhaustively exercise all possible facets of media use allowed according to the IP NI ASN.
- Indicate other levels of testing that could be performed at the same time, such as verification related to signaling transport or SIP.

Some of the scenarios below could be combined into a single stimulus call. The reason to separate out into different scenarios here is to focus on the different aspects of the protocol to be tested, which are the third column of Table 2.

---

1

♦*SIP indication of priority treatment for a 911 call:* The use of the 911 number itself is covered in the first call stimulus scenario.

♦ *Calling party name on a PSTN-originated call explicitly captured in a SIP header:* The calling party name (whether private or not) on a call that originated in a PSTN/ISUP network is only passed in SIP as part of the encapsulated ISUP IAM. I.e., it is not mapped to SIP header content. See T1.679-2004, Annexes B.24 and B.25.

♦ *Called party preferences in SIP:* While there can be specific "caller preferences" content in SIP as described in RFC 3841, there is no such corresponding content SIP or methods for call*ed* party preferences. Called party preferences can be stored in a SIP Proxy or User Agent and acted upon, but such information is not conveyed in SIP.

**Table 2. Call Stimulus Scenarios for Media**

| # | Scenario Name/Description | Media aspect to be exercised & verified | Comments |
|---|---|---|---|
| 1. | Simple SIP originated VoIP from call CPE that support various coding formats | Various voice coding formats such as G.711, G.729, etc. | *RFC 3264* |
| 2. | PSTN originated call, enter digits from the keypad after call is answered | Passing of DTMF digits using the RTP Payload Format for Named Events | *RFC 2833* |
| 3. | Call between SIP end-devices that starts with one audio coding format (INVITE with, e.g., G.711) and later switches to another audio coding format (a re-INVITE with, e.g., G.726) | RTP packets passed according to the first coding and then the other coding format | *RFC 3264* |
| 4. | Call between IP end-devices performing a fax (facsimile) transmission using the IFP protocol over UDPTL/UDP. | Support for the IFP protocol, and for IFP running over UDPTL/UDP. | *ITU-T T.38*<br><br>In this case IFP is transported using UDP with the UDPTL header. |
| 5. | Call between IP end-devices performing a fax transmission using the IFP protocol over TPKT/TCP | Support for the IFP protocol, and for IFP running over TPKT/TCP. | *ITU-T T.38*<br><br>In this case IFP is transported using TCP with the TPKT header. |
| 6. | Call between IP end-devices performing a fax transmission using the IFP protocol over RTP | Support for the IFP protocol, and for IFP running over RTP. | *ITU-T T.38,*<br>*RFC 4612*<br><br>In this case IFP is transported using RTP (over UDP). |
| 7. | Call between Group 3 fax devices connected to the PSTN at either end, performing a fax transmission.<br><br>Intermediate VoIP networks pass the fax as audio using G.711, and do not convert to IFP.<br><br>The particular image transmission method/rate is not specified as part of this scenario. It will be negotiated by the fax end-devices. | Passing of an inband fax transmission.<br><br>Passing of fax control/communication tone-based information using the RTP Payload Format for Named Events:<br><br>- ANS<br>- CNG<br><br>- V.21 channel 1, "0" bit<br>- V.21 channel 1, "1" bit<br>- V.21 channel 2, "0" bit<br>- V.21 channel 2, "1" bit | *ITU-T T.30,*<br>*RFC 2833*<br><br>Note: In this case, where an audio coding of the fax is used, the distinction between voice and fax in RTP is that conveyance of fax tones will involve 'named events' different from DTMF. |
| 8. | Call from one VoIP device to another using G.711. The calling VoIP device also supports Voice Activity Detection and Comfort Noise Generation.<br><br>The caller does not speak and there is no background noise (i.e., audio input into the VoIP device is silence). | Passing of comfort noise payload in RTP Silence Insertion Descriptor frames | *RFC 3389*<br><br>For this kind of originating device, during a period when the caller isn't speaking the G.711 encoder will not generate RTP audio packets encoding the non-voice. Instead, the device will send RTP comfort noise packets. |

| # | Scenario Name/Description | Media aspect to be exercised & verified | Comments |
|---|---|---|---|
| 9. | Voice call between two endpoints. | Passing of RTCP packets associated with the voice RTP stream<br><br>In this case, compound RTCP packets consisting of Sender Report (SR) and Source Description (SDES) RTCP packets. | *RFC 3550*<br><br>RTCP itself does not pass media, but provides for the exchange of performance and control information related to the RTP media stream. |
| 10. | Call between Super Group 3 fax devices connected to the PTSN at either end.<br><br>Intermediate VoIP networks pass the fax as audio using G.711, and do not convert to IFP. | Same as the Group 3 fax scenario, except that ANSam is seen from the called fax terminal instead of ANS. | *ITU-T V.34,*<br>*ITU-T T.30,*<br>*RFC 2833,* |
| 11. | Calls between fax or modem devices that support V.8bis. The fax or modem devices are connected to the PSTN at either end.<br><br>Intermediate VoIP networks pass the fax or data as audio using G.711. | Passing of tone-based capability or mode information using the RTP Payload Format for Named Events<br>CRdi<br>CRdr<br>CRe<br>ESi<br>ESr<br>MRdi<br>MRdr<br>MRe | *ITU-T V.8bis,*<br>*RFC 2833*<br><br>Note: V.8bis would precede V.8 (ANS, ANSam) in the end-end communication. |
| 12. | 64 kbps clear-channel ISDN-originated and -terminated call; application could be, e.g., low grade video or Group 4 fax | Support for the equivalent of a 64 kbps clear channel connection | *T1.679-2004* |
| 13. | VoIP call between SIP end- devices that support the RTCP Extended Reports (XR) capability | During the call RTCP XR packets are passed | *RFC 3611* |

