SIP Protocol Trunk Features

Revised: May 3, 2007, OL-5352-12

As the previous chapter described, Cisco BTS 10200 Release 4.5.x supports the SIP protocol by addressing two aspects of SIP: SIP subscribers and SIP trunks. This chapter encompasses SIP trunks.

The purpose of SIP trunks is to service SIP calls between Cisco BTS 10200 and external SIP entities other than local SIP subscribers, such as a voice-mail server, remote call agent or SIP proxy.

SIP Trunk Properties

Cisco BTS 10200 can be configured to use UDP or TCP transport for communications over a SIP trunk. A SIP trunk is configured in Cisco BTS 10200 with the following:

- IP address or Fully Qualified Domain Name (FQDN) and port for address information of external SIP entity.
- Dial plan and dialed digit string entries for routing.
- Profile to define the feature set for a SIP trunk.

SIP Trunk Characteristics

SIP trunk characteristics include the following:

- Typically, one trunk is defined for each external SIP entity communicating with Cisco BTS 10200 over SIP.
- Multiple trunks can be associated to a provisioned route set providing “route advance” functionality.
- SIP trunks have OAM state and status, and can be set “in service” and “out of service” by the administrator.
- SIP trunks currently will not set themselves “out of service” if the remote SIP entity does not respond.
- Trunks can be defined as one of three possible trunk types: SIP, SIP-T and CMSS.
- External SIP entities are addressed as follows:
  - SIP-T trunk must communicate with Cisco BTS 10200 using the SIP-T protocol.
  - CMSS trunk must communicate with Cisco BTS 10200 using the PacketCable CMSS specification (partially supported in Release 4.5.x).

  - SIP trunk must communicate with Cisco BTS 10200 using standard SIP protocol.
- A regular SIP call may be received on a SIP-T trunk.
- Multiple trunks can be defined to the same external SIP entity IP address and port, using the BGID/TGID SIP trunk feature.

Outbound Cisco BTS 10200 SIP Call

Inbound calls on Cisco BTS 10200 are processed by the Cisco BTS 10200 routing system. The routing system selects an outbound SIP trunk based on the digits dialed and dial plan of the originating entity. The SIP call is then transmitted out a TCP or UDP socket toward the IP address associated to the trunk selected by routing. SIP call features and characteristics are applied to the outbound call based on the feature selections in the trunk profile associated with the trunk.

RFC 3398 states that any outbound SIP number with NOA of NATIONAL must be prefixed with "+CCnumber" which is an international format, and any number with NOA=subscriber must be formatted also with international significance. The sending of the full E.164 format is enabled by a flag (send-full-e164) in the softsw-tg-profile table to enable interworking with downstream devices that require this number format.

Inbound Cisco BTS 10200 SIP Call

For inbound calls, the SIP call is received on a TCP or UDP socket. The Cisco BTS 10200 determines which SIP trunk the call is associated with, by comparing the address of the previous hop SIP entity in the VIA header of a request, with the IP addresses associated with the provisioned SIP trunks, for a match.

If the previous hop SIP entity is represented by an FQDN, then Cisco BTS 10200 compares it against SIP trunks associated to this FQDN. If the SIP call is not associated to any trunk, the call is refused, unless of course it is identified to be from a local Cisco BTS 10200 subscriber.

The SIP call is then sent to the routing system with the trunk identification. The routing system uses the dial plan associated with the inbound trunk and the dialed digits to make routing decisions for the outbound direction.

SIP Trunk Features

- Session Timers
- SIP Timer Values
- SIP-T, ISUP Version, ISUP-Transparency, and GTD
- DTMF SIP Signaling
- Asserted Identity and User-Level Privacy
- Third-Party Call Control
- ANI-Based Routing
- Trunk Group Audit for the SIP Adapter
- T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface

Validation of Source IP Address for Incoming SIP Messages (Release 4.5.1, Maintenance Release 1)

The system is capable of performing source IP address validation of incoming messages received on SIP trunks. This validation process is intended to reduce the risk of security attacks, which can occur if a packet is sniffed in the network and then sent from a different or rogue IP address, or domain, as present in the Via header. By default, IP address validation is disabled on the Cisco BTS 10200 Softswitch. The service provider can enable this capability using the SIA-TG-VALIDATE-SOURCE-IP token in the ca-config table. This is a switch-wide parameter, and applies to all SIP trunk groups.

Provisioning details can be found in the Chapter 2 of the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Hop Counter and Maximum Forwards Parameters

The system supports provisionable parameters in the softsw-tg-table that allow control of the maximum-forwards and hop-counter fields of the SIP Invite message:

- HOP-COUNTER-MAX
- HOP-COUNTER-SUPP
- MAX-FORWARDS
- SCALE-FACTOR

Note The hop count between SIP and SS7 networks is scaled appropriately in the Cisco BTS 10200 Softswitch based on the provisioning of the SCALE-FACTOR token.

The description and relationship of these parameters are provided in the "Softswitch Trunk Group Profile" section on page 5-2.

Call Redirection

Call Redirection allows a remote SIP endpoint receiving a call from the Cisco BTS 10200 to re-route the call back on the Cisco BTS 10200, using one or more destinations provided by the endpoint. It also supports load sharing and redundancy solutions used by other switches or applications interworking with Cisco BTS 10200 using SIP. These solutions typically involve a front-end SIP network management server to manage load sharing and redundancy for back-end servers.

The Cisco BTS 10200 honors the redirection (SIP 300 class) response to a SIP INVITE call request, and redirects the call using the specifications outlined in RFC 3261. The Cisco BTS 10200 Softswitch does not support sending a redirection response.

When a redirection response is received with multiple contacts, multiple redirections are attempted in serial in the order the contacts were received. This includes contacts received in subsequent redirection responses, in which case the contacts are appended to the serial list of redirections being attempted. Redirections are attempted up to a provisioned limit at which point Cisco BTS 10200 releases the call. There is also a provisioned limit to the number of 300 class responses received for any given call.

Cisco BTS 10200 requires redirection contacts to have a SIP URL format. The user information field of the SIP URL must be present and contain a numeric phone number and a host name. The following example illustrates the SIP URI format:

```
sip:2125553333@phone.cisco.com
```

Call redirection is not supported on SIP trunks provisioned with a business group. Cisco BTS 10200 does not support an incoming 300 class response from a local Cisco BTS 10200 SIP subscriber.

When the Cisco BTS 10200 selects a contact from the 300 class redirection response to perform a call redirection, it decides how the redirection is done based on the number and host name in the contact's SIP URL. If the host name is the same as the configured SIP contact, the Cisco BTS 10200 routes the call using the number in the user portion of the redirected contact URL. If this number also matches the called number in the redirected INVITE, then the Cisco BTS 10200 routes by advancing to the next trunk in the provisioned route set. This is called "route-advance." If this number does not match the previously called number, the Cisco BTS 10200 determines the next trunk to send the call out by performing routing on the new number. This is called a "reroute."

Note A provisionable parameter allows the service provider to force the system to use the reroute method regardless of whether the redirect number matches the number in the initial INVITE. This parameter is part of the call agent configuration and affects all SIP trunks on the switch.

If the host name field of the redirection contact selected for call redirection matches the provisioned TSAP address of a provisioned Cisco BTS 10200 SIP trunk, the Cisco BTS 10200 redirects the call out this trunk without going through the Cisco BTS 10200 routing system. The number in the contact is set as the called party number in the Request URI of the redirected INVITE.

If the host name field does not match the SIP contact of the Cisco BTS 10200 or the TSAP address of any of the provisioned SIP trunks, then the call is redirected toward the host identified in the contact UR. This contact URI is used as the request URL for the redirected call. The redirected call uses the properties of the SIP trunk in the previous call attempt, and the call does not go through the Cisco BTS 10200 routing system. However, if the profile of this SIP trunk restricts redirection to contacts having host names matching only SIP trunks or Cisco BTS 10200 contact, then redirection is not performed for this contact.

If the diversion feature is enabled for the Cisco BTS 10200 SIP trunk selected for call redirection, and the last redirection response received contained diversion headers, these headers are populated in the newly redirected call. This follows the diversion rules.

With call redirection, users can provision a limit on the maximum number of 300 class redirection responses the Cisco BTS 10200 accepts while performing redirection on any given call attempt; the default is 1. The feature also allows a user provisioned limit for the maximum number of actual call redirection attempts the Cisco BTS 10200 makes on any given call attempt; the default is 5. These provisioning parameters are part of the call agent configuration and apply to all SIP trunks.

Users can enable or disable call redirection for any provisioned SIP trunk. By default, call is enabled to accept contacts only with host names of the Cisco BTS 10200 SIP contact, or the TSAP address of any provisioned SIP trunks. This provisioning parameter is part of the Softswitch trunk group profile.

Provisioning details for call redirection can be found in the Call Redirection section in Chapter 2 of the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Locating SIP Servers Using DNS Queries

This section explains how the system locates SIP servers, which it can do by either of the following methods:

- Using information from an incoming request.
- Using the SIP trunk provisioning in the database.

Locating SIP Servers from an Incoming Request

The Cisco BTS 10200 Softswitch can request and accept TCP connections. The system provides for the selection of TCP or UDP on trunk groups with or without SRV support. When accepting connections, the Cisco BTS 10200 Softswitch listens for and accepts TCP connection requests. It also listens for incoming requests on UDP. Once a request is received, the system sends SIP responses using the same transport type as the associated request. If this occurs over a TCP connection and the connection still exists, the system reuses that connection. If the connection is gone, the system attempts to establish a new connection to the same address.

Locating SIP Servers from an Outbound Request

The NAPTR and SRV DNS functions allow the Cisco BTS 10200 Softswitch SIP interface to correctly interoperate with proxy farms and find proxies and redirect servers. Operators can designate some service hosts as primary servers, and others as backup. When provisioned to support NAPTR and SRV functions, the Cisco BTS 10200 Softswitch discovers the most preferred transport protocol of the locally supported destination, and obtains an SRV query string to locate a server supporting that protocol. The system follows the procedures described in RFC2782 and RFC3263 to determine the transport, IP address, and port for the next hop.

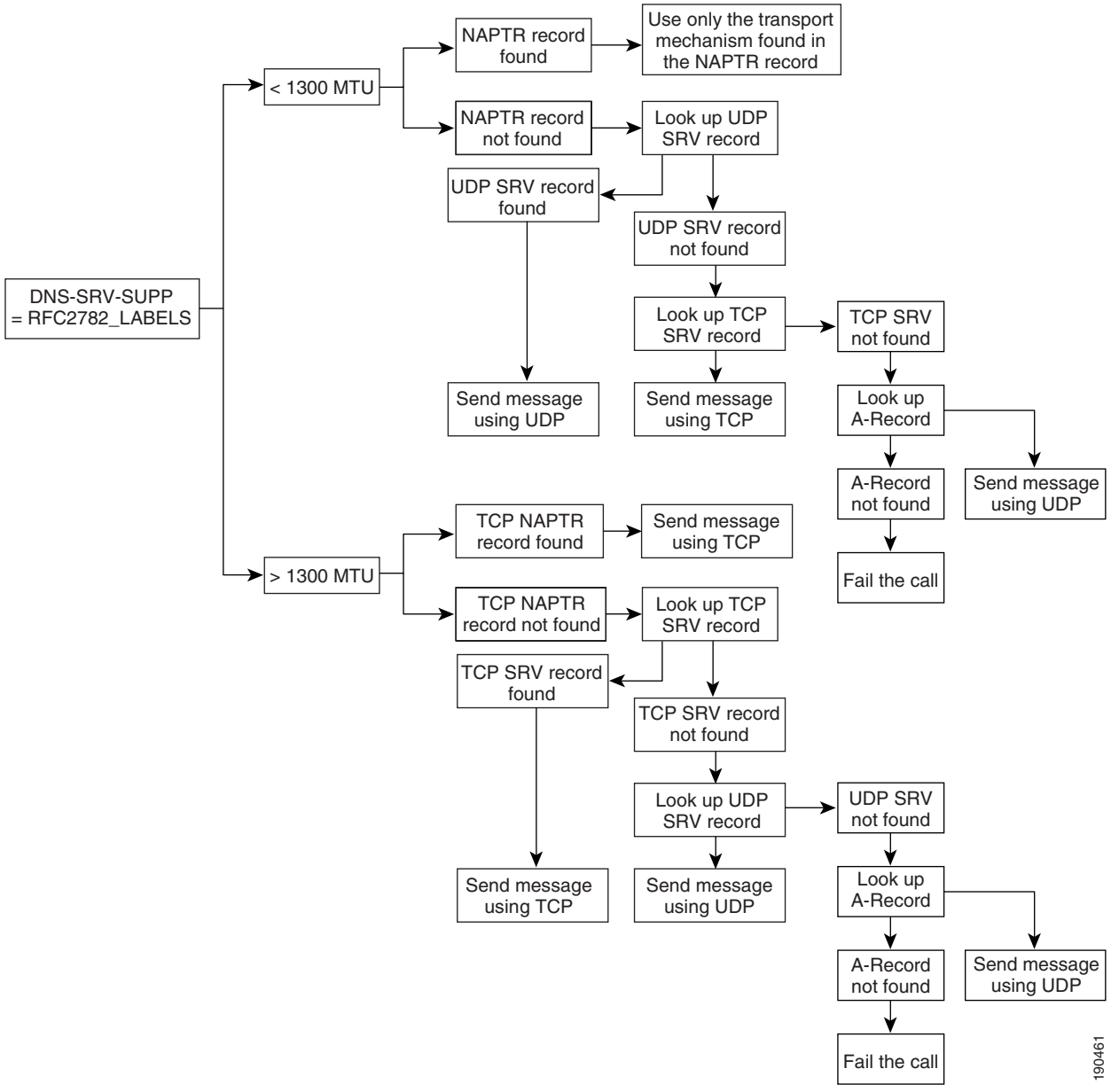
Note To provision NAPTR and SRV support, set the DNS-SRV-SUPP field in the SOFTSW-TG-PROFILE table to RFC2782_LABELS.

The NAPTR lookup procedure depends on the size of the message compared to the path maximum transmission unit (MTU) size stated in RFC3261 and RFC3263 (typically 1300 bytes). The implementation in the Cisco BTS 10200 Softswitch is based on the SIP Working Group Document

Issue 760 (http://bugs.sipit.net/show_bug.cgi?id=760). That document provides guidance regarding the conflicting directives between RFC3261 and RFC3263 when a message size exceeds the MTU limit and NAPTR lookups are involved. The system processes the lookup as described in this section.

Figure 3-1 shows the transport selection procedure for sending SIP requests based on NAPTR and SRV records, that is, when the value of the DNS-SRV-SUPP token is provisioned as RFC2782_LABELS.

Figure 3-1 Transport Selection for Sending SIP Requests Based on NAPTR and SRV



Following is an explanation of the logic shown in Figure 3-1.

- If the message size is less than the path MTU limit, the sequence is as follows:

a. The system looks up a NAPTR record, and chooses a transport protocol based on the priority of the NAPTR record. Only that chosen transport protocol is used to route the message, and servers associated with other protocols are not contacted.

b. If no NAPTR record is found, the system performs a best-effort lookup by assuming that an SRV record exists that has the same name as the NAPTR record. The procedure continues as follows:

– A UDP SRV record is looked up first, using the _sip._udp prefix. If it is resolved, the servers on the resulting list are contacted and UDP transport is used to send the message.

– If no UDP SRV record is found, a TCP SRV record is searched, using the _sip._tcp prefix. If it is resolved, the servers on the resulting list are contacted and TCP transport is used to send the message.

- If the message size is greater than the path MTU limit, the sequence is as follows:

a. The system performs a NAPTR lookup for records supporting TCP transport only. The resulting query string from the NAPTR lookup is used to perform an SRV lookup. If it is resolved, the servers on the resulting list are contacted and TCP transport is used to send the message.

b. If no NAPTR record is found, the system performs a best-effort lookup by assuming that an SRV record exists. the procedure continues as follows:

– A locally generated query string is used to query SRV records, using TCP as preferred transport and the _sip._tcp prefix. If such a record is found, servers on the resulting list are contacted and TCP transport is used to send the message.

– If no TCP SRV record is found, a UDP SRV record for the same TSAP address (prefixed with _sip._udp) is searched. If such a record is found, all servers on the resulting list are contacted and UDP transport is used to send the message.

The following details apply to all DNS queries described above:

- The above procedure (selecting only a single transport) applies only to NAPTR or SRV provisioning, that is, when the following are both true:
  – The SIP trunk profile is provisioned with SRV support enabled.
  – The TSAP address is provisioned with either a NAPTR or SRV name.
- After the system selects a transport type, only that type is used for signaling. If the chosen transport does not work, the system does not attempt any other transport mechanism, and the call fails.
- If the NAPTR and SRV queries fail, the system attempts a best-effort A-record query and uses UDP to send the message.

Tip These steps add overhead to the process of resolving an address. Therefore, SRV should only be enabled if the benefits of the address resolution procedure are required.

Traversing the SRV List for Failure Responses and Retransmission Timeouts

This section describes how the Cisco BTS 10200 Softswitch traverses the SRV list.

- 503 Response—When the Cisco BTS 10200 Softswitch receives a 503 response (service unavailable) from the server in the SRV list that was last attempted, it resubmits the same request as a new transaction (with a new branch ID) to the next IP address in the SRV list.

- Retransmission timer expires—If an SRV server receiving the INVITE does not respond within the retransmission timer period, the Cisco BTS 10200 Softswitch can send the next retransmission of the same request to the same server (as recommended in RFC3263), or to the next server in the SRV list (legacy Cisco BTS 10200 Softswitch behavior). This is controlled using a provisionable flag, DNS_SRV_ADV_ON_RETRANS_TIMEOUT on the SOFTSW-TG-PROFILE table:
  - If DNS_SRV_ADV_ON_RETRANS_TIMEOUT is set to N, all retransmissions of a message are exhausted sending to a single address before attempting to send to the next address. Keep in mind that some calls may not complete if one of the nodes in an SRV list returns a 503 message, even though other nodes in the list are capable of handling the request successfully.
  - If it is set to Y (the default value), the system retransmits the same request as a new transaction (with a new branch ID) to the next IP address in the SRV list.

A-Record DNS Queries for Outgoing Messages

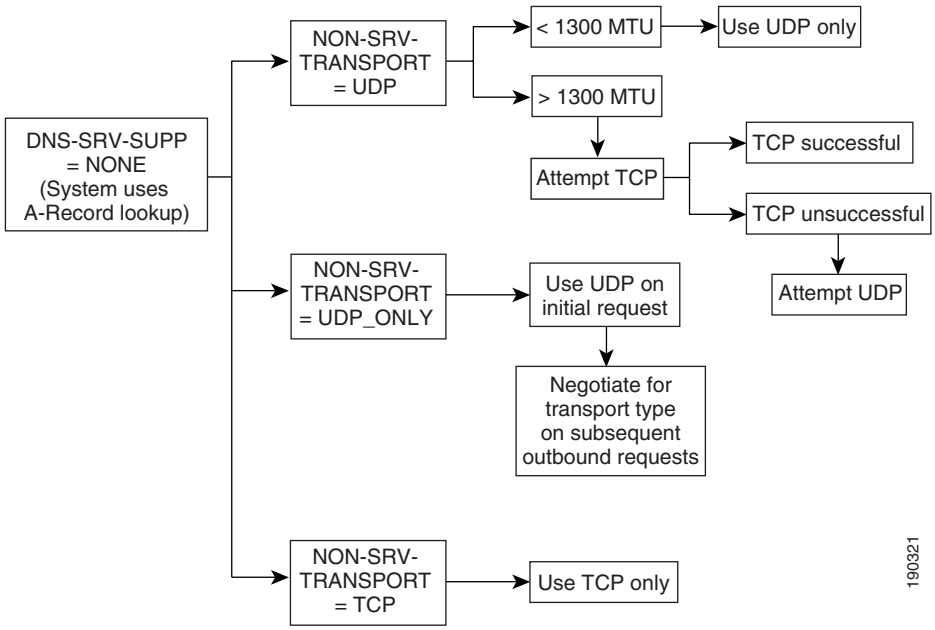
The system can use A-record DNS queries to locate SIP servers. The system selects this DNS query and the transport mechanism based on the value of the DNS-SRV-SUPP field in the SOFTSW-TG-PROFILE table. If this field is set to NONE, the transport is selected based on the NON-SRV-TRANSPORT field of the SOFTSW-TG-PROFILE table. Possible values for this field are as follows:

- UDP (default)—If the message size is less than 1300 bytes as described in RFC 3261 and RFC 3263, the system uses UDP. If the message size is greater than 1300 bytes, the system uses TCP; however, if TCP fails, the system attempts to use UDP.
- UDP-ONLY—The initial outbound request uses UDP regardless of the message size. However, the transport used for subsequent outbound requests is based on the negotiated transport type exchanged in the Contact: header during dialog establishment.
- TCP—Use TCP only.

When performing an A-record DNS query, the system tries each IP address to which the FQDN resolves, (in succession) when there is a failure to communicate with the destination SIP endpoint. The system does this for both UDP and TCP transport mechanisms.

Figure 3-2 shows the transport selection procedure for sending SIP requests based on A-Record queries, that is, when the value of the DNS-SRV-SUPP token is provisioned as NONE.

Figure 3-2 Transport Selection for Sending SIP Requests Based on A-Record Lookup



Provisioning Commands

To provision the parameters in the SIP trunk that affect DNS query procedures, see the DNS query provisioning procedure in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

Type of Service

The SIP Type of Service (ToS) feature provides the ability to configure the Cisco BTS 10200 such that SIP signaling traffic is sent at a desired priority over IP. This is important because SIP messages travel over the same network as the voice traffic. If this network is congested, the voice data may delay the SIP signaling packets, causing unnatural delay when calls are set up. Raising the SIP packets priority in relation to other traffic reduces the delay.

Users can set the ToS value on a system-wide basis or on a per trunk group basis. The policy is selected in the call agent configuration. If system-wide ToS is selected, the ToS value is also specified in the call agent configuration.

The default SIP ToS value for system level ToS selection is as follows:

- Precedence = FLASH (3)
- Delay = low (Y)
- Throughput = normal (N)
- Reliability = normal (N)

Note Cisco does not recommend using any value other than the specified default. Changing the value from its default may significantly impact network performance. Consult Cisco support for assistance.

Caution If you change any parameters in the ca-config table, these changes do not take effect until the CA platform switches over or restarts.

If Cisco BTS 10200 cannot read the SIP ToS configuration values from the call agent configuration, it initializes the ToS level to the default and selects the system level ToS policy.

If SIA-TRUNK-GRP-LEVEL-SIG-TOS is set to Y in the call agent configuration, Cisco BTS 10200 uses the trunk group's ToS level for every message sent on the trunk group. If any message is sent out to any endpoint other than a provisioned trunk group, the system level ToS is used.

Alternately, Cisco BTS 10200 can be provisioned to use the SIP trunk's provisioned ToS level for every SIP message sent out a particular SIP trunk. The system level ToS is used for SIP messages sent out to the Cisco BTS 10200 local SIP subscriber endpoints.

Reliable Provisional Responses

SIP defines two types of responses, provisional and final. Final responses convey the result of the request processing, and are sent reliably. Provisional responses provide progress information about the request processing, but are not sent reliably in the base SIP protocol. The reliable provisional responses feature provides end-to-end reliability of provisional responses across Cisco BTS 10200 SIP trunks.

Provisional responses in SIP telephony calls represent backward alerting and progress signaling messages, which are important when interoperating with PSTN networks. Therefore, for SIP-T calls on the Cisco BTS 10200, reliable provisional responses are mandatory. They are optional for regular SIP calls.

