IPv6 READY Logo Phase 2

IP Multimedia subsystem

Test item priority
User Equipment

Version 0.4.0

IPv6 Forum *http://www.ipv6forum.org*
Converged Test Specification *http://www.ipv6ready.org*
IPv6 Ready Logo Committee
IPv6 Promotion Council (Japan)

Modification Record

Version 0.4.0	Nov. 26, 2010	Major version up (trial version) - Updated for 3GPP relase8

Acknowledgement

IPv6 Forum would like to acknowledge the efforts of the following organizations and commentators in the development of this test specification.

－ IPv6 Promotion Council
Certification Working Group
SIP IPv6 Sub Working Group
BII Group

- Commentators:

Table of Contents

1 Overview

This document describes the IMS functions and the functional classifications for IMS UE .

Table 1-1 The description of Test item priority Table

Item	Explanation
No	The name of RFC, section number, sequence number in the section.
RFC Section	The number of the section in the RFC where the sentence is described.
RFC Section Title	The title of section where the sentence is described.
Functional Specification	The whole sentence that include a keyword, such as 'MUST', 'SHOULD', 'RECOMMENDED', 'MUST NOT', 'SHOULD NOT', 'NOT RECOMMENDED.'
RFC Status	The keyword that the sentence includes: 'MUST', 'SHOULD', 'RECOMMENDED', 'MUST NOT', 'SHOULD NOT', 'NOT RECOMMENDED.'
Test Priority	The priority based on the importance of interoperability. There are four categories: BASIC, ADVANCED, NOT COVERED, NOT AVAILABLE.
Test Profile	The test profile that is referred to in the test.

2 Test item priority for IMS UE

This section described the Test item priority for IMS UE.

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-7-1	7	SIP Messages	The start-line, each message-header line, and the empty line MUST be terminated by a carriage-return line-feed sequence (CRLF).	MUST	BASIC	generic_sip_message
RFC3261-7-2			Note that the empty line MUST be present even if the message-body is not.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_200-NOTIFY generic_180-INVITE generic_ACK generic_BYE generic_200-BYE generic_CANCEL generic_200-CANCEL generic_3XX-6XX generic_ACK-non2XX generic_OPTIONS
RFC3261-7.1-1	7.1	Requests	The Request-URI MUST NOT contain unescaped spaces or control characters and MUST NOT be enclosed in "<>".	MUST NOT	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-7.1-2				MUST NOT	BASIC	
RFC3261-7.1-3			To be compliant with this specification, applications sending SIP messages MUST include a SIP-Version of "SIP/2.0".	MUST	BASIC	generic_sip_message
RFC3261-7.1-4			The SIP-Version string is case-insensitive, but implementations MUST send upper-case.	MUST	BASIC	generic_sip_message
RFC3261-7.3-1	7.3.1	Header Field Format	However, it is RECOMMENDED that header fields which are needed for proxy processing (Via, Route, Record-Route, Proxy-Require, Max-Forwards, and Proxy-Authorization, for example) appear towards the top of the message to facilitate rapid parsing.	RECOMMENDED	NOT REQUIRED	
RFC3261-7.3-2			It MUST be possible to combine the multiple header field rows into one "field-name: field-value" pair, without changing the semantics of the message, by appending each subsequent field-value to the first, each separated by a comma.	MUST	OUT OF SCOPE	
RFC3261-7.3-3			Multiple header field rows with these names MAY be present in a message, but since their grammar does not follow the general form listed in Section 7.3, they MUST NOT be combined into a single header field row.	MUST NOT	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3261-7.3-4			Implementations MUST be able to process multiple header field rows with the same name in any combination of the single-value-per-line or comma-separated value forms.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-7.3-5			Even though an arbitrary number of parameter pairs may be attached to a header field value, any given parameter-name MUST NOT appear more than once.	MUST NOT	OUT OF SCOPE	
RFC3261-7.3-1	7.3.2	Header Field Classification	If a header field appears in a message not matching its category (such as a request header field in a response), it MUST be ignored.	MUST	NOT REQUIRED	
RFC3261-7.3-2	7.3.3	Compact Form	Implementations MUST accept both the long and short forms of each header name.	MUST	NOT REQUIRED	
RFC3261-7.4-1	7.4.1	Message Body Type	The Internet media type of the message body MUST be given by the Content-Type header field.	MUST	BASIC	generic_INVITE genric_200-INVITE genric_200-OPTIONS
RFC3261-7.4-2			If the body has undergone any encoding such as compression, then this MUST be indicated by the Content- Encoding header field; otherwise, Content-Encoding MUST be omitted.	MUST	NOT REQUIRED	
RFC3261-7.4-3				MUST	BASIC	generic_INVITE genric_200-INVITE genric_200-OPTIONS
RFC3261-7.4-4			Implementations that send requests containing multipart message bodies MUST send a session description as a non-multipart message body if the remote implementation requests this through an Accept header field that does not contain multipart.	MUST	NOT REQUIRED	
RFC3261-7.4-5	7.4.2	Message Body Length	The "chunked" transfer encoding of HTTP/1.1 MUST NOT be used for SIP.	MUST NOT	OUT OF SCOPE	
RFC3261-7.5-1	7.5	Framing SIP Messages	Implementations processing SIP messages over stream-oriented transports MUST ignore any CRLF appearing before the start-line [H4.1].	MUST	NOT REQUIRED	
RFC3261-8.1-1	8.1.1	Generating the Request	A valid SIP request formulated by a UAC MUST, at a minimum, contain the following header fields: To, From, CSeq, Call-ID, Max-Forwards, and Via; all of these header fields are mandatory in all SIP requests.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_CANCEL generic_ACK-non2XX generic_OPTIONS generic_INVITE generic_ACK generic_BYE
RFC3261-8.1-2	8.1.1.1	Request-URI	The initial Request-URI of the message SHOULD be set to the value of the URI in the To field.	SHOULD	BASIC	generic_SUBSCRIBE generic_OPTIONS generic_INVITE

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.1-3			When a provider wishes to configure a UA with an outbound proxy, it is RECOMMENDED that this be done by providing it with a pre-existing route set with a single URI, that of the outbound proxy.	RECOMMENDED	NOT REQUIRED	
RFC3261-8.1-4			When a pre-existing route set is present, the procedures for populating the Request-URI and Route header field detailed in Section 12.2.1.1 MUST be followed (even though there is no dialog), using the desired Request-URI as the remote target URI.	MUST	BASIC	doc_reference
RFC3261-8.1-5	8.1.1.2	To	All SIP implementations MUST support the SIP URI scheme.	MUST	OUT OF SCOPE	
RFC3261-8.1-6			Any implementation that supports TLS MUST support the SIPS URI scheme.	MUST	NOT REQUIRED	
RFC3261-8.1-7			A request outside of a dialog MUST NOT contain a To tag; the tag in the To field of a request identifies the peer of the dialog.	MUST NOT	BASIC	generic_REGISTER generic_SUBSCRIBE generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_INVITE generic_OPTIONS
RFC3261-8.1-8	8.1.1.3	From	A UAC SHOULD use the display name "Anonymous", along with a syntactically correct, but otherwise meaningless URI (like sip:thisis@anonymous.invalid), if the identity of the client is to remain hidden.	SHOULD	ADVANCED	
RFC3261-8.1-9			The From field MUST contain a new "tag" parameter, chosen by the UAC.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_OPTIONS generic_INVITE
RFC3261-8.1-10	8.1.1.4	Call-ID	It MUST be the same for all requests and responses sent by either UA in a dialog.	MUST	BASIC	generic_Re_SUBSCRIBE generic_200-NOTIFY generic_ACK generic_BYE generic_200-INVITE generic_200-BYE
RFC3261-8.1-11			It SHOULD be the same in each registration from a UA.	SHOULD	BASIC	generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3261-8.1-12			In a new request created by a UAC outside of any dialog, the Call-ID header field MUST be selected by the UAC as a globally unique identifier over space and time unless overridden by method-specific behavior.	MUST	OUT OF SCOPE	
RFC3261-8.1-13			Use of cryptographically random identifiers (RFC 1750 [12]) in the generation of Call-IDs is RECOMMENDED.	RECOMMENDED	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.1-14	8.1.1.5	CSeq	The method MUST match that of the request.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-15			The sequence number value MUST be expressible as a 32-bit unsigned integer and MUST be less than 2**31.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-16				MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-17	8.1.1.6	Max-Forwards	A UAC MUST insert a Max-Forwards header field into each request it originates with a value that SHOULD be 70.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_CANCEL generic_ACK-non2XX generic_OPTIONS generic_INVITE generic_ACK generic_BYE
RFC3261-8.1-18				SHOULD	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-19	8.1.1.7	Via	When the UAC creates a request, it MUST insert a Via into that request.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-20			The protocol name and protocol version in the header field MUST be SIP and 2.0, respectively.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-21			The Via header field value MUST contain a branch parameter.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-22			The branch parameter value MUST be unique across space and time for all requests sent by the UA.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.1-23			The branch ID inserted by an element compliant with this specification MUST always begin with the characters "z9hG4bK".	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-8.1-24	8.1.1.8	Contact	The Contact header field MUST be present and contain exactly one SIP or SIPS URI in any request that can result in the establishment of a dialog.	MUST	BASIC	generic_SUBSCRIBE generic_INVITE
RFC3261-8.1-25			That is, the Contact header field value contains the URI at which the UA would like to receive requests, and this URI MUST be valid even if used in subsequent requests outside of any dialogs.	MUST	OUT OF SCOPE	
RFC3261-8.1-26			If the Request-URI or top Route header field value contains a SIPS URI, the Contact header field MUST contain a SIPS URI as well.	MUST	NOT REQUIRED	
RFC3261-8.1-27	8.1.1.9	Supported and Require	If the UAC supports extensions to SIP that can be applied by the server to the response, the UAC SHOULD include a Supported header field in the request listing the option tags (Section 19.2) for those extensions.	SHOULD	OUT OF SCOPE	
RFC3261-8.1-28			The option tags listed MUST only refer to extensions defined in standards-track RFCs.	MUST	OUT OF SCOPE	
RFC3261-8.1-29			If the UAC wishes to insist that a UAS understand an extension that the UAC will apply to the request in order to process the request, it MUST insert a Require header field into the request listing the option tag for that extension.	MUST	ADVANCED	
RFC3261-8.1-30			If the UAC wishes to apply an extension to the request and insist that any proxies that are traversed understand that extension, it MUST insert a Proxy-Require header field into the request listing the option tag for that extension.	MUST	OUT OF SCOPE	
RFC3261-8.1-31			As with the Supported header field, the option tags in the Require and Proxy-Require header fields MUST only refer to extensions defined in standards-track RFCs.	MUST	OUT OF SCOPE	
RFC3261-8.1-32	8.1.2	Sending the Request	Unless there is local policy specifying otherwise, the destination MUST be determined by applying the DNS procedures described in [4] as follows.	MUST	NOT REQUIRED	
RFC3261-8.1-33			If the first element in the route set indicated a strict router (resulting in forming the request as described in Section 12.2.1.1), the procedures MUST be applied to the Request-URI of the request.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.1-34			Independent of which URI is used as input to the procedures of [4], if the Request-URI specifies a SIPS resource, the UAC MUST follow the procedures of [4] as if the input URI were a SIPS URI.	MUST	NOT REQUIRED	
RFC3261-8.1-35			If the Request-URI contains a SIPS URI, any alternate destinations MUST be contacted with TLS.	MUST	NOT REQUIRED	
RFC3261-8.1-36			However, that approach for configuring an outbound proxy is NOT RECOMMENDED; a pre-existing route set with a single URI SHOULD be used instead.	RECOMMENDED	OUT OF SCOPE	
RFC3261-8.1-37				SHOULD	OUT OF SCOPE	
RFC3261-8.1-38			If the request contains a Route header field, the request SHOULD be sent to the locations derived from its topmost value, but MAY be sent to any server that the UA is certain will honor the Route and Request-URI policies specified in this document (as opposed to those in RFC 2543).	SHOULD	BASIC	generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_OPTIONS
RFC3261-8.1-39			In particular, a UAC configured with an outbound proxy SHOULD attempt to send the request to the location indicated in the first Route header field value instead of adopting the policy of sending all messages to the outbound proxy.	SHOULD	NOT REQUIRED	
RFC3261-8.1-40			The UAC SHOULD follow the procedures defined in [4] for stateful elements, trying each address until a server is contacted.	SHOULD	NOT REQUIRED	
RFC3261-8.1-41	8.1.3.1	Transaction Layer Errors	When a timeout error is received from the transaction layer, it MUST be treated as if a 408 (Request Timeout) status code has been received.	MUST	OUT OF SCOPE	
RFC3261-8.1-42			If a fatal transport error is reported by the transport layer (generally, due to fatal ICMP errors in UDP or connection failures in TCP), the condition MUST be treated as a 503 (Service Unavailable) status code.	MUST	NOT REQUIRED	
RFC3261-8.1-43	8.1.3.2	Unrecognized Responses	A UAC MUST treat any final response it does not recognize as being equivalent to the x00 response code of that class, and MUST be able to process the x00 response code for all classes.	MUST	NOT REQUIRED	
RFC3261-8.1-44				MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.1-45			A UAC MUST treat any provisional response different than 100 that it does not recognize as 183 (Session Progress).	MUST	NOT REQUIRED	
RFC3261-8.1-46			A UAC MUST be able to process 100 and 183 responses.	MUST	BASIC	reference （UE-RR-B-1-AKA） (UE-RR-B-4-AKA） （UE-RR-B-1-DIP） (UE-RR-B-4-DIP）
RFC3261-8.1-47	8.1.3.3	Vias	If more than one Via header field value is present in a response, the UAC SHOULD discard the message.	SHOULD	NOT REQUIRED	
RFC3261-8.1-48	8.1.3.4	Processing 3xx Responses	Upon receipt of a redirection response (for example, a 301 response status code), clients SHOULD use the URI(s) in the Contact header field to formulate one or more new requests based on the redirected request.	SHOULD	NOT REQUIRED	
RFC3261-8.1-49			As with proxy recursion, a client processing 3xx class responses MUST NOT add any given URI to the target set more than once.	MUST NOT	NOT REQUIRED	
RFC3261-8.1-50			If the original request had a SIPS URI in the Request- URI, the client MAY choose to recurse to a non-SIPS URI, but SHOULD inform the user of the redirection to an insecure URI.	SHOULD	NOT REQUIRED	
RFC3261-8.1-51			Failures SHOULD be detected through failure response codes (codes greater than 399); for network errors the client transaction will report any transport layer failures to the transaction user.	SHOULD	NOT REQUIRED	
RFC3261-8.1-52			When a failure for a particular contact address is received, the client SHOULD try the next contact address.	SHOULD	NOT REQUIRED	
RFC3261-8.1-53			In order to create a request based on a contact address in a 3xx response, a UAC MUST copy the entire URI from the target set into the Request-URI, except for the "method-param" and "header" URI parameters (see Section 19.1.1 for a definition of these parameters).	MUST	NOT REQUIRED	
RFC3261-8.1-54			It is RECOMMENDED that the UAC reuse the same To, From, and Call-ID used in the original redirected request, but the UAC MAY also choose to update the Call-ID header field value for new requests, for example.	RECOMMENDED	NOT REQUIRED	
RFC3261-8.1-55			Finally, once the new request has been constructed, it is sent using a new client transaction, and therefore MUST have a new branch ID in the top Via field as discussed in Section 8.1.1.7.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.1-56			In all other respects, requests sent upon receipt of a redirect response SHOULD re-use the header fields and bodies of the original request.	SHOULD	NOT REQUIRED	
RFC3261-8.1-57	8.1.3.5	Processing 4xx Responses	If a 401 (Unauthorized) or 407 (Proxy Authentication Required) response is received, the UAC SHOULD follow the authorization procedures of Section 22.2 and Section 22.3 to retry the request with credentials.	SHOULD	BASIC	doc_reference
RFC3261-8.1-58			If possible, the UAC SHOULD retry the request, either omitting the body or using one of a smaller length.	SHOULD	ADVANCED	
RFC3261-8.1-59			The UAC SHOULD retry sending the request, this time only using content with types listed in the Accept header field in the response, with encodings listed in the Accept-Encoding header field in the response, and with languages listed in the Accept-Language in the response.	SHOULD	NOT REQUIRED	
RFC3261-8.1-60			The client SHOULD retry the request, this time, using a SIP URI.	SHOULD	OUT OF SCOPE	
RFC3261-8.1-61			The UAC SHOULD retry the request, this time omitting any extensions listed in the Unsupported header field in the response.	SHOULD	OUT OF SCOPE	
RFC3261-8.1-62			This new request constitutes a new transaction and SHOULD have the same value of the Call-ID, To, and From of the previous request, but the CSeq should contain a new sequence number that is one higher than the previous.	SHOULD	BASIC	generic_Auth_REGISTER UE-RG-B-18-AKA UE-RG-B-19-AKA UE-RG-B-19-DIP
RFC3261-8.2-1	8.2	UAS Behavior	If a request is accepted, all state changes associated with it MUST be performed.	MUST	OUT OF SCOPE	
RFC3261-8.2-2			If it is rejected, all state changes MUST NOT be performed.	MUST NOT	OUT OF SCOPE	
RFC3261-8.2-3			UASs SHOULD process the requests in the order of the steps that follow in this section (that is, starting with authentication, then inspecting the method, the header fields, and so on throughout the remainder of this section).	SHOULD	OUT OF SCOPE	
RFC3261-8.2-4	8.2.1	Method Inspection	Once a request is authenticated (or authentication is skipped), the UAS MUST inspect the method of the request.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.2-5			If the UAS recognizes but does not support the method of a request, it MUST generate a 405 (Method Not Allowed) response.	MUST	BASIC	reference (UE-SR-B-3-AKA) (UE-SR-B-3-DIP)
RFC3261-8.2-6			The UAS MUST also add an Allow header field to the 405 (Method Not Allowed) response.	MUST	BASIC	UE-SR-B-3-AKA UE-SR-B-3-DIP
RFC3261-8.2-7			The Allow header field MUST list the set of methods supported by the UAS generating the message.	MUST	OUT OF SCOPE	
RFC3261-8.2-8	8.2.2	Header Inspection	If a UAS does not understand a header field in a request (that is, the header field is not defined in this specification or in any supported extension), the server MUST ignore that header field and continue processing the message.	MUST	NOT REQUIRED	
RFC3261-8.2-9			A UAS SHOULD ignore any malformed header fields that are not necessary for processing requests.	SHOULD	NOT REQUIRED	
RFC3261-8.2-10	8.2.2.1	To and Request-URI	However, it is RECOMMENDED that a UAS accept requests even if they do not recognize the URI scheme (for example, a tel: URI) in the To header field, or if the To header field does not address a known or current user of this UAS.	RECOMMENDED	NOT REQUIRED	
RFC3261-8.2-11			If, on the other hand, the UAS decides to reject the request, it SHOULD generate a response with a 403 (Forbidden) status code and pass it to the server transaction for transmission.	SHOULD	NOT REQUIRED	
RFC3261-8.2-12			If the Request-URI uses a scheme not supported by the UAS, it SHOULD reject the request with a 416 (Unsupported URI Scheme) response.	SHOULD	OUT OF SCOPE	
RFC3261-8.2-13			If the Request-URI does not identify an address that the UAS is willing to accept requests for, it SHOULD reject the request with a 404 (Not Found) response.	SHOULD	NOT REQUIRED	
RFC3261-8.2-14	8.2.2.2	Merged Requests	If the request has no tag in the To header field, the UAS core MUST check the request against ongoing transactions.	MUST	OUT OF SCOPE	
RFC3261-8.2-15			If the From tag, Call-ID, and CSeq exactly match those associated with an ongoing transaction, but the request does not match that transaction (based on the matching rules in Section 17.2.3), the UAS core SHOULD generate a 482 (Loop Detected) response and pass it to the server transaction.	SHOULD	BASIC	reference (UE-SR-B-10-AKA) (UE-SR-B-10-DIP)

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.2-16	8.2.2.3	Require	If a UAS does not understand an option-tag listed in a Require header field, it MUST respond by generating a response with status code 420 (Bad Extension).	MUST	BASIC	reference (UE-SR-B-8-AKA) (UE-SR-B-8-DIP)
RFC3261-8.2-17			The UAS MUST add an Unsupported header field, and list in it those options it does not understand amongst those in the Require header field of the request.	MUST	BASIC	UE-SR-B-8-AKA UE-SR-B-8-DIP
RFC3261-8.2-18			Note that Require and Proxy-Require MUST NOT be used in a SIP CANCEL request, or in an ACK request sent for a non-2xx response.	MUST NOT	BASIC	generic_CANCEL generic_ACK-non2XX
RFC3261-8.2-19			These header fields MUST be ignored if they are present in these requests.	MUST	NOT REQUIRED	
RFC3261-8.2-20			An ACK request for a 2xx response MUST contain only those Require and Proxy-Require values that were present in the initial request.	MUST	NOT REQUIRED	
RFC3261-8.2-21	8.2.3	Content Processing	If there are any bodies whose type (indicated by the Content-Type), language (indicated by the Content-Language) or encoding (indicated by the Content-Encoding) are not understood, and that body part is not optional (as indicated by the Content- Disposition header field), the UAS MUST reject the request with a 415 (Unsupported Media Type) response.	MUST	BASIC	reference (UE-SR-B-6-AKA) (UE-SR-B-6-DIP)
RFC3261-8.2-22			The response MUST contain an Accept header field listing the types of all bodies it understands, in the event the request contained bodies of types not supported by the UAS.	MUST	BASIC	UE-SR-B-6-AKA UE-SR-B-6-DIP
RFC3261-8.2-23			If the request contained content encodings not understood by the UAS, the response MUST contain an Accept-Encoding header field listing the encodings understood by the UAS.	MUST	BASIC	UE-SR-B-6-AKA UE-SR-B-6-DIP
RFC3261-8.2-24			If the request contained content with languages not understood by the UAS, the response MUST contain an Accept-Language header field indicating the languages understood by the UAS.	MUST	BASIC	UE-SR-B-6-AKA UE-SR-B-6-DIP
RFC3261-8.2-25	8.2.4	Applying Extensions	A UAS that wishes to apply some extension when generating the response MUST NOT do so unless support for that extension is indicated in the Supported header field in the request.	MUST NOT	OUT OF SCOPE	
RFC3261-8.2-26			If the desired extension is not supported, the server SHOULD rely only on baseline SIP and any other extensions supported by the client.	SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.2-27			The needed extension(s) MUST be included in a Require header field in the response.	MUST	NOT REQUIRED	
RFC3261-8.2-28			This behavior is NOT RECOMMENDED, as it will generally break interoperability.	NOT RECOMMENDED	NOT REQUIRED	
RFC3261-8.2-29			Any extensions applied to a non-421 response MUST be listed in a Require header field included in the response.	MUST	NOT REQUIRED	
RFC3261-8.2-30			Of course, the server MUST NOT apply extensions not listed in the Supported header field in the request.	MUST NOT	NOT REQUIRED	
RFC3261-8.2-31	8.2.6.1	Sending a Provisional Response	One largely non-method-specific guideline for the generation of responses is that UASs SHOULD NOT issue a provisional response for a non-INVITE request.	SHOULD NOT	NOT REQUIRED	
RFC3261-8.2-32			Rather, UASs SHOULD generate a final response to a non-INVITE request as soon as possible.	SHOULD	OUT OF SCOPE	
RFC3261-8.2-33			When a 100 (Trying) response is generated, any Timestamp header field present in the request MUST be copied into this 100 (Trying) response.	MUST	NOT REQUIRED	
RFC3261-8.2-34			If there is a delay in generating the response, the UAS SHOULD add a delay value into the Timestamp value in the response.	SHOULD	NOT REQUIRED	
RFC3261-8.2-35			This value MUST contain the difference between the time of sending of the response and receipt of the request, measured in seconds.	MUST	NOT REQUIRED	
RFC3261-8.2-36	8.2.6.2	Headers and Tags	The From field of the response MUST equal the From header field of the request.	MUST	BASIC	generic_200-NOTIFY generic_180-INVITE generic_200-INVITE generic_200-BYE generic_3XX-6XX generic_200-CANCEL generic_200-OPTIONS
RFC3261-8.2-37			The Call-ID header field of the response MUST equal the Call-ID header field of the request.	MUST	BASIC	generic_200-NOTIFY generic_180-INVITE generic_200-INVITE generic_200-BYE generic_3XX-6XX generic_200-CANCEL generic_200-OPTIONS

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.2-38			The CSeq header field of the response MUST equal the CSeq field of the request.	MUST	BASIC	generic_200-NOTIFY generic_180-INVITE generic_200-INVITE generic_200-BYE generic_3XX-6XX generic_200-CANCEL generic_200-OPTIONS
RFC3261-8.2-39			The Via header field values in the response MUST equal the Via header field values in the request and MUST maintain the same ordering.	MUST	BASIC	generic_200-NOTIFY generic_180-INVITE generic_200-INVITE generic_200-BYE generic_3XX-6XX generic_200-CANCEL generic_200-OPTIONS
RFC3261-8.2-40				MUST	BASIC	generic_200-NOTIFY generic_180-INVITE generic_200-INVITE generic_200-BYE generic_3XX-6XX generic_200-CANCEL generic_200-OPTIONS
RFC3261-8.2-41			If a request contained a To tag in the request, the To header field in the response MUST equal that of the request.	MUST	BASIC	generic_200-NOTIFY generic_200-BYE generic_3XX-6XX
RFC3261-8.2-42			However, if the To header field in the request did not contain a tag, the URI in the To header field in the response MUST equal the URI in the To header field; additionally, the UAS MUST add a tag to the To header field in the response (with the exception of the 100 (Trying) response, in which a tag MAY be present).	MUST	BASIC	generic_180-INVITE generic_200-INVITE generic_200-CANCEL generic_3XX-6XX generic_200-OPTIONS
RFC3261-8.2-43				MUST	BASIC	generic_180-INVITE generic_200-INVITE generic_200-CANCEL generic_3XX-6XX generic_200-OPTIONS
RFC3261-8.2-44			The same tag MUST be used for all responses to that request, both final and provisional (again excepting the 100 (Trying)).	MUST	BASIC	generic_200-BYE generic_3XX-6XX generic_200-INVITE
RFC3261-8.2-45	8.2.7	Stateless UAS Behavior	A stateless UAS MUST NOT send provisional (1xx) responses.	MUST NOT	NOT REQUIRED	
RFC3261-8.2-46			A stateless UAS MUST NOT retransmit responses.	MUST NOT	NOT REQUIRED	
RFC3261-8.2-47			A stateless UAS MUST ignore ACK requests.	MUST	NOT REQUIRED	
RFC3261-8.2-48			A stateless UAS MUST ignore CANCEL requests.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-8.2-49			To header tags MUST be generated for responses in a stateless manner - in a manner that will generate the same tag for the same request consistently.	MUST	NOT REQUIRED	
RFC3261-8.3-1	8.3	Redirect Servers	For well-formed CANCEL requests, it SHOULD return a 2xx response.	SHOULD	NOT REQUIRED	
RFC3261-8.3-2			However, redirect servers MUST NOT redirect a request to a URI equal to the one in the Request-URI; instead, provided that the URI does not point to itself, the server MAY proxy the request to the destination URI, or MAY reject it with a 404.	MUST NOT	NOT REQUIRED	
RFC3261-8.3-3			Malformed values SHOULD be treated as equivalent to 3600.	SHOULD	NOT REQUIRED	
RFC3261-8.3-4			Redirect servers MUST ignore features that are not understood (including unrecognized header fields, any unknown option tags in Require, or even method names) and proceed with the redirection of the request in question.	MUST	NOT REQUIRED	
RFC3261-9.1-1	9.1	Client Behavior	A CANCEL request SHOULD NOT be sent to cancel a request other than INVITE.	SHOULD NOT	OUT OF SCOPE	
RFC3261-9.1-2			The Request-URI, Call-ID, To, the numeric part of CSeq, and From header fields in the CANCEL request MUST be identical to those in the request being cancelled, including tags.	MUST	BASIC	generic_CANCEL
RFC3261-9.1-3			A CANCEL constructed by a client MUST have only a single Via header field value matching the top Via value in the request being cancelled.	MUST	BASIC	generic_CANCEL
RFC3261-9.1-4			However, the method part of the CSeq header field MUST have a value of CANCEL.	MUST	BASIC	generic_CANCEL
RFC3261-9.1-5			If the request being cancelled contains a Route header field, the CANCEL request MUST include that Route header field's values.	MUST	BASIC	generic_CANCEL
RFC3261-9.1-6			The CANCEL request MUST NOT contain any Require or Proxy-Require header fields.	MUST NOT	BASIC	generic_CANCEL

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−9.1−7			Once the CANCEL is constructed, the client SHOULD check whether it has received any response (provisional or final) for the request being cancelled (herein referred to as the "original request").	SHOULD	OUT OF SCOPE	
RFC3261−9.1−8			If no provisional response has been received, the CANCEL request MUST NOT be sent; rather, the client MUST wait for the arrival of a provisional response before sending the request.	MUST NOT	NOT REQUIRED	
RFC3261−9.1−9				MUST	OUT OF SCOPE	
RFC3261−9.1−10			If the original request has generated a final response, the CANCEL SHOULD NOT be sent, as it is an effective no-op, since CANCEL has no effect on requests that have already generated a final response.	SHOULD NOT	OUT OF SCOPE	
RFC3261−9.1−11			The destination address, port, and transport for the CANCEL MUST be identical to those used to send the original request.	MUST	BASIC	generic_CANCEL
RFC3261−9.1−12			If there is no final response for the original request in 64*T1 seconds (T1 is defined in Section 17.1.1.1), the client SHOULD then consider the original transaction cancelled and SHOULD destroy the client transaction handling the original request.	SHOULD	NOT REQUIRED	
RFC3261−9.1−13				SHOULD	NOT REQUIRED	
RFC3261−9.2−1	9.2	Server Behavior	If the UAS did not find a matching transaction for the CANCEL according to the procedure above, it SHOULD respond to the CANCEL with a 481 (Call Leg/Transaction Does Not Exist).	SHOULD	BASIC	UE−TM−B−4−AKA UE−TM−B−4−DIP
RFC3261−9.2−2			If the original request was an INVITE, the UAS SHOULD immediately respond to the INVITE with a 487 (Request Terminated).	SHOULD	BASIC	UE−SE−B−6−AKA UE−SE−B−6−DIP
RFC3261−9.2−3			This response is constructed following the procedures described in Section 8.2.6 noting that the To tag of the response to the CANCEL and the To tag in the response to the original request SHOULD be the same.	SHOULD	BASIC	doc_reference
RFC3261−10.1−1	10.1	Overview	The only requirement is that a registrar for some domain MUST be able to read and write data to the location service, and a proxy or a redirect server for that domain MUST be capable of reading that same data.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-10.1-2				MUST	OUT OF SCOPE	
RFC3261-10.2-1	10.2	Constructing the REGISTER Request	The Record-Route header field has no meaning in REGISTER requests or responses, and MUST be ignored if present.	MUST	NOT REQUIRED	
RFC3261-10.2-2			In particular, the UAC MUST NOT create a new route set based on the presence or absence of a Record-Route header field in any response to a REGISTER request.	MUST NOT	NOT REQUIRED	
RFC3261-10.2-3			The following header fields, except Contact, MUST be included in a REGISTER request.	MUST	BASIC	doc_reference
RFC3261-10.2-4			The "userinfo" and "@" components of the SIP URI MUST NOT be present.	MUST NOT	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3261-10.2-5			This address-of-record MUST be a SIP URI or SIPS URI.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3261-10.2-6			Call-ID: All registrations from a UAC SHOULD use the same Call-ID header field value for registrations sent to a particular registrar.	SHOULD	BASIC	generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3261-10.2-7			A UA MUST increment the CSeq value by one for each REGISTER request with the same Call-ID.	MUST	BASIC	generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3261-10.2-8			UAs MUST NOT send a new registration (that is, containing new Contact header field values, as opposed to a retransmission) until they have received a final response from the registrar for the previous one or the previous REGISTER request has timed out.	MUST NOT	OUT OF SCOPE	
RFC3261-10.2-9			UACs SHOULD NOT use the "action" parameter.	SHOULD NOT	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3261-10.2-10			Malformed values SHOULD be treated as equivalent to 3600.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-10.2-11	10.2.1	Adding Bindings	If the address-of-record in the To header field of a REGISTER request is a SIPS URI, then any Contact header field values in the request SHOULD also be SIPS URIs.	SHOULD	NOT REQUIRED	
RFC3261-10.2-12	10.2.2	Removing Bindings	UAs SHOULD support this mechanism so that bindings can be removed before their expiration interval has passed.	SHOULD	OUT OF SCOPE	
RFC3261-10.2-13			The REGISTER-specific Contact header field value of "*" applies to all registrations, but it MUST NOT be used unless the Expires header field is present with a value of "0".	MUST NOT	BASIC	generic_de_REGISTER
RFC3261-10.2-14	10.2.4	Refreshing Bindings	A UA SHOULD NOT refresh bindings set up by other UAs.	SHOULD NOT	OUT OF SCOPE	
RFC3261-10.2-15			A UA SHOULD use the same Call-ID for all registrations during a single boot cycle.	SHOULD	BASIC	generic_re_REGISTER
RFC3261-10.2-16			Registration refreshes SHOULD be sent to the same network address as the original registration, unless redirected.	SHOULD	BASIC	generic_re_REGISTER
RFC3261-10.2-17	10.2.6	Discovering a Registrar	If there is no configured registrar address, the UA SHOULD use the host part of the address- of-record as the Request-URI and address the request there, using the normal SIP server location mechanisms [4].	SHOULD	NOT REQUIRED	
RFC3261-10.2-18	10.2.7	Transmitting a Request	If the transaction layer returns a timeout error because the REGISTER yielded no response, the UAC SHOULD NOT immediately re-attempt a registration to the same registrar.	SHOULD NOT	BASIC	UE-RG-B-15-AKA UE-RG-B-15-DIP
RFC3261-10.3-1	10.3	Processing REGISTER Requests	A registrar MUST not generate 6xx responses.	MUST NOT	OUT OF SCOPE	
RFC3261-10.3-2			Registrars MUST ignore the Record-Route header field if it is included in a REGISTER request.	MUST	NOT REQUIRED	
RFC3261-10.3-3			Registrars MUST NOT include a Record-Route header field in any response to a REGISTER request.	MUST NOT	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-10.3-4			REGISTER requests MUST be processed by a registrar in the order that they are received.	MUST	NOT REQUIRED	
RFC3261-10.3-5			REGISTER requests MUST also be processed atomically, meaning that a particular REGISTER request is either processed completely or not at all.	MUST	NOT REQUIRED	
RFC3261-10.3-6			Each REGISTER message MUST be processed independently of any other registration or binding changes.	MUST	NOT REQUIRED	
RFC3261-10.3-7			If not, and if the server also acts as a proxy server, the server SHOULD forward the request to the addressed domain, following the general behavior for proxying messages described in Section 16.	SHOULD	NOT REQUIRED	
RFC3261-10.3-8			2. To guarantee that the registrar supports any necessary extensions, the registrar MUST process the Require header field values as described for UASs in Section 8.2.2.	MUST	NOT REQUIRED	
RFC3261-10.3-9			3. A registrar SHOULD authenticate the UAC.	SHOULD	NOT REQUIRED	
RFC3261-10.3-10			4. The registrar SHOULD determine if the authenticated user is authorized to modify registrations for this address-of-record.	SHOULD	OUT OF SCOPE	
RFC3261-10.3-11			If the authenticated user is not authorized to modify bindings, the registrar MUST return a 403 (Forbidden) and skip the remaining steps.	MUST	OUT OF SCOPE	
RFC3261-10.3-12			If the address-of-record is not valid for the domain in the Request-URI, the registrar MUST send a 404 (Not Found) response and skip the remaining steps.	MUST	NOT REQUIRED	
RFC3261-10.3-13			The URI MUST then be converted to a canonical form.	MUST	NOT REQUIRED	
RFC3261-10.3-14			To do that, all URI parameters MUST be removed (including the user-param), and any escaped characters MUST be converted to their unescaped form.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-10.3-15				MUST	NOT REQUIRED	
RFC3261-10.3-16			If the request has additional Contact fields or an expiration time other than zero, the request is invalid, and the server MUST return a 400 (Invalid Request) and skip the remaining steps.	MUST	NOT REQUIRED	
RFC3261-10.3-17			If not, it MUST remove the binding.	MUST	NOT REQUIRED	
RFC3261-10.3-18			If it does agree, it MUST remove the binding only if the CSeq in the request is higher than the value stored for that binding.	MUST	NOT REQUIRED	
RFC3261-10.3-19			Otherwise, the update MUST be aborted and the request fails.	MUST	NOT REQUIRED	
RFC3261-10.3-20			If the field value has an "expires" parameter, that value MUST be taken as the requested expiration.	MUST	NOT REQUIRED	
RFC3261-10.3-21			If there is no such parameter, but the request has an Expires header field, that value MUST be taken as the requested expiration.	MUST	NOT REQUIRED	
RFC3261-10.3-22			If there is neither, a locally-configured default value MUST be taken as the requested expiration.	MUST	NOT REQUIRED	
RFC3261-10.3-23			This response MUST contain a Min-Expires header field that states the minimum expiration interval the registrar is willing to honor.	MUST	NOT REQUIRED	
RFC3261-10.3-24			If the Call-ID value in the existing binding differs from the Call-ID value in the request, the binding MUST be removed if the expiration time is zero and updated otherwise.	MUST	NOT REQUIRED	
RFC3261-10.3-25			If the value is higher than that of the existing binding, it MUST update or remove the binding as above.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-10.3-26			If not, the update MUST be aborted and the request fails.	MUST	NOT REQUIRED	
RFC3261-10.3-27			The binding updates MUST be committed (that is, made visible to the proxy or redirect server) if and only if all binding updates and additions succeed.	MUST	NOT REQUIRED	
RFC3261-10.3-28			If any one of them fails (for example, because the back-end database commit failed), the request MUST fail with a 500 (Server Error) response and all tentative binding updates MUST be removed.	MUST	NOT REQUIRED	
RFC3261-10.3-29				MUST	NOT REQUIRED	
RFC3261-10.3-30			The response MUST contain Contact header field values enumerating all current bindings.	MUST	NOT REQUIRED	
RFC3261-10.3-31			Each Contact value MUST feature an "expires" parameter indicating its expiration interval chosen by the registrar.	MUST	NOT REQUIRED	
RFC3261-10.3-32			The response SHOULD include a Date header field.	SHOULD	NOT REQUIRED	
RFC3261-11-1	11	Querying for Capabilities	All UAs MUST support the OPTIONS method.	MUST	BASIC	reference (UE-OP-B-1-AKA) (UE-OP-B-2-AKA) (UE-OP-B-1-DIP) (UE-OP-B-2-DIP) generic_200-OPTIONS
RFC3261-11.1-1	11.1	Construction of OPTIONS Request	An Accept header field SHOULD be included to indicate the type of message body the UAC wishes to receive in the response.	SHOULD	BASIC	reference (UE-OP-B-1-AKA) (UE-OP-B-2-AKA) (UE-OP-B-1-DIP) (UE-OP-B-2-DIP) generic_OPTIONS
RFC3261-11.2-1	11.2	Processing of OPTIONS Request	The response code chosen MUST be the same that would have been chosen had the request been an INVITE.	MUST	OUT OF SCOPE	
RFC3261-11.2-2			Allow, Accept, Accept-Encoding, Accept-Language, and Supported header fields SHOULD be present in a 200 (OK) response to an OPTIONS request.	SHOULD	BASIC	reference (UE-OP-B-2-AKA) (UE-OP-B-2-DIP) generic_200-OPTIONS

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-11.2-3			If the response is generated by a proxy, the Allow header field SHOULD be omitted as it is ambiguous since a proxy is method agnostic.	SHOULD	NOT REQUIRED	
RFC3261-11.2-4			If the types include one that can describe media capabilities, the UAS SHOULD include a body in the response for that purpose.	SHOULD	BASIC	reference (UE-OP-B-2-AKA) (UE-OP-B-2-DIP) generic_200-OPTIONS
RFC3261-12.1-1	12.1	Creation of a Dialog	UAs MUST assign values to the dialog ID components as described below.	MUST	BASIC	doc_reference
RFC3261-12.1-2	12.1.1	UAS behavior	When a UAS responds to a request with a response that establishes a dialog (such as a 2xx to INVITE), the UAS MUST copy all Record-Route header field values from the request into the response (including the URIs, URI parameters, and any Record-Route header field parameters, whether they are known or unknown to the UAS) and MUST maintain the order of those values.	MUST	BASIC	generic_200-INVITE
RFC3261-12.1-3				MUST	BASIC	generic_200-INVITE
RFC3261-12.1-4			The UAS MUST add a Contact header field to the response.	MUST	BASIC	generic_200-INVITE
RFC3261-12.1-5			The URI provided in the Contact header field MUST be a SIP or SIPS URI.	MUST	BASIC	generic_200-INVITE
RFC3261-12.1-6			If the request that initiated the dialog contained a SIPS URI in the Request-URI or in the top Record-Route header field value, if there was any, or the Contact header field if there was no Record-Route header field, the Contact header field in the response MUST be a SIPS URI.	MUST	NOT REQUIRED	
RFC3261-12.1-7			The URI SHOULD have global scope (that is, the same URI can be used in messages outside this dialog).	SHOULD	NOT REQUIRED	
RFC3261-12.1-8			This state MUST be maintained for the duration of the dialog.	MUST	OUT OF SCOPE	
RFC3261-12.1-9			The route set MUST be set to the list of URIs in the Record-Route header field from the request, taken in order and preserving all URI parameters.	MUST	BASIC	generic_200-INVITE

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-12.1-10			If no Record-Route header field is present in the request, the route set MUST be set to the empty set.	MUST	NOT REQUIRED	
RFC3261-12.1-11			The remote target MUST be set to the URI from the Contact header field of the request.	MUST	OUT OF SCOPE	
RFC3261-12.1-12			The remote sequence number MUST be set to the value of the sequence number in the CSeq header field of the request.	MUST	OUT OF SCOPE	
RFC3261-12.1-13			The local sequence number MUST be empty.	MUST	OUT OF SCOPE	
RFC3261-12.1-14			The call identifier component of the dialog ID MUST be set to the value of the Call-ID in the request.	MUST	OUT OF SCOPE	
RFC3261-12.1-15			The local tag component of the dialog ID MUST be set to the tag in the To field in the response to the request (which always includes a tag), and the remote tag component of the dialog ID MUST be set to the tag from the From field in the request.	MUST	OUT OF SCOPE	
RFC3261-12.1-16				MUST	OUT OF SCOPE	
RFC3261-12.1-17			A UAS MUST be prepared to receive a request without a tag in the From field, in which case the tag is considered to have a value of null.	MUST	OUT OF SCOPE	
RFC3261-12.1-18			The remote URI MUST be set to the URI in the From field, and the local URI MUST be set to the URI in the To field.	MUST	OUT OF SCOPE	
RFC3261-12.1-19				MUST	OUT OF SCOPE	
RFC3261-12.1-20	12.1.2	UAC Behavior	When a UAC sends a request that can establish a dialog (such as an INVITE) it MUST provide a SIP or SIPS URI with global scope (i.e., the same SIP URI can be used in messages outside this dialog) in the Contact header field of the request.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-12.1-21			If the request has a Request- URI or a topmost Route header field value with a SIPS URI, the Contact header field MUST contain a SIPS URI.	MUST	NOT REQUIRED	
RFC3261-12.1-22			This state MUST be maintained for the duration of the dialog.	MUST	OUT OF SCOPE	
RFC3261-12.1-23			The route set MUST be set to the list of URIs in the Record-Route header field from the response, taken in reverse order and preserving all URI parameters.	MUST	OUT OF SCOPE	
RFC3261-12.1-24			If no Record-Route header field is present in the response, the route set MUST be set to the empty set.	MUST	OUT OF SCOPE	
RFC3261-12.1-25			The remote target MUST be set to the URI from the Contact header field of the response.	MUST	OUT OF SCOPE	
RFC3261-12.1-26			The local sequence number MUST be set to the value of the sequence number in the CSeq header field of the request.	MUST	OUT OF SCOPE	
RFC3261-12.1-27			The remote sequence number MUST be empty (it is established when the remote UA sends a request within the dialog).	MUST	OUT OF SCOPE	
RFC3261-12.1-28			The call identifier component of the dialog ID MUST be set to the value of the Call-ID in the request.	MUST	OUT OF SCOPE	
RFC3261-12.1-29			The local tag component of the dialog ID MUST be set to the tag in the From field in the request, and the remote tag component of the dialog ID MUST be set to the tag in the To field of the response.	MUST	OUT OF SCOPE	
RFC3261-12.1-30				MUST	OUT OF SCOPE	
RFC3261-12.1-31			A UAC MUST be prepared to receive a response without a tag in the To field, in which case the tag is considered to have a value of null.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-12.1-32			The remote URI MUST be set to the URI in the To field, and the local URI MUST be set to the URI in the From field.	MUST	OUT OF SCOPE	
RFC3261-12.1-33				MUST	OUT OF SCOPE	
RFC3261-12.2-1	12.2.1.1	Generating the Request	The URI in the To field of the request MUST be set to the remote URI from the dialog state.	MUST	BASIC	generic_Re_SUBSCRIBE generic_ACK generic_BYE
RFC3261-12.2-2			The tag in the To header field of the request MUST be set to the remote tag of the dialog ID.	MUST	BASIC	generic_Re_SUBSCRIBE generic_ACK generic_BYE
RFC3261-12.2-3			The From URI of the request MUST be set to the local URI from the dialog state.	MUST	BASIC	generic_Re_SUBSCRIBE generic_ACK generic_BYE
RFC3261-12.2-4			The tag in the From header field of the request MUST be set to the local tag of the dialog ID.	MUST	BASIC	generic_Re_SUBSCRIBE generic_ACK generic_BYE
RFC3261-12.2-5			If the value of the remote or local tags is null, the tag parameter MUST be omitted from the To or From header fields, respectively.	MUST	NOT REQUIRED	
RFC3261-12.2-6			The Call-ID of the request MUST be set to the Call-ID of the dialog.	MUST	BASIC	generic_Re_SUBSCRIBE generic_ACK generic_BYE
RFC3261-12.2-7			Requests within a dialog MUST contain strictly monotonically increasing and contiguous CSeq sequence numbers (increasing-by-one) in each direction (excepting ACK and CANCEL of course, whose numbers equal the requests being acknowledged or cancelled).	MUST	BASIC	generic_Re_SUBSCRIBE generic_BYE
RFC3261-12.2-8			Therefore, if the local sequence number is not empty, the value of the local sequence number MUST be incremented by one, and this value MUST be placed into the CSeq header field.	MUST	BASIC	generic_Re_SUBSCRIBE generic_BYE
RFC3261-12.2-9				MUST	BASIC	generic_Re_SUBSCRIBE generic_BYE

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-12.2-10			If the local sequence number is empty, an initial value MUST be chosen using the guidelines of Section 8.1.1.5.	MUST	BASIC	doc_reference
RFC3261-12.2-11			The method field in the CSeq header field value MUST match the method of the request.	MUST	BASIC	generic_Re_SUBSCRIBE generic_BYE
RFC3261-12.2-12			If the route set is empty, the UAC MUST place the remote target URI into the Request-URI.	MUST	NOT REQUIRED	
RFC3261-12.2-13			The UAC MUST NOT add a Route header field to the request.	MUST NOT	NOT REQUIRED	
RFC3261-12.2-14			If the route set is not empty, and the first URI in the route set contains the lr parameter (see Section 19.1.1), the UAC MUST place the remote target URI into the Request-URI and MUST include a Route header field containing the route set values in order, including all parameters.	MUST	BASIC	generic_Re_SUBSCRIBE generic_ACK generic_BYE
RFC3261-12.2-15				MUST	BASIC	generic_Re_SUBSCRIBE generic_ACK generic_BYE
RFC3261-12.2-16			If the route set is not empty, and its first URI does not contain the lr parameter, the UAC MUST place the first URI from the route set into the Request-URI, stripping any parameters that are not allowed in a Request-URI.	MUST	NOT REQUIRED	
RFC3261-12.2-17			The UAC MUST add a Route header field containing the remainder of the route set values in order, including all parameters.	MUST	NOT REQUIRED	
RFC3261-12.2-18			The UAC MUST then place the remote target URI into the Route header field as the last value.	MUST	NOT REQUIRED	
RFC3261-12.2-19			A UAC SHOULD include a Contact header field in any target refresh requests within a dialog, and unless there is a need to change it, the URI SHOULD be the same as used in previous requests within the dialog.	SHOULD	NOT REQUIRED	
RFC3261-12.2-20				SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−12.2−21			If the ″secure″ flag is true, that URI MUST be a SIPS URI.	MUST	ADVANCED	
RFC3261−12.2−22	12.2.1.2	Processing the Responses	When a UAC receives a 2xx response to a target refresh request, it MUST replace the dialog's remote target URI with the URI from the Contact header field in that response, if present.	MUST	NOT REQUIRED	
RFC3261−12.2−23			If the response for a request within a dialog is a 481 (Call/Transaction Does Not Exist) or a 408 (Request Timeout), the UAC SHOULD terminate the dialog.	SHOULD	BASIC	UE−RG−B−9−AKA UE−RG−B−9−DIP
RFC3261−12.2−24			A UAC SHOULD also terminate a dialog if no response at all is received for the request (the client transaction would inform the TU about the timeout.)	SHOULD	NOT REQUIRED	
RFC3261−12.2−25	12.2.2	UAS Behavior	If the UAS wishes to reject the request because it does not wish to recreate the dialog, it MUST respond to the request with a 481 (Call/Transaction Does Not Exist) status code and pass that to the server transaction.	MUST	NOT REQUIRED	
RFC3261−12.2−26			If the remote sequence number is empty, it MUST be set to the value of the sequence number in the CSeq header field value in the request.	MUST	NOT REQUIRED	
RFC3261−12.2−27			If the remote sequence number was not empty, but the sequence number of the request is lower than the remote sequence number, the request is out of order and MUST be rejected with a 500 (Server Internal Error) response.	MUST	BASIC	reference （UE−SR−B−12−AKA） （UE−SR−B−12−DIP）
RFC3261−12.2−28			This is not an error condition, and a UAS SHOULD be prepared to receive and process requests with CSeq values more than one higher than the previous received request.	SHOULD	NOT REQUIRED	
RFC3261−12.2−29			The UAS MUST then set the remote sequence number to the value of the sequence number in the CSeq header field value in the request.	MUST	NOT REQUIRED	
RFC3261−12.2−30			When a UAS receives a target refresh request, it MUST replace the dialog's remote target URI with the URI from the Contact header field in that request, if present.	MUST	OUT OF SCOPE	
RFC3261−13.1−1	13.1	Overview	A UA that supports INVITE MUST also support ACK, CANCEL and BYE.	MUST	BASIC	generic_200−OPTIONS generic_INVITE generic_200−INVITE

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-13.2-1	13.2.1	Creating the Initial INVITE	An Allow header field (Section 20.5) SHOULD be present in the INVITE.	SHOULD	BASIC	generic_INVITE
RFC3261-13.2-2			For example, a UA capable of receiving INFO requests within a dialog [34] SHOULD include an Allow header field listing the INFO method.	SHOULD	NOT REQUIRED	
RFC3261-13.2-3			A Supported header field (Section 20.37) SHOULD be present in the INVITE.	SHOULD	BASIC	generic_INVITE
RFC3261-13.2-4			If the time indicated in the Expires header field is reached and no final answer for the INVITE has been received, the UAC core SHOULD generate a CANCEL request for the INVITE, as per Section 9.	SHOULD	ADVANCED	
RFC3261-13.2-5			The initial offer MUST be in either an INVITE or, if not there, in the first reliable non-failure message from the UAS back to the UAC.	MUST	NOT REQUIRED	
RFC3261-13.2-6			If the initial offer is in an INVITE, the answer MUST be in a reliable non-failure message from UAS back to UAC which is correlated to that INVITE.	MUST	BASIC	generic_200-INVITE
RFC3261-13.2-7			The UAC MUST treat the first session description it receives as the answer, and MUST ignore any session descriptions in subsequent responses to the initial INVITE.	MUST	NOT REQUIRED	
RFC3261-13.2-8				MUST	NOT REQUIRED	
RFC3261-13.2-9			If the initial offer is in the first reliable non-failure message from the UAS back to UAC, the answer MUST be in the acknowledgement for that message (in this specification, ACK for a 2xx response).	MUST	NOT REQUIRED	
RFC3261-13.2-10			Once the UAS has sent or received an answer to the initial offer, it MUST NOT generate subsequent offers in any responses to the initial INVITE.	MUST NOT	NOT REQUIRED	
RFC3261-13.2-11			All user agents that support INVITE MUST support these two exchanges.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-13.2-12			The Session Description Protocol (SDP) (RFC 2327 [1]) MUST be supported by all user agents as a means to describe sessions, and its usage for constructing offers and answers MUST follow the procedures defined in [13].	MUST	BASIC	generic_200-OPTIONS generic_INVITE generic-200-INVITE
RFC3261-13.2-13				MUST	NOT REQUIRED	
RFC3261-13.2-14	13.2.2.3	4xx, 5xx and 6xx Responses	Subsequent final responses (which would only arrive under error conditions) MUST be ignored.	MUST	NOT REQUIRED	
RFC3261-13.2-15	13.2.2.4	2xx Responses	If the dialog identifier in the 2xx response matches the dialog identifier of an existing dialog, the dialog MUST be transitioned to the "confirmed" state, and the route set for the dialog MUST be recomputed based on the 2xx response using the procedures of Section 12.2.1.2.	MUST	NOT REQUIRED	
RFC3261-13.2-16				MUST	NOT REQUIRED	
RFC3261-13.2-17			Otherwise, a new dialog in the "confirmed" state MUST be constructed using the procedures of Section 12.1.2.	MUST	OUT OF SCOPE	
RFC3261-13.2-18			The UAC core MUST generate an ACK request for each 2xx received from the transaction layer.	MUST	BASIC	UE-SE-B-10-AKA UE-SE-B-10-DIP
RFC3261-13.2-19			The sequence number of the CSeq header field MUST be the same as the INVITE being acknowledged, but the CSeq method MUST be ACK.	MUST	BASIC	generic_ACK
RFC3261-13.2-20				MUST	BASIC	generic_ACK
RFC3261-13.2-21			The ACK MUST contain the same credentials as the INVITE.	MUST	NOT REQUIRED	
RFC3261-13.2-22			If the 2xx contains an offer (based on the rules above), the ACK MUST carry an answer in its body.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-13.2-23			If the offer in the 2xx response is not acceptable, the UAC core MUST generate a valid answer in the ACK and then send a BYE immediately.	MUST	NOT REQUIRED	
RFC3261-13.2-24			The ACK MUST be passed to the client transport every time a retransmission of the 2xx final response that triggered the ACK arrives.	MUST	OUT OF SCOPE	
RFC3261-13.2-25			If, after acknowledging any 2xx response to an INVITE, the UAC does not want to continue with that dialog, then the UAC MUST terminate the dialog by sending a BYE request as described in Section 15.	MUST	OUT OF SCOPE	
RFC3261-13.3-1	13.3.1	Processing of the INVITE	If the invitation expires before the UAS has generated a final response, a 487 (Request Terminated) response SHOULD be generated.	SHOULD	ADVANCED	
RFC3261-13.3-2			It MUST provide the offer in its first non-failure reliable message back to the UAC.	MUST	NOT REQUIRED	
RFC3261-13.3-3	13.3.1.1	Progress	Each of these MUST indicate the same dialog ID.	MUST	ADVANCED	
RFC3261-13.3-4			To prevent cancellation, the UAS MUST send a non-100 provisional response at every minute, to handle the possibility of lost provisional responses.	MUST	NOT REQUIRED	
RFC3261-13.3-5	13.3.1.2	The INVITE is Redirected	A 300 (Multiple Choices), 301 (Moved Permanently) or 302 (Moved Temporarily) response SHOULD contain a Contact header field containing one or more URIs of new addresses to be tried.	SHOULD	NOT REQUIRED	
RFC3261-13.3-6	13.3.1.3	The INVITE is Rejected	A 486 (Busy Here) SHOULD be returned in such a scenario.	SHOULD	BASIC	reference (UE-SR-B-9-AKA) (UE-SR-B-9-DIP)
RFC3261-13.3-7			If the UAS knows that no other end system will be able to accept this call, a 600 (Busy Everywhere) response SHOULD be sent instead.	SHOULD	NOT REQUIRED	
RFC3261-13.3-8			A UAS rejecting an offer contained in an INVITE SHOULD return a 488 (Not Acceptable Here) response.	SHOULD	BASIC	reference (UE-SD-B-2-AKA) (UE-SD-B-2-DIP)

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-13.3-9			Such a response SHOULD include a Warning header field value explaining why the offer was rejected.	SHOULD	BASIC	UE-SD-B-2-AKA UE-SD-B-2-DIP
RFC3261-13.3-10	13.3.1.4	The INVITE is Accepted	A 2xx response to an INVITE SHOULD contain the Allow header field and the Supported header field, and MAY contain the Accept header field.	SHOULD	BASIC	generic-200-INVITE
RFC3261-13.3-11			If the INVITE request contained an offer, and the UAS had not yet sent an answer, the 2xx MUST contain an answer.	MUST	BASIC	generic-200-INVITE
RFC3261-13.3-12			If the INVITE did not contain an offer, the 2xx MUST contain an offer if the UAS had not yet sent an offer.	MUST	NOT REQUIRED	
RFC3261-13.3-13			If the server retransmits the 2xx response for 64*T1 seconds without receiving an ACK, the dialog is confirmed, but the session SHOULD be terminated.	SHOULD	NOT REQUIRED	
RFC3261-14-1	14	Modifying an Existing Session	However, automated generation of re-INVITE or BYE is NOT RECOMMENDED to avoid flooding the network with traffic when there is congestion.	RECOMMENDED	NOT REQUIRED	
RFC3261-14-2			In any case, if these messages are sent automatically, they SHOULD be sent after some randomized interval.	SHOULD	OUT OF SCOPE	
RFC3261-14.1-1	14.1	UAC Behavior	If the session description format has the capability for version numbers, the offerer SHOULD indicate that the version of the session description has changed.	SHOULD	ADVANCED	
RFC3261-14.1-2			Note that a UAC MUST NOT initiate a new INVITE transaction within a dialog while another INVITE transaction is in progress in either direction.	MUST NOT	NOT REQUIRED	
RFC3261-14.1-3			1. If there is an ongoing INVITE client transaction, the TU MUST wait until the transaction reaches the completed or terminated state before initiating the new INVITE.	MUST	OUT OF SCOPE	
RFC3261-14.1-4			2. If there is an ongoing INVITE server transaction, the TU MUST wait until the transaction reaches the confirmed or terminated state before initiating the new INVITE.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-14.1-5			If a UA receives a non-2xx final response to a re-INVITE, the session parameters MUST remain unchanged, as if no re-INVITE had been issued.	MUST	ADVANCED	
RFC3261-14.1-6			If a UAC receives a 491 response to a re-INVITE, it SHOULD start a timer with a value T chosen as follows:	SHOULD	NOT REQUIRED	
RFC3261-14.1-7			When the timer fires, the UAC SHOULD attempt the re-INVITE once more, if it still desires for that session modification to take place.	SHOULD	ADVANCED	
RFC3261-14.2-1	14.2	UAS Behavior	A UAS that receives a second INVITE before it sends the final response to a first INVITE with a lower CSeq sequence number on the same dialog MUST return a 500 (Server Internal Error) response to the second INVITE and MUST include a Retry-After header field with a randomly chosen value of between 0 and 10 seconds.	MUST	ADVANCED	
RFC3261-14.2-2				MUST	ADVANCED	
RFC3261-14.2-3			A UAS that receives an INVITE on a dialog while an INVITE it had sent on that dialog is in progress MUST return a 491 (Request Pending) response to the received INVITE.	MUST	ADVANCED	
RFC3261-14.2-4			If a UA receives a re-INVITE for an existing dialog, it MUST check any version identifiers in the session description or, if there are no version identifiers, the content of the session description to see if it has changed.	MUST	OUT OF SCOPE	
RFC3261-14.2-5			If the session description has changed, the UAS MUST adjust the session parameters accordingly, possibly after asking the user for confirmation.	MUST	OUT OF SCOPE	
RFC3261-14.2-6			This response SHOULD include a Warning header field.	SHOULD	ADVANCED	
RFC3261-14.2-7			If a UAS generates a 2xx response and never receives an ACK, it SHOULD generate a BYE to terminate the dialog.	SHOULD	ADVANCED	
RFC3261-14.2-8			A UAS providing an offer in a 2xx (because the INVITE did not contain an offer) SHOULD construct the offer as if the UAS were making a brand new call, subject to the constraints of sending an offer that updates an existing session, as described in [13] in the case of SDP.	SHOULD	ADVANCED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-14.2-9			Specifically, this means that it SHOULD include as many media formats and media types that the UA is willing to support.	SHOULD	ADVANCED	
RFC3261-14.2-10			The UAS MUST ensure that the session description overlaps with its previous session description in media formats, transports, or other parameters that require support from the peer.	MUST	ADVANCED	
RFC3261-14.2-11			If, however, it is unacceptable to the UAC, the UAC SHOULD generate an answer with a valid session description, and then send a BYE to terminate the session.	SHOULD	ADVANCED	
RFC3261-15-1	15	Terminating a Session	When a BYE is received on a dialog, any session associated with that dialog SHOULD terminate.	SHOULD	OUT OF SCOPE	
RFC3261-15-2			A UA MUST NOT send a BYE outside of a dialog.	MUST NOT	OUT OF SCOPE	
RFC3261-15-3			The caller's UA MAY send a BYE for either confirmed or early dialogs, and the callee's UA MAY send a BYE on confirmed dialogs, but MUST NOT send a BYE on early dialogs.	MUST NOT	NOT REQUIRED	
RFC3261-15-4			However, the callee's UA MUST NOT send a BYE on a confirmed dialog until it has received an ACK for its 2xx response or until the server transaction times out.	MUST NOT	NOT REQUIRED	
RFC3261-15.1-1	15.1.1	UAC Behavior	The UAC MUST consider the session terminated (and therefore stop sending or listening for media) as soon as the BYE request is passed to the client transaction.	MUST	NOT REQUIRED	
RFC3261-15.1-2			If the response for the BYE is a 481 (Call/Transaction Does Not Exist) or a 408 (Request Timeout) or no response at all is received for the BYE (that is, a timeout is returned by the client transaction), the UAC MUST consider the session and the dialog terminated.	MUST	OUT OF SCOPE	
RFC3261-15.1-3	15.1.2	UAS Behavior	If the BYE does not match an existing dialog, the UAS core SHOULD generate a 481 (Call/Transaction Does Not Exist) response and pass that to the server transaction.	SHOULD	NOT REQUIRED	
RFC3261-15.1-4			A UAS core receiving a BYE request for an existing dialog MUST follow the procedures of Section 12.2.2 to process the request.	MUST	BASIC	doc_reference