NOTE - Group 4 fax is not included as a scenario because it does not appear as a separate media type or involve any special control signaling on an IP NNI. [2]

# 8 ENCRYPTION

Testing should employ whatever encryption measures are defined in the SLA. Encryption must be working correctly for other tests to succeed, so there are no recommended tests for it provided here. (If some other test does *not* succeed, trouble-shooting should take into account that faulty/absent encryption on one side could be a cause.)

# 9 SIP MESSAGE BOUNDARY TESTING

SIP-based messages are text-based, can be relatively long, and may contain a multiplicity of fields, tags, etc., in the various headers. Within the SIP syntax, there can also be variations in the way the same

[2] Group 4 fax applies to a network scenario involving PSTN origination or termination, and is invisible to any IP networks other than supporting 64 kbps clear channel. Group 4 fax (ITU-T T.563) is a purely digital form of fax transmission and control. In a circuit switched telephony setting it requires ISDN at either end using a 64 kbps connection. It is otherwise transparent to intermediate networks – the identification of Group 4 fax as the application only shows up in the Q.931 High Layer Compatibility Information Element, which is used by the end-systems and not used by intermediate networks.

information is contained in a message. It would be prudent to demonstrate the ability of each network to robustly and efficiently process long, unusual, and/or complicated -- but legitimate -- SIP messages received from another network, to handle allowed variations in information representation, and to detect the limits (if any) of a network to be able to do so.

The recommended way to exercise this SIP 'message boundary testing' is to have VoIP Test Set equipment connected to both IP networks, where the Test Sets can run test scripts, and where the relevant tests would involve SIP signaling and/or call establishment across the NNI. It should be recognized that there is the possibility that network equipment may normalize/homogenize some of the possible variations in SIP content produced by the Test Set equipment.

One source of examples for such test scripts is the set of so-called SIP "torture tests", described in an IETF information draft[3], and born out of SIPIT[4] (SIP Interoperability Testing) events. Another example of a set of SIP tests is the PROTOS suite[5].

NOTE - Each of those contains examples of messages that are legitimate and others that are not. The latter is out of the scope of this TR.

# 10 NETWORK-NETWORK ADDRESSING AND ROUTING

The use of specific IP Addresses and Port numbers for the various protocols should be verified for SCTP, SIP, RTP, RTCP, etc.

# 11 REGISTRATION

The SIP Register method must be supported across the NNI. See scenario #47 in Section 7.1, "SIP – Call Stimulus Scenarios".

# 12 TESTING ORGANIZATION

This TR does not recommend any particular levels of aggregation or sequencing for conducting tests. That is because the best testing strategy may be different depending on various factors, especially the level of confidence that testing will be successful. For example, that level of confidence may depend on whether the network provider is testing the interface for the first time or the Nth time, or whether the whole interface is being tested or only increments to prior testing.

Furthermore, the degree to which there are different perceived levels of risk/concern may vary by specific area (e.g., a simple voice SIP call versus one involving a SIP REFER interaction, or a voice call versus a fax call, or a fax call using T.30 versus T.38, or the use of UDP versus SCTP for SIP signaling transport, or the workings of RTCP, etc.).

---

[3] See < http://www.ietf.org/rfc/rfc4475.txt >.

[4] See < http://www.sipit.net >.

[5] See < http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/ >.

# 13 SECURITY

The SLA between the network providers should include security services, mechanisms, and practices to protect the interconnected networks and the communications and traffic across the NNI. Refer to ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks* [4] for an overall security framework. The testing of security mechanisms identified in the SLA and that are visible across the NNI must not put the networks at risk.

# 14 REFERENCES

For the specific protocols, extensions, versions, etc., specified as part of the VoIP NNI ANS,[1] the reader is referred to that document.

[1] ATIS-1000009.2006, *IP Network-to-Network Interface (NNI) Standard for VoIP*.[6]

[2] ISO 7498, *Open System Interconnection (OSI) Model: The Basic Model*.[7]

[3] ATIS-1000010.2006, *Support of Emergency Telecommunications Service (ETS) in IP Networks*.[6]

[4] ATIS-1000007.2006, *Generic Signaling and Control Plane Security Requirements for Evolving Networks*.[6]

[5] T1.679-2004, *Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control or ISDN User Part*.[6]

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

[7] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >