SIP Core SIP Technology Enhancements

Last Updated: December 20, 2011

The SIP: Core SIP Technology Enhancements feature updates Cisco SIP VoIP gateways with the latest changes in RFC 2543-bis-04. All changes are compatible with older RFC versions. Compliance to RFC 2543-bis-04 adds enhanced SIP support and ensures smooth interoperability and compatibility with multiple vendors.

The enhanced areas are as follows:

SIP URL Comparison

When a URL is received, the URLs are compared for equality. URL comparison can be done between two From SIP URLs, or it can be done between two To SIP URLs. For two URLs to be equal, the user, password, host, and port parameters must match. The order of the parameters does not to match.

The SIP: Core SIP Technology Enhancements feature changes the parameters allowed in SIP URLs. The maddr parameter and the transport parameter are not allowed in Cisco SIP gateway implementations. The user-param parameter is now the parameter for comparison.

If a compared parameter is omitted or not present, it is matched on the basis of its default value. The table below shows a list of SIP URL compared parameters and their default values.

Table 1   SIP URL Parameter Comparison

SIP URL Compared Parameter	Default
host	mandatory
password	--
port	5060
user	--
user-param	ip

The following is an example of equivalent URLs:

Original URL:

sip:36602@172.18.193.120

Equivalent URLs:

sip:36602@172.18.193.120:

sip:36602@172.18.193.120;tag=499270-A62;pname=pvalue

sip:36602@172.18.193.120;user=ip

sip:36602@172.18.193.120:5060

487 Sent for BYE Requests

RFC 2543-bis-04 requires that a user agent server (UAS) that receives a BYE request first send a response to any pending requests for that call before disconnecting. The SIP: Core SIP Technology Enhancements feature recommends that after receiving a BYE request the UAS respond with a 487 (Request Cancelled) status message.

3xx Redirection Responses

The processing of 3*xx* redirection responses was updated in the SIP: Core SIP Technology Enhancements feature as follows:

- The Uniform Resource Identifier (URI) of the redirected INVITE is updated to contain the new contact information provided by the 3*xx* redirect message.
- The transmitted CSeq number found in the CSeq header is increased by one. The new INVITE includes the updated CSeq.
- The To, From, and Call ID headers that identify the call leg remain the same. The same Call ID gives consistency when capturing billing history.
- The user agent client (UAC) retries the request at the new address given by the 3*xx* Contact header field.

See the for a sample call flow that shows the updated CSeq numbers.

DNS SRV Query Procedure

When a Request URI or the session target in the dial peer contains a fully qualified domain name (FQDN), the UAC needs to determine the protocol, port, and IP address of the endpoint before it forwards the request. SIP on Cisco gateways uses a Domain Name System Server (DNS SRV) query to determine the protocol, port, and IP address of the user endpoint.

Before the SIP: Core SIP Technology Enhancements feature, the DNS query procedure did not take into account the destination port.

CANCEL Request Route Header

The SIP: Core SIP Technology Enhancements feature does not allow a CANCEL message sent by a UAC on an initial INVITE request to have a Route header. Route headers cannot appear in a CANCEL message because they take the same path as INVITE requests, and INVITE requests cannot contain Route headers.

Interpret User Parameters

Telephone-subscriber or user parameters in an incoming INVITE message may contain extra characters to incorporate space, control characters, quotation marks, hash marks, and other characters. The SIP: Core SIP Technology Enhancements feature allows, the telephone-subscriber or user parameter to be interpreted before dial-peer matching is done. For example, the telephone number in an incoming INVITE message may appear as:

-%32%32%32

Although 222 is a valid telephone number, it requires interpretation. If the interpretation is not done, the call attempt fails when the user parameter is matched with the dial-peer destination pattern.

user=phone Parameter

A SIP URL identifies a user's address, whose appearance is similar to that of an e-mail address. The form of the user's address is *user@host* where *user* is the user identification and *host* is either a domain name or a numeric network address. For example, the request line of an outgoing INVITE request might appear as:

INVITE sip:5550002@companyb.com

With the SIP: Core SIP Technology Enhancements feature.The *user=phone* parameter formerly required in a SIP URL is no longer necessary. However, if an incoming SIP message has a SIP URL with *user=phone, user=phone* is parsed and used in the subsequent messages of the transaction.

303 and 411 SIP Cause Codes

The SIP: Core SIP Technology Enhancements feature obsoletes the SIP cause codes 303 *Redirection: See Other* and 411 *Client Error: Length required* .

Flexibility of Content-Type Header

The SIP: Core SIP Technology Enhancements feature allows the Content-Type header, which specifies the media type of the message body, to have an empty Session Description Protocol (SDP) body.

Optional SDP s= Line

The SIP: Core SIP Technology Enhancements feature accepts the "s=" line in SDP as optional. The "s=" line describes the reason or subject for SDP information. Cisco SIP gateways can create messages with an "s=" line in SDP bodies and can accept messages that have no "s=" line.

Allow Header Addition to INVITEs and 2xx Responses

The SIP: Core SIP Technology Enhancements feature enables the use of the Allow header in an initial or re-INVITE request or in any 2*xx* class response to an INVITE. The Allow header lists the set of methods supported by the user agent that is generating the message. Because it advertises what methods should be invoked on the user agent sending the message, it avoids congesting the message traffic unnecessarily. The Allow header can contain any or all of the following: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, NOTIFY, INFO, SUBSCRIBE.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information

about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Simultaneous Cancel and 2xx Class Response

According to RFC 2543-bis-04, if the UAC desires to end the call before a response is received to an INVITE, the UAC sends a CANCEL. However, if the CANCEL and a 2*xx* class response to the INVITE "pass on the wire", the UAC also receives a 2*xx* to the INVITE. The SIP: Core SIP Technology Enhancements feature ensures that when the two messages pass, the UAC terminate the call by sending a BYE request.

Prerequisites for SIP Core SIP Technology Enhancements

- Ensure that your Cisco router has the minimum memory requirements necessary for voice capabilities.
- Establish a working IP network.
- Configure VoIP.

Cisco Unified Border Element

- Cisco IOS Release 12.2(13)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for SIP Core SIP Technology Enhancements

- Via handling for TCP was not implemented in the Cisco SIP: Core SIP Technology Enhancements feature.

How to Configure SIP Core SIP Technology Enhancements

The SIP: Core SIP Technology Enhancements features are all enabled by default, and no special configurations is necessary. However, several of these features can be monitored through the use of various commands. See the following sections for monitoring tasks for the SIP: Core SIP Technology Enhancements feature. Each task in the list is optional:

Monitoring 487 Sent for BYE Requests

When a UAS responds with a 487 after receiving a BYE request, the *Client Error: Request Cancelled* counter increments in the **show sip-ua statistics** command.

SUMMARY STEPS

1. **enable**
2. **show sip-ua statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**show sip-ua statistics** **Example:** `Router# show sip-ua statistics`	(Optional) Displays response, traffic, and retry statistics for the SIP user agent (UA).

Example

The following sample output from the **show sip-ua statistics** command with the *Client Error: Request Cancelled* counter incremented:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
    Success:
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OKSubscribe 0/0, OkNotify 0/0,
      202Accepted 0/0
    Redirection (Inbound only):
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0, UseProxy 0,
      AlternateService 0
    Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
      UnsupportedMediaType 0/0, BadExtension 0/0,
```

```
                TempNotAvailable 0/0, CallLegNonExistent 0/0,
                LoopDetected 0/0, TooManyHops 0/0,
                AddrIncomplete 0/0, Ambiguous 0/0,
                BusyHere 0/0, RequestCancel 0/1
                NotAcceptableMedia 0/0, BadEvent 0/0
            Server Error:
                InternalError 0/0, NotImplemented 0/0,
                BadGateway 0/0, ServiceUnavail 0/0,
                GatewayTimeout 0/0, BadSipVer 0/0,
                PreCondFailure 0/0
            Global Failure:
                BusyEverywhere 0/0, Decline 0/0,
                NotExistAnywhere 0/0, NotAcceptable 0/0
    SIP Total Traffic Statistics (Inbound/Outbound)
            Invite 0/0, Ack 0/0, Bye 0/0,
            Cancel 0/0, Options 0/0,
            Prack 0/0, Comet 0/0,
            Subscribe 0/0, Notify 0/0,
            Refer 0/0
    Retry Statistics
            Invite 0, Bye 0, Cancel 0, Response 0,
            Prack 0, Comet 0, Reliable1xx 0, Notify 0
    SDP application statistics:
     Parses: 0,  Builds 0
     Invalid token order: 0,  Invalid param: 0
     Not SDP desc: 0,  No resource: 0
```

Monitoring 3xx Redirection Responses

The processing for 3*xx* redirection responses was updated in the SIP: Core SIP Technology Enhancements feature. The new implementation can be monitored with the **debug ccsip messages** command.

SUMMARY STEPS

1. **enable**
2. **debug ccsip message**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ccsip message** **Example:** Router# debug ccsip message	Displays all SIP Service Provider Interface (SPI) message tracing. • Use this command to enable traces for SIP messages exchanged between the SIP user agent client (UAC) and the access server.

Example

The following is **debug ccsip message** output from an originating gateway. The output shows message transactions including the new INVITE message for the redirected address. The output has been updated as follows:

- The URI of the redirected INVITE is updated to contain new contact information provided by the 3*xx* redirect message.
- The transmitted CSeq number found in the CSeq header is increased by one. The new INVITE includes the updated CSeq.
- The To, From, and Call ID headers that identify the call leg remain the same.
- The UAC retries the request at the new address given by the 3*xx* Contact header field.