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-15.1-5			Once done, the UAS SHOULD terminate the session (and therefore stop sending and listening for media).	SHOULD	OUT OF SCOPE	
RFC3261-15.1-6			Whether or not it ends its participation on the session, the UAS core MUST generate a 2xx response to the BYE, and MUST pass that to the server transaction for transmission.	MUST	NOT REQUIRED	
RFC3261-15.1-7				MUST	NOT REQUIRED	
RFC3261-15.1-8			The UAS MUST still respond to any pending requests received for that dialog.	MUST	OUT OF SCOPE	
RFC3261-15.1-9			It is RECOMMENDED that a 487 (Request Terminated) response be generated to those pending requests.	RECOMMENDED	OUT OF SCOPE	
RFC3261-16.1-1	16.1	Overview	When responding directly to a request, the element is playing the role of a UAS and MUST behave as described in Section 8.2.	MUST	NOT REQUIRED	
RFC3261-16.1-2			Any request that is forwarded to more than one location MUST be handled statefully.	MUST	NOT REQUIRED	
RFC3261-16.1-3			Requests forwarded between different types of transports where the proxy's TU must take an active role in ensuring reliable delivery on one of the transports MUST be forwarded transaction statefully.	MUST	NOT REQUIRED	
RFC3261-16.1-4			The proxy SHOULD NOT initiate a CANCEL request.	SHOULD NOT	OUT OF SCOPE	
RFC3261-16.2-1	16.2	Stateful Proxy	The proxy core MUST behave as a UAS with respect to sending an immediate provisional on that server transaction (such as 100 Trying) as described in Section 8.2.6.	MUST	NOT REQUIRED	
RFC3261-16.2-2			Thus, a stateful proxy SHOULD NOT generate 100 (Trying) responses to non-INVITE requests.	SHOULD NOT	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.2-3			For all new requests, including any with unknown methods, an element intending to proxy the request MUST:	MUST	OUT OF SCOPE	
RFC3261-16.3-1	16.3	Request Validation	Before an element can proxy a request, it MUST verify the message's validity.	MUST	OUT OF SCOPE	
RFC3261-16.3-2			If any of these checks fail, the element MUST behave as a user agent server (see Section 8.2) and respond with an error code.	MUST	OUT OF SCOPE	
RFC3261-16.3-3			Notice that a proxy is not required to detect merged requests and MUST NOT treat merged requests as an error condition.	MUST NOT	OUT OF SCOPE	
RFC3261-16.3-4			The request MUST be well-formed enough to be handled with a server transaction.	MUST	NOT REQUIRED	
RFC3261-16.3-5			Any components involved in the remainder of these Request Validation steps or the Request Forwarding section MUST be well-formed.	MUST	NOT REQUIRED	
RFC3261-16.3-6			Any other components, well-formed or not, SHOULD be ignored and remain unchanged when the message is forwarded.	SHOULD	NOT REQUIRED	
RFC3261-16.3-7			An element MUST NOT refuse to proxy a request because it contains a method or header field it does not know about.	MUST NOT	NOT REQUIRED	
RFC3261-16.3-8			If the Request-URI has a URI whose scheme is not understood by the proxy, the proxy SHOULD reject the request with a 416 (Unsupported URI Scheme) response.	SHOULD	NOT REQUIRED	
RFC3261-16.3-9			If the request contains a Max-Forwards header field with a field value of zero (0), the element MUST NOT forward the request.	MUST NOT	NOT REQUIRED	
RFC3261-16.3-10			Otherwise, the element MUST return a 483 (Too many hops) response.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.3-11			If the request contains a Proxy-Require header field (Section 20.29) with one or more option-tags this element does not understand, the element MUST return a 420 (Bad Extension) response.	MUST	NOT REQUIRED	
RFC3261-16.3-12			The response MUST include an Unsupported (Section 20.40) header field listing those option-tags the element did not understand.	MUST	NOT REQUIRED	
RFC3261-16.3-13			If an element requires credentials before forwarding a request, the request MUST be inspected as described in Section 22.3.	MUST	OUT OF SCOPE	
RFC3261-16.4-1	16.4	Route Information Preprocessing	The proxy MUST inspect the Request-URI of the request.	MUST	OUT OF SCOPE	
RFC3261-16.4-2			If the Request-URI of the request contains a value this proxy previously placed into a Record-Route header field (see Section 16.6 item 4), the proxy MUST replace the Request-URI in the request with the last value from the Route header field, and remove that value from the Route header field.	MUST	NOT REQUIRED	
RFC3261-16.4-3			The proxy MUST then proceed as if it received this modified request.	MUST	NOT REQUIRED	
RFC3261-16.4-4			If the Request-URI contains a maddr parameter, the proxy MUST check to see if its value is in the set of addresses or domains the proxy is configured to be responsible for.	MUST	OUT OF SCOPE	
RFC3261-16.4-5			If the Request-URI has a maddr parameter with a value the proxy is responsible for, and the request was received using the port and transport indicated (explicitly or by default) in the Request-URI, the proxy MUST strip the maddr and any non-default port or transport parameter and continue processing as if those values had not been present in the request.	MUST	OUT OF SCOPE	
RFC3261-16.4-6			If the first value in the Route header field indicates this proxy, the proxy MUST remove that value from the request.	MUST	NOT REQUIRED	
RFC3261-16.5-1	16.5	Determining Request Targets	If the Request-URI of the request contains an maddr parameter, the Request-URI MUST be placed into the target set as the only target URI, and the proxy MUST proceed to Section 16.6.	MUST	NOT REQUIRED	
RFC3261-16.5-2				MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.5-3			If the domain of the Request-URI indicates a domain this element is not responsible for, the Request-URI MUST be placed into the target set as the only target, and the element MUST proceed to the task of Request Forwarding (Section 16.6).	MUST	NOT REQUIRED	
RFC3261-16.5-4				MUST	OUT OF SCOPE	
RFC3261-16.5-5			When accessing the location service constructed by a registrar, the Request-URI MUST first be canonicalized as described in Section 10.3 before being used as an index.	MUST	NOT REQUIRED	
RFC3261-16.5-6			If the Request-URI does not provide sufficient information for the proxy to determine the target set, it SHOULD return a 485 (Ambiguous) response.	SHOULD	OUT OF SCOPE	
RFC3261-16.5-7			This response SHOULD contain a Contact header field containing URIs of new addresses to be tried.	SHOULD	OUT OF SCOPE	
RFC3261-16.5-8			If a target URI is already present in the set (based on the definition of equality for the URI type), it MUST NOT be added again.	MUST NOT	OUT OF SCOPE	
RFC3261-16.5-9			A proxy MUST NOT add additional targets to the target set if the Request-URI of the original request does not indicate a resource this proxy is responsible for.	MUST NOT	OUT OF SCOPE	
RFC3261-16.5-10			If a proxy uses a dynamic source of information while building the target set (for instance, if it consults a SIP Registrar), it SHOULD monitor that source for the duration of processing the request.	SHOULD	OUT OF SCOPE	
RFC3261-16.5-11			New locations SHOULD be added to the target set as they become available.	SHOULD	OUT OF SCOPE	
RFC3261-16.5-12			As above, any given URI MUST NOT be added to the set more than once.	MUST NOT	OUT OF SCOPE	
RFC3261-16.5-13			If the Request-URI indicates a resource at this proxy that does not exist, the proxy MUST return a 404 (Not Found) response.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.5-14			If the target set remains empty after applying all of the above, the proxy MUST return an error response, which SHOULD be the 480 (Temporarily Unavailable) response.	MUST	NOT REQUIRED	
RFC3261-16.5-15				SHOULD	NOT REQUIRED	
RFC3261-16.6-1	16.6	Request Forwarding	The copy MUST initially contain all of the header fields from the received request.	MUST	NOT REQUIRED	
RFC3261-16.6-2			Fields not detailed in the processing described below MUST NOT be removed.	MUST NOT	NOT REQUIRED	
RFC3261-16.6-3			The copy SHOULD maintain the ordering of the header fields as in the received request.	SHOULD	NOT REQUIRED	
RFC3261-16.6-4			The proxy MUST NOT reorder field values with a common field name (See Section 7.3.1).	MUST NOT	NOT REQUIRED	
RFC3261-16.6-5			The proxy MUST NOT add to, modify, or remove the message body.	MUST NOT	NOT REQUIRED	
RFC3261-16.6-6			The Request-URI in the copy's start line MUST be replaced with the URI for this target.	MUST	NOT REQUIRED	
RFC3261-16.6-7			If the URI contains any parameters not allowed in a Request-URI, they MUST be removed.	MUST	NOT REQUIRED	
RFC3261-16.6-8			If the copy contains a Max-Forwards header field, the proxy MUST decrement its value by one (1).	MUST	NOT REQUIRED	
RFC3261-16.6-9			If the copy does not contain a Max-Forwards header field, the proxy MUST add one with a field value, which SHOULD be 70.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.6-10				SHOULD	NOT REQUIRED	
RFC3261-16.6-11			If this proxy wishes to remain on the path of future requests in a dialog created by this request (assuming the request creates a dialog), it MUST insert a Record-Route header field value into the copy before any existing Record-Route header field values, even if a Route header field is already present.	MUST	NOT REQUIRED	
RFC3261-16.6-12			If this request is already part of a dialog, the proxy SHOULD insert a Record-Route header field value if it wishes to remain on the path of future requests in the dialog.	SHOULD	NOT REQUIRED	
RFC3261-16.6-13			The URI placed in the Record-Route header field value MUST be a SIP or SIPS URI.	MUST	NOT REQUIRED	
RFC3261-16.6-14			This URI MUST contain an lr parameter (see Section 19.1.1).	MUST	NOT REQUIRED	
RFC3261-16.6-15			The URI SHOULD NOT contain the transport parameter unless the proxy has knowledge (such as in a private network) that the next downstream element that will be in the path of subsequent requests supports that transport.	SHOULD NOT	NOT REQUIRED	
RFC3261-16.6-16			The URI placed in the Record-Route header field MUST resolve to the element inserting it (or a suitable stand-in) when the server location procedures of [4] are applied to it, so that subsequent requests reach the same SIP element.	MUST	OUT OF SCOPE	
RFC3261-16.6-17			If the Request-URI contains a SIPS URI, or the topmost Route header field value (after the post processing of bullet 6) contains a SIPS URI, the URI placed into the Record-Route header field MUST be a SIPS URI.	MUST	NOT REQUIRED	
RFC3261-16.6-18			Furthermore, if the request was not received over TLS, the proxy MUST insert a Record-Route header field.	MUST	NOT REQUIRED	
RFC3261-16.6-19			In a similar fashion, a proxy that receives a request over TLS, but generates a request without a SIPS URI in the Request-URI or topmost Route header field value (after the post processing of bullet 6), MUST insert a Record-Route header field that is not a SIPS URI.	MUST	NOT REQUIRED	
RFC3261-16.6-20			If the URI placed in the Record-Route header field needs to be rewritten when it passes back through in a response, the URI MUST be distinct enough to locate at that time.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.6-21			If a proxy needs to be in the path of any type of dialog (such as one straddling a firewall), it SHOULD add a Record-Route header field value to every request with a method it does not understand since that method may have dialog semantics.	SHOULD	NOT REQUIRED	
RFC3261-16.6-22			Endpoints MUST NOT use a URI obtained from a Record-Route header field outside the dialog in which it was provided.	MUST NOT	OUT OF SCOPE	
RFC3261-16.6-23			A proxy MUST ensure that all such proxies are loose routers.	MUST	OUT OF SCOPE	
RFC3261-16.6-24			This set MUST be pushed into the Route header field of the copy ahead of any existing values, if present.	MUST	OUT OF SCOPE	
RFC3261-16.6-25			If the Route header field is absent, it MUST be added, containing that list of URIs.	MUST	OUT OF SCOPE	
RFC3261-16.6-26			If the request has a Route header field, this alternative MUST NOT be used unless it is known that next hop proxy is a loose router.	MUST NOT	OUT OF SCOPE	
RFC3261-16.6-27			Furthermore, if the Request-URI contains a SIPS URI, TLS MUST be used to communicate with that proxy.	MUST	NOT REQUIRED	
RFC3261-16.6-28			If the copy contains a Route header field, the proxy MUST inspect the URI in its first value.	MUST	NOT REQUIRED	
RFC3261-16.6-29			If that URI does not contain an lr parameter, the proxy MUST modify the copy as follows:	MUST	NOT REQUIRED	
RFC3261-16.6-30			The proxy MUST place the Request-URI into the Route header field as the last value.	MUST	NOT REQUIRED	
RFC3261-16.6-31			The proxy MUST then place the first Route header field value into the Request-URI and remove that value from the Route header field.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.6-32			Such a policy MUST NOT be used if the proxy is not certain that the IP address, port, and transport correspond to a server that is a loose router.	MUST NOT	OUT OF SCOPE	
RFC3261-16.6-33			However, this mechanism for sending the request through a specific next hop is NOT RECOMMENDED; instead a Route header field should be used for that purpose as described above.	NOT RECOMMENDED	OUT OF SCOPE	
RFC3261-16.6-34			If the proxy has reformatted the request to send to a strict-routing element as described in step 6 above, the proxy MUST apply those procedures to the Request-URI of the request.	MUST	NOT REQUIRED	
RFC3261-16.6-35			Otherwise, the proxy MUST apply the procedures to the first value in the Route header field, if present, else the Request-URI.	MUST	NOT REQUIRED	
RFC3261-16.6-36			Independently of which URI is being used as input to the procedures of [4], if the Request-URI specifies a SIPS resource, the proxy MUST follow the procedures of [4] as if the input URI were a SIPS URI.	MUST	NOT REQUIRED	
RFC3261-16.6-37			As described in [4], the proxy MUST attempt to deliver the message to the first tuple in that set, and proceed through the set in order until the delivery attempt succeeds.	MUST	NOT REQUIRED	
RFC3261-16.6-38			For each tuple attempted, the proxy MUST format the message as appropriate for the tuple and send the request using a new client transaction as detailed in steps 8 through 10.	MUST	NOT REQUIRED	
RFC3261-16.6-39			Thus, the branch parameter provided with the Via header field inserted in step 8 MUST be different for each attempt.	MUST	NOT REQUIRED	
RFC3261-16.6-40			The proxy MUST insert a Via header field value into the copy before the existing Via header field values.	MUST	NOT REQUIRED	
RFC3261-16.6-41			A proxy choosing to detect loops SHOULD create a branch parameter separable into two parts by the implementation.	SHOULD	NOT REQUIRED	
RFC3261-16.6-42			The first part MUST satisfy the constraints of Section 8.1.1.7 as described above.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.6-43			The value placed in this part of the branch parameter SHOULD reflect all of those fields (including any Route, Proxy-Require and Proxy- Authorization header fields).	SHOULD	NOT REQUIRED	
RFC3261-16.6-44			If a proxy wishes to detect loops, the "branch" parameter it supplies MUST depend on all information affecting processing of a request, including the incoming Request-URI and any header fields affecting the request's admission or routing.	MUST	NOT REQUIRED	
RFC3261-16.6-45			The request method MUST NOT be included in the calculation of the branch parameter.	MUST NOT	NOT REQUIRED	
RFC3261-16.6-46			In particular, CANCEL and ACK requests (for non-2xx responses) MUST have the same branch value as the corresponding request they cancel or acknowledge.	MUST	NOT REQUIRED	
RFC3261-16.6-47			If the request will be sent to the next hop using a stream-based transport and the copy contains no Content-Length header field, the proxy MUST insert one with the correct value for the body of the request (see Section 20.14).	MUST	NOT REQUIRED	
RFC3261-16.6-48			A stateful proxy MUST create a new client transaction for this request as described in Section 17.1 and instructs the transaction to send the request using the address, port and transport determined in step 7.	MUST	OUT OF SCOPE	
RFC3261-16.6-49			Timer C MUST be set for each client transaction when an INVITE request is proxied.	MUST	NOT REQUIRED	
RFC3261-16.6-50			The timer MUST be larger than 3 minutes.	MUST	NOT REQUIRED	
RFC3261-16.7-1	16.7	Response Processing	If none is found, the element MUST process the response (even if it is an informational response) as a stateless proxy (described below).	MUST	NOT REQUIRED	
RFC3261-16.7-2			As client transactions pass responses to the proxy layer, the following processing MUST take place:	MUST	OUT OF SCOPE	
RFC3261-16.7-3			The following processing MUST be performed on each response that is forwarded.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.7-4			For an INVITE transaction, if the response is a provisional response with status codes 101 to 199 inclusive (i.e., anything but 100), the proxy MUST reset timer C for that client transaction.	MUST	NOT REQUIRED	
RFC3261-16.7-5			The timer MAY be reset to a different value, but this value MUST be greater than 3 minutes.	MUST	NOT REQUIRED	
RFC3261-16.7-6			If no Via header field values remain in the response, the response was meant for this element and MUST NOT be forwarded.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-7			If the proxy chooses to recurse on any contacts in a 3xx response by adding them to the target set, it MUST remove them from the response before adding the response to the response context.	MUST	NOT REQUIRED	
RFC3261-16.7-8			However, a proxy SHOULD NOT recurse to a non-SIPS URI if the Request-URI of the original request was a SIPS URI.	SHOULD NOT	NOT REQUIRED	
RFC3261-16.7-9			If the proxy recurses on all of the contacts in a 3xx response, the proxy SHOULD NOT add the resulting contactless response to the response context.	SHOULD NOT	NOT REQUIRED	
RFC3261-16.7-10			If a proxy receives a 416 (Unsupported URI Scheme) response to a request whose Request-URI scheme was not SIP, but the scheme in the original received request was SIP or SIPS (that is, the proxy changed the scheme from SIP or SIPS to something else when it proxied a request), the proxy SHOULD add a new URI to the target set.	SHOULD	NOT REQUIRED	
RFC3261-16.7-11			This URI SHOULD be a SIP URI version of the non-SIP URI that was just tried.	SHOULD	NOT REQUIRED	
RFC3261-16.7-12			As with a 3xx response, if a proxy "recurses" on the 416 by trying a SIP or SIPS URI instead, the 416 response SHOULD NOT be added to the response context.	SHOULD NOT	NOT REQUIRED	
RFC3261-16.7-13			Until a final response has been sent on the server transaction, the following responses MUST be forwarded immediately:	MUST	NOT REQUIRED	
RFC3261-16.7-14			If a 6xx response is received, it is not immediately forwarded, but the stateful proxy SHOULD cancel all client pending transactions as described in Section 10, and it MUST NOT create any new branches in this context.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.7-15				MUST NOT	NOT REQUIRED	
RFC3261-16.7-16			After a final response has been sent on the server transaction, the following responses MUST be forwarded immediately:	MUST	NOT REQUIRED	
RFC3261-16.7-17			A stateful proxy MUST NOT immediately forward any other responses.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-18			In particular, a stateful proxy MUST NOT forward any 100 (Trying) response.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-19			Any response chosen for immediate forwarding MUST be processed as described in steps "Aggregate Authorization Header Field Values" through "Record-Route".	MUST	NOT REQUIRED	
RFC3261-16.7-20			A stateful proxy MUST send a final response to a response context's server transaction if no final responses have been immediately forwarded by the above rules and all client transactions in this response context have been terminated.	MUST	NOT REQUIRED	
RFC3261-16.7-21			The stateful proxy MUST choose the "best" final response among those received and stored in the response context.	MUST	NOT REQUIRED	
RFC3261-16.7-22			If there are no final responses in the context, the proxy MUST send a 408 (Request Timeout) response to the server transaction.	MUST	NOT REQUIRED	
RFC3261-16.7-23			Otherwise, the proxy MUST forward a response from the responses stored in the response context.	MUST	NOT REQUIRED	
RFC3261-16.7-24			It MUST choose from the 6xx class responses if any exist in the context.	MUST	NOT REQUIRED	
RFC3261-16.7-25			If no 6xx class responses are present, the proxy SHOULD choose from the lowest response class stored in the response context.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.7-26			The proxy SHOULD give preference to responses that provide information affecting resubmission of this request, such as 401, 407, 415, 420, and 484 if the 4xx class is chosen.	SHOULD	OUT OF SCOPE	
RFC3261-16.7-27			A proxy which receives a 503 (Service Unavailable) response SHOULD NOT forward it upstream unless it can determine that any subsequent requests it might proxy will also generate a 503.	SHOULD NOT	NOT REQUIRED	
RFC3261-16.7-28			If the only response that was received is a 503, the proxy SHOULD generate a 500 response and forward that upstream.	SHOULD	NOT REQUIRED	
RFC3261-16.7-29			The forwarded response MUST be processed as described in steps "Aggregate Authorization Header Field Values" through "Record- Route".	MUST	OUT OF SCOPE	
RFC3261-16.7-30			A proxy MUST NOT insert a tag into the To header field of a 1xx or 2xx response if the request did not contain one.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-31			A proxy MUST NOT modify the tag in the To header field of a 1xx or 2xx response.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-32			An element SHOULD preserve the To tag when simply forwarding a 3-6xx response to a request that did not contain a To tag.	SHOULD	NOT REQUIRED	
RFC3261-16.7-33			A proxy MUST NOT modify the To tag in any forwarded response to a request that contains a To tag.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-34			If the selected response is a 401 (Unauthorized) or 407 (Proxy Authentication Required), the proxy MUST collect any WWW-Authenticate and Proxy-Authenticate header field values from all other 401 (Unauthorized) and 407 (Proxy Authentication Required) responses received so far in this response context and add them to this response without modification before forwarding.	MUST	OUT OF SCOPE	
RFC3261-16.7-35			If the proxy received the request over TLS, and sent it out over a non-TLS connection, the proxy MUST rewrite the URI in the Record-Route header field to be a SIPS URI.	MUST	NOT REQUIRED	
RFC3261-16.7-36			If the proxy received the request over a non-TLS connection, and sent it out over TLS, the proxy MUST rewrite the URI in the Record-Route header field to be a SIP URI.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.7-37			The new URI provided by the proxy MUST satisfy the same constraints on URIs placed in Record-Route header fields in requests (see Step 4 of Section 16.6) with the following modifications:	MUST	NOT REQUIRED	
RFC3261-16.7-38			The URI SHOULD NOT contain the transport parameter unless the proxy has knowledge that the next upstream (as opposed to downstream) element that will be in the path of subsequent requests supports that transport.	SHOULD NOT	NOT REQUIRED	
RFC3261-16.7-39			A RECOMMENDED mechanism to achieve this is for the proxy to append a unique identifier for the proxy instance to the user portion of the URI.	RECOMMENDED	NOT REQUIRED	
RFC3261-16.7-40			The proxy MUST NOT add to, modify, or remove the message body.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-41			Unless otherwise specified, the proxy MUST NOT remove any header field values other than the Via header field value discussed in Section 16.7 Item 3.	MUST NOT	OUT OF SCOPE	
RFC3261-16.7-42			In particular, the proxy MUST NOT remove any "received" parameter it may have added to the next Via header field value while processing the request associated with this response.	MUST NOT	NOT REQUIRED	
RFC3261-16.7-43			The proxy MUST pass the response to the server transaction associated with the response context.	MUST	OUT OF SCOPE	
RFC3261-16.7-44			If the server transaction is no longer available to handle the transmission, the element MUST forward the response statelessly by sending it to the server transport.	MUST	NOT REQUIRED	
RFC3261-16.7-45			The proxy MUST maintain the response context until all of its associated transactions have been terminated, even after forwarding a final response.	MUST	OUT OF SCOPE	
RFC3261-16.7-46			If the forwarded response was a final response, the proxy MUST generate a CANCEL request for all pending client transactions associated with this response context.	MUST	NOT REQUIRED	
RFC3261-16.7-47			A proxy SHOULD also generate a CANCEL request for all pending client transactions associated with this response context when it receives a 6xx response.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.8-1	16.8	Processing Timer C	If timer C should fire, the proxy MUST either reset the timer with any value it chooses, or terminate the client transaction.	MUST	NOT REQUIRED	
RFC3261-16.8-2			If the client transaction has received a provisional response, the proxy MUST generate a CANCEL request matching that transaction.	MUST	NOT REQUIRED	
RFC3261-16.8-3			If the client transaction has not received a provisional response, the proxy MUST behave as if the transaction received a 408 (Request Timeout) response.	MUST	NOT REQUIRED	
RFC3261-16.9-1	16.9	Handling Transport Errors	If the transport layer notifies a proxy of an error when it tries to forward a request (see Section 18.4), the proxy MUST behave as if the forwarded request received a 503 (Service Unavailable) response.	MUST	NOT REQUIRED	
RFC3261-16.9-2			The proxy SHOULD NOT cancel any outstanding client transactions associated with this response context due to this notification.	SHOULD NOT	OUT OF SCOPE	
RFC3261-16.10-1	16.10	CANCEL Processing	A proxy MUST cancel any pending client transactions associated with a response context when it receives a matching CANCEL request.	MUST	NOT REQUIRED	
RFC3261-16.10-2			If a matching response context is found, the element MUST immediately return a 200 (OK) response to the CANCEL request.	MUST	NOT REQUIRED	
RFC3261-16.10-3			Furthermore, the element MUST generate CANCEL requests for all pending client transactions in the context as described in Section 16.7 step 10.	MUST	NOT REQUIRED	
RFC3261-16.10-4			It MUST statelessly forward the CANCEL request (it may have statelessly forwarded the associated request previously).	MUST	OUT OF SCOPE	
RFC3261-16.11-1	16.11	Stateless Proxy	Furthermore, when handling a request statelessly, an element MUST NOT generate its own 100 (Trying) or any other provisional response.	MUST NOT	NOT REQUIRED	
RFC3261-16.11-2			A stateless proxy MUST validate a request as described in Section 16.3	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.11-3			A stateless proxy MUST follow the request processing steps described in Sections 16.4 through 16.5 with the following exception:	MUST	NOT REQUIRED	
RFC3261-16.11-4			A stateless proxy MUST choose one and only one target from the target set.	MUST	NOT REQUIRED	
RFC3261-16.11-5			This choice MUST only rely on fields in the message and time-invariant properties of the server.	MUST	NOT REQUIRED	
RFC3261-16.11-6			In particular, a retransmitted request MUST be forwarded to the same destination each time it is processed.	MUST	NOT REQUIRED	
RFC3261-16.11-7			Furthermore, CANCEL and non-Routed ACK requests MUST generate the same choice as their associated INVITE.	MUST	NOT REQUIRED	
RFC3261-16.11-8			A stateless proxy MUST follow the request processing steps described in Section 16.6 with the following exceptions:	MUST	NOT REQUIRED	
RFC3261-16.11-9			Therefore, the component of the branch parameter that makes it unique MUST be the same each time a retransmitted request is forwarded.	MUST	NOT REQUIRED	
RFC3261-16.11-10			Thus for a stateless proxy, the branch parameter MUST be computed as a combinatoric function of message parameters which are invariant on retransmission.	MUST	NOT REQUIRED	
RFC3261-16.11-11			However, the following procedure is RECOMMENDED.	RECOMMENDED	NOT REQUIRED	
RFC3261-16.11-12			All other message transformations specified in Section 16.6 MUST result in the same transformation of a retransmitted request.	MUST	NOT REQUIRED	
RFC3261-16.11-13			In particular, if the proxy inserts a Record-Route value or pushes URIs into the Route header field, it MUST place the same values in retransmissions of the request.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-16.11-14			As for the Via branch parameter, this implies that the transformations MUST be based on time-invariant configuration or retransmission-invariant properties of the request.	MUST	NOT REQUIRED	
RFC3261-16.11-15			Stateless proxies MUST NOT perform special processing for CANCEL requests.	MUST NOT	NOT REQUIRED	
RFC3261-16.11-16			When a response arrives at a stateless proxy, the proxy MUST inspect the sent-by value in the first (topmost) Via header field value.	MUST	NOT REQUIRED	
RFC3261-16.11-17			If that address matches the proxy, (it equals a value this proxy has inserted into previous requests) the proxy MUST remove that header field value from the response and forward the result to the location indicated in the next Via header field value.	MUST	NOT REQUIRED	
RFC3261-16.11-18			The proxy MUST NOT add to, modify, or remove the message body.	MUST NOT	NOT REQUIRED	
RFC3261-16.11-19			Unless specified otherwise, the proxy MUST NOT remove any other header field values.	MUST NOT	NOT REQUIRED	
RFC3261-16.11-20			If the address does not match the proxy, the message MUST be silently discarded.	MUST	NOT REQUIRED	
RFC3261-17.1-1	17.1	Client Transaction	Because of the non-INVITE transaction's reliance on a two-way handshake, TUs SHOULD respond immediately to non-INVITE requests.	SHOULD	BASIC	generic_200-NOTIFY generic-200-BYE generic_200-CANCEL generic_200-OPTIONS
RFC3261-17.1-2	17.1.1.2	Formal Description	The initial state, ″calling″, MUST be entered when the TU initiates a new client transaction with an INVITE request.	MUST	OUT OF SCOPE	
RFC3261-17.1-3			The client transaction MUST pass the request to the transport layer for transmission (see Section 18).	MUST	OUT OF SCOPE	
RFC3261-17.1-4			If an unreliable transport is being used, the client transaction MUST start timer A with a value of T1.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-17.1-5			If a reliable transport is being used, the client transaction SHOULD NOT start timer A (Timer A controls request retransmissions).	SHOULD NOT	NOT REQUIRED	
RFC3261-17.1-6			For any transport, the client transaction MUST start timer B with a value of 64*T1 seconds (Timer B controls transaction timeouts).	MUST	BASIC	reference (UE-TM-B-1-AKA) (UE-TM-B-1-DIP)
RFC3261-17.1-7			When timer A fires, the client transaction MUST retransmit the request by passing it to the transport layer, and MUST reset the timer with a value of 2*T1.	MUST	BASIC	reference (UE-TM-B-1-AKA) (UE-TM-B-1-DIP)
RFC3261-17.1-8				MUST	BASIC	
RFC3261-17.1-9			When timer A fires 2*T1 seconds later, the request MUST be retransmitted again (assuming the client transaction is still in this state).	MUST	OUT OF SCOPE	
RFC3261-17.1-10			This process MUST continue so that the request is retransmitted with intervals that double after each transmission.	MUST	OUT OF SCOPE	
RFC3261-17.1-11			These retransmissions SHOULD only be done while the client transaction is in the "calling" state.	SHOULD	OUT OF SCOPE	
RFC3261-17.1-12			Elements MAY (though it is NOT RECOMMENDED) use smaller values of T1 within closed, private networks that do not permit general Internet connection.	NOT RECOMMENDED	NOT REQUIRED	
RFC3261-17.1-13			T1 MAY be chosen larger, and this is RECOMMENDED if it is known in advance (such as on high latency access links) that the RTT is larger.	RECOMMENDED	NOT REQUIRED	
RFC3261-17.1-14			Whatever the value of T1, the exponential backoffs on retransmissions described in this section MUST be used.	MUST	OUT OF SCOPE	
RFC3261-17.1-15			If the client transaction is still in the "Calling" state when timer B fires, the client transaction SHOULD inform the TU that a timeout has occurred.	SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-17.1-16			The client transaction MUST NOT generate an ACK.	MUST NOT	BASIC	UE-TM-B-1-AKA UE-TM-B-1-DIP
RFC3261-17.1-17			If the client transaction receives a provisional response while in the "Calling" state, it transitions to the "Proceeding" state. In the "Proceeding" state, the client transaction SHOULD NOT retransmit the request any longer. Furthermore, the provisional response MUST be passed to the TU.	SHOULD NOT	BASIC	UE-RR-B-1-AKA UE-RR-B-1-DIP
RFC3261-17.1-18				MUST	OUT OF SCOPE	
RFC3261-17.1-19			Any further provisional responses MUST be passed up to the TU while in the "Proceeding" state.	MUST	OUT OF SCOPE	
RFC3261-17.1-20			When in either the "Calling" or "Proceeding" states, reception of a response with status code from 300-699 MUST cause the client transaction to transition to "Completed".	MUST	OUT OF SCOPE	
RFC3261-17.1-21			The client transaction MUST pass the received response up to the TU, and the client transaction MUST generate an ACK request, even if the transport is reliable (guidelines for constructing the ACK from the response are given in Section 17.1.1.3) and then pass the ACK to the transport layer for transmission.	MUST	OUT OF SCOPE	
RFC3261-17.1-22				MUST	NOT REQUIRED	
RFC3261-17.1-23			The ACK MUST be sent to the same address, port, and transport to which the original request was sent.	MUST	BASIC	generic_ACK-non2XX
RFC3261-17.1-24			The client transaction SHOULD start timer D when it enters the "Completed" state, with a value of at least 32 seconds for unreliable transports, and a value of zero seconds for reliable transports.	SHOULD	BASIC	reference (UE-TM-B-2-AKA) (UE-TM-B-2-DIP)
RFC3261-17.1-25			Any retransmissions of the final response that are received while in the "Completed" state MUST cause the ACK to be re-passed to the transport layer for retransmission, but the newly received response MUST NOT be passed up to the TU.	MUST	BASIC	UE-TM-B-2-AKA UE-TM-B-2-DIP
RFC3261-17.1-26				MUST NOT	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−17.1−27			If timer D fires while the client transaction is in the ″Completed″ state, the client transaction MUST move to the terminated state.	MUST	BASIC	reference （UE−TM−B−2−AKA） （UE−TM−B−2−DIP）
RFC3261−17.1−28			When in either the ″Calling″ or ″Proceeding″ states, reception of a 2xx response MUST cause the client transaction to enter the ″Terminated″ state, and the response MUST be passed up to the TU.	MUST	OUT OF SCOPE	
RFC3261−17.1−29				MUST	OUT OF SCOPE	
RFC3261−17.1−30			The client transaction MUST be destroyed the instant it enters the ″Terminated″ state.	MUST	OUT OF SCOPE	
RFC3261−17.1−31	17.1.1.3	Construction of the ACK Request	A UAC core that generates an ACK for 2xx MUST instead follow the rules described in Section 13.	MUST	BASIC	doc_reference
RFC3261−17.1−32			The ACK request constructed by the client transaction MUST contain values for the Call−ID, From, and Request−URI that are equal to the values of those header fields in the request passed to the transport by the client transaction (call this the ″original request″).	MUST	BASIC	generic_ACK−non2XX
RFC3261−17.1−33			The To header field in the ACK MUST equal the To header field in the response being acknowledged, and therefore will usually differ from the To header field in the original request by the addition of the tag parameter.	MUST	BASIC	generic_ACK−non2XX
RFC3261−17.1−34			The ACK MUST contain a single Via header field, and this MUST be equal to the top Via header field of the original request.	MUST	BASIC	generic_ACK−non2XX
RFC3261−17.1−35				MUST	BASIC	generic_ACK−non2XX
RFC3261−17.1−36			The CSeq header field in the ACK MUST contain the same value for the sequence number as was present in the original request, but the method parameter MUST be equal to ″ACK″.	MUST	BASIC	generic_ACK−non2XX
RFC3261−17.1−37				MUST	BASIC	generic_ACK−non2XX