Cisco BTS 10200 support for this feature follows the specifications described in RFC 3262. A provisioning flag is provided to enable or disable this feature, and is disabled by default. For SIP trunks provisioned as "SIP-T," the system internally ignores the flag and enables the feature always. In this case, the feature is mandatory. Therefore, the ability to enable or disable the feature applies to regular SIP trunks only. There is one exception: SIP-T trunks receiving SIP-T calls (calls with ISUP attachments) may also receive incoming regular SIP calls. In this case, the feature (enabled or disabled) for that regular SIP call is determined by the provisioning flag on that SIP-T trunk. The provisioning flag (PRACK_FLAG) is a member of the Softswitch Trunk Group profile. For provisioning details, refer to the provisioning guide.

For calls received on a Cisco BTS 10200 regular SIP trunk, or regular SIP (non-SIP-T) calls received on a SIP-T trunk, the following feature behavior applies:

- If the received INVITE indicates this feature is required, all provisional responses are sent reliably, regardless of the provisioned feature setting on the trunk.
- If the received INVITE indicates this feature is supported, then all provisional responses are sent reliably if the feature is provisioned enabled on the trunk.
- If the received INVITE indicates the feature is not supported, the call is refused if the feature is enabled on the trunk.
- If the received INVITE indicates the feature is not supported, the call is accepted if the feature is disabled on the trunk. Provisional responses are not sent reliably.

For calls sent out a Cisco BTS 10200 regular SIP trunk, the following feature behavior applies:

- If the feature is provisioned enabled on the trunk, the SIP Invite message sent contains a 'Required' header with a tag value of '100rel'.

- If the feature is enabled on the trunk, and the remote endpoint supports or requires the feature, all provisional responses are sent reliably to Cisco BTS 10200.
- If the feature is enabled on the trunk, and the remote endpoint does not support the feature, the remote endpoint refuses the call.
- If the feature is disabled on the trunk, the SIP Invite message sent contains a 'Supported' header with a tag value of '100rel'.
- If the feature is disabled on the trunk, and the remote endpoint supports the feature, the remote endpoint controls which provisional response sent requires reliability.
- If the feature is disabled on the trunk, and the remote endpoint does not support the feature, provisional responses are not received reliably.

For SIP-T calls received on a Cisco BTS 10200 SIP trunk provisioned as SIP-T, the following feature behavior applies:

- If the received INVITE indicates this feature is required or supported, all provisional responses are sent reliably.
- If the received INVITE indicates the feature is not supported, the call is refused.

For all calls sent out a Cisco BTS 10200 SIP trunk provisioned as SIP-T, the following feature behavior applies:

- The SIP-T INVITE message sent contains a 'Required' header with a tag value of '100rel.'
- If the remote endpoint supports or requires the feature, all provisional responses are sent reliably to Cisco BTS 10200.
- If the remote endpoint does not support the feature, the remote endpoint refuses the call.

Diversion Indication

Diversion indication provides supplemental redirection information to the SIP entity receiving the call. The SIP entity uses this information to identify from whom the call was diverted, and why the call was diverted. It also provides information for each redirection if multiple redirections occurred. This is provided in the form of a SIP 'Diversion:' header.

Forwarding information allows applications such as SIP voice-mail servers to access the mailbox of the original called party for proper outgoing greeting and message deposit when a forwarded call is received. Billing systems also use the information to determine the charged party of the call where it is the last forwarding party that is billed.

The BTS 10200 supports this feature following the specifications described in the IETF draft draft-levy-sip-diversion-02.txt. For incoming calls, Cisco BTS 10200 uses the party number information from the top-most and bottom-most diversion headers. The Cisco BTS 10200 reads the diversion counter, across all diversion headers to determine the total diversion count. For outgoing calls, The BTS 10200 sends 0, 1 or 2 diversion headers, depending on the forwarding information of the call.

Diversion header parameters support is limited to the diversion 'counter' and the diversion 'reason.' These two parameters in diversion headers are populated for outgoing calls and interpreted on incoming calls.

For INVITEs sent out on a BTS 10200 SIP trunk with the diversion feature enabled, the following behavior applies:

- If no diversion information is available, no diversion headers are included.
- If there is an 'original called' party, one diversion header is added to the outgoing INVITE message.