```
Sent:
INVITE sip:3111100@64.102.17.80:5060; SIP/2.0
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 730947050
Contact: <sip:36601@172.18.193.98:5060>
Expires: 180
Content-Type: application/sdp
Content-Length: 160
v=0
o=CiscoSystemsSIP-GW-UserAgent 2378 4662 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 19202 RTP/AVP 18
a=rtpmap:18 G729/8000
Received:
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 //Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 101 INVITE
Contact: Anonymous <sip:36602@172.18.193.120 //Provides Request URI with the new contact
address.
Contact: Anonymous <sip:36601@172.18.193.98>
Sent:
ACK sip:3111100@64.102.17.80:5060; SIP/2.0
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Max-Forwards: 6
Content-Length: 0
CSeq: 101 ACK
Sent:
INVITE sip:36602@172.18.193.120:5060 SIP/2.0 //URI updated with new contact/redirect
address.
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 102 INVITE //Transmitted CSeq is increased by one.
Max-Forwards: 6
Timestamp: 730947050
```

```
Contact: <sip:36601@172.18.193.98:5060>
Expires: 180
Content-Type: application/sdp
Content-Length: 159
v=0
o=CiscoSystemsSIP-GW-UserAgent 5957 524 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 17018 RTP/AVP 18
a=rtpmap:18 G729/8000
```

Monitoring the Deletion of 303 and 411 Cause Codes

The processing for Monitoring the Deletion of 303 and 411 Cause Codes was updated in the SIP: Core SIP Technology Enhancements feature. The new implementation can be monitored with the **show sip-ua statistics** and **show sip-ua map** commands.

SUMMARY STEPS

1. **enable**
2. **show sip-ua statistics**
3. **show sip-ua map**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show sip-ua statistics** **Example:** `Router# show sip-ua statistics`	Displays response, traffic, and retry statistics for the SIP UA. • Can be used to verify the deletion of the 303 and 411 cause codes.
Step 3	**show sip-ua map** **Example:** `Router# show sip-ua map`	Displays the mapping table of PSTN cause codes and their corresponding SIP error status codes or the mapping table of SIP-to-PSTN codes. • Can be used to verify the deletion of 411 cause codes.

Examples

The following examples provide different ways to monitor the deletion of the 303 and 411 cause codes.

show sip-ua statistics Command

The following is sample output of the **show sip-ua statistics** command that includes the *SeeOther* (303) and *LengthRequired* (411) fields is from the Cisco IOS version before the SIP: Core SIP Technology Enhancements feature:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/4, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/5
    Success:
      OkInvite 0/2, OkBye 1/1,
      OkCancel 0/2, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OkNotify 0/0, 202Accepted 0/0
    Redirection (Inbound only):
      MultipleChoice 0, MovedPermanently 0,
MovedTemporarily 0, SeeOther 0,
      UseProxy 0, AlternateService 0
    Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      LengthRequired 0/0, ReqEntityTooLarge 0/0,
      ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
      BadExtension 0/0, TempNotAvailable 0/0,
      CallLegNonExistent 0/0, LoopDetected 0/0,
      TooManyHops 0/0, AddrIncomplete 0/0,
      Ambiguous 0/0, BusyHere 0/0
      RequestCancel 0/2, NotAcceptableMedia 0/0
    Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
    Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 5/0, Ack 4/0, Bye 1/1,
    Cancel 2/0, Options 0/0,
    Prack 0/0, Comet 0/0,
    Notify 0/0, Refer 0/0
Retry Statistics
    Invite 0, Bye 0, Cancel 0, Response 0,
    Prack 0, Comet 0, Reliable1xx 0, Notify 0
```

The following is sample output of the **show sip-ua statistics** command from a Cisco IOS version after implementing the SIP: Core SIP Technology Enhancements feature and shows that the *SeeOther* and *LengthRequired* fields are now omitted is from fields:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
    Success:
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OKSubscribe 0/0, OkNotify 0/0,
      202Accepted 0/0
    Redirection (Inbound only):
```