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-17.1-38			If the INVITE request whose response is being acknowledged had Route header fields, those header fields MUST appear in the ACK.	MUST	BASIC	generic_ACK-non2XX
RFC3261-17.1-39			Therefore, placement of bodies in ACK for non-2xx is NOT RECOMMENDED, but if done, the body types are restricted to any that appeared in the INVITE, assuming that the response to the INVITE was not 415.	NOT RECOMMENDED	NOT REQUIRED	
RFC3261-17.1-40	17.1.2.2	Formal Description	When entering this state, the client transaction SHOULD set timer F to fire in 64*T1 seconds.	SHOULD	BASIC	reference (UE-TM-B-5-AKA) (UE-TM-B-5-DIP)
RFC3261-17.1-41			The request MUST be passed to the transport layer for transmission.	MUST	OUT OF SCOPE	
RFC3261-17.1-42			If an unreliable transport is in use, the client transaction MUST set timer E to fire in T1 seconds.	MUST	BASIC	reference (UE-TM-B-5-AKA) (UE-TM-B-5-DIP)
RFC3261-17.1-43			If Timer F fires while the client transaction is still in the "Trying" state, the client transaction SHOULD inform the TU about the timeout, and then it SHOULD enter the "Terminated" state.	SHOULD	BASIC	reference (UE-TM-B-5-AKA) (UE-TM-B-5-DIP)
RFC3261-17.1-44				SHOULD	OUT OF SCOPE	
RFC3261-17.1-45			If a provisional response is received while in the "Trying" state, the response MUST be passed to the TU, and then the client transaction SHOULD move to the "Proceeding" state.	MUST	OUT OF SCOPE	
RFC3261-17.1-46				SHOULD	OUT OF SCOPE	
RFC3261-17.1-47			If a final response (status codes 200-699) is received while in the "Trying" state, the response MUST be passed to the TU, and the client transaction MUST transition to the "Completed" state.	MUST	OUT OF SCOPE	
RFC3261-17.1-48				MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-17.1-49			If Timer E fires while in the "Proceeding" state, the request MUST be passed to the transport layer for retransmission, and Timer E MUST be reset with a value of T2 seconds.	MUST	OUT OF SCOPE	
RFC3261-17.1-50				MUST	OUT OF SCOPE	
RFC3261-17.1-51			If timer F fires while in the "Proceeding" state, the TU MUST be informed of a timeout, and the client transaction MUST transition to the terminated state.	MUST	OUT OF SCOPE	
RFC3261-17.1-52				MUST	OUT OF SCOPE	
RFC3261-17.1-53			If a final response (status codes 200-699) is received while in the "Proceeding" state, the response MUST be passed to the TU, and the client transaction MUST transition to the "Completed" state.	MUST	OUT OF SCOPE	
RFC3261-17.1-54				MUST	OUT OF SCOPE	
RFC3261-17.1-55			Once the client transaction enters the "Completed" state, it MUST set Timer K to fire in T4 seconds for unreliable transports, and zero seconds for reliable transports.	MUST	OUT OF SCOPE	
RFC3261-17.1-56			If Timer K fires while in this state, the client transaction MUST transition to the "Terminated" state.	MUST	OUT OF SCOPE	
RFC3261-17.1-57			Once the transaction is in the terminated state, it MUST be destroyed immediately.	MUST	OUT OF SCOPE	
RFC3261-17.1-58	17.1.4	Handling Transport Errors	The client transaction SHOULD inform the TU that a transport failure has occurred, and the client transaction SHOULD transition directly to the "Terminated" state.	SHOULD	OUT OF SCOPE	
RFC3261-17.1-59				SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-17.2-1	17.2.1	INVITE Server Transaction	The server transaction MUST generate a 100 (Trying) response unless it knows that the TU will generate a provisional or final response within 200 ms, in which case it MAY generate a 100 (Trying) response.	MUST	NOT REQUIRED	
RFC3261-17.2-2			The 100 (Trying) response is constructed according to the procedures in Section 8.2.6, except that the insertion of tags in the To header field of the response (when none was present in the request) is downgraded from MAY to SHOULD NOT.	SHOULD NOT	NOT REQUIRED	
RFC3261-17.2-3			The request MUST be passed to the TU.	MUST	OUT OF SCOPE	
RFC3261-17.2-4			So long as the server transaction is in the "Proceeding" state, each of these MUST be passed to the transport layer for transmission.	MUST	OUT OF SCOPE	
RFC3261-17.2-5			If a request retransmission is received while in the "Proceeding" state, the most recent provisional response that was received from the TU MUST be passed to the transport layer for retransmission.	MUST	NOT REQUIRED	
RFC3261-17.2-6			If, while in the "Proceeding" state, the TU passes a 2xx response to the server transaction, the server transaction MUST pass this response to the transport layer for transmission.	MUST	OUT OF SCOPE	
RFC3261-17.2-7			The server transaction MUST then transition to the "Terminated" state.	MUST	OUT OF SCOPE	
RFC3261-17.2-8			While in the "Proceeding" state, if the TU passes a response with status code from 300 to 699 to the server transaction, the response MUST be passed to the transport layer for transmission, and the state machine MUST enter the "Completed" state.	MUST	OUT OF SCOPE	
RFC3261-17.2-9				MUST	OUT OF SCOPE	
RFC3261-17.2-10			When the "Completed" state is entered, timer H MUST be set to fire in 64*T1 seconds for all transports.	MUST	BASIC	reference (UE-TM-B-3-AKA) (UE-TM-B-3-DIP)
RFC3261-17.2-11			Furthermore, while in the "Completed" state, if a request retransmission is received, the server SHOULD pass the response to the transport for retransmission.	SHOULD	BASIC	reference (UE-TM-B-3-AKA) (UE-TM-B-3-DIP)

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−17.2−12			If an ACK is received while the server transaction is in the ″Completed″ state, the server transaction MUST transition to the ″Confirmed″ state.	MUST	NOT REQUIRED	
RFC3261−17.2−13			In this case, the server transaction MUST transition to the ″Terminated″ state, and MUST indicate to the TU that a transaction failure has occurred.	MUST	OUT OF SCOPE	
RFC3261−17.2−14				MUST	OUT OF SCOPE	
RFC3261−17.2−15			Once timer I fires, the server MUST transition to the ″Terminated″ state.	MUST	OUT OF SCOPE	
RFC3261−17.2−16			Once the transaction is in the ″Terminated″ state, it MUST be destroyed immediately.	MUST	OUT OF SCOPE	
RFC3261−17.2−17	17.2.2	Non−INVITE Server Transaction	While in the ″Trying″ state, if the TU passes a provisional response to the server transaction, the server transaction MUST enter the ″Proceeding″ state.	MUST	OUT OF SCOPE	
RFC3261−17.2−18			The response MUST be passed to the transport layer for transmission.	MUST	OUT OF SCOPE	
RFC3261−17.2−19			Any further provisional responses that are received from the TU while in the ″Proceeding″ state MUST be passed to the transport layer for transmission.	MUST	OUT OF SCOPE	
RFC3261−17.2−20			If a retransmission of the request is received while in the ″Proceeding″ state, the most recently sent provisional response MUST be passed to the transport layer for retransmission.	MUST	OUT OF SCOPE	
RFC3261−17.2−21			If the TU passes a final response (status codes 200−699) to the server while in the ″Proceeding″ state, the transaction MUST enter the ″Completed″ state, and the response MUST be passed to the transport layer for transmission.	MUST	OUT OF SCOPE	
RFC3261−17.2−22				MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-17.2-23			When the server transaction enters the "Completed" state, it MUST set Timer J to fire in 64*T1 seconds for unreliable transports, and zero seconds for reliable transports.	MUST	BASIC	reference （UE-TM-B-4-AKA） （UE-TM-B-4-DIP）
RFC3261-17.2-24			While in the "Completed" state, the server transaction MUST pass the final response to the transport layer for retransmission whenever a retransmission of the request is received.	MUST	OUT OF SCOPE	
RFC3261-17.2-25			Any other final responses passed by the TU to the server transaction MUST be discarded while in the "Completed" state.	MUST	OUT OF SCOPE	
RFC3261-17.2-26			The server transaction remains in this state until Timer J fires, at which point it MUST transition to the "Terminated" state.	MUST	OUT OF SCOPE	
RFC3261-17.2-27			The server transaction MUST be destroyed the instant it enters the "Terminated" state.	MUST	OUT OF SCOPE	
RFC3261-17.2-28	17.2.4	Handling Transport Errors	If those should all fail, based on the definition of failure in [4], the server transaction SHOULD inform the TU that a failure has occurred, and SHOULD transition to the terminated state.	SHOULD	OUT OF SCOPE	
RFC3261-17.2-29				SHOULD	OUT OF SCOPE	
RFC3261-18-1	18	Transport	It is RECOMMENDED that connections be kept open for some implementation-defined duration after the last message was sent or received over that connection.	RECOMMENDED	NOT REQUIRED	
RFC3261-18-2			This duration SHOULD at least equal the longest amount of time the element would need in order to bring a transaction from instantiation to the terminated state.	SHOULD	NOT REQUIRED	
RFC3261-18-3			All SIP elements MUST implement UDP and TCP.	MUST	NOT REQUIRED	
RFC3261-18-4			It has arisen out of the need to handle larger messages, which MUST use TCP, as discussed below.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-18.1-1	18.1.1	Sending Requests	If a request is within 200 bytes of the path MTU, or if it is larger than 1300 bytes and the path MTU is unknown, the request MUST be sent using an RFC 2914 [43] congestion controlled transport protocol, such as TCP. If this causes a change in the transport protocol from the one indicated in the top Via, the value in the top Via MUST be changed.	MUST	NOT REQUIRED	
RFC3261-18.1-2				MUST	NOT REQUIRED	
RFC3261-18.1-3			However, implementations MUST be able to handle messages up to the maximum datagram packet size.	MUST	NOT REQUIRED	
RFC3261-18.1-4			If an element sends a request over TCP because of these message size constraints, and that request would have otherwise been sent over UDP, if the attempt to establish the connection generates either an ICMP Protocol Not Supported, or results in a TCP reset, the element SHOULD retry the request, using UDP.	SHOULD	NOT REQUIRED	
RFC3261-18.1-5			A client that sends a request to a multicast address MUST add the "maddr" parameter to its Via header field value containing the destination multicast address, and for IPv4, SHOULD add the "ttl" parameter with a value of 1.	MUST	NOT REQUIRED	
RFC3261-18.1-6				SHOULD	NOT REQUIRED	
RFC3261-18.1-7			Before a request is sent, the client transport MUST insert a value of the "sent-by" field into the Via header field.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_OPTIONS
RFC3261-18.1-8			The usage of an FQDN is RECOMMENDED.	RECOMMENDED	NOT REQUIRED	
RFC3261-18.1-9			Therefore, the client transport MUST be prepared to receive the response on the same connection used to send the request.	MUST	NOT REQUIRED	
RFC3261-18.1-10			To handle this case, the transport layer MUST also be prepared to receive an incoming connection on the source IP address from which the request was sent and port number in the "sent-by" field.	MUST	NOT REQUIRED	
RFC3261-18.1-11			It also MUST be prepared to receive incoming connections on any address and port that would be selected by a server based on the procedures described in Section 5 of [4].	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-18.1-12			For unreliable unicast transports, the client transport MUST be prepared to receive responses on the source IP address from which the request is sent (as responses are sent back to the source address) and the port number in the "sent-by" field.	MUST	OUT OF SCOPE	
RFC3261-18.1-13			The client MUST be prepared to receive responses on any address and port that would be selected by a server based on the procedures described in Section 5 of [4].	MUST	OUT OF SCOPE	
RFC3261-18.1-14			For multicast, the client transport MUST be prepared to receive responses on the same multicast group and port to which the request is sent (that is, it needs to be a member of the multicast group it sent the request to.)	MUST	NOT REQUIRED	
RFC3261-18.1-15			If a request is destined to an IP address, port, and transport to which an existing connection is open, it is RECOMMENDED that this connection be used to send the request, but another connection MAY be opened and used.	RECOMMENDED	NOT REQUIRED	
RFC3261-18.1-16	18.1.2	Receiving Responses	If the value of the "sent-by" parameter in that header field value does not correspond to a value that the client transport is configured to insert into requests, the response MUST be silently discarded.	MUST	NOT REQUIRED	
RFC3261-18.1-17			If there is a match, the response MUST be passed to that transaction.	MUST	OUT OF SCOPE	
RFC3261-18.1-18			Otherwise, the response MUST be passed to the core (whether it be stateless proxy, stateful proxy, or UA) for further processing.	MUST	OUT OF SCOPE	
RFC3261-18.2-1	18.2.1	Receiving Requests	A server SHOULD be prepared to receive requests on any IP address, port and transport combination that can be the result of a DNS lookup on a SIP or SIPS URI [4] that is handed out for the purposes of communicating with that server.	SHOULD	OUT OF SCOPE	
RFC3261-18.2-2			It is also RECOMMENDED that a server listen for requests on the default SIP ports (5060 for TCP and UDP, 5061 for TLS over TCP) on all public interfaces.	RECOMMENDED	NOT REQUIRED	
RFC3261-18.2-3			For any port and interface that a server listens on for UDP, it MUST listen on that same port and interface for TCP.	MUST	NOT REQUIRED	
RFC3261-18.2-4			When the server transport receives a request over any transport, it MUST examine the value of the "sent-by" parameter in the top Via header field value.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−18.2−5			If the host portion of the ″sent−by″ parameter contains a domain name, or if it contains an IP address that differs from the packet source address, the server MUST add a ″received″ parameter to that Via header field value.	MUST	BASIC	generic_200−NOTIFY generic_180−INVITE generic_200−INVITE generic_200−BYE generic_200−CANCEL generic_3XX−6XX generic_200−OPTIONS
RFC3261−18.2−6			This parameter MUST contain the source address from which the packet was received.	MUST	BASIC	generic_200−NOTIFY generic_180−INVITE generic_200−INVITE generic_200−BYE generic_200−CANCEL generic_3XX−6XX generic_200−OPTIONS
RFC3261−18.2−7	18.2.2	Sending Responses	It MUST follow the following process:	MUST	BASIC	doc_reference
RFC3261−18.2−8			If the ″sent−protocol″ is a reliable transport protocol such as TCP or SCTP, or TLS over those, the response MUST be sent using the existing connection to the source of the original request that created the transaction, if that connection is still open.	MUST	NOT REQUIRED	
RFC3261−18.2−9			If that connection is no longer open, the server SHOULD open a connection to the IP address in the ″received″ parameter, if present, using the port in the ″sent−by″ value, or the default port for that transport, if no port is specified.	SHOULD	OUT OF SCOPE	
RFC3261−18.2−10			If that connection attempt fails, the server SHOULD use the procedures in [4] for servers in order to determine the IP address and port to open the connection and send the response to.	SHOULD	NOT REQUIRED	
RFC3261−18.2−11			Otherwise, if the Via header field value contains a ″maddr″ parameter, the response MUST be forwarded to the address listed there, using the port indicated in ″sent−by″, or port 5060 if none is present.	MUST	ADVANCED	
RFC3261−18.2−12			If the address is a multicast address, the response SHOULD be sent using the TTL indicated in the ″ttl″ parameter, or with a TTL of 1 if that parameter is not present.	SHOULD	NOT REQUIRED	
RFC3261−18.2−13			Otherwise (for unreliable unicast transports), if the top Via has a ″received″ parameter, the response MUST be sent to the address in the ″received″ parameter, using the port indicated in the ″sent−by″ value, or using port 5060 if none is specified explicitly.	MUST	BASIC	generic_200−NOTIFY generic_180−INVITE generic_200−INVITE generic_200−BYE generic_200−CANCEL generic_3XX−6XX generic_200−OPTIONS
RFC3261−18.2−14			If this fails, for example, elicits an ICMP ″port unreachable″ response, the procedures of Section 5 of [4] SHOULD be used to determine where to send the response.	SHOULD	NOT REQUIRED	
RFC3261−18.2−15			Otherwise, if it is not receiver−tagged, the response MUST be sent to the address indicated by the ″sent−by″ value, using the procedures in Section 5 of [4].	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-18.3-1	18.3	Framing	If there are additional bytes in the transport packet beyond the end of the body, they MUST be discarded.	MUST	OUT OF SCOPE	
RFC3261-18.3-2			If the message is a response, it MUST be discarded.	MUST	OUT OF SCOPE	
RFC3261-18.3-3			If the message is a request, the element SHOULD generate a 400 (Bad Request) response.	SHOULD	BASIC	reference (UE-SR-B-1-AKA) (UE-SR-B-1-DIP)
RFC3261-18.3-4			The Content- Length header field MUST be used with stream oriented transports.	MUST	NOT REQUIRED	
RFC3261-18.4-1	18.4	Error Handling	Host, network, port or protocol unreachable errors, or parameter problem errors SHOULD cause the transport layer to inform the transport user of a failure in sending.	SHOULD	OUT OF SCOPE	
RFC3261-18.4-2			Source quench and TTL exceeded ICMP errors SHOULD be ignored.	SHOULD	NOT REQUIRED	
RFC3261-18.4-3			If the transport user asks for a request to be sent over a reliable transport, and the result is a connection failure, the transport layer SHOULD inform the transport user of a failure in sending.	SHOULD	NOT REQUIRED	
RFC3261-19.1-1	19.1.1	SIP and SIPS URI Components	If the @ sign is present in a SIP or SIPS URI, the user field MUST NOT be empty.	MUST NOT	OUT OF SCOPE	
RFC3261-19.1-2			While the SIP and SIPS URI syntax allows this field to be present, its use is NOT RECOMMENDED, because the passing of authentication information in clear text (such as URIs) has proven to be a security risk in almost every case where it has been used.	NOT RECOMMENDED	NOT REQUIRED	
RFC3261-19.1-3			Using the fully-qualified domain name form is RECOMMENDED whenever possible.	RECOMMENDED	OUT OF SCOPE	
RFC3261-19.1-4			Even though an arbitrary number of URI parameters may be included in a URI, any given parameter-name MUST NOT appear more than once.	MUST NOT	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−19.1−5			For a SIPS URI, the transport parameter MUST indicate a reliable transport.	MUST	NOT REQUIRED	
RFC3261−19.1−6			The ttl parameter determines the time−to−live value of the UDP multicast packet and MUST only be used if maddr is a multicast address and the transport protocol is UDP.	MUST	NOT REQUIRED	
RFC3261−19.1−7			If the user string contains a telephone number formatted as a telephone−subscriber, the user parameter value ″phone″ SHOULD be present.	SHOULD	ADVANCED	
RFC3261−19.1−8			Since the uri−parameter mechanism is extensible, SIP elements MUST silently ignore any uri−parameters that they do not understand.	MUST	NOT REQUIRED	
RFC3261−19.1−9			Elements processing URIs SHOULD ignore any disallowed components if they are present.	SHOULD	NOT REQUIRED	
RFC3261−19.1−10	19.1.2	Character Escaping Requirements	Excluded US− ASCII characters (RFC 2396 [5]), such as space and control characters and characters used as URI delimiters, also MUST be escaped.	MUST	NOT REQUIRED	
RFC3261−19.1−11			URIs MUST NOT contain unescaped space and control characters.	MUST NOT	NOT REQUIRED	
RFC3261−19.1−12			All other characters MUST be escaped.	MUST	NOT REQUIRED	
RFC3261−19.1−13			Expanding the hname and hvalue tokens in Section 25 show that all URI reserved characters in header field names and values MUST be escaped.	MUST	NOT REQUIRED	
RFC3261−19.1−14			Any characters occurring in a telephone−subscriber that do not appear in an expansion of the BNF for the user rule MUST be escaped.	MUST	NOT REQUIRED	
RFC3261−19.1−15			Current implementations MUST NOT attempt to improve robustness by treating received escaped characters in the host component as literally equivalent to their unescaped counterpart.	MUST NOT	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−19.1−16	19.1.4	URI Comparison	Any present header component MUST be present in both URIs and match for the URIs to match.	MUST	OUT OF SCOPE	
RFC3261−19.1−17	19.1.5	Forming Requests from a URI	An implementation MUST include any provided transport, maddr, ttl, or user parameter in the Request−URI of the formed request.	MUST	NOT REQUIRED	
RFC3261−19.1−18			If the URI contains a method parameter, its value MUST be used as the method of the request.	MUST	NOT REQUIRED	
RFC3261−19.1−19			The method parameter MUST NOT be placed in the Request−URI.	MUST NOT	NOT REQUIRED	
RFC3261−19.1−20			Unknown URI parameters MUST be placed in the message's Request−URI.	MUST	NOT REQUIRED	
RFC3261−19.1−21			An implementation SHOULD treat the presence of any headers or body parts in the URI as a desire to include them in the message, and choose to honor the request on a per−component basis.	SHOULD	OUT OF SCOPE	
RFC3261−19.1−22			An implementation SHOULD NOT honor these obviously dangerous header fields: From, Call−ID, CSeq, Via, and Record−Route.	SHOULD NOT	OUT OF SCOPE	
RFC3261−19.1−23			An implementation SHOULD NOT honor any requested Route header field values in order to not be used as an unwitting agent in malicious attacks.	SHOULD NOT	OUT OF SCOPE	
RFC3261−19.1−24			An implementation SHOULD NOT honor requests to include header fields that may cause it to falsely advertise its location or capabilities.	SHOULD NOT	OUT OF SCOPE	
RFC3261−19.1−25			An implementation SHOULD verify the accuracy of any requested descriptive header fields, including: Content−Disposition, Content− Encoding, Content−Language, Content−Length, Content−Type, Date, Mime−Version, and Timestamp.	SHOULD	OUT OF SCOPE	
RFC3261−19.1−26			An implementation MUST NOT proceed with transmitting the request.	MUST NOT	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−19.1−27			An implementation SHOULD refuse to send these requests rather than modifying them to match their capabilities.	SHOULD	OUT OF SCOPE	
RFC3261−19.1−28			An implementation MUST NOT send a request requiring an extension that it does not support.	MUST NOT	OUT OF SCOPE	
RFC3261−19.1−29	19.1.6	Relating SIP URIs and tel URLs	To mitigate this problem, elements constructing telephone−subscriber fields to place in the userinfo part of a SIP or SIPS URI SHOULD fold any case−insensitive portion of telephone−subscriber to lower case, and order the telephone−subscriber parameters lexically by parameter name, excepting isdn−subaddress and post−dial, which occur first and in that order.	SHOULD	ADVANCED	
RFC3261−19.3−1	19.3	Tags	When a tag is generated by a UA for insertion into a request or response, it MUST be globally unique and cryptographically random with at least 32 bits of randomness.	MUST	OUT OF SCOPE	
RFC3261−20−1	20	Header Fields	m*: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field.	SHOULD	OUT OF SCOPE	
RFC3261−20−2			t: The header field SHOULD be sent, but clients/servers need to be prepared to receive messages without that header field.	SHOULD	OUT OF SCOPE	
RFC3261−20−3			If a stream−based protocol (such as TCP) is used as a transport, then the header field MUST be sent.	MUST	NOT REQUIRED	
RFC3261−20−4			A ″mandatory″ header field MUST be present in a request, and MUST be understood by the UAS receiving the request.	MUST	NOT REQUIRED	
RFC3261−20−5				MUST	NOT REQUIRED	
RFC3261−20−6			A mandatory response header field MUST be present in the response, and the header field MUST be understood by the UAC processing the response.	MUST	NOT REQUIRED	
RFC3261−20−7				MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-20-8			″Not applicable″ means that the header field MUST NOT be present in a request.	MUST NOT	NOT REQUIRED	
RFC3261-20-9			If one is placed in a request by mistake, it MUST be ignored by the UAS receiving the request.	MUST	NOT REQUIRED	
RFC3261-20-10			Similarly, a header field labeled ″not applicable″ for a response means that the UAS MUST NOT place the header field in the response, and the UAC MUST ignore the header field in the response.	MUST NOT	NOT REQUIRED	
RFC3261-20-11				MUST	NOT REQUIRED	
RFC3261-20-12			A UA SHOULD ignore extension header parameters that are not understood.	SHOULD	NOT REQUIRED	
RFC3261-20-13			If the URI contains a comma, question mark or semicolon, the URI MUST be enclosed in angle brackets (< and >).	MUST	OUT OF SCOPE	
RFC3261-20.1-1	20.1	Accept	The semantics are also identical, with the exception that if no Accept header field is present, the server SHOULD assume a default value of application/sdp.	SHOULD	OUT OF SCOPE	
RFC3261-20.2-1	20.2	Accept-Encoding	If no Accept-Encoding header field is present, the server SHOULD assume a default value of identity.	SHOULD	OUT OF SCOPE	
RFC3261-20.3-1	20.3	Accept-Language	If no Accept-Language header field is present, the server SHOULD assume all languages are acceptable to the client.	SHOULD	OUT OF SCOPE	
RFC3261-20.4-1	20.4	Alert-Info	In addition, a user SHOULD be able to disable this feature selectively.	SHOULD	OUT OF SCOPE	
RFC3261-20.5-1	20.5	Allow	All methods, including ACK and CANCEL, understood by the UA MUST be included in the list of methods in the Allow header field, when present.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−20.5−2			The absence of an Allow header field MUST NOT be interpreted to mean that the UA sending the message supports no methods.	MUST NOT	OUT OF SCOPE	
RFC3261−20.7−1	20.7	Authorization	Although not a comma− separated list, this header field name may be present multiple times, and MUST NOT be combined into a single header line using the usual rules described in Section 7.3.	MUST NOT	OUT OF SCOPE	
RFC3261−20.9−1	20.9	Call−Info	Therefore, it is RECOMMENDED that a UA only render the information in the Call−Info header field if it can verify the authenticity of the element that originated the header field and trusts that element.	RECOMMENDED	OUT OF SCOPE	
RFC3261−20.10−1	20.10	Contact	Even if the "display−name" is empty, the "name−addr" form MUST be used if the "addr−spec" contains a comma, semicolon, or question mark.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_200−INVITE
RFC3261−20.11−1	20.11	Content−Disposition	For backward−compatibility, if the Content−Disposition header field is missing, the server SHOULD assume bodies of Content−Type application/sdp are the disposition "session", while other content types are "render".	SHOULD	OUT OF SCOPE	
RFC3261−20.11−2			If the handling parameter is missing, the value "required" SHOULD be assumed.	SHOULD	OUT OF SCOPE	
RFC3261−20.12−1	20.12	Content−Encoding	When present, its value indicates what additional content codings have been applied to the entity−body, and thus what decoding mechanisms MUST be applied in order to obtain the media−type referenced by the Content−Type header field.	MUST	OUT OF SCOPE	
RFC3261−20.12−2			If multiple encodings have been applied to an entity−body, the content codings MUST be listed in the order in which they were applied.	MUST	NOT REQUIRED	
RFC3261−20.12−3			The server MUST only use encodings listed in the Accept−Encoding header field in the request.	MUST	NOT REQUIRED	
RFC3261−20.14−1	20.14	Content−Length	Applications SHOULD use this field to indicate the size of the message−body to be transferred, regardless of the media type of the entity.	SHOULD	BASIC	generic_sip_message
RFC3261−20.14−2			If a stream−based protocol (such as TCP) is used as transport, the header field MUST be used.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-20.14-3			If no body is present in a message, then the Content-Length header field value MUST be set to zero.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_200-NOTIFY generic_180-INVITE generic_ACK generic_BYE generic_200-BYE generic_CANCEL generic_ACK-non2XX generic_200-CANCEL generic_3XX-6XX generic_OPTIONS
RFC3261-20.15-1	20.15	Content-Type	The Content-Type header field MUST be present if the body is not empty.	MUST	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC3261-20.16-1	20.16	CSeq	The sequence number MUST be expressible as a 32-bit unsigned integer.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_ACK generic_BYE generic_CANCEL generic_ACK-non2XX generic_OPTIONS
RFC3261-20.20-1	20.20	From	A system SHOULD use the display name "Anonymous" if the identity of the client is to remain hidden.	SHOULD	ADVANCED	
RFC3261-20.20-2			Even if the "display- name" is empty, the "name-addr" form MUST be used if the "addr-spec" contains a comma, question mark, or semicolon.	MUST	BASIC	generic_sip_message
RFC3261-20.26-1	20.26	Priority	For these decisions, a message containing no Priority header field SHOULD be treated as if it specified a Priority of "normal".	SHOULD	NOT REQUIRED	
RFC3261-20.26-2			It is RECOMMENDED that the value of "emergency" only be used when life, limb, or property are in imminent danger.	RECOMMENDED	NOT REQUIRED	
RFC3261-20.28-1	20.28	Proxy-Authorization	Although not a comma-separated list, this header field name may be present multiple times, and MUST NOT be combined into a single header line using the usual rules described in Section 7.3.1.	MUST NOT	NOT REQUIRED	
RFC3261-20.31-1	20.31	Reply-To	If the user wished to remain anonymous, the header field SHOULD either be omitted from the request or populated in such a way that does not reveal any private information.	SHOULD	NOT REQUIRED	
RFC3261-20.31-2			Even if the "display-name" is empty, the "name-addr" form MUST be used if the "addr-spec" contains a comma, question mark, or semicolon.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-20.32-1	20.32	Require	Although an optional header field, the Require MUST NOT be ignored if it is present.	MUST NOT	NOT REQUIRED	
RFC3261-20.32-2			Each option tag defines a SIP extension that MUST be understood to process the request.	MUST	OUT OF SCOPE	
RFC3261-20.32-3			A UAC compliant to this specification MUST only include option tags corresponding to standards-track RFCs.	MUST	OUT OF SCOPE	
RFC3261-20.35-1	20.35	Server	Implementers SHOULD make the Server header field a configurable option.	SHOULD	NOT REQUIRED	
RFC3261-20.37-1	20.37	Supported	A UA compliant to this specification MUST only include option tags corresponding to standards-track RFCs.	MUST	NOT REQUIRED	
RFC3261-20.41-1	20.41	User-Agent	Implementers SHOULD make the User-Agent header field a configurable option.	SHOULD	NOT REQUIRED	
RFC3261-20.42-1	20.42	Via	For implementations compliant to this specification, the value of the branch parameter MUST start with the magic cookie "z9hG4bK", as discussed in Section 8.1.1.7.	MUST	BASIC	doc_reference
RFC3261-20.43-1	20.43	Warning	A system receiving this warning MUST NOT take any automated action.	MUST NOT	NOT REQUIRED	
RFC3261-21-1	21	Response Codes	Other HTTP/1.1 response codes SHOULD NOT be used.	SHOULD NOT	OUT OF SCOPE	
RFC3261-21.3-1	21.3.1	300 Multiple Choices	The choices SHOULD also be listed as Contact fields (Section 20.10).	SHOULD	NOT REQUIRED	
RFC3261-21.3-2	21.3.2	301 Moved Permanently	The user can no longer be found at the address in the Request-URI, and the requesting client SHOULD retry at the new address given by the Contact header field (Section 20.10).	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-21.3-3			The requestor SHOULD update any local directories, address books, and user location caches with this new value and redirect future requests to the address(es) listed.	SHOULD	NOT REQUIRED	
RFC3261-21.3-4	21.3.3	302 Moved Temporarily	The requesting client SHOULD retry the request at the new address(es) given by the Contact header field (Section 20.10).	SHOULD	NOT REQUIRED	
RFC3261-21.3-5			If there is no explicit expiration time, the address is only valid once for recursing, and MUST NOT be cached for future transactions.	MUST NOT	NOT REQUIRED	
RFC3261-21.3-6	21.3.4	305 Use Proxy	The requested resource MUST be accessed through the proxy given by the Contact field.	MUST	NOT REQUIRED	
RFC3261-21.3-7			305 (Use Proxy) responses MUST only be generated by UASs.	MUST	NOT REQUIRED	
RFC3261-21.4-1	21.4	Request Failure 4xx	The client SHOULD NOT retry the same request without modification (for example, adding appropriate authorization).	SHOULD NOT	BASIC	generic_Auth_REGISTER UE-RG-B-7-AKA UE-RG-B-11-AKA UE-RG-B-18-AKA UE-RG-B-19-AKA UE-RG-B-7-DIP UE-RG-B-11-DIP
RFC3261-21.4-2	21.4.1	400 Bad Request	The Reason-Phrase SHOULD identify the syntax problem in more detail, for example, "Missing Call-ID header field".	SHOULD	OUT OF SCOPE	
RFC3261-21.4-3	21.4.4	403 Forbidden	Authorization will not help, and the request SHOULD NOT be repeated.	SHOULD NOT	ADVANCED	UE-RG-B-18-DIP
RFC3261-21.4-4	21.4.6	405 Method Not Allowed	The response MUST include an Allow header field containing a list of valid methods for the indicated address.	MUST	BASIC	UE-SR-B-3-AKA UE-SR-B-3-DIP
RFC3261-21.4-5	21.4.8	407 Proxy Authentication Required	This code is similar to 401 (Unauthorized), but indicates that the client MUST first authenticate itself with the proxy.	MUST	OUT OF SCOPE	
RFC3261-21.4-6	21.4.10	410 Gone	If the server does not know, or has no facility to determine, whether or not the condition is permanent, the status code 404 (Not Found) SHOULD be used instead.	SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-21.4-7	21.4.11	413 Request Entity Too Large	If the condition is temporary, the server SHOULD include a Retry- After header field to indicate that it is temporary and after what time the client MAY try again.	SHOULD	OUT OF SCOPE	
RFC3261-21.4-8	21.4.13	415 Unsupported Media Type	The server MUST return a list of acceptable formats using the Accept, Accept-Encoding, or Accept-Language header field, depending on the specific problem with the content.	MUST	BASIC	UE-SR-B-6-AKA UE-SR-B-6-DIP
RFC3261-21.4-9	21.4.15	420 Bad Extension	The server MUST include a list of the unsupported extensions in an Unsupported header field in the response.	MUST	BASIC	UE-SR-B-8-AKA UE-SR-B-8-DIP
RFC3261-21.4-10	21.4.16	421 Extension Required	Responses with this status code MUST contain a Require header field listing the required extensions.	MUST	NOT REQUIRED	
RFC3261-21.4-11			A UAS SHOULD NOT use this response unless it truly cannot provide any useful service to the client.	SHOULD NOT	NOT REQUIRED	
RFC3261-21.4-12			Instead, if a desirable extension is not listed in the Supported header field, servers SHOULD process the request using baseline SIP capabilities and any extensions supported by the client.	SHOULD	NOT REQUIRED	
RFC3261-21.4-13	21.4.18	480 Temporarily Unavailable	The reason phrase SHOULD indicate a more precise cause as to why the callee is unavailable.	SHOULD	OUT OF SCOPE	
RFC3261-21.4-14			This value SHOULD be settable by the UA.	SHOULD	OUT OF SCOPE	
RFC3261-21.4-15	21.4.22	484 Address Incomplete	Additional information SHOULD be provided in the reason phrase.	SHOULD	ADVANCED	
RFC3261-21.4-16	21.4.23	485 Ambiguous	It MUST be possible to configure a server to respond with status 404 (Not Found) or to suppress the listing of possible choices for ambiguous Request-URIs.	MUST	OUT OF SCOPE	
RFC3261-21.4-17	21.4.24	486 Busy Here	Status 600 (Busy Everywhere) SHOULD be used if the client knows that no other end system will be able to accept this call.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-21.5-1	21.5.4	503 Service Unavailable	If no Retry-After is given, the client MUST act as if it had received a 500 (Server Internal Error) response.	MUST	OUT OF SCOPE	
RFC3261-21.5-2			A client (proxy or UAC) receiving a 503 (Service Unavailable) SHOULD attempt to forward the request to an alternate server.	SHOULD	NOT REQUIRED	
RFC3261-21.5-3			It SHOULD NOT forward any other requests to that server for the duration specified in the Retry-After header field, if present.	SHOULD NOT	NOT REQUIRED	
RFC3261-22-1	22	Usage of HTTP Authentication	Once the originator has been identified, the recipient of the request SHOULD ascertain whether or not this user is authorized to make the request in question.	SHOULD	NOT REQUIRED	
RFC3261-22-2			Servers MUST NOT accept credentials using the "Basic" authorization scheme, and servers also MUST NOT challenge with "Basic".	MUST NOT	NOT REQUIRED	
RFC3261-22-3				MUST NOT	NOT REQUIRED	
RFC3261-22.1-1	22.1	Framework	Additionally, registrars and redirect servers MAY make use of 401 (Unauthorized) responses for authentication, but proxies MUST NOT, and instead MAY use the 407 (Proxy Authentication Required)	MUST NOT	NOT REQUIRED	
RFC3261-22.1-2			Operators of user agents or proxy servers that will authenticate received requests MUST adhere to the following guidelines for creation of a realm string for their server:	MUST	NOT REQUIRED	
RFC3261-22.1-3			Realm strings MUST be globally unique.	MUST	NOT REQUIRED	
RFC3261-22.1-4			It is RECOMMENDED that a realm string contain a hostname or domain name, following the recommendation in Section 3.2.1 of RFC 2617 [17].	RECOMMENDED	NOT REQUIRED	
RFC3261-22.1-5			Realm strings SHOULD present a human-readable identifier that can be rendered to a user.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-22.1-6			For this reason, any credentials in the INVITE that were accepted by a server MUST be accepted by that server for the ACK.	MUST	NOT REQUIRED	
RFC3261-22.1-7			Servers MUST NOT attempt to challenge an ACK.	MUST NOT	NOT REQUIRED	
RFC3261-22.1-8			Although the CANCEL method does take a response (a 2xx), servers MUST NOT attempt to challenge CANCEL requests since these requests cannot be resubmitted.	MUST NOT	NOT REQUIRED	
RFC3261-22.1-9			Generally, a CANCEL request SHOULD be accepted by a server if it comes from the same hop that sent the request being canceled (provided that some sort of transport or network layer security association, as described in Section 26.2.1, is in place).	SHOULD	NOT REQUIRED	
RFC3261-22.1-10			When a UAC receives a challenge, it SHOULD render to the user the contents of the "realm" parameter in the challenge (which appears in either a WWW-Authenticate header field or Proxy-Authenticate header field) if the UAC device does not already know of a credential for the realm in question.	SHOULD	NOT REQUIRED	
RFC3261-22.1-11			A UAC MUST NOT re-attempt requests with the credentials that have just been rejected (though the request may be retried if the nonce was stale).	MUST NOT	ADVANCED	UE-RG-B-19-DIP
RFC3261-22.2-1	22.2	User-to-User Authentication	The WWW-Authenticate response-header field MUST be included in 401 (Unauthorized) response messages.	MUST	NOT REQUIRED	
RFC3261-22.2-2			When the originating UAC receives the 401 (Unauthorized), it SHOULD, if it is able, re-originate the request with the proper credentials.	SHOULD	NOT REQUIRED	
RFC3261-22.2-3			Once authentication credentials have been supplied (either directly by the user, or discovered in an internal keyring), UAs SHOULD cache the credentials for a given value of the To header field and "realm" and attempt to re-use these values on the next request for that destination.	SHOULD	NOT REQUIRED	
RFC3261-22.2-4			When a UAC resubmits a request with its credentials after receiving a 401 (Unauthorized) or 407 (Proxy Authentication Required) response, it MUST increment the CSeq header field value as it would normally when sending an updated request.	MUST	NOT REQUIRED	
RFC3261-22.2-5	22.3	Proxy-to-User Authentication	The proxy MUST populate the 407 (Proxy Authentication Required) message with a Proxy- Authenticate header field value applicable to the proxy for the requested resource.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-22.2-6			Proxies MUST NOT add values to the Proxy-Authorization header field.	MUST NOT	NOT REQUIRED	
RFC3261-22.2-7			All 407 (Proxy Authentication Required) responses MUST be forwarded upstream toward the UAC following the procedures for any other response.	MUST	NOT REQUIRED	
RFC3261-22.2-8			When the originating UAC receives the 407 (Proxy Authentication Required) it SHOULD, if it is able, re-originate the request with the proper credentials.	SHOULD	NOT REQUIRED	
RFC3261-22.2-9			The UAC SHOULD also cache the credentials used in the re-originated request.	SHOULD	NOT REQUIRED	
RFC3261-22.2-10			The following rule is RECOMMENDED for proxy credential caching:	RECOMMENDED	NOT REQUIRED	
RFC3261-22.2-11			These credentials MUST NOT be cached across dialogs; however, if a UA is configured with the realm of its local outbound proxy, when one exists, then the UA MAY cache credentials for that realm across dialogs.	MUST NOT	NOT REQUIRED	
RFC3261-22.2-12			When multiple proxies are used in a chain, a Proxy-Authorization header field value MUST NOT be consumed by any proxy whose realm does not match the "realm" parameter specified in that value.	MUST NOT	NOT REQUIRED	
RFC3261-22.2-13			Note that if an authentication scheme that does not support realms is used in the Proxy-Authorization header field, a proxy server MUST attempt to parse all Proxy-Authorization header field values to determine whether one of them has what the proxy server considers to be valid credentials.	MUST	NOT REQUIRED	
RFC3261-22.2-14			Because this is potentially very time- consuming in large networks, proxy servers SHOULD use an authentication scheme that supports realms in the Proxy-Authorization header field.	SHOULD	NOT REQUIRED	
RFC3261-22.2-15			Each WWW-Authenticate and Proxy-Authenticate value received in responses to the forked request MUST be placed into the single response that is sent by the forking proxy to the UA; the ordering of these header field values is not significant.	MUST	NOT REQUIRED	
RFC3261-22.2-16			As noted above, multiple credentials in a request SHOULD be differentiated by the "realm" parameter.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-22.2-17			The same credentials SHOULD be used for the same realm.	SHOULD	NOT REQUIRED	
RFC3261-22.4-18	22.4	The Digest Authentication Scheme	Since RFC 2543 is based on HTTP Digest as defined in RFC 2069 [39], SIP servers supporting RFC 2617 MUST ensure they are backwards compatible with RFC 2069.	MUST	NOT REQUIRED	
RFC3261-22.4-19			Note, however, that SIP servers MUST NOT accept or request Basic authentication.	MUST NOT	NOT REQUIRED	
RFC3261-22.4-20			For SIP, the 'uri' MUST be enclosed in quotation marks.	MUST	ADVANCED	generic_Auth_REGISTER *SIP Digest only
RFC3261-22.4-21			RFC 2617 notes that a cnonce value MUST NOT be sent in an Authorization (and by extension Proxy-Authorization) header field if no qop directive has been sent.	MUST NOT	NOT REQUIRED	
RFC3261-22.4-22			However, servers MUST always send a "qop" parameter in WWW-Authenticate and Proxy-Authenticate header field values.	MUST	NOT REQUIRED	
RFC3261-22.4-23			If a client receives a "qop" parameter in a challenge header field, it MUST send the "qop" parameter in any resulting authorization header field.	MUST	ADVANCED	generic_Auth_REGISTER *SIP Digest only
RFC3261-22.4-24			These mechanisms MUST be used by a server to determine if the client supports the new mechanisms in RFC 2617 that were not specified in RFC 2069.	MUST	NOT REQUIRED	
RFC3261-23.1-1	23.1	S/MIME Certificates	Each user agent that supports S/MIME MUST contain a keyring specifically for end-users' certificates.	MUST	NOT REQUIRED	
RFC3261-23.1-2			Over time, users SHOULD use the same certificate when they populate the originating URI of signaling (the From header field) with the same address-of-record.	SHOULD	NOT REQUIRED	
RFC3261-23.1-3			However, users SHOULD acquire certificates from known public certificate authorities.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-23.1-4			However, the holder of a certificate SHOULD publish their certificate in any public directories as appropriate.	SHOULD	NOT REQUIRED	
RFC3261-23.1-5			Similarly, UACs SHOULD support a mechanism for importing (manually or automatically) certificates discovered in public directories corresponding to the target URIs of SIP requests.	SHOULD	NOT REQUIRED	
RFC3261-23.2-1	23.2	S/MIME Key Exchange	Whenever the CMS SignedData message is used in S/MIME for SIP, it MUST contain the certificate bearing the public key necessary to verify the signature.	MUST	NOT REQUIRED	
RFC3261-23.2-2			When a UAC sends a request containing an S/MIME body that initiates a dialog, or sends a non-INVITE request outside the context of a dialog, the UAC SHOULD structure the body as an S/MIME 'multipart/signed' CMS SignedData body.	SHOULD	NOT REQUIRED	
RFC3261-23.2-3			If the desired CMS service is EnvelopedData (and the public key of the target user is known), the UAC SHOULD send the EnvelopedData message encapsulated within a SignedData message.	SHOULD	NOT REQUIRED	
RFC3261-23.2-4			When a UAS receives a request containing an S/MIME CMS body that includes a certificate, the UAS SHOULD first validate the certificate, if possible, with any available root certificates for certificate authorities.	SHOULD	NOT REQUIRED	
RFC3261-23.2-5			The UAS SHOULD also determine the subject of the certificate (for S/MIME, the SubjectAltName will contain the appropriate identity) and compare this value to the From header field of the request.	SHOULD	NOT REQUIRED	
RFC3261-23.2-6			If the certificate cannot be verified, because it is self-signed, or signed by no known authority, or if it is verifiable but its subject does not correspond to the From header field of request, the UAS MUST notify its user of the status of the certificate (including the subject of the certificate, its signer, and any key fingerprint information) and request explicit permission before proceeding.	MUST	NOT REQUIRED	
RFC3261-23.2-7			If the certificate was successfully verified and the subject of the certificate corresponds to the From header field of the SIP request, or if the user (after notification) explicitly authorizes the use of the certificate, the UAS SHOULD add this certificate to a local keyring, indexed by the address-of-record of the holder of the certificate.	SHOULD	NOT REQUIRED	
RFC3261-23.2-8			When a UAS sends a response containing an S/MIME body that answers the first request in a dialog, or a response to a non-INVITE request outside the context of a dialog, the UAS SHOULD structure the body as an S/MIME 'multipart/signed' CMS SignedData body.	SHOULD	NOT REQUIRED	
RFC3261-23.2-9			If the desired CMS service is EnvelopedData, the UAS SHOULD send the EnvelopedData message encapsulated within a SignedData message.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-23.2-10			When a UAC receives a response containing an S/MIME CMS body that includes a certificate, the UAC SHOULD first validate the certificate, if possible, with any appropriate root certificate.	SHOULD	NOT REQUIRED	
RFC3261-23.2-11			The UAC SHOULD also determine the subject of the certificate and compare this value to the To field of the response; although the two may very well be different, and this is not necessarily indicative of a security breach.	SHOULD	NOT REQUIRED	
RFC3261-23.2-12			If the certificate cannot be verified because it is self-signed, or signed by no known authority, the UAC MUST notify its user of the status of the certificate (including the subject of the certificate, its signator, and any key fingerprint information) and request explicit permission before proceeding.	MUST	NOT REQUIRED	
RFC3261-23.2-13			If the certificate was successfully verified, and the subject of the certificate corresponds to the To header field in the response, or if the user (after notification) explicitly authorizes the use of the certificate, the UAC SHOULD add this certificate to a local keyring, indexed by the address-of-record of the holder of the certificate.	SHOULD	NOT REQUIRED	