```
                     MultipleChoice 0, MovedPermanently 0,
                     MovedTemporarily 0, UseProxy 0,
                     AlternateService 0
                  Client Error:
                     BadRequest 0/0, Unauthorized 0/0,
                     PaymentRequired 0/0, Forbidden 0/0,
                     NotFound 0/0, MethodNotAllowed 0/0,
                     NotAcceptable 0/0, ProxyAuthReqd 0/0,
                     ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
                     ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
                     UnsupportedMediaType 0/0, BadExtension 0/0,
                     TempNotAvailable 0/0, CallLegNonExistent 0/0,
                     LoopDetected 0/0, TooManyHops 0/0,
             AddrIncomplete 0/0, Ambiguous 0/0,
                     BusyHere 0/0, RequestCancel 0/0
                     NotAcceptableMedia 0/0, BadEvent 0/0
                  Server Error:
                     InternalError 0/0, NotImplemented 0/0,
                     BadGateway 0/0, ServiceUnavail 0/0,
                     GatewayTimeout 0/0, BadSipVer 0/0,
                     PreCondFailure 0/0
                  Global Failure:
                     BusyEverywhere 0/0, Decline 0/0,
                     NotExistAnywhere 0/0, NotAcceptable 0/0
             SIP Total Traffic Statistics (Inbound/Outbound)
                  Invite 0/0, Ack 0/0, Bye 0/0,
                  Cancel 0/0, Options 0/0,
                  Prack 0/0, Comet 0/0,
                  Subscribe 0/0, Notify 0/0,
                  Refer 0/0
             Retry Statistics
                  Invite 0, Bye 0, Cancel 0, Response 0,
                  Prack 0, Comet 0, Reliable1xx 0, Notify 0
             SDP application statistics:
              Parses: 0,  Builds 0
              Invalid token order: 0,  Invalid param: 0
              Not SDP desc: 0,  No resource: 0
```

show sip-ua map

The following example is sample output from the **show sip-ua map** command and shows that SIP cause code 411 is omitted from the group of cause codes.

```
Router# show sip-ua map sip-pstn
SIP-Status    Configured      Default
              PSTN-Cause      PSTN-Cause
400           127             127
401            57             57
402            21             21
403            57             57
404             1             1
405           127             127
406           127             127
407            21             21
408           102             102
409            41             41
410             1             1
413           127             127
414           127             127
415            79             79
420           127             127
480            18             18
481           127             127
482           127             127
483           127             1
```

Configuration Examples for SIP Core SIP Technology Enhancements

This section provides a general SIP configuration example:

SIP Core SIP Technology Enhancements Example

This example contains output from the **show running-config** command.

```
Router# show running-config
Building configuration...
Current configuration : 2791 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
interface FastEthernet2/0
ip address 172.18.200.24 255.255.255.0
duplex auto
no shut
speed 10
ip rsvp bandwidth 7500 7500
!
voice-port 1/1/1
no supervisory disconnect lcfo
!
dial-peer voice 1 pots
application session
destination-pattern 5550111
port 1/1/1
!
dial-peer voice 3 voip
application session
destination-pattern 5550112
session protocol sipv2
session target ipv4:172.18.200.36
codec g711ulaw
!
dial-peer voice 4 voip
application session
destination-pattern 5550133
session protocol sipv2
session target ipv4:172.18.200.33
codec g711ulaw
!
gateway
!
sip-ua
   retry invite 1
   retry bye 1
!
line con 0
line aux 0
line vty 0 4
```

```
login
!
end
```

Feature Information for SIP Core SIP Technology Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

ISR Feature History Information.

Table 2   *Feature Information for SIP: Core SIP Technology Enhancements*

Feature Name	Releases	Feature Information
SIP: Core SIP Technology Enhancements	12.2(13)T 12.2(15)T	Compliance to RFC 2543-bis-04 adds enhanced SIP support and ensures smooth interoperability and compatibility with multiple vendors. The following commands were modified: **debug ccsip messages, show sip-ua map**, **show sip-ua statistics**,and.

ASR Feature History Information.

Table 3   *Feature Information for SIP: Core SIP Technology Enhancements*

Feature Name	Releases	Feature Information
SIP: Core SIP Technology Enhancements	Cisco IOS XE Release 2.5	Compliance to RFC 2543-bis-04 adds enhanced SIP support and ensures smooth interoperability and compatibility with multiple vendors. The following commands were modified: **debug ccsip messages, show sip-ua map**, **show sip-ua statistics**,and.