RFC3261-23.2-14			If the UAC had not transmitted its own certificate to the UAS in any previous transaction, it SHOULD use a CMS SignedData body for its next request or response.	SHOULD	NOT REQUIRED	
RFC3261-23.2-15			On future occasions, when the UA receives requests or responses that contain a From header field corresponding to a value in its keyring, the UA SHOULD compare the certificate offered in these messages with the existing certificate in its keyring.	SHOULD	NOT REQUIRED	
RFC3261-23.2-16			If there is a discrepancy, the UA MUST notify its user of a change of the certificate (preferably in terms that indicate that this is a potential security breach) and acquire the user's permission before continuing to process the signaling.	MUST	NOT REQUIRED	
RFC3261-23.2-17			If the user authorizes this certificate, it SHOULD be added to the keyring alongside any previous value(s) for this address-of-record.	SHOULD	NOT REQUIRED	
RFC3261-23.2-18			If a UA receives an S/MIME body that has been encrypted with a public key unknown to the recipient, it MUST reject the request with a 493 (Undecipherable) response.	MUST	NOT REQUIRED	
RFC3261-23.2-19			This response SHOULD contain a valid certificate for the respondent (corresponding, if possible, to any address of record given in the To header field of the rejected request) within a MIME body with a 'certs-only' "smime-type" parameter.	SHOULD	NOT REQUIRED	
RFC3261-23.2-20			Note that a user agent that receives a request containing an S/MIME body that is not optional (with a Content-Disposition header "handling" parameter of "required") MUST reject the request with a 415 Unsupported Media Type response if the MIME type is not understood.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−23.2−21			A user agent that receives such a response when S/MIME is sent SHOULD notify its user that the remote device does not support S/MIME, and it MAY subsequently resend the request without S/MIME, if appropriate; however, this 415 response may constitute a downgrade attack.	SHOULD	NOT REQUIRED	
RFC3261−23.2−22			If a user agent sends an S/MIME body in a request, but receives a response that contains a MIME body that is not secured, the UAC SHOULD notify its user that the session could not be secured.	SHOULD	NOT REQUIRED	
RFC3261−23.2−23			However, if a user agent that supports S/MIME receives a request with an unsecured body, it SHOULD NOT respond with a secured body, but if it expects S/MIME from the sender (for example, because the sender's From header field value corresponds to an identity on its keychain), the UAS SHOULD notify its user that the session could not be secured.	SHOULD NOT	NOT REQUIRED	
RFC3261−23.2−24				SHOULD	NOT REQUIRED	
RFC3261−23.2−25			Finally, if during the course of a dialog a UA receives a certificate in a CMS SignedData message that does not correspond with the certificates previously exchanged during a dialog, the UA MUST notify its user of the change, preferably in terms that indicate that this is a potential security breach.	MUST	NOT REQUIRED	
RFC3261−23.3−1	23.3	Securing MIME bodies	"multipart/signed" MUST be used only with CMS detached signatures.	MUST	NOT REQUIRED	
RFC3261−23.3−2			S/MIME bodies SHOULD have a Content−Disposition header field, and the value of the "handling" parameter SHOULD be "required."	SHOULD	NOT REQUIRED	
RFC3261−23.3−3				SHOULD	NOT REQUIRED	
RFC3261−23.3−4			UACs MAY send an initial request such as an OPTIONS message with a CMS detached signature in order to solicit the certificate of the remote side (the signature SHOULD be over a "message/sip" body of the type described in Section 23.4).	SHOULD	NOT REQUIRED	
RFC3261−23.3−5			Senders of S/MIME bodies SHOULD use the "SMIMECapabilities" (see Section 2.5.2 of [24]) attribute to express their capabilities and preferences for further communications.	SHOULD	NOT REQUIRED	
RFC3261−23.3−6			S/MIME implementations MUST at a minimum support SHA1 as a digital signature algorithm, and 3DES as an encryption algorithm.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-23.3-7			Each S/MIME body in a SIP message SHOULD be signed with only one certificate.	SHOULD	NOT REQUIRED	
RFC3261-23.3-8			Parallel signatures SHOULD NOT be used.	SHOULD NOT	NOT REQUIRED	
RFC3261-23.4-1	23.4	SIP Header Privacy and Integrity using S/MIME: Tunneling SIP	If a UAS receives a request that contains a tunneled "message/sip" S/MIME body, it SHOULD include a tunneled "message/sip" body in the response with the same smime-type.	SHOULD	NOT REQUIRED	
RFC3261-23.4-2			Any traditional MIME bodies (such as SDP) SHOULD be attached to the "inner" message so that they can also benefit from S/MIME security.	SHOULD	NOT REQUIRED	
RFC3261-23.4-3	23.4.1	Integrity and Confidentiality Properties of SIP Headers	Note that for the purposes of loose timestamping, all SIP messages that tunnel "message/sip" SHOULD contain a Date header in both the "inner" and "outer" headers.	SHOULD	NOT REQUIRED	
RFC3261-23.4-4	23.4.1.1	Integrity	If these header fields are not intact end-to-end, implementations SHOULD NOT consider this a breach of security.	SHOULD NOT	NOT REQUIRED	
RFC3261-23.4-5			Changes to any other header fields defined in this document constitute an integrity violation; users MUST be notified of a discrepancy.	MUST	NOT REQUIRED	
RFC3261-23.4-6	23.4.1.2	Confidentiality	If the From header field in an encrypted body differs from the value in the "outer" message, the value within the encrypted body SHOULD be displayed to the user, but MUST NOT be used in the "outer" header fields of any future messages.	SHOULD	NOT REQUIRED	
RFC3261-23.4-7				MUST NOT	NOT REQUIRED	
RFC3261-23.4-8			They SHOULD NOT however be used in the "outer" headers of any future messages.	SHOULD NOT	NOT REQUIRED	
RFC3261-23.4-9			If present, the Date header field MUST always be the same in the "inner" and "outer" headers.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261−23.4−10			UAs SHOULD never include these in an "inner" message if they are not included in the "outer" message.	SHOULD	NOT REQUIRED	
RFC3261−23.4−11			UAs that receive any of these header fields in an encrypted body SHOULD ignore the encrypted values.	SHOULD	NOT REQUIRED	
RFC3261−23.4−12			If a SIP UA encounters an unknown header field with an integrity violation, it MUST ignore the header field.	MUST	NOT REQUIRED	
RFC3261−23.4−13	23.4.2	Tunneling Integrity and Authentication	In order to eliminate possible confusions about the addition or subtraction of entire header fields, senders SHOULD replicate all header fields from the request within the signed body.	SHOULD	NOT REQUIRED	
RFC3261−23.4−14			Any message bodies that require integrity protection MUST be attached to the "inner" message.	MUST	NOT REQUIRED	
RFC3261−23.4−15			If a Date header is present in a message with a signed body, the recipient SHOULD compare the header field value with its own internal clock, if applicable.	SHOULD	NOT REQUIRED	
RFC3261−23.4−16			If a significant time discrepancy is detected (on the order of an hour or more), the user agent SHOULD alert the user to the anomaly, and note that it is a potential security breach.	SHOULD	NOT REQUIRED	
RFC3261−23.4−17			UAs SHOULD notify users of this circumstance and request explicit guidance on how to proceed.	SHOULD	NOT REQUIRED	
RFC3261−23.4−18	23.4.3	Tunneling Encryption	The message must first be decrypted, and the "inner" From header field MUST be used as an index.	MUST	NOT REQUIRED	
RFC3261−23.4−19			In order to provide end−to−end integrity, encrypted "message/sip" MIME bodies SHOULD be signed by the sender.	SHOULD	NOT REQUIRED	
RFC3261−25.1−1	25.1	Basic Rules	These special characters MUST be in a quoted string to be used within a parameter value.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-25.1-2			Note, however, that any characters allowed there that are not allowed in the user part of the SIP URI MUST be escaped.	MUST	NOT REQUIRED	
RFC3261-26.2-1	26.2.1	Transport and Network Layer Security	The TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite [6] MUST be supported at a minimum by implementers when TLS is used in a SIP application.	MUST	NOT REQUIRED	
RFC3261-26.2-2			For purposes of backwards compatibility, proxy servers, redirect servers, and registrars SHOULD support TLS_RSA_WITH_3DES_EDE_CBC_SHA.	SHOULD	NOT REQUIRED	
RFC3261-26.2-3	26.2.2	SIPS URI Scheme	The use of SIPS in particular entails that mutual TLS authentication SHOULD be employed, as SHOULD the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA.	SHOULD	NOT REQUIRED	
RFC3261-26.2-4				SHOULD	NOT REQUIRED	
RFC3261-26.2-5			Certificates received in the authentication process SHOULD be validated with root certificates held by the client; failure to validate a certificate SHOULD result in the failure of the request.	SHOULD	NOT REQUIRED	
RFC3261-26.2-6				SHOULD	NOT REQUIRED	
RFC3261-26.3-1	26.3.1	Requirements for Implementers of SIP	Proxy servers, redirect servers, and registrars MUST implement TLS, and MUST support both mutual and one-way authentication.	MUST	NOT REQUIRED	
RFC3261-26.3-2				MUST	NOT REQUIRED	
RFC3261-26.3-3			It is strongly RECOMMENDED that UAs be capable initiating TLS; UAs MAY also be capable of acting as a TLS server.	RECOMMENDED	NOT REQUIRED	
RFC3261-26.3-4			Proxy servers, redirect servers, and registrars SHOULD possess a site certificate whose subject corresponds to their canonical hostname.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-26.3-5			All SIP elements that support TLS MUST have a mechanism for validating certificates received during TLS negotiation; this entails possession of one or more root certificates issued by certificate authorities (preferably well-known distributors of site certificates comparable to those that issue root certificates for web browsers).	MUST	NOT REQUIRED	
RFC3261-26.3-6			All SIP elements that support TLS MUST also support the SIPS URI scheme.	MUST	NOT REQUIRED	
RFC3261-26.3-7			When a UA attempts to contact a proxy server, redirect server, or registrar, the UAC SHOULD initiate a TLS connection over which it will send SIP messages.	SHOULD	NOT REQUIRED	
RFC3261-26.3-8			Proxy servers, redirect servers, registrars, and UAs MUST implement Digest Authorization, encompassing all of the aspects required in 22.	MUST	NOT REQUIRED	
RFC3261-26.3-9			Proxy servers, redirect servers, and registrars SHOULD be configured with at least one Digest realm, and at least one "realm" string supported by a given server SHOULD correspond to the server's hostname or domainname.	SHOULD	NOT REQUIRED	
RFC3261-26.3-10				SHOULD	NOT REQUIRED	
RFC3261-26.3-11			If a UA holds one or more root certificates of certificate authorities in order to validate certificates for TLS or IPSec, it SHOULD be capable of reusing these to verify S/MIME certificates, as appropriate.	SHOULD	NOT REQUIRED	
RFC3261-26.3-12	26.3.2.1	Registration	When a UA comes online and registers with its local administrative domain, it SHOULD establish a TLS connection with its registrar (Section 10 describes how the UA reaches its registrar).	SHOULD	NOT REQUIRED	
RFC3261-26.3-13			The registrar SHOULD offer a certificate to the UA, and the site identified by the certificate MUST correspond with the domain in which the UA intends to register; for example, if the UA intends to register the address-of-record 'alice@atlanta.com', the site certificate must identify a host within the atlanta.com domain (such as sip.atlanta.com).	SHOULD	NOT REQUIRED	
RFC3261-26.3-14				MUST	NOT REQUIRED	
RFC3261-26.3-15			When it receives the TLS Certificate message, the UA SHOULD verify the certificate and inspect the site identified by the certificate.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-26.3-16			If the certificate is invalid, revoked, or if it does not identify the appropriate party, the UA MUST NOT send the REGISTER message and otherwise proceed with the registration.	MUST NOT	NOT REQUIRED	
RFC3261-26.3-17			The UA then creates a REGISTER request that SHOULD be addressed to a Request-URI corresponding to the site certificate received from the registrar.	SHOULD	NOT REQUIRED	
RFC3261-26.3-18			When the UA sends the REGISTER request over the existing TLS connection, the registrar SHOULD challenge the request with a 401 (Proxy Authentication Required) response.	SHOULD	NOT REQUIRED	
RFC3261-26.3-19			The "realm" parameter within the Proxy-Authenticate header field of the response SHOULD correspond to the domain previously given by the site certificate.	SHOULD	NOT REQUIRED	
RFC3261-26.3-20			When the UAC receives the challenge, it SHOULD either prompt the user for credentials or take an appropriate credential from a keyring corresponding to the "realm" parameter in the challenge.	SHOULD	NOT REQUIRED	
RFC3261-26.3-21			The username of this credential SHOULD correspond with the "userinfo" portion of the URI in the To header field of the REGISTER request.	SHOULD	NOT REQUIRED	
RFC3261-26.3-22			Once the registration has been accepted by the registrar, the UA SHOULD leave this TLS connection open provided that the registrar also acts as the proxy server to which requests are sent for users in this administrative domain.	SHOULD	NOT REQUIRED	
RFC3261-26.3-23	26.3.2.2	Interdomain Requests	Assuming that the client has completed the registration process described in the preceding section, it SHOULD reuse the TLS connection to the local proxy server when it sends an INVITE request to another user.	SHOULD	NOT REQUIRED	
RFC3261-26.3-24			The UA SHOULD reuse cached credentials in the INVITE to avoid prompting the user unnecessarily.	SHOULD	NOT REQUIRED	
RFC3261-26.3-25			When the local outbound proxy server has validated the credentials presented by the UA in the INVITE, it SHOULD inspect the Request-URI to determine how the message should be routed (see [4]).	SHOULD	NOT REQUIRED	
RFC3261-26.3-26			The local outbound proxy server at atlanta.com SHOULD therefore establish a TLS connection with the remote proxy server at biloxi.com.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-26.3-27			Since both of the participants in this TLS connection are servers that possess site certificates, mutual TLS authentication SHOULD occur.	SHOULD	NOT REQUIRED	
RFC3261-26.3-28			Each side of the connection SHOULD verify and inspect the certificate of the other, noting the domain name that appears in the certificate for comparison with the header fields of SIP messages.	SHOULD	NOT REQUIRED	
RFC3261-26.3-29			The atlanta.com proxy server, for example, SHOULD verify at this stage that the certificate received from the remote side corresponds with the biloxi.com domain.	SHOULD	NOT REQUIRED	
RFC3261-26.3-30			The proxy server at biloxi.com SHOULD inspect the certificate of the proxy server at atlanta.com in turn and compare the domain asserted by the certificate with the "domainname" portion of the From header field in the INVITE request.	SHOULD	NOT REQUIRED	
RFC3261-26.3-31			Once the INVITE has been approved by the biloxi proxy, the proxy server SHOULD identify the existing TLS channel, if any, associated with the user targeted by this request (in this case "bob@biloxi.com").	SHOULD	NOT REQUIRED	
RFC3261-26.3-32			Before they forward the request, both proxy servers SHOULD add a Record-Route header field to the request so that all future requests in this dialog will pass through the proxy servers.	SHOULD	NOT REQUIRED	
RFC3261-26.3-33	26.3.2.3	Peer-to-Peer Requests	When Carol wishes to send an INVITE to "bob@biloxi.com", her UA SHOULD initiate a TLS connection with the biloxi proxy directly (using the mechanism described in [4] to determine how to best to reach the given Request-URI).	SHOULD	NOT REQUIRED	
RFC3261-26.3-34			When her UA receives a certificate from the biloxi proxy, it SHOULD be verified normally before she passes her INVITE across the TLS connection.	SHOULD	NOT REQUIRED	
RFC3261-26.3-35			Carol SHOULD then establish a TCP connection with the designated address and send a new INVITE with a Request-URI containing the received contact address (recomputing the signature in the body as the request is readied).	SHOULD	NOT REQUIRED	
RFC3261-26.3-36	26.3.2.4	DoS Protection	When the host on which a SIP proxy server is operating is routable from the public Internet, it SHOULD be deployed in an administrative domain with defensive operational policies (blocking source-routed traffic, preferably filtering ping traffic).	SHOULD	NOT REQUIRED	
RFC3261-26.3-37			UAs and proxy servers SHOULD challenge questionable requests with only a single 401 (Unauthorized) or 407 (Proxy Authentication Required), forgoing the normal response retransmission algorithm, and thus behaving statelessly towards unauthenticated requests.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3261-26.4-1	26.4.2	S/MIME	For that reason, it is RECOMMENDED that TCP should be used as a transport protocol when S/MIME tunneling is employed.	RECOMMENDED	NOT REQUIRED	
RFC3261-26.4-2	26.4.4	SIPS URIs	To address these concerns, it is RECOMMENDED that recipients of a request whose Request-URI contains a SIP or SIPS URI inspect the To header field value to see if it contains a SIPS URI (though note that it does not constitute a breach of security if this URI has the same scheme but is not equivalent to the URI in the To header field).	RECOMMENDED	NOT REQUIRED	
RFC3261-26.4-3			If the UAS has reason to believe that the scheme of the Request-URI has been improperly modified in transit, the UA SHOULD notify its user of a potential security breach.	SHOULD	NOT REQUIRED	
RFC3261-26.5-1	26.5	Privacy	A user location service can infringe on the privacy of the recipient of a session invitation by divulging their specific whereabouts to the caller; an implementation consequently SHOULD be able to restrict, on a per-user basis, what kind of location and availability information is given out to certain classes of callers.	SHOULD	OUT OF SCOPE	
RFC3261-27.1-1	27.1	Option Tags	The name MAY be of any length, but SHOULD be no more than twenty characters long.	SHOULD	NOT REQUIRED	
RFC3261-27.1-2			The name MUST consist of alphanum (Section 25) characters only.	MUST	NOT REQUIRED	
RFC3261-28.1-1	28.1	Major Functional Changes	This was changed to MUST.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC2617-1-1	1.2	Access Authentication Framework	This response MUST include a WWW-Authenticate header field containing at least one challenge applicable to the requested resource.	MUST	OUT OF SCOPE	
RFC2617-1-2			The 407 (Proxy Authentication Required) response message is used by a proxy to challenge the authorization of a client and MUST include a Proxy- Authenticate header field containing at least one challenge applicable to the proxy for the requested resource.	MUST	OUT OF SCOPE	
RFC2617-1-3			The user agent MUST choose to use one of the challenges with the strongest auth-scheme it understands and request credentials from the user based upon that challenge.	MUST	NOT REQUIRED	
RFC2617-1-4			If the origin server does not wish to accept the credentials sent with a request, it SHOULD return a 401 (Unauthorized) response.	SHOULD	OUT OF SCOPE	
RFC2617-1-5			The response MUST include a WWW-Authenticate header field containing at least one (possibly new) challenge applicable to the requested resource.	MUST	OUT OF SCOPE	
RFC2617-1-6			If a proxy does not accept the credentials sent with a request, it SHOULD return a 407 (Proxy Authentication Required).	SHOULD	OUT OF SCOPE	
RFC2617-1-7			The response MUST include a Proxy-Authenticate header field containing a (possibly new) challenge applicable to the proxy for the requested resource.	MUST	OUT OF SCOPE	
RFC2617-1-8			Proxies MUST be completely transparent regarding user agent authentication by origin servers.	MUST	OUT OF SCOPE	
RFC2617-2-1	2	Basic Authentication Scheme	A client SHOULD assume that all paths at or deeper than the depth of the last symbolic element in the path field of the Request-URI also are within the protection space specified by the Basic realm value of the current challenge.	SHOULD	NOT REQUIRED	
RFC2617-3-1	3.2.1	The WWW-Authenticate Response Header	qop-options This directive is optional, but is made so only for backward compatibility with RFC 2069 [6]; it SHOULD be used by all implementations compliant with this version of the Digest scheme.	SHOULD	OUT OF SCOPE	
RFC2617-3-2			Unrecognized options MUST be ignored.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC2617-3-3			Any unrecognized directive MUST be ignored.	MUST	OUT OF SCOPE	
RFC2617-3-4	3.2.2	The Authorization Request Header	If present, its value MUST be one of the alternatives the server indicated it supports in the WWW-Authenticate header.	MUST	ADVANCED	generic_Auth_REGISTER
RFC2617-3-5			This directive is optional in order to preserve backward compatibility with a minimal implementation of RFC 2069 [6], but SHOULD be used if the server indicated that qop is supported by providing a qop directive in the WWW-Authenticate header field.	SHOULD	ADVANCED	generic_Auth_REGISTER
RFC2617-3-6			cnonce This MUST be specified if a qop directive is sent (see above), and MUST NOT be specified if the server did not send a qop directive in the WWW-Authenticate header field.	MUST	ADVANCED	generic_Auth_REGISTER
RFC2617-3-7				MUST NOT	ADVANCED	generic_Auth_REGISTER
RFC2617-3-8			nonce-count This MUST be specified if a qop directive is sent (see above), and MUST NOT be specified if the server did not send a qop directive in the WWW-Authenticate header field.	MUST	ADVANCED	generic_Auth_REGISTER
RFC2617-3-9				MUST NOT	ADVANCED	generic_Auth_REGISTER
RFC2617-3-10			Any unrecognized directive MUST be ignored.	MUST	NOT REQUIRED	
RFC2617-3-11	3.2.2.5	Various considerations	This may be ″*″, an ″absoluteURL″ or an ″abs_path″ as specified in section 5.1.2 of [2], but it MUST agree with the Request-URI.	MUST	NOT REQUIRED	
RFC2617-3-12			In particular, it MUST be an ″absoluteURL″ if the Request-URI is an ″absoluteURL″.	MUST	NOT REQUIRED	
RFC2617-3-13			The authenticating server must assure that the resource designated by the ″uri″ directive is the same as the resource specified in the Request-Line; if they are not, the server SHOULD return a 400 Bad Request error.	SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC2617-3-14			The HTTP/1.1 protocol specifies that when a shared cache (see section 13.7 of [2]) has received a request containing an Authorization header and a response from relaying that request, it MUST NOT return that response as a reply to any other request, unless one of two Cache-Control (see section 14.9 of [2]) directives was present in the response.	MUST NOT	NOT REQUIRED	
RFC2617-3-15			If the original response included the "must-revalidate" Cache-Control directive, the cache MAY use the entity of that response in replying to a subsequent request, but MUST first revalidate it with the origin server, using the request headers from the new request to allow the origin server to authenticate the new request.	MUST	NOT REQUIRED	
RFC2617-3-16	3.2.3	The Authentication-Info Header	If the nextnonce field is present the client SHOULD use it when constructing the Authorization header for its next request.	SHOULD	NOT REQUIRED	
RFC2617-3-17			The server SHOULD use the same value for the message- qop directive in the response as was sent by the client in the corresponding request.	SHOULD	OUT OF SCOPE	
RFC2617-3-18			The "cnonce-value" and "nc- value" MUST be the ones for the client request to which this message is the response.	MUST	NOT REQUIRED	
RFC2617-3-19			The "response-auth", "cnonce", and "nonce-count" directives MUST BE present if "qop=auth" or "qop=auth-int" is specified.	MUST	NOT REQUIRED	
RFC2617-4-1	4.1	Authentication of Clients using Basic Authentication	Because Basic authentication involves the cleartext transmission of passwords it SHOULD NOT be used (without enhancements) to protect sensitive or valuable information.	SHOULD NOT	NOT REQUIRED	
RFC2617-4-2			Server implementers SHOULD guard against the possibility of this sort of counterfeiting by gateways or CGI scripts.	SHOULD	OUT OF SCOPE	
RFC2617-4-3	4.6	Weakness Created by Multiple Authentication Schemes	A user agent MUST choose to use the strongest auth-scheme it understands and request credentials from the user based upon that challenge.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-3.1-1	3.1.1	Subscription Duration	SUBSCRIBE requests SHOULD contain an "Expires" header (defined in SIP [1]).	SHOULD	BASIC	generic_SUBSCRIBE generic_Re_SUBSCRIBE
RFC3265-3.1-2			200-class responses to SUBSCRIBE requests also MUST contain an "Expires" header.	MUST	NOT REQUIRED	
RFC3265-3.1-3			The period of time in the response MAY be shorter but MUST NOT be longer than specified in the request.	MUST NOT	NOT REQUIRED	
RFC3265-3.1-4	3.1.2	Identification of Subscribed Events and Event Classes	Subscribers MUST include exactly one "Event" header in SUBSCRIBE requests, indicating to which event or class of events they are subscribing.	MUST	BASIC	generic_SUBSCRIBE generic_Re_SUBSCRIBE
RFC3265-3.1-5	3.1.3	Additional SUBSCRIBE Header Values	Event packages MUST define the behavior for SUBSCRIBE requests without "Accept" headers; usually, this will connote a single, default body type.	MUST	NOT REQUIRED	
RFC3265-3.1-6	3.1.4.4	Confirmation of Subscription Creation	Documents which define new event packages MUST define this "neutral state" in such a way that makes sense for their application (see section 4.4.7.).	MUST	NOT REQUIRED	
RFC3265-3.1-7			Due to the potential for both out-of-order messages and forking, the subscriber MUST be prepared to receive NOTIFY messages before the SUBSCRIBE transaction has completed.	MUST	OUT OF SCOPE	
RFC3265-3.1-8	3.1.5	Proxy SUBSCRIBE Behavior	If a proxy wishes to see all of the SUBSCRIBE and NOTIFY requests for a given dialog, it MUST record-route the initial SUBSCRIBE and any dialog-establishing NOTIFY requests.	MUST	NOT REQUIRED	
RFC3265-3.1-9			Such proxies SHOULD also record-route all other SUBSCRIBE and NOTIFY requests.	SHOULD	NOT REQUIRED	
RFC3265-3.1-10	3.1.6.1	Initial SUBSCRIBE Transaction Processing	In particular, notifiers MUST NOT wait for a user response before returning a final response to a SUBSCRIBE request.	MUST	NOT REQUIRED	
RFC3265-3.1-11			The notifier SHOULD check that the event package specified in the "Event" header is understood.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-3.1-12			If not, the notifier SHOULD return a "489 Bad Event" response to indicate that the specified event/event class is not understood.	SHOULD	NOT REQUIRED	
RFC3265-3.1-13			The notifier SHOULD also perform any necessary authentication and authorization per its local policy.	SHOULD	NOT REQUIRED	
RFC3265-3.1-14			The "Expires" values present in SUBSCRIBE 200-class responses behave in the same way as they do in REGISTER responses: the server MAY shorten the interval, but MUST NOT lengthen it.	MUST	NOT REQUIRED	
RFC3265-3.1-15	3.1.6.2	Confirmation of Subscription Creation/Refreshing	Upon successfully accepting or refreshing a subscription, notifiers MUST send a NOTIFY message immediately to communicate the current resource state to the subscriber.	MUST	NOT REQUIRED	
RFC3265-3.1-16	3.1.6.3	Authentication/Authorization of SUBSCRIBE requests	If authorization fails based on an access list or some other automated mechanism (i.e., it can be automatically authoritatively determined that the subscriber is not authorized to subscribe), the notifier SHOULD reply to the request with a "403 Forbidden" or "603 Decline" response, unless doing so might reveal information that should stay private; see section 5.2.	SHOULD	NOT REQUIRED	
RFC3265-3.1-17	3.1.6.4	Refreshing of Subscriptions	As with the initial subscription, the server MAY shorten the amount of time until expiration, but MUST NOT increase it.	MUST	NOT REQUIRED	
RFC3265-3.1-18			If the duration specified in a SUBSCRIBE message is unacceptably short, the notifier SHOULD respond with a "423 Subscription Too Brief" message.	SHOULD	NOT REQUIRED	
RFC3265-3.1-19			When removing a subscription, the notifier SHOULD send a NOTIFY message with a "Subscription-State" value of "terminated" to inform it that the subscription is being removed.	SHOULD	NOT REQUIRED	
RFC3265-3.1-20			If such a message is sent, the "Subscription-State" header SHOULD contain a "reason=timeout" parameter.	SHOULD	NOT REQUIRED	
RFC3265-3.2-1	3.2	Description of NOTIFY Behavior	The latter behavior is invalid, and MUST receive a "481 Subscription does not exist" response (unless some other 400- or 500-class error code is more applicable), as described in section 3.2.4.	MUST	NOT REQUIRED	
RFC3265-3.2-2	3.2.1	Identification of Reported Events, Event Classes, and Current State	The package name in the "Event" header MUST match the "Event" header in the corresponding SUBSCRIBE message.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-3.2-3			If an "id" parameter was present in the SUBSCRIBE message, that "id" parameter MUST also be present in the corresponding NOTIFY messages.	MUST	NOT REQUIRED	
RFC3265-3.2-4			When present, the body of the NOTIFY request MUST be formatted into one of the body formats specified in the "Accept" header of the corresponding SUBSCRIBE request.	MUST	NOT REQUIRED	
RFC3265-3.2-5	3.2.2	Notifier NOTIFY Behavior	When a SUBSCRIBE request is answered with a 200-class response, the notifier MUST immediately construct and send a NOTIFY request to the subscriber.	MUST	NOT REQUIRED	
RFC3265-3.2-6			When a change in the subscribed state occurs, the notifier SHOULD immediately construct and send a NOTIFY request, subject to authorization, local policy, and throttling considerations.	SHOULD	NOT REQUIRED	
RFC3265-3.2-7			If the NOTIFY request fails (as defined above) due to a timeout condition, and the subscription was installed using a soft-state mechanism (such as SUBSCRIBE), the notifier SHOULD remove the subscription.	SHOULD	NOT REQUIRED	
RFC3265-3.2-8			If the NOTIFY request fails (as defined above) due to an error response, and the subscription was installed using a soft-state mechanism, the notifier MUST remove the corresponding subscription.	MUST	NOT REQUIRED	
RFC3265-3.2-9			If a NOTIFY request receives a 481 response, the notifier MUST remove the corresponding subscription even if such subscription was installed by non-SUBSCRIBE means (such as an administrative interface).	MUST	NOT REQUIRED	
RFC3265-3.2-10			NOTIFY requests MUST contain a "Subscription-State" header with a value of "active", "pending", or "terminated".	MUST	NOT REQUIRED	
RFC3265-3.2-11			If the value of the "Subscription-State" header is "active" or "pending", the notifier SHOULD also include in the "Subscription- State" header an "expires" parameter which indicates the time remaining on the subscription.	SHOULD	NOT REQUIRED	
RFC3265-3.2-12			The notifier MAY use this mechanism to shorten a subscription; however, this mechanism MUST NOT be used to lengthen a subscription.	MUST	NOT REQUIRED	
RFC3265-3.2-13			If the value of the "Subscription-State" header is "terminated", the notifier SHOULD also include a "reason" parameter.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-3.2-14	3.2.3	Proxy NOTIFY Behavior	If a proxy wishes to see all of the SUBSCRIBE and NOTIFY requests for a given dialog, it MUST record-route the initial SUBSCRIBE and any dialog-establishing NOTIFY requests.	MUST	NOT REQUIRED	
RFC3265-3.2-15			Such proxies SHOULD also record-route all other SUBSCRIBE and NOTIFY requests.	SHOULD	NOT REQUIRED	
RFC3265-3.2-16	3.2.4	Subscriber NOTIFY Behavior	Upon receiving a NOTIFY request, the subscriber SHOULD check that it matches at least one of its outstanding subscriptions;	SHOULD	OUT OF SCOPE	
RFC3265-3.2-16			if not, it MUST return a "481 Subscription does not exist" response unless another 400- or 500-class response is more appropriate.	MUST	NOT REQUIRED	
RFC3265-3.2-17			To prevent spoofing of events, NOTIFY requests SHOULD be authenticated, using any defined SIP authentication mechanism.	SHOULD	NOT REQUIRED	
RFC3265-3.2-18			NOTIFY requests MUST contain "Subscription-State" headers which indicate the status of the subscription.	MUST	NOT REQUIRED	
RFC3265-3.2-19			If the header also contains an "expires" parameter, the subscriber SHOULD take it as the authoritative subscription duration and adjust accordingly.	SHOULD	OUT OF SCOPE	
RFC3265-3.2-21			If no reason code or an unknown reason code is present, the client MAY attempt to re-subscribe at any time (unless a "retry-after" parameter is present, in which case the client SHOULD NOT attempt re-subscription until after the number of seconds specified by the "retry-after" parameter).	SHOULD	BASIC	UE-RG-B-22-AKA UE-RG-B-22-DIP
RFC3265-3.2-22			deactivated: The subscription has been terminated, but the subscriber SHOULD retry immediately with a new subscription.	SHOULD	BASIC	UE-RG-B-6-AKA UE-RG-B-6-DIP
RFC3265-3.2-23			probation: The subscription has been terminated, but the client SHOULD retry at some later time.	SHOULD	NOT REQUIRED	
RFC3265-3.2-24			If a "retry-after" parameter is also present, the client SHOULD wait at least the number of seconds specified by that parameter before attempting to re- subscribe.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-3.2-25			Clients SHOULD NOT attempt to re-subscribe.	SHOULD	NOT REQUIRED	
RFC3265-3.2-26			If a "retry- after" parameter is also present, the client SHOULD wait at least the number of seconds specified by that parameter before attempting to re-subscribe; otherwise, the client MAY retry immediately, but will likely get put back into pending state.	SHOULD	NOT REQUIRED	
RFC3265-3.2-27			Clients SHOULD NOT attempt to re-subscribe.	SHOULD	NOT REQUIRED	
RFC3265-3.2-28			Once the notification is deemed acceptable to the subscriber, the subscriber SHOULD return a 200 response.	SHOULD	BASIC	reference （UE-RR-B-1-AKA UE-SR-B-11-AKA UE-RR-B-1-DIP UE-SR-B-11-DIP）
RFC3265-3.2-29			In particular, subscribers MUST NOT wait for a user response before returning a final response to a NOTIFY request.	MUST	NOT REQUIRED	
RFC3265-3.3-1	3.3.3	Forking	The subscriber MUST therefore be prepared to receive NOTIFY requests with "From:" tags which differ from the "To:" tag received in the SUBSCRIBE 200-class response.	MUST	NOT REQUIRED	
RFC3265-3.3-2	3.3.5	State Agents and Notifier Migration	Upon receipt of this NOTIFY message, the subscriber SHOULD attempt to re-subscribe (as described in the preceding sections).	SHOULD	NOT REQUIRED	
RFC3265-3.3-3	3.3.6	Polling Resource State	In particular, polling SHOULD NOT be used in circumstances in which it will typically result in more network messages than long-running subscriptions.	SHOULD	OUT OF SCOPE	
RFC3265-3.3-4			When polling is used, subscribers SHOULD attempt to cache authentication credentials between polls so as to reduce the number of messages sent.	SHOULD	OUT OF SCOPE	
RFC3265-3.3-5	3.3.7	Allow-Events header usage	Any node implementing one or more event packages SHOULD include an appropriate "Allow-Events" header indicating all supported events in all methods which initiate dialogs and their responses (such as INVITE) and OPTIONS responses.	SHOULD	BASIC	generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_200-OPTIONS generic_INVITE generic_200-INVITE
RFC3265-3.3-6			Note that "Allow-Events" headers MUST NOT be inserted by proxies.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-3.3-7	3.3.8	PINT Compatibility	If a server does not support PINT, it SHOULD return "489 Bad Event" to any SUBSCRIBE messages without an "Event" header.	SHOULD	NOT REQUIRED	
RFC3265-4.3-1	4.3.2	State Deltas	Any event package that supports delta changes to states MUST include a version number that increases by exactly one for each NOTIFY transaction in a subscription.	MUST	NOT REQUIRED	
RFC3265-4.4-1	4.4	Event Package Responsibilities	Note that any behavior designated with "SHOULD" or "MUST" in this document is not allowed to be weakened by extension documents;	SHOULD	NOT REQUIRED	
RFC3265-4.4-2				MUST	NOT REQUIRED	
RFC3265-4.4-3			however, such documents may elect to strengthen "SHOULD" requirements to "MUST" strength if required by their application.	SHOULD	NOT REQUIRED	
RFC3265-4.4-4				MUST	NOT REQUIRED	
RFC3265-4.4-5	4.4.1	Event Package Name	This section, which MUST be present, defines the token name to be used to designate the event package.	MUST	NOT REQUIRED	
RFC3265-4.4-6			It MUST include the information which appears in the IANA registration of the token.	MUST	NOT REQUIRED	
RFC3265-4.4-7	4.4.2	Event Package Parameters	If parameters are to be used on the "Event" header to modify the behavior of the event package, the syntax and semantics of such headers MUST be clearly defined.	MUST	NOT REQUIRED	
RFC3265-4.4-8	4.4.4	Subscription Duration	It is RECOMMENDED that event packages give a suggested range of times considered reasonable for the duration of a subscription.	RECOMMENDED	NOT REQUIRED	
RFC3265-4.4-9			Such packages MUST also define a default "Expires" value to be used if none is specified.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-4.4-10	4.4.5	NOTIFY Bodies	Each package MUST define what type or types of event bodies are expected in NOTIFY requests.	MUST	NOT REQUIRED	
RFC3265-4.4-11			Such packages MUST specify or cite detailed specifications for the syntax and semantics associated with such event body.	MUST	NOT REQUIRED	
RFC3265-4.4-12			Event packages also MUST define which MIME type is to be assumed if none are specified in the "Accept" header of the SUBSCRIBE request.	MUST	NOT REQUIRED	
RFC3265-4.4-13	4.4.9	Handling of forked requests	Each event package MUST specify whether forked SUBSCRIBE requests are allowed to install multiple subscriptions.	MUST	NOT REQUIRED	
RFC3265-4.4-14			In the case that multiple subscriptions are allowed, the event package MUST specify whether merging of the notifications to form a single state is required, and how such merging is to be performed.	MUST	NOT REQUIRED	
RFC3265-4.4-15			Note that it is possible that some event packages may be defined in such a way that each dialog is tied to a mutually exclusive state which is unaffected by the other dialogs; this MUST be clearly stated if it is the case.	MUST	NOT REQUIRED	
RFC3265-4.4-16	4.4.10	Rate of notifications	Each event package is expected to define a requirement (SHOULD or MUST strength) which defines an absolute maximum on the rate at which notifications are allowed to be generated by a single notifier.	SHOULD	NOT REQUIRED	
RFC3265-4.4-17				MUST	NOT REQUIRED	
RFC3265-4.4-18	4.4.11	State Agents	If state agents are to be used by the package, the package MUST specify how such state agents aggregate information and how they provide authentication and authorization.	MUST	NOT REQUIRED	
RFC3265-4.4-19	4.4.12	Examples	Event packages SHOULD include several demonstrative message flow diagrams paired with several typical, syntactically correct, and complete messages.	SHOULD	NOT REQUIRED	
RFC3265-4.4-20			It is RECOMMENDED that documents describing event packages clearly indicate that such examples are informative and not normative, with instructions that implementors refer to the main text of the document for exact protocol details.	RECOMMENDED	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-5.2-1	5.2	Notifier Privacy Mechanism	In these cases, the notifier SHOULD always return a 202 response.	SHOULD	NOT REQUIRED	
RFC3265-5.2-2			While the subsequent NOTIFY message may not convey true state, it MUST appear to contain a potentially correct piece of data from the point of view of the subscriber, indistinguishable from a valid response.	MUST	NOT REQUIRED	
RFC3265-5.3-1	5.3	Denial-of-Service attacks	To reduce the chances of such an attack, implementations of notifiers SHOULD require authentication.	SHOULD	NOT REQUIRED	
RFC3265-5.4-1	5.4	Replay Attacks	To prevent such attacks, implementations SHOULD require authentication with anti-replay protection.	SHOULD	NOT REQUIRED	
RFC3265-5.5-1	5.5	Man-in-the middle attacks	To prevent such attacks, implementations SHOULD provide integrity protection across "Contact", "Route", "Expires", "Event", and "To" headers of SUBSCRIBE messages, at a minimum.	SHOULD	NOT REQUIRED	
RFC3265-5.5-2			If SUBSCRIBE bodies are used to define further information about the state of the call, they SHOULD be included in the integrity protection scheme.	SHOULD	NOT REQUIRED	
RFC3265-5.5-3			To prevent such attacks, implementations SHOULD provide integrity protection across the "Call-ID", "CSeq", and "Subscription-State" headers and the bodies of NOTIFY messages.	SHOULD	NOT REQUIRED	
RFC3265-5.6-1	5.6	Confidentiality	To allow the remote party to hide information it considers sensitive, all implementations SHOULD be able to handle encrypted SUBSCRIBE and NOTIFY messages.	SHOULD	NOT REQUIRED	
RFC3265-6.1-1	6	IANA Considerations	To avoid confusion, template-package names and package names share the same namespace; in other words, an event template-package MUST NOT share a name with a package.	MUST	NOT REQUIRED	
RFC3265-6.1-2			Registrations with the IANA MUST include the token being registered and whether the token is a package or a template-package.	MUST	NOT REQUIRED	
RFC3265-6.1-3			Further, packages MUST include contact information for the party responsible for the registration and/or a published document which describes the event package.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3265-6.1-4			Event template-package token registrations MUST include a pointer to the published RFC which defines the event template-package.	MUST	NOT REQUIRED	
RFC3265-6.1-5			Registered tokens to designate packages and template-packages MUST NOT contain the character ".", which is used to separate template- packages from packages.	MUST	NOT REQUIRED	
RFC3265-7.2-1	7.2.1	Event" header"	These values will be defined by individual event packages, and MUST be registered with the IANA.	MUST	NOT REQUIRED	
RFC3265-7.2-2			There MUST be exactly one event type listed per event header.	MUST	BASIC	generic_SUBSCRIBE generic_Re_SUBSCRIBE

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3310-3.1-1	3.1	Algorithm Directive	If the directive is not understood, the nonce SHOULD be ignored, and another challenge (if one is present) should be used instead.	SHOULD	NOT REQUIRED	
RFC3310-3.1-2			If the entropy of the used RES value is limited (e.g., only 32 bits), reuse of the same RES value in authenticating subsequent requests and responses is NOT RECOMMENDED.	RECOMMENDED	NOT REQUIRED	
RFC3310-3.1-3			Such a RES value SHOULD only be used as a one-time password,	SHOULD	NOT REQUIRED	
RFC3310-3.1-4			and algorithms such as "MD5-sess", which limit the amount of material hashed with a single key, by producing a session key for authentication, SHOULD NOT be used.	SHOULD	NOT REQUIRED	
RFC3310-3.2-1	3.2	Creating a Challenge	If the server receives a client authentication containing the "auts" parameter defined in Section 3.4, that includes a valid AKA AUTS parameter, the server MUST use it to generate a new challenge to the client.	MUST	NOT REQUIRED	
RFC3310-3.4-1	3.4	Synchronization Failure	Instead, the client MUST calculate its credentials using an empty password (password of "").	MUST	BASIC	UE-RG-B-19-AKA
RFC3310-5.3-1	5.3	Multiple Authentication Schemes and Algorithms	In HTTP authentication, a user agent MUST choose the strongest authentication scheme it understands and request credentials from the user, based upon that challenge.	MUST	NOT REQUIRED	
RFC3310-5.3-2			Digest AKA passwords MUST NOT be re-used with such HTTP authentication schemes, which send the password in clear.	MUST	NOT REQUIRED	
RFC3310-5.3-3			In particular, AKA passwords MUST NOT be re-used with HTTP Basic.	MUST	NOT REQUIRED	
RFC3310-5.3-4			A client receiving an HTTP Digest challenge with several available algorithms MUST choose the strongest algorithm it understands.	MUST	NOT REQUIRED	
RFC3310-6-1	6	IANA Considerations	Registrations with the IANA MUST include the version number being registered, including the "AKAv" prefix.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3310-6-2			Further, the registration MUST include contact information for the party responsible for the registration.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3320-3.3-1	3.3	SigComp Parameters	Each parameter has a minimum value that MUST be offered by all receiving SigComp endpoints.	MUST	OUT OF SCOPE	
RFC3320-3.3-2	3.3.1	Memory Size and UDVM Cycles	All endpoints implementing SigComp MUST offer a decompression_memory_size of at least 2048 bytes.	MUST	OUT OF SCOPE	
RFC3320-3.3-3			An endpoint MUST offer a minimum of 16 cycles_per_bit.	MUST	OUT OF SCOPE	
RFC3320-3.3-4			Each of the three parameter values MUST be chosen from the limited set given below, so that the parameters can be efficiently encoded for transmission using the SigComp feedback mechanism.	MUST	OUT OF SCOPE	
RFC3320-4.2-1	4.2	Decompressor Dispatcher	The dispatcher MUST NOT make more than one SigComp message available to a given instance of the UDVM.	MUST	OUT OF SCOPE	
RFC3320-4.2-2			In particular, the dispatcher MUST NOT concatenate two SigComp messages to form a single message.	MUST	OUT OF SCOPE	
RFC3320-4.2-3	4.2.2	Record Marking	In UDVM version 0x01, any occurrence of the combinations 0xFF80 to 0xFFFE that are not protected by quoting causes decompression failure; the decompressor SHOULD close the stream-based transport in this case.	SHOULD	OUT OF SCOPE	
RFC3320-5-1	5	SigComp Compressor	The overall requirement placed on the compressor is that of transparency, i.e., the compressor MUST NOT send bytecode which causes the UDVM to incorrectly decompress a given SigComp message.	MUST	OUT OF SCOPE	
RFC3320-5-2			2. The compressor MUST ensure that the message can be decompressed using the resources available at the remote endpoint.	MUST	OUT OF SCOPE	
RFC3320-5-3			3. If the transport is message-based, then the compressor MUST map each application message to exactly one SigComp message.	MUST	OUT OF SCOPE	
RFC3320-5-4			4. If the transport is stream-based but the application defines its own internal message boundaries, then the compressor SHOULD map each application message to exactly one SigComp message.	SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3320-5-5			Additionally, if the state handler passes some requested feedback to the compressor, then it SHOULD be returned in the next SigComp message generated by the compressor (unless the state handler passes some newer requested feedback before the older feedback has been sent, in which case the older feedback is deleted).	SHOULD	OUT OF SCOPE	
RFC3320-5-6			If present, the requested feedback item SHOULD be copied unmodified into the returned_feedback_item field provided in the SigComp message.	SHOULD	OUT OF SCOPE	
RFC3320-5-7			The compressor SHOULD also upload the local SigComp parameters to the remote endpoint, unless the endpoint has indicated that it does not wish to receive these parameters or the compressor determines that the parameters have already successfully arrived (see Section 5.1 for details of how this can be achieved).	SHOULD	OUT OF SCOPE	
RFC3320-5.1-1	5.1	Ensuring Successful Decompression	A compressor MUST be certain that all of the data needed to decompress a SigComp message is available at the receiving endpoint.	MUST	OUT OF SCOPE	
RFC3320-5.2-1	5.2	Compression Failure	The compressor SHOULD make every effort to successfully compress an application message, but in certain cases this might not be possible (particularly if resources are scarce at the receiving endpoint). In this case a "compression failure" is called.	SHOULD	OUT OF SCOPE	
RFC3320-5.2-2			The dispatcher MUST report this failure to the application so that it can try other methods to deliver the message.	MUST	OUT OF SCOPE	
RFC3320-6.2-1	6.2	Memory Management	1. The state handler MUST reject all state creation requests that are not accompanied by a valid compartment identifier, or if the compartment is allocated 0 bytes of state memory. Note that if a state creation request fails due to lack of state memory then it does not mean that the corresponding SigComp message is damaged;	MUST	OUT OF SCOPE	
RFC3320-7.2-1	7.2	Accessing Stored State	Future versions of SigComp can use these locations for additional Useful Values, so a decompressor MUST NOT rely on these values being zero.	MUST	OUT OF SCOPE	
RFC3320-7.2-2			Any remaining addresses in the UDVM memory that have not yet been initialized MUST be set to 0.	MUST	OUT OF SCOPE	
RFC3320-8.2-1	8.2	Requesting Additional Compressed Data	If an INPUT instruction is encountered and the P- bit has changed since the last INPUT instruction, any fraction of a byte still held by the dispatcher MUST be discarded (even if the INPUT instruction requests zero bits).	MUST	OUT OF SCOPE	
RFC3320-8.4-1	8.4	Byte copying	If this occurs, then the byte copying operation MUST be completed as if the original instruction were still in place in the UDVM memory (this also applies if byte_copy_left or byte_copy_right are overwritten).	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3320-8.6-1	8.6	UDVM Cycles	Note that the number of UDVM cycles MUST NOT be increased if a request for additional compressed data fails.	MUST	OUT OF SCOPE	
RFC3320-8.7-1	8.7	Decompression Failure	In general a dispatcher SHOULD discard the compressed message (or the compressed stream if the transport is stream-based) and any decompressed data that has been outputted but not yet passed to the application.	SHOULD	OUT OF SCOPE	
RFC3320-9.4-1	9.4.2	INPUT-BYTES	If the INPUT-BYTES is encountered after an INPUT-BITS or an INPUT- HUFFMAN instruction has been used, and the dispatcher currently holds a fraction of a byte, then the fraction MUST be discarded before any data is passed to the UDVM.	MUST	OUT OF SCOPE	
RFC3320-9.4-2	9.4.5	STATE-ACCESS	The value of state_length MUST be taken from the returned item of state in the case that the state_length operand is set to 0.	MUST	OUT OF SCOPE	
RFC3320-9.4-3	9.4.6	STATE-CREATE	Decompression failure MUST occur if more than four state creation requests are made before the END-MESSAGE instruction is encountered.	MUST	OUT OF SCOPE	
RFC3320-9.4-4	9.4.7	STATE-FREE	Decompression failure MUST occur if more than four state free requests are made before the END-MESSAGE instruction is encountered.	MUST	OUT OF SCOPE	
RFC3320-10.2-1	10.2.3	Availability Risks (Avoiding DoS Vulnerabilities)	The application MUST limit the number of packets reflected to a potential target - even if SigComp is used to generate a large amount of information from a small incoming attack packet.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3327-4-1	4	Path Header Field Definition and Syntax	As suggested therein, such values MUST include the loose-routing indicator parameter ";lr" for full compliance with [1].	MUST	NOT REQUIRED	
RFC3327-5.1-1	5.1	Procedures at the UA	The UA SHOULD include the option tag "path" as a header field value in all Supported header fields, and SHOULD include a Supported header field in all requests.	SHOULD	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3327-5.1-2				SHOULD	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3327-5.2-1	5.2	Procedures at Intermediate Proxies	Intermediate proxies SHOULD NOT add a Path header field to a request unless the UA has indicated support for this extension with a Supported header field value.	SHOULD	NOT REQUIRED	
RFC3327-5.2-2			If the UA has indicated support and the proxy requires the registrar to support the Path extension, then the proxy SHOULD insert a Requires header field value for this extension.	SHOULD	NOT REQUIRED	
RFC3327-5.2-3			If the UA has not indicated support for the extension and the proxy requires support for it in the registrar, the proxy SHOULD reject the request with a 421 response indicating a requirement for the extension.	SHOULD	NOT REQUIRED	
RFC3327-5.2-4			Proxies processing a REGISTER response SHOULD NOT alter any Path header field values that may be present in the response.	SHOULD	NOT REQUIRED	
RFC3327-5.2-5			Proxies SHOULD only consider altering the value of a Path header field in the REGISTER response if they have the credentials to correctly alter the S/MIME body to account for the change.	SHOULD	NOT REQUIRED	
RFC3327-6.1-1	6.1	Considerations in REGISTER Request Processing	Systems using the Path mechanism SHOULD use appropriate mechanisms (TLS, IPSEC, etc.) to provide message integrity and mutual authentication.	SHOULD	NOT REQUIRED	
RFC3327-6.1-2			UAs SHOULD use "sips:" to request transitive protection.	SHOULD	NOT REQUIRED	
RFC3327-6.1-3			The registering UA SHOULD use S/MIME mechanisms to provide a protected copy of the original request to the registrar.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3327-6.1-4			In this case, the UA SHOULD include a Supported header field with a value indicating support for the Path extension in the protected copy.	SHOULD	NOT REQUIRED	
RFC3327-6.1-5			Registrars receiving such as request MUST honor the Path extension only if support is indicated in the protected header field.	MUST	NOT REQUIRED	
RFC3327-6.1-6			Further, they SHOULD compare the unprotected Supported header field with the protected Supported header field and take appropriate action in the event that an intermediate has altered the message to indicate support for Path when it was not indicated by the requesting UA.	SHOULD	NOT REQUIRED	
RFC3327-6.2-1	6.2	Considerations in REGISTER Response Processing	In addition to the hop-by-hop integrity protection and mutual authentication measures suggested for REGISTER request processing in the preceding section, systems using Path header fields SHOULD implement end-to-end protection using S/MIME.	SHOULD	NOT REQUIRED	
RFC3327-6.2-2			More specifically, registrars returning a Path header field SHOULD attach a signed S/MIME of the response, and UAs receiving a REGISTER response containing a Path header field SHOULD validate the message using the S/MIME technique.	SHOULD	NOT REQUIRED	
RFC3327-6.2-3				SHOULD	NOT REQUIRED	
RFC3327-6.2-4			Furthermore, UAs receiving a Path header field in a REGISTER response SHOULD render it to the user, or (where feasible) check it programmatically.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3329-2.2-1	2.2	Syntax	All the security mechanisms MUST have different "q" values.	MUST	NOT REQUIRED	
RFC3329-2.2-2			All linear white spaces in the Security-Server header field MUST be replaced by a single SP before calculating or interpreting the digest-verify parameter.	MUST	OUT OF SCOPE	
RFC3329-2.3-1	2.3.1	Client Initiated	If a client ends up using TLS to contact the server because it has followed the rules specified in [5], the client MUST NOT use the security agreement procedure of this specification.	MUST	NOT REQUIRED	
RFC3329-2.3-2			A client wishing to use the security agreement of this specification MUST add a Security-Client header field to a request addressed to its first-hop proxy (i.e., the destination of the request is the first- hop proxy).	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3329-2.3-3			The client SHOULD NOT add preference parameters to this list.	SHOULD	OUT OF SCOPE	
RFC3329-2.3-4			The client MUST add both a Require and Proxy-Require header field with the value "sec-agree" to its request.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER
RFC3329-2.3-5			A server receiving an unprotected request that contains a Require or Proxy-Require header field with the value "sec-agree" MUST respond to the client with a 494 (Security Agreement Required) response.	MUST	NOT REQUIRED	
RFC3329-2.3-6			The server MUST add a Security-Server header field to this response listing the security mechanisms that the server supports.	MUST	NOT REQUIRED	
RFC3329-2.3-7			The server MUST add its list to the response even if there are no common security mechanisms in the client's and server's lists.	MUST	NOT REQUIRED	
RFC3329-2.3-8			The server's list MUST NOT depend on the contents of the client's list.	MUST	NOT REQUIRED	
RFC3329-2.3-9			The server MUST compare the list received in the Security-Client header field with the list to be sent in the Security-Server header field.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3329-2.3-10			Therefore, the server MUST add the necessary information so that the client can initiate that mechanism (e.g., a Proxy-Authenticate header field for HTTP Digest).	MUST	NOT REQUIRED	
RFC3329-2.3-11			When the client receives a response with a Security-Server header field, it MUST choose the security mechanism in the server's list with the highest "q" value among all the mechanisms that are known to the client.	MUST	OUT OF SCOPE	
RFC3329-2.3-12			Then, it MUST initiate that particular security mechanism as described in Section 3.5.	MUST	BASIC	doc_refer
RFC3329-2.3-13			A client detecting such a lack of information in the response MUST consider the current security agreement process aborted, and MAY try to start it again by sending a new request with a Security-Client header field as described above.	MUST	OUT OF SCOPE	
RFC3329-2.3-14			All the subsequent SIP requests sent by the client to that server SHOULD make use of the security mechanism initiated in the previous step.	SHOULD	BASIC	generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_OPTIONS generic_BYE
RFC3329-2.3-15			These requests MUST contain a Security-Verify header field that mirrors the server's list received previously in the Security- Server header field.	MUST	BASIC	generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_OPTIONS generic_BYE
RFC3329-2.3-16			These requests MUST also have both a Require and Proxy-Require header fields with the value "sec-agree".	MUST	BASIC	generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_INVITE generic_OPTIONS generic_BYE
RFC3329-2.3-17			The server MUST check that the security mechanisms listed in the Security-Verify header field of incoming requests correspond to its static list of supported security mechanisms.	MUST	NOT REQUIRED	
RFC3329-2.3-18			If modification of the list is detected, the server MUST respond to the client with a 494 (Security Agreement Required) response.	MUST	NOT REQUIRED	
RFC3329-2.3-19			This response MUST include the server's unmodified list of supported security mechanisms.	MUST	NOT REQUIRED	
RFC3329-2.3-20			If the list was not modified, and the server is a proxy, it MUST remove the "sec-agree" value from both the Require and Proxy-Require header fields, and then remove the header fields if no values remain.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3329-2.3-21			The user of a UA SHOULD be informed about the results of the security mechanism agreement.	SHOULD	NOT REQUIRED	
RFC3329-2.3-22	2.3.2	Server Initiated	If there are several Via entries, the server is not the first-hop SIP entity, and it MUST NOT use this mechanism.	MUST	NOT REQUIRED	
RFC3329-2.3-23			A server that decides to use this agreement mechanism MUST challenge unprotected requests with one Via entry regardless of the presence or the absence of any Require, Proxy-Require or Supported header fields in incoming requests.	MUST	NOT REQUIRED	
RFC3329-2.3-24			A server that by policy requires the use of this specification and receives a request that does not have the sec-agree option tag in a Require, Proxy-Require or Supported header field MUST return a 421 (Extension Required) response.	MUST	NOT REQUIRED	
RFC3329-2.3-25			If the request had the sec-agree option tag in a Supported header field, it MUST return a 494 (Security Agreement Required) response.	MUST	NOT REQUIRED	
RFC3329-2.3-26			In both situation the server MUST also include in the response a Security-Server header field listing its capabilities and a Require header field with an option- tag "sec-agree" in it.	MUST	NOT REQUIRED	
RFC3329-2.3-27			The server MUST also add necessary information so that the client can initiate the preferred security mechanism (e.g., a Proxy-Authenticate header field for HTTP Digest).	MUST	NOT REQUIRED	
RFC3329-2.3-28			Clients that support the extension defined in this document SHOULD add a Supported header field with a value of "sec-agree".	SHOULD	NOT REQUIRED	
RFC3329-2.4-1	2.4	Security Mechanism Initiation	However, if the URI is a SIP URI, it MUST treat the scheme as if it were sips, not sip.	MUST	NOT REQUIRED	
RFC3329-2.4-2			If the URI scheme is not sip, the request MUST be sent using TLS.	MUST	NOT REQUIRED	
RFC3329-2.4-3			The client MUST use the algorithm and qop parameters in the Security-Server header field to replace the same parameters in the HTTP Digest challenge.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3329-2.4-4			The client MUST also use the digest-verify parameter in the Security-Verify header field to protect the Security-Server header field as specified in 2.2.	MUST	NOT REQUIRED	
RFC3329-2.4-5			If the IKE connection attempt fails, the agreement procedure MUST be considered to have failed, and MUST be terminated.	MUST	NOT REQUIRED	
RFC3329-2.4-6				MUST	NOT REQUIRED	
RFC3329-3-1	3	Backwards Compatibility	UA and server implementations MUST be configurable to operate with or without this extension.	MUST	NOT REQUIRED	
RFC3329-5-1	5	Security Considerations	All clients that implement this specification MUST select HTTP Digest, TLS, IPsec, or any stronger method for the protection of the second request.	MUST	BASIC	generic_Auth_REGISTER
RFC3329-6-1	6	IANA Considerations	Registrations with the IANA MUST include the mechanism-name token being registered, and a pointer to a published RFC describing the details of the corresponding security mechanism.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3455−4.1−1	4.1	The P−Associated−URI header	A UAC MUST NOT assume that the associated URIs are registered.	MUST	OUT OF SCOPE	
RFC3455−4.1−2	4.1.2	Usage of the P−Associated−URI header	If the registrar supports the P−Associated−URI header extension, then the registrar MUST always insert the P−Associated−URI header field in all the 200 OK responses to a REGISTER request, regardless of whether the REGISTER was an initial registration, re−registration, or de−registration and regardless of whether there are zero or more associated URIs.	MUST	NOT REQUIRED	
RFC3455−4.1−3	4.1.2.2	Procedures at the registrar	A registrar that supports this specification MUST include a P−Associated−URI header field in the 200 OK response to a REGISTER request.	MUST	NOT REQUIRED	
RFC3455−4.1−4			The header MUST be populated with a comma−separated list of SIP or SIPS URIs which are associated to the address−of−record under registration.	MUST	NOT REQUIRED	
RFC3455−4.1−5			In case the address−of−record under registration does not have any other SIP or SIPS URIs associated, the registrar MUST include an empty P−Associated−URI header value.	MUST	NOT REQUIRED	
RFC3455−4.2−1	4.2.2.1	Procedures at the UA	A UAC MUST NOT insert a P−Called−Party−ID header field in any SIP request or response.	MUST	BASIC	generic_REGISTER generic_Auth_REGISTER generic_re_REGISTER generic_de_REGISTER generic_SUBSCRIBE generic_Re_SUBSCRIBE generic_200−NOTIFY generic_CANCEL generic_ACK−non2xx generic_200−CANCEL generic_3XX−6XX generic_OPTIONS generic_200−OPTIONS generic_INVITE generic_200−INVITE generic_180−INVITE generic_BYE generic_200−BYE generic_ACK
RFC3455−4.2−2	4.2.2.2	Procedures at the proxy	The proxy MUST populate the header value with the contents of the Request−URI present in the SIP request that the proxy received.	MUST	NOT REQUIRED	
RFC3455−4.2−3			A SIP proxy MUST NOT insert a P−Called−Party−ID header in REGISTER requests.	MUST	NOT REQUIRED	
RFC3455−4.3−1	4.3.2.1	Procedures at the UA	User agent clients SHOULD NOT insert a P−Visited−Network−ID header in any SIP message.	SHOULD	NOT REQUIRED	
RFC3455−4.3−2	4.3.2.2	Procedures at the registrar and proxy	The header MUST be populated with the contents of a text string or a token that identifies the administrative domain of the network where the proxy is operating at the user's home network.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3455-4.3-3			A SIP proxy which is located in the home network MUST delete this header when forwarding the message outside the home network administrative domain, in order to retain the user's privacy.	MUST	NOT REQUIRED	
RFC3455-4.3-4			A SIP proxy which is located in the home network SHOULD delete this header when the home proxy has used the contents of the header or the request is routed based on the called party, even when the request is not forwarded outside the home network administrative domain.	SHOULD	NOT REQUIRED	
RFC3455-4.4-1	4.4.2.1	UA behavior	The UA inserting this information MUST trust the proxy that is providing services to protect its privacy by deleting the header before forwarding the message outside of the proxy's domain.	MUST	OUT OF SCOPE	
RFC3455-4.4-2	4.4.2.2	Proxy behavior	A proxy MUST NOT insert or modify the value of the P-Access-Network-Info header.	MUST	NOT REQUIRED	
RFC3455-4.4-3			A proxy that provides services to the user, the proxy typically located in the home network, and therefore trusted, MUST delete the header when the SIP signaling is forwarded to a SIP server located in a non-trusted administrative network domain.	MUST	NOT REQUIRED	
RFC3455-4.5-1	4.5	The P-Charging-Function-Addresses header	In case there are more than a single instance of either the CCF or the ECF addresses, implementations SHOULD attempt sending the charging data to the ECF or CCF address, starting with the first address of the sequence (if any) in the P-Charging-Function-Addresses header.	SHOULD	NOT REQUIRED	
RFC3455-4.5-2			Only one instance of the header MUST be present in a particular request or response.	MUST	NOT REQUIRED	
RFC3455-4.5-3	4.5.2.2	Procedures at the Proxy	If the next hop for the message is within the administrative domain of the proxy, then the proxy SHOULD include the P-Charging-Function-Addresses header in the outbound message.	SHOULD	NOT REQUIRED	
RFC3455-4.5-4			However, if the next hop for the message is outside the administrative domain of the proxy, then the proxy MUST remove the P-Charging-Function-Addresses header.	MUST	NOT REQUIRED	
RFC3455-4.6-1	4.6	The P-Charging-Vector header	ICID MUST be a globally unique value.	MUST	NOT REQUIRED	
RFC3455-4.6-2			Only one instance of the header MUST be present in a particular request or response.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3455-4.6-3	4.6.2.2	Procedures at the Proxy	If the next hop for the message is within the trusted domain, then the proxy SHOULD include the P-Charging-Vector header in the outbound message.	SHOULD	NOT REQUIRED	
RFC3455-6.1-1	6.1	P-Associated-URI	Therefore it is RECOMMENDED that this extension is used in a secured environment, where encryption of SIP messages is provided either end-to-end or hop-by-hop.	RECOMMENDED	NOT REQUIRED	
RFC3455-6.2-1	6.2	P-Called-Party-ID	To mitigate this problem, this extension SHOULD only be used in a secured environment, where encryption of SIP messages is provided either end-to-end or hop-by-hop.	SHOULD	NOT REQUIRED	
RFC3455-6.3-1	6.3	P-Visited-Network-ID	Therefore intermediaries participating in this mechanism MUST apply a hop-by-hop integrity protection mechanism such us IPsec or other available mechanisms in order to prevent such attacks.	MUST	NOT REQUIRED	
RFC3455-6.4-1	6.4	P-Access-Network-Info	Therefore the information MUST NOT be sent outside of the 3GPP domain.	MUST	NOT REQUIRED	
RFC3455-6.4-2			The 3GPP UA is aware of whether or not a secure association to the home network domain for transporting SIP signaling, is currently available, and as such the sensitive information carried in the P-Access-Network-Info header SHOULD NOT be sent in any initial unauthenticated and unprotected requests (e.g., REGISTER).	SHOULD	BASIC	generic_REGISTER
RFC3455-6.4-3			Any UA that is using this extension and is not part of a private trusted domain should not consider the mechanism as secure and as such SHOULD NOT send sensitive information in the P-Access-Network-Info header.	SHOULD	OUT OF SCOPE	
RFC3455-6.5-1	6.5	P-Charging-Function-Addresses	However, these proxies that share this information MUST have a trust relationship.	MUST	NOT REQUIRED	
RFC3455-6.5-2			Therefore, an integrity protection mechanism such as IPsec or other available mechanisms MUST be applied in order to prevent such attacks.	MUST	NOT REQUIRED	
RFC3455-6.6-1	6.6	P-Charging-Vector	However, these proxies that share this information MUST have a trust relationship.	MUST	NOT REQUIRED	
RFC3455-6.6-2			Therefore, an integrity protection mechanism such as IPsec or other available mechanisms MUST be applied in order to prevent such attacks.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3485-2-1	2	Design considerations	The static dictionary is unique and MUST be available in all SigComp implementations for SIP/SDP.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3486-3-1	3	SigComp implementations for SIP	Every SIP implementation that supports SigComp MUST implement the procedures described in this document.	MUST	BASIC	doc_reference
RFC3486-4-1	4	Sending a Request to a Server	If the next-hop URI contains the parameter comp=sigcomp, the client SHOULD compress the request using SigComp as defined in [2].	SHOULD	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC3486-4-2			If the next-hop URI is a SIPS URI, the request SHOULD be compressed before it is passed to the TLS layer.	SHOULD	NOT REQUIRED	
RFC3486-4-3			A client MUST NOT send a compressed request to a server if it does not know whether or not the server supports SigComp.	MUST	NOT REQUIRED	
RFC3486-4-4			Regardless of whether the request is sent compressed or not, if a client would like to receive subsequent requests within the same dialog in the UAS->UAC direction compressed, this client SHOULD add the parameter comp=sigcomp to the URI in the Contact header field if it is a user agent client.	SHOULD	BASIC	UE-SC-B-1-AKA
RFC3486-4-5			If the client is a proxy, it SHOULD add the parameter comp=sigcomp to its URI in the Record-Route header field.	SHOULD	NOT REQUIRED	
RFC3486-4-6			If a user agent client sends a compressed request, it SHOULD add the parameter comp=sigcomp to the URI in the Contact header field.	SHOULD	BASIC	UE-SC-B-1-AKA
RFC3486-4-7			If a proxy that Record-Routes sends a compressed request, it SHOULD add comp=sigcomp to its URI in the Record-Route header field.	SHOULD	NOT REQUIRED	
RFC3486-4-8			If a client sends a compressed request, it SHOULD add the parameter comp=sigcomp to the topmost entry of the Via header field.	SHOULD	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC3486-4-9			If a client does not know whether or not the server supports SigComp, but in case the server supported it, it would like to receive compressed responses, this client SHOULD add the parameter comp=sigcomp to the topmost entry of the Via header field.	SHOULD	NOT REQUIRED	
RFC3486-4.1-1	4.1	Obtaining a SIP or SIPS URI with comp=sigcomp	In this case, the client SHOULD send an uncompressed OPTIONS request to its outbound proxy.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3486-5-1	5	Sending a Response to a Client	If the topmost Via header field contains the parameter comp=sigcomp, the response SHOULD be compressed.	SHOULD	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC3486-5-2			Otherwise, the response MUST NOT be compressed.	MUST	NOT REQUIRED	
RFC3486-5-3			If this URI contains the parameter comp=sigcomp, the proxy SHOULD add comp=sigcomp to its entry in the Record-Route header field.	SHOULD	NOT REQUIRED	
RFC3486-5-4			If this URI does not contain the parameter comp=sigcomp, the proxy SHOULD remove comp=sigcomp (if it is present) from its entry in the Record- Route header field.	SHOULD	NOT REQUIRED	
RFC3486-5-5			The same way, a user agent server SHOULD add comp=sigcomp to the Contact header field of the response if the URI of the next upstream hop in the route set contained the parameter comp=sigcomp.	SHOULD	BASIC	UE-SC-B-2-AKA
RFC3486-7-1	7	Error Situations	If a SIP client sends a compressed request and the client transaction times out without having received any response, the client SHOULD retry the same request without using compression.	SHOULD	NOT REQUIRED	
RFC3486-7-2			If the compressed request was sent over a TCP connection, the client SHOULD close that connection and open a new one to send the uncompressed request.	SHOULD	NOT REQUIRED	
RFC3486-11-1	11	IANA Considerations	The IANA Considerations section of the RFC MUST include the following information, which appears in the IANA registry along with the RFC number of the publication.	MUST	NOT REQUIRED	
RFC3486-11-2			Token value to be used. The token MAY be of any length, but SHOULD be no more than ten characters long.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3608-5-1	5	Syntax	Note that the Service-Route header field values MUST conform to the syntax of a Route element as defined in [3].	MUST	NOT REQUIRED	
RFC3608-5-2			As suggested therein, such values MUST include the loose-routing indicator parameter ";lr" for full compliance with [3].	MUST	NOT REQUIRED	
RFC3608-6.1-1	6.1	Procedures at the UA	If the re-registration request is refused or if an existing registration expires and the UA chooses not to re-register, the UA SHOULD discard any stored service route for that address-of-record.	SHOULD	OUT OF SCOPE	
RFC3608-6.1-2			The UA MUST preserve the order, in case there is more than one Service-Route header field or header field value.	MUST	NOT REQUIRED	
RFC3608-6.1-3			However, for the result to function, the combination MUST provide valid routing in the local environment.	MUST	NOT REQUIRED	
RFC3608-6.2-1	6.2	Procedures at the Proxy	Consequently, intermediate proxies SHOULD NOT alter the value of Service-Route in REGISTER responses, and if they do, the UA MUST NOT be required to accept the alteration.	SHOULD	NOT REQUIRED	
RFC3608-6.2-2				MUST	OUT OF SCOPE	
RFC3608-6.2-3			Instead of following the procedure in [3], proxies used with Service-Route that are inserting Record-Route or Path header field values SHOULD record not one but two route values when processing the request.	SHOULD	NOT REQUIRED	
RFC3608-6.3-1	6.3	Procedures at the Registrar	A REGISTER operation performing a Fetching Bindings (i.e., no Contact header field is present in the request) SHOULD return the same value of Service-Route as returned in the corresponding previous REGISTER response for the address-of-record in question.	SHOULD	NOT REQUIRED	
RFC3608-6.3-2			Note that the inserted Service-Route element(s) MUST conform to the syntax of a Route element as defined in [3].	MUST	NOT REQUIRED	
RFC3608-6.3-3			As suggested therein, such route elements MUST include the loose-routing indicator parameter ";lr" for full compliance with [3].	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3608-7-1	7	Security Considerations	Systems using Service-Route SHOULD provide hop-by-hop message integrity and mutual authentication.	SHOULD	NOT REQUIRED	
RFC3608-7-2			UAs SHOULD request this support by using a "sips:" URI.	SHOULD	NOT REQUIRED	
RFC3608-7-3			Registrars returning a Service-Route MUST implement end-to-end protection using S/MIME and SHOULD use S/MIME to protect all such responses.	MUST	NOT REQUIRED	
RFC3608-7-4				SHOULD	NOT REQUIRED	
RFC3608-7-5			UAs receiving Service-Route SHOULD authenticate attached S/MIME bodies if present.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3680-4.5-1	4.5	NOTIFY Bodies	All subscribers and notifiers MUST support the "application/reginfo+xml" format described in Section 5.	MUST	NOT REQUIRED	
RFC3680-4.5-2			If the header field is present, it MUST include "application/reginfo+xml", and MAY include any other types capable of representing registration information.	MUST	NOT REQUIRED	
RFC3680-4.5-3			Of course, the notifications generated by the server MUST be in one of the formats specified in the Accept header field in the SUBSCRIBE request.	MUST	NOT REQUIRED	
RFC3680-4.6-1	4.6	Notifier Processing of SUBSCRIBE Requests	Therefore, all subscriptions to it SHOULD be authenticated and authorized before approval.	SHOULD	BASIC	reference (UE-RG-B-1-AKA, UE-RG-B-1-DIP)
RFC3680-4.6-2			It is RECOMMENDED that a user be allowed to subscribe to their own registration state.	RECOMMENDED	OUT OF SCOPE	
RFC3680-4.7-1	4.7.1	The Registration State Machine	This transition is invisible, in that it MUST NOT ever be reported to a subscriber in a NOTIFY request.	MUST NOT	NOT REQUIRED	
RFC3680-4.7-2	4.7.2	Applying the state machine	As noted above, a notification MUST NOT be sent in this case.	MUST NOT	NOT REQUIRED	
RFC3680-4.7-3			As a general rule, when a subscriber is authorized to receive notifications about a set of registrations, it is RECOMMENDED that notifications contain information about those contacts which have changed state (and thus triggered a notification), instead of delivering the current state of every contact in all registrations.	RECOMMENDED	NOT REQUIRED	
RFC3680-4.7-4			However, notifications triggered as a result of a fetch operation (a SUBSCRIBE with Expires of 0) SHOULD result in the full state of all contacts for all registrations to be present in the NOTIFY.	SHOULD	NOT REQUIRED	
RFC3680-4.9-1	4.9	Handling of Forked Requests	As a result, a subscriber MUST NOT create multiple dialogs as a result of a single subscription request.	MUST NOT	NOT REQUIRED	
RFC3680-4.10-1	4.10	Rate of Notifications	As a result, it is RECOMMENDED that the server not generate notifications for a single subscriber at a rate faster than once every 5 seconds.	RECOMMENDED	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3680-5.1-1	5.1	Structure of Registration Information	Registration information is an XML document [4] that MUST be well-formed and SHOULD be valid.	MUST	NOT REQUIRED	
RFC3680-5.1-2				SHOULD	NOT REQUIRED	
RFC3680-5.1-3			Registration information documents MUST be based on XML 1.0 and MUST be encoded using UTF-8.	MUST	NOT REQUIRED	
RFC3680-5.1-4				MUST	NOT REQUIRED	
RFC3680-5.1-5			The registration information for a particular address-of-record MUST be contained within a single "registration" element; it cannot be spread across multiple "registration" elements within a document.	MUST	NOT REQUIRED	
RFC3680-5.1-6			Other elements from different namespaces MAY be present for the purposes of extensibility; elements or attributes from unknown namespaces MUST be ignored.	MUST	OUT OF SCOPE	
RFC3680-5.1-7			There are two attributes associated with the "reginfo" element, both of which MUST be present:	MUST	NOT REQUIRED	
RFC3680-5.1-8			Versions MUST be representable using a 32 bit integer.	MUST	NOT REQUIRED	
RFC3680-5.1-9			Other elements from different namespaces MAY be present for the purposes of extensibility; elements or attributes from unknown namespaces MUST be ignored.	MUST	OUT OF SCOPE	
RFC3680-5.1-10			There are three attributes associated with the "registration" element, all of which MUST be present:	MUST	NOT REQUIRED	
RFC3680-5.1-11			It MUST be unique amongst all other id attributes present in other registration elements conveyed to the subscriber within the scope of their subscription.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3680-5.1-12			In particular, if two URI identifying an address-of-record differ after their canonicalization according to the procedures in step 5 of Section 10.3 of RFC 3261 [1], the id attributes in the "registration" elements for those addresses-of-record MUST differ.	MUST	NOT REQUIRED	
RFC3680-5.1-13			Furthermore, the id attribute for a "registration" element for a particular address-of-record MUST be the same across all notifications sent within the subscription.	MUST	NOT REQUIRED	
RFC3680-5.1-14			Other elements from different namespaces MAY be present for the purposes of extensibility; elements or attributes from unknown namespaces MUST be ignored.	MUST	OUT OF SCOPE	
RFC3680-5.1-15			There are several attributes associated with the "contact" element which MUST be present:	MUST	NOT REQUIRED	
RFC3680-5.1-16			It MUST be unique amongst all other id attributes present in other contact elements conveyed to the subscriber within the scope of their subscription.	MUST	NOT REQUIRED	
RFC3680-5.1-17			In particular, if the URI for two contacts differ (based on the URI comparison rules in RFC 3261 [1]), the id attributes for those contacts MUST differ.	MUST	NOT REQUIRED	
RFC3680-5.1-18			However, unlike the id attribute for an address- of-record, if the URI for two contacts are the same, their id attributes SHOULD be the same across notifications.	SHOULD	NOT REQUIRED	
RFC3680-5.1-19			This requirement is at SHOULD strength, and not MUST strength, since it is difficult to compute such an ID as a function of the URI without retaining additional state.	SHOULD	OUT OF SCOPE	
RFC3680-5.1-20				MUST	OUT OF SCOPE	
RFC3680-5.1-21			No hash function applied to the URI can, in fact, meet a MUST requirement.	MUST	OUT OF SCOPE	
RFC3680-5.1-22			If the event attribute has a value of shortened, the "expires" attribute MUST be present.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC3680-5.1-23			If the event attribute has a value of probation, the "retry-after" attribute MUST be present.	MUST	NOT REQUIRED	
RFC3680-5.2-1	5.2	Computing Registrations from the Document	The version number MUST be initialized with the value of the "version" attribute from the "reginfo" element in the first document received.	MUST	OUT OF SCOPE	
RFC3680-5.2-2			If the value in the document is more than one higher than the local version number, the local version number is set to the value in the new document, the document is processed, and the subscriber SHOULD generate a refresh request to trigger a full state notification.	SHOULD	OUT OF SCOPE	
RFC3680-7-1	7	Security Considerations	Subscriptions to this event package SHOULD be authenticated and authorized according to local policy.	SHOULD	BASIC	reference (UE-RG-B-1-AKA, UE-RG-B-1-DIP)
RFC3680-7-2			In addition, notifications SHOULD be sent in such a way to ensure confidentiality, message integrity and verification of subscriber identity, such as sending subscriptions and notifications using a SIPS URL or protecting the notification bodies with S/MIME.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4320-4.1-1	4.1	Action 1	An SIP element MUST NOT send any provisional response with a Status-Code other than 100 to a non-INVITE request.	MUST	OUT OF SCOPE	
RFC4320-4.1-2			An SIP element MUST NOT respond to a non-INVITE request with a Status-Code of 100 over any unreliable transport, such as UDP, before the amount of time it takes a client transaction's Timer E to be reset to T2.	MUST	NOT REQUIRED	
RFC4320-4.1-3			Without regard to transport, an SIP element MUST respond to a non- INVITE request with a Status-Code of 100 if it has not otherwise responded after the amount of time it takes a client transaction's Timer E to be reset to T2.	MUST	OUT OF SCOPE	
RFC4320-4.2-1	4.2	Action 2	A transaction-stateful SIP element MUST NOT send a response with Status-Code of 408 to a non-INVITE request.	MUST	OUT OF SCOPE	
RFC4320-4.2-2			A transaction-stateful SIP proxy MUST NOT send any response to a non-INVITE request unless it has a matching server transaction that is not in the Terminated state.	MUST	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-4.1-1	4.1	Media and Transport Information	By default, this SHOULD be the remote address and remote port to which data is sent.	SHOULD	OUT OF SCOPE	
RFC4566-4.1-2			Some media types may redefine this behaviour, but this is NOT RECOMMENDED since it complicates implementations (including middleboxes that must parse the addresses to open Network Address Translation (NAT) or firewall pinholes).	RECOMMENDED	OUT OF SCOPE	
RFC4566-5-1	5	SDP Specification	where <type> MUST be exactly one case-significant character and <value> is structured text whose format depends on <type>.	MUST	OUT OF SCOPE	
RFC4566-5-2			Whitespace MUST NOT be used on either side of the "=" sign.	MUST	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC4566-5-3			Some lines in each description are REQUIRED and some are OPTIONAL, but all MUST appear in exactly the order given here (the fixed order greatly enhances error detection and allows for a simple parser).	REQUIRED	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC4566-5-4				MUST	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC4566-5-5			The set of type letters is deliberately small and not intended to be extensible -- an SDP parser MUST completely ignore any session description that contains a type letter that it does not understand.	MUST	NOT REQUIRED	
RFC4566-5-6			An SDP parser MUST ignore any attribute it doesn't understand.	MUST	NOT REQUIRED	
RFC4566-5-7			The sequence CRLF (0x0d0a) is used to end a record, although parsers SHOULD be tolerant and also accept records terminated with a single newline character.	SHOULD	NOT REQUIRED	
RFC4566-5-8			If the "a=charset" attribute is not present, these octet strings MUST be interpreted as containing ISO-10646 characters in UTF-8 encoding (the presence of the "a=charset" attribute may force some fields to be interpreted differently).	MUST	OUT OF SCOPE	
RFC4566-5-9			Any domain name used in SDP MUST comply with [1], [2].	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-5-10			Internationalised domain names (IDNs) MUST be represented using the ASCII Compatible Encoding (ACE) form defined in [11] and MUST NOT be directly represented in UTF-8 or any other encoding (this requirement is for compatibility with RFC 2327 and other SDP-related standards, which predate the development of internationalised domain names).	MUST	NOT REQUIRED	
RFC4566-5-11				MUST	NOT REQUIRED	
RFC4566-5.2-1	5.2	Origin (o=")"	The <username> MUST NOT contain spaces.	MUST	OUT OF SCOPE	
RFC4566-5.2-2			Again, it is RECOMMENDED that an NTP format timestamp is used.	RECOMMENDED	OUT OF SCOPE	
RFC4566-5.2-3			For both IP4 and IP6, the fully qualified domain name is the form that SHOULD be given unless this is unavailable, in which case the globally unique address MAY be substituted.	SHOULD	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC4566-5.2-4			A local IP address MUST NOT be used in any context where the SDP description might leave the scope in which the address is meaningful (for example, a local address MUST NOT be included in an application-level referral that might leave the scope).	MUST	NOT REQUIRED	
RFC4566-5.2-5				MUST	NOT REQUIRED	
RFC4566-5.3-1	5.3	Session Name (s=")"	There MUST be one and only one "s=" field per session description.	MUST	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC4566-5.3-2			The "s=" field MUST NOT be empty and SHOULD contain ISO 10646 characters (but see also the "a=charset" attribute).	MUST	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC4566-5.3-3				SHOULD	NOT REQUIRED	
RFC4566-5.3-4			If a session has no meaningful name, the value "s= " SHOULD be used (i.e., a single space as the session name).	SHOULD	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-5.4-1	5.4	Session Information (i=")"	There MUST be at most one session-level "i=" field per session description, and at most one "i=" field per media.	MUST	NOT REQUIRED	
RFC4566-5.4-2			If the "a=charset" attribute is not present, the "i=" field MUST contain ISO 10646 characters in UTF-8 encoding.	MUST	NOT REQUIRED	
RFC4566-5.5-1	5.5	URI (u=")"	This field is OPTIONAL, but if it is present it MUST be specified before the first media field.	MUST	NOT REQUIRED	
RFC4566-5.6-1	5.6	Email Address and Phone Number (e=" and "p=")"	Note that the previous version of SDP specified that either an email field or a phone field MUST be specified, but this was widely ignored.	MUST	OUT OF SCOPE	
RFC4566-5.6-2			If an email address or phone number is present, it MUST be specified before the first media field.	MUST	NOT REQUIRED	
RFC4566-5.6-3			Phone numbers SHOULD be given in the form of an international public telecommunication number (see ITU-T Recommendation E.164) preceded by a "+".	SHOULD	NOT REQUIRED	
RFC4566-5.6-4			This MUST be enclosed in parentheses if it is present.	MUST	NOT REQUIRED	
RFC4566-5.6-5			The free text string SHOULD be in the ISO-10646 character set with UTF-8 encoding, or alternatively in ISO-8859-1 or other encodings if the appropriate session-level "a=charset" attribute is set.	SHOULD	NOT REQUIRED	
RFC4566-5.7-1	5.7	Connection Data (c=")"	A session description MUST contain either at least one "c=" field in each media description or a single "c=" field at the session level.	MUST	BASIC	generic_200-OPTIONS generic_INVITE generic_200-INVITE
RFC4566-5.7-2			Sessions using an IPv4 multicast connection address MUST also have a time to live (TTL) value present in addition to the multicast address.	MUST	NOT REQUIRED	
RFC4566-5.7-3			TTL values MUST be in the range 0-255.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-5.7-4			Although the TTL MUST be specified, its use to scope multicast traffic is deprecated;	MUST	NOT REQUIRED	
RFC4566-5.7-5			applications SHOULD use an administratively scoped address instead.	SHOULD	NOT REQUIRED	
RFC4566-5.7-6			IPv6 multicast does not use TTL scoping, and hence the TTL value MUST NOT be present for IPv6 multicast.	MUST	NOT REQUIRED	
RFC4566-5.7-7			They MUST NOT be specified for a session-level "c=" field.	MUST	BASIC	generic_INVITE generic_200-INVITE generic_200-OPTIONS
RFC4566-5.7-8			The slash notation for multiple addresses described above MUST NOT be used for IP unicast addresses.	MUST	OUT OF SCOPE	
RFC4566-5.8-1	5.8	Bandwidth (b=")"	CT If the bandwidth of a session or media in a session is different from the bandwidth implicit from the scope, a "b=CT:..." line SHOULD be supplied for the session giving the proposed upper limit to the bandwidth used (the "conference total" bandwidth).	SHOULD	NOT REQUIRED	
RFC4566-5.8-2			b=X-YZ:128 Use of the "X-" prefix is NOT RECOMMENDED: instead new modifiers SHOULD be registered with IANA in the standard namespace.	RECOMMENDED	NOT REQUIRED	
RFC4566-5.8-3				SHOULD	NOT REQUIRED	
RFC4566-5.8-4			SDP parsers MUST ignore bandwidth fields with unknown modifiers.	MUST	NOT REQUIRED	
RFC4566-5.8-5			Modifiers MUST be alphanumeric and, although no length limit is given, it is recommended that they be short.	MUST	NOT REQUIRED	
RFC4566-5.9-1	5.9	Timing (t=")"	Since SDP uses an arbitrary length decimal representation, this should not cause an issue (SDP timestamps MUST continue counting seconds since 1900, NTP will use the value modulo the 64-bit limit).	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-5.9-2			User interfaces SHOULD strongly discourage the creation of unbounded and permanent sessions as they give no information about when the session is actually going to terminate, and so make scheduling difficult.	SHOULD	NOT REQUIRED	
RFC4566-5.9-3			If behaviour other than this is required, an end-time SHOULD be given and modified as appropriate when new information becomes available about when the session should really end.	SHOULD	NOT REQUIRED	
RFC4566-5.12-1	5.12	Encryption Keys (k=")"	A simple mechanism for key exchange is provided by the key field ("k="), although this is primarily supported for compatibility with older implementations and its use is NOT RECOMMENDED.	RECOMMENDED	NOT REQUIRED	
RFC4566-5.12-2			If there is a need to convey this information within SDP, the extensions mentioned previously SHOULD be used.	SHOULD	NOT REQUIRED	
RFC4566-5.12-3			This method MUST NOT be used unless it can be guaranteed that the SDP is conveyed over a secure channel.	MUST	NOT REQUIRED	
RFC4566-5.12-4			This method MUST NOT be used unless it can be guaranteed that the SDP is conveyed over a secure channel.	MUST	NOT REQUIRED	
RFC4566-5.12-5			The use of user-specified keys is NOT RECOMMENDED, since such keys tend to have weak security properties.	RECOMMENDED	NOT REQUIRED	
RFC4566-5.12-6			The key field MUST NOT be used unless it can be guaranteed that the SDP is conveyed over a secure and trusted channel.	MUST	NOT REQUIRED	
RFC4566-5.13-1	5.13	Attributes (a=")"	Attribute names MUST use the US-ASCII subset of ISO-10646/UTF-8.	MUST	NOT REQUIRED	
RFC4566-5.13-2			Attributes MUST be registered with IANA (see Section 8).	MUST	NOT REQUIRED	
RFC4566-5.13-3			If an attribute is received that is not understood, it MUST be ignored by the receiver.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-5.14-1	5.14	Media Descriptions (m=")"	If non-contiguous ports are used or if they don't follow the parity rule of even RTP ports and odd RTCP ports, the "a=rtcp:" attribute MUST be used.	MUST	NOT REQUIRED	
RFC4566-5.14-2			Applications that are requested to send media to a <port> that is odd and where the "a=rtcp:" is present MUST NOT subtract 1 from the RTP port: that is, they MUST send the RTP to the port indicated in <port> and send the RTCP to the port indicated in the "a=rtcp" attribute.	MUST	NOT REQUIRED	
RFC4566-5.14-3				MUST	NOT REQUIRED	
RFC4566-5.14-4			When a list of payload type numbers is given, this implies that all of these payload formats MAY be used in the session, but the first of these formats SHOULD be used as the default format for the session.	SHOULD	OUT OF SCOPE	
RFC4566-5.14-5			For dynamic payload type assignments the "a=rtpmap:" attribute (see Section 6) SHOULD be used to map from an RTP payload type number to a media encoding name that identifies the payload format.	SHOULD	OUT OF SCOPE	
RFC4566-5.14-6			If the <proto> sub-field is "udp" the <fmt> sub-fields MUST reference a media type describing the format under the "audio", "video", "text", "application", or "message" top-level media types.	MUST	NOT REQUIRED	
RFC4566-5.14-7			The media type registration SHOULD define the packet format for use with UDP transport.	SHOULD	NOT REQUIRED	
RFC4566-5.14-8			Rules for interpretation of the <fmt> sub- field MUST be defined when registering new protocols (see Section 8.2.2).	MUST	NOT REQUIRED	
RFC4566-6-1	6		For frame-based codecs, the time SHOULD be an integer multiple of the frame size.	SHOULD	NOT REQUIRED	
RFC4566-6-2			RTP profiles that specify the use of dynamic payload types MUST define the set of valid encoding names and/or a means to register encoding names if that profile is to be used with SDP.	MUST	NOT REQUIRED	
RFC4566-6-3			Additional encoding parameters MAY be defined in the future, but codec-specific parameters SHOULD NOT be added.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-6-4			Parameters added to an "a=rtpmap:" attribute SHOULD only be those required for a session directory to make the choice of appropriate media to participate in a session.	SHOULD	NOT REQUIRED	
RFC4566-6-5			Note that recvonly applies to the media only, not to any associated control protocol (e.g., an RTP-based system in recvonly mode SHOULD still send RTCP packets).	SHOULD	NOT REQUIRED	
RFC4566-6-6			If none of the attributes "sendonly", "recvonly", "inactive", and "sendrecv" is present, "sendrecv" SHOULD be assumed as the default for sessions that are not of the conference type "broadcast" or "H332" (see below).	SHOULD	NOT REQUIRED	
RFC4566-6-7			Note that sendonly applies only to the media, and any associated control protocol (e.g., RTCP) SHOULD still be received and processed as normal.	SHOULD	NOT REQUIRED	
RFC4566-6-8			Note that an RTP-based system SHOULD still send RTCP, even if started inactive.	SHOULD	NOT REQUIRED	
RFC4566-6-9			The charset specified MUST be one of those registered with IANA, such as ISO-8859-1.	MUST	NOT REQUIRED	
RFC4566-6-10			The character set identifier is a US-ASCII string and MUST be compared against the IANA identifiers using a case-insensitive comparison.	MUST	NOT REQUIRED	
RFC4566-6-11			If the identifier is not recognised or not supported, all strings that are affected by it SHOULD be regarded as octet strings.	SHOULD	NOT REQUIRED	
RFC4566-6-12			Note that a character set specified MUST still prohibit the use of bytes 0x00 (Nul), 0x0A (LF), and 0x0d (CR).	MUST	NOT REQUIRED	
RFC4566-6-13			Character sets requiring the use of these characters MUST define a quoting mechanism that prevents these bytes from appearing within text fields.	MUST	NOT REQUIRED	
RFC4566-6-14			Instead, multiple descriptions SHOULD be sent describing the session, one in each language.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-6-15			However, this is not possible with all transport mechanisms, and so multiple sdplang attributes are allowed although NOT RECOMMENDED.	RECOMMENDED	NOT REQUIRED	
RFC4566-6-16			An "sdplang" attribute SHOULD be specified when a session is of sufficient scope to cross geographic boundaries where the language of recipients cannot be assumed, or where the session is in a different language from the locally assumed norm.	SHOULD	NOT REQUIRED	
RFC4566-6-17			A "lang" attribute SHOULD be specified when a session is of sufficient scope to cross geographic boundaries where the language of recipients cannot be assumed, or where the session is in a different language from the locally assumed norm.	SHOULD	NOT REQUIRED	
RFC4566-7-1	7	Security Considerations	Entities receiving and acting upon an SDP message SHOULD be aware that a session description cannot be trusted unless it has been obtained by an authenticated transport protocol from a known and trusted source.	SHOULD	OUT OF SCOPE	
RFC4566-7-2			In case a session description has not been obtained in a trusted manner, the endpoint SHOULD exercise care because, among other attacks, the media sessions received may not be the intended ones, the destination where media is sent to may not be the expected one, any of the parameters of the session may be incorrect, or the media security may be compromised.	SHOULD	OUT OF SCOPE	
RFC4566-7-3			Software that parses a session description MUST NOT be able to start other software except that which is specifically configured as appropriate software to participate in multimedia sessions.	MUST	NOT REQUIRED	
RFC4566-7-4			Thus, a session description arriving by session announcement, email, session invitation, or WWW page MUST NOT deliver the user into an interactive multimedia session unless the user has explicitly pre-authorised such action.	MUST	NOT REQUIRED	
RFC4566-7-5			If this is done, an application parsing a session description containing such attributes SHOULD either ignore them or inform the user that joining this session will result in the automatic transmission of multimedia data.	SHOULD	NOT REQUIRED	
RFC4566-7-6			These behaviours are NOT RECOMMENDED unless the session description is conveyed in such a manner that allows the intermediary system to conduct proper checks to establish the authenticity of the session description, and the authority of its source to establish such communication sessions.	RECOMMENDED	NOT REQUIRED	
RFC4566-7-7			SDP MUST NOT be used to convey key material, unless it can be guaranteed that the channel over which the SDP is delivered is both private and authenticated.	MUST	NOT REQUIRED	
RFC4566-7-8			The use of the "k=" line is NOT RECOMMENDED, as discussed in Section 5.12.	RECOMMENDED	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-8.2-1	8.2.1	Media Types (media")"	The set of media types is intended to be small and SHOULD NOT be extended except under rare circumstances.	SHOULD	NOT REQUIRED	
RFC4566-8.2-2			For media other than existing top-level media content types, a Standards Track RFC MUST be produced for a new top-level content type to be registered, and the registration MUST provide good justification why no existing media name is appropriate (the "Standards Action" policy of RFC 2434 [8].	MUST	NOT REQUIRED	
RFC4566-8.2-3				MUST	NOT REQUIRED	
RFC4566-8.2-4			If these media types are considered useful in the future, a Standards Track RFC MUST be produced to document their use.	MUST	NOT REQUIRED	
RFC4566-8.2-5			Until that is done, applications SHOULD NOT use these types and SHOULD NOT declare support for them in SIP capabilities declarations (even though they exist in the registry created by RFC 3840).	SHOULD	NOT REQUIRED	
RFC4566-8.2-6				SHOULD	NOT REQUIRED	
RFC4566-8.2-7	8.2.2	Transport Protocols (proto")"	This SHOULD reference a standards-track protocol RFC.	SHOULD	NOT REQUIRED	
RFC4566-8.2-8			If other RTP profiles are defined in the future, their "proto" name SHOULD be specified in the same manner.	SHOULD	NOT REQUIRED	
RFC4566-8.2-9			New transport protocols SHOULD be registered with IANA.	SHOULD	NOT REQUIRED	
RFC4566-8.2-10			Registrations MUST reference an RFC describing the protocol.	MUST	NOT REQUIRED	
RFC4566-8.2-11			Registrations MUST also define the rules by which their "fmt" namespace is managed (see below).	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-8.2-12	8.2.3	Media Formats (fmt")"	RTP payload formats under the "RTP/AVP" and "RTP/SAVP" profiles MUST use the payload type number as their "fmt" value.	MUST	NOT REQUIRED	
RFC4566-8.2-13			If the payload type number is dynamically assigned by this session description, an additional "rtpmap" attribute MUST be included to specify the format name and parameters as defined by the media type registration for the payload format.	MUST	NOT REQUIRED	
RFC4566-8.2-14			It is RECOMMENDED that other RTP profiles that are registered (in combination with RTP) as SDP transport protocols specify the same rules for the "fmt" namespace.	RECOMMENDE D	NOT REQUIRED	
RFC4566-8.2-15			For the "udp" protocol, new formats SHOULD be registered.	SHOULD	NOT REQUIRED	
RFC4566-8.2-16			If no media subtype exists, it is RECOMMENDED that a suitable one be registered through the IETF process [31] by production of, or reference to, a standards-track RFC that defines the transport protocol for the format.	RECOMMENDE D	NOT REQUIRED	
RFC4566-8.2-17			Registrations of new formats MUST specify which transport protocols they apply to.	MUST	NOT REQUIRED	
RFC4566-8.2-18	8.2.4	Attribute Names (att-field")"	Attribute field names ("att-field") MUST be registered with IANA and documented, because of noticeable issues due to conflicting attributes under the same name.	MUST	NOT REQUIRED	
RFC4566-8.2-19			Attributes that are expected to see widespread use and interoperability SHOULD be documented with a standards-track RFC that specifies the attribute more precisely.	SHOULD	NOT REQUIRED	
RFC4566-8.2-20	8.2.5	Bandwidth Specifiers (bwtype")"	New bandwidth specifiers ("bwtype" fields) MUST be registered with IANA.	MUST	NOT REQUIRED	
RFC4566-8.2-21			The submission MUST reference a standards-track RFC specifying the semantics of the bandwidth specifier precisely, and indicating when it should be used, and why the existing registered bandwidth specifiers do not suffice.	MUST	NOT REQUIRED	
RFC4566-8.2-22	8.2.6	Network Types (nettype")"	A new network type registration MUST reference an RFC that gives details of the network type and address type and specifies how and when they would be used.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4566-8.2-23	8.2.7	Address Types (addrtype")"	An address type is only meaningful in the context of a network type, and any registration of an address type MUST specify a registered network type or be submitted along with a network type registration.	MUST	NOT REQUIRED	
RFC4566-8.2-24			A new address type registration MUST reference an RFC giving details of the syntax of the address type.	MUST	NOT REQUIRED	
RFC4566-8.2-25	8.2.8	Registration Procedure	In the RFC documentation that registers SDP "media", "proto", "fmt", "bwtype", "nettype", and "addrtype" fields, the authors MUST include the following information for IANA to place in the appropriate registry:	MUST	NOT REQUIRED	
RFC4566-8.3-1	8.3	Encryption Key Access Methods	New registrations MUST NOT be accepted.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4896-3.1-1	3.1	Data Input Instructions	The intent is that if n bytes/bits are requested, but only m are left in the message (where m < n), then the decompression dispatcher MUST NOT return any bytes/bits to the UDVM, and the m bytes/bits that are there MUST remain in the message unchanged.	MUST	NOT REQUIRED	
RFC4896-3.1-2				MUST	NOT REQUIRED	
RFC4896-3.2-1	3.2	MULTILOAD	Additionally, if there is any indirection of parameters, the indirection MUST be done at execution time.	MUST	NOT REQUIRED	
RFC4896-3.2-2			Any implementation technique other than a step-by-step implementation (e.g., decode all operands then execute, which is the model of all other instructions) MUST yield the same result as a step-by-step implementation would.	MUST	NOT REQUIRED	
RFC4896-3.4-1	3.4	Using the Stack	In the very rare case that the value of stack_fill is 0xFFFF when a value is pushed onto the stack, then the original stack_fill value MUST be increased by 1 to 0x0000 and written back to stack_location and stack_location + 1 (which will overwrite the value that has been pushed onto the stack).	MUST	NOT REQUIRED	
RFC4896-5.2-1	5.2	Multiple State Retention Priorities	The retention priority MUST be associated with the compartment and not with the piece of state.	MUST	NOT REQUIRED	
RFC4896-5.2-2			If the same piece of state is created within a compartment with a different priority, then one copy of it should be stored with the new priority and it MUST count only once against SMS.	MUST	NOT REQUIRED	
RFC4896-5.3-1	5.3	Retention Priority 65535 (or -1)	SigComp [1] also states that a compressor MUST be certain that all of the data needed to decompress a SigComp message is available at the receiving endpoint.	MUST	NOT REQUIRED	
RFC4896-5.3-2			Thus, it SHOULD NOT reference any state unless it can be sure that the state exists.	SHOULD	NOT REQUIRED	
RFC4896-5.3-3			Consequently, where NACK is not supported or for NACK averse compressors, the recommendation is that only one piece of minimum priority state SHOULD be present in a compartment at any one time.	SHOULD	NOT REQUIRED	
RFC4896-6-1	6	Duplicate State	If a piece of state is created in a compartment in which it already exists, the time of its creation SHOULD be updated as if it had just been created, irrespective of whether or not there is a new state retention priority.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4896-7-1	7	State Identifier Clashes	If it does, and the state item is not identical, then the new creation MUST fail.	MUST	NOT REQUIRED	
RFC4896-8-1	8	Message Misordering	However, the statement that the 'compressor MUST ensure that the message can be decompressed using the resources available at the remote endpoint' puts the onus on the compressor to take account of the possibility of misordering occurring.	MUST	NOT REQUIRED	
RFC4896-9.1-1	9.1	Feedback When SMS Is Zero	If an endpoint receives a request for feedback, then it SHOULD return the feedback even if its SMS is zero.	SHOULD	NOT REQUIRED	
RFC4896-9.2-1	9.2	Updating Feedback Requests	Therefore, an endpoint SHOULD transmit feedback repeatedly until it receives another valid message that updates the feedback.	SHOULD	NOT REQUIRED	
RFC4896-9.2-2			However, there is no indication of whether this means that the existing feedback data is left untouched or if this means that the existing feedback data SHOULD be overwritten to be 'no feedback data'.	SHOULD	NOT REQUIRED	
RFC4896-9.2-3			If requested_feedback_location equals zero, the existing feedback data SHOULD be left untouched and returned in any subsequent messages as before.	SHOULD	NOT REQUIRED	
RFC4896-9.2-4			In this case, the existing feedback data SHOULD be overwritten to be 'no feedback data'.	SHOULD	NOT REQUIRED	
RFC4896-10.1-1	10.1	The I-bit and Local State Items	The remote endpoint SHOULD still advertise its parameters such as DMS and state memory size (SMS).	SHOULD	NOT REQUIRED	
RFC4896-10.2-1	10.2	Dynamic Update of Resources	The compressor MUST NOT use more than the most recently advertised resources.	MUST	NOT REQUIRED	
RFC4896-10.2-2			Reducing the resources has potential synchronization issues and so SHOULD NOT be done unless absolutely necessary.	SHOULD	NOT REQUIRED	
RFC4896-10.2-3			If this is the case then the memory MUST NOT be reclaimed until the remote endpoint has acknowledged the message sent with the advertisement.	MUST	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4896-10.2-4			If state is to be deleted to accommodate a reduction in SMS then both endpoints MUST delete it according to the state retention priority (see RFC 3320- Section 6.2).	MUST	NOT REQUIRED	
RFC4896-10.2-5			The compressor MUST NOT then use more than the amount of resources most recently advertised.	MUST	NOT REQUIRED	
RFC4896-10.3-1	10.3	Advertisement of Locally Available State Items	Note that any definitions of uses of locally available state items MUST NOT conflict with any other uses.	MUST	NOT REQUIRED	
RFC4896-10.3-2	10.3.1	Basic SigComp	Without further definition, locally available state SHOULD NOT be used.	SHOULD	NOT REQUIRED	
RFC4896-10.3-3			RFC 3320-Section 6.2 allows for the possibility to map locally available state items to a compartment and states that, if this is done, the state items MUST have state retention priority 65535 in order to not interfere with state created at the request of the remote compressor.	MUST	NOT REQUIRED	
RFC4896-10.3-4			Note that Section 5.3 also recommends that only one such piece of state SHOULD be created per compartment.	SHOULD	NOT REQUIRED	
RFC4896-10.3-5	10.3.3	SigComp Extended Mechanisms	Since there is no guarantee of such state being available beyond its normally defined lifetime, endpoints SHOULD only attempt to access the state after this time where it is known that NACK [3] is available.	SHOULD	NOT REQUIRED	
RFC4896-16.2-1	16.2	Informative References	Each line of message-header MUST be terminated with CRLF.	MUST	NOT REQUIRED	
RFC4896-16.2-2			The empty line MUST be present even if the message-body is not.	MUST	NOT REQUIRED	
RFC4896-16.2-3			For implementation according to this appendix, the DAP-version MUST be set to 1.	MUST	NOT REQUIRED	
RFC4896-16.2-4			Therefore, the receiver SHOULD use the (endpoint-ID, compartment-ID) pair carried in a message to determine the decompressor compartment identifier for that message.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC4896-16.2-5			As mentioned above, the response message MUST be compressed by, and sent from, the local compressor compartment that is a peer of the remote compressor compartment.	MUST	NOT REQUIRED	
RFC4896-16.2-6			A sensible implementation of a DAP sender SHOULD NOT blindly set this field to TRUE unless a response is desired.	SHOULD	NOT REQUIRED	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC5049-3-1	3	Compliance with This Specification	Any SigComp implementation that is used for the compression of SIP messages MUST conform to this document, as well as to [RFC3320].	MUST	BASIC	doc_reference
RFC5049-4-1	4	Minimum Values of SigComp Parameters for SIP/SigComp	For each parameter, [RFC3320] specifies a minimum value that any SigComp endpoint MUST support for ANY/SigComp.	MUST	OUT OF SCOPE	
RFC5049-5-1	5	Delimiting SIP Messages and SigComp Messages on the Same Port	Note that SigComp message delimiters MUST NOT be used if the stream contains uncompressed SIP messages.	MUST	NOT REQUIRED	
RFC5049-5-2			Applications MUST NOT mix SIP messages and SigComp messages on a single TCP connection.	MUST	NOT REQUIRED	
RFC5049-5-3			If the TCP connection is used to carry SigComp messages, then all messages sent over the connection MUST have a SigComp header and be delimited by the use of 0xFFFF, as described in [RFC3320].	MUST	NOT REQUIRED	
RFC5049-7-1	7	Too-Large SIP Messages	Therefore, if a SIP application sending compressed SIP messages to another SIP application over a transport connection (e.g., a TCP connection) needs to send a SIP message larger than 64k, the SIP application MUST NOT send the message over the same TCP connection.	MUST	NOT REQUIRED	
RFC5049-7-2			The SIP application SHOULD send the message over a different transport connection (to do this, the SIP application may need to establish a new transport connection).	SHOULD	NOT REQUIRED	
RFC5049-8-1	8	SIP Retransmissions	Implementations MUST NOT cache the result of compressing the message and retransmit such a cached result.	MUST	OUT OF SCOPE	
RFC5049-9.1-1	9.1	Remote Application Identification	Each SIP/SigComp application MUST have a SIP/SigComp identifier URN (Uniform Resource Name) that uniquely identifies the application.	MUST	OUT OF SCOPE	
RFC5049-9.1-2			This URN MUST be persistent as long as the application stores compartment state related to other SIP/SigComp applications.	MUST	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC5049-9.1-3			A SIP/SigComp application SHOULD use a UUID (Universally Unique IDentifier) URN as its SIP/SigComp identifier, due to the difficulties in equality comparisons for other kinds of URNs.	SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC5049-9.1-4			If a URN scheme other than UUID is used, the URN MUST be selected such that the application can be certain that no other SIP/SigComp application would choose the same URN value.	MUST	OUT OF SCOPE	
RFC5049-9.1-5			A device with a globally unique instance identifier SHOULD use its instance identifier as its SIP/SigComp identifier.	SHOULD	OUT OF SCOPE	
RFC5049-9.1-6			Server farms that share SIP/SigComp state across servers MUST use the same SIP/SigComp identifier for all their servers.	MUST	NOT REQUIRED	
RFC5049-9.1-7			The SIP URI 'sigcomp-id' parameter MUST contain a URN [RFC2141].	MUST	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC5049-9.1-8			The Via 'sigcomp-id' parameter MUST contain a URN [RFC2141].	MUST	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC5049-9.1-9			A SIP/SigComp application placing its URI with the 'comp=sigcomp' parameter in a header field MUST add a 'sigcomp-id' parameter with its SIP/SigComp identifier to that URI.	MUST	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC5049-9.1-10			A SIP/SigComp application generating its own Via entry containing the 'comp=sigcomp' parameter MUST add a 'sigcomp-id' parameter with its SIP/SigComp identifier to that Via entry.	MUST	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC5049-9.2-1	9.2	Identifier Comparison Rules	As a result, the SIP/SigComp application SHOULD provide lexically equivalent URNs in each registration it generates.	SHOULD	NOT REQUIRED	
RFC5049-9.3-1	9.3	Compartment Opening and Closure	A SIP application that needs to send a compressed SIP REGISTER (i.e., a user agent generating a REGISTER or a proxy server relaying one to its next hop) SHOULD open a compartment for the request's remote application identifier.	SHOULD	OUT OF SCOPE	
RFC5049-9.3-2			A SIP application that receives a compressed SIP REGISTER (i.e., the registrar or a proxy relaying the REGISTER to its next-hop) SHOULD open a compartment for the request's remote application identifier.	SHOULD	NOT REQUIRED	
RFC5049-9.3-3			For a given successful registration, applications SHOULD NOT close their associated compartments until the registration is over.	SHOULD	OUT OF SCOPE	

Priority Number	Section	Section Title	Functional Specification	Status	Test Priority	Test Profile
RFC5049-9.3-4			If, following the rules above, a SIP application is supposed to open a compartment for a remote application identifier for which it already has a compartment (e.g., the SIP application registers towards a second registrar using the same edge proxy server as for its registration towards its first registrar), the SIP application MUST use the already existing compartment.	MUST	OUT OF SCOPE	
RFC5049-9.3-5			That is, the SIP application MUST NOT open a new compartment.	MUST	OUT OF SCOPE	
RFC5049-9.4-1	9.4	Lack of a Compartment	"If the next-hop URI contains the parameter comp=sigcomp, the client SHOULD compress the request using SigComp".	SHOULD	BASIC	UE-SC-B-1-AKA UE-SC-B-2-AKA
RFC5049-10-1	10	Recommendations for Network Administrators	It is RECOMMENDED that registrars are configured so that proxies performing SigComp compression appear in both routes.	RECOMMENDED	NOT REQUIRED	
RFC5049-10-2			It is RECOMMENDED that the proxies performing SigComp that are in the route for requests outside a dialog are configured to place themselves (by inserting themselves in the Record-Route header fields) in the routes used for requests inside dialogs.	RECOMMENDED	NOT REQUIRED	
RFC5049-10-3			In order to avoid this situation, it is RECOMMENDED that user agents are registered as long as they are involved in a dialog.	RECOMMENDED	OUT OF SCOPE	
RFC5049-13-1	13	Interactions with Transport Layer Security (TLS)	Since the gain of having SigComp code compressed should be minimal in most cases, it is NOT RECOMMENDED to use TLS compression when SigComp compression is being used.	RECOMMENDED	NOT REQUIRED	