- If there is a ‘last forwarding’ party, a second diversion header is added on top of the original called party diversion header.
- Each outgoing diversion header is populated with the party number, the diversion reason and diversion count. A BGID is added to a diversion header as a token parameter if the feature for business group identification is enabled, and the diversion number is in a Centrex format.
- For Release 4.5.1, Maintenance Release 2 and later—Privacy parameters are sent and received in the Diversion header.

For INVITEs received on a SIP trunk with the diversion feature enabled, the following behaviors apply:

- If no diversion headers are present in the incoming message, no diversion information is identified.
- If exactly one diversion header is present in the incoming message, the number in the diversion header is identified as the ‘original called’ party number. The diversion ‘reason’ and ‘count’ are also interpreted.
- If more than one diversion headers are present in the incoming message, the bottom-most diversion header determines the ‘original called’ number. The top-most diversion header determines the ‘last forwarding’ party and diversion reason. The total diversion count is determined by the summation of the diversion counter values across all the diversion headers received. The rest of the diversion information is ignored.
- If the diversion feature is disabled and diversion headers are present, the diversion headers do not determine diversion information for call processing. They are ignored.
- If the diversion feature is disabled on a provisioned SIP-T trunk, and the trunk receives a call on that trunk with an INVITE number in the ‘To:’ field that differs from the Request URL number, then the ‘To:’ field number is interpreted as the ‘original called’ number. Any diversion headers present are ignored.

Users can enable or disable diversion indication for a provisioned SIP trunk in the softswitch trunk group profile table; the feature is disabled by default. For provisioning details, see the “Diversion Indication” section in the *SIP Protocol Provisioning Guide*.

Carrier Identification Code over SIP

Support for the carrier identification code (CIC) over SIP allows a SIP to PSTN gateway entity receiving a call to determine which carrier the originator prefers to handle the call. This parameter value may indicate which long distance carrier the originator has subscribed to handle the call.

Cisco BTS 10200 support for this feature follows the specifications described in the IETF draft ‘draft-yu-tel-url-07.’ Support for CIC is limited to local CIC formats. Global CIC formats, which use country code, are not supported. If a global CIC is received, the global part is ignored and the call is processed using the local portion.

For calls sent out over a Cisco BTS 10200 SIP trunk, the CIC, when available, can be added as a parameter of the user portion of the Request URI of the outgoing INVITE message. The CIC value is derived either from the subscriber record, in the case of local subscriber originated call, or from the 'transit-network-select' information if the call was received from a PSTN origination. The option to send the CIC parameter on the outbound SIP trunk is provisioned using the send-cic-param token in the softsw-tg-profile table.

For calls received on a Cisco BTS 10200 SIP trunk, if the CIC parameter is present in the received SIP INVITE then the value of the CIC is identified for call processing. If the CIC was received in global format, the country code component of the CIC is ignored.

For local Cisco BTS 10200 subscribers, the CIC is provisioned in the subscriber record.

Number Portability Information over SIP

Number portability (NP) allows a subscriber to move geographically within the network domain without requiring a change to the subscriber's phone number. NP information is sent with the initial SIP INVITE message. The information indicates to the receiving switch if a previous switch has performed a database query to get routing information of the terminating subscriber. If the terminating subscriber has moved, the NP information routing number (RN) indicates the destination switch the terminating subscriber has moved to.

Cisco BTS 10200 support for this feature follows the specifications described in the IETF draft 'draft-yu-tel-url-07.'

For calls sent out a Cisco BTS 10200 SIP trunk, the NP information is added as parameters in the user portion of the Request URL of the outgoing INVITE message. A number portability dip indication (NPDI) flag is added to indicate a database query for NP information was performed, and the routing number (RN) parameter value pair is added to indicate the switch the terminating subscriber has moved to.

For calls received on a Cisco BTS 10200 SIP trunk, if the NPDI and RN parameters are present in the received SIP INVITE, then this NP information is identified for call processing.

The signal ported number flag in the trunk group configuration enables or disables the population of NP information for SIP calls sent out a SIP trunk. The default is to send NP information on the outgoing SIP call if the information is available. If NP information is included for an incoming call, the information is used in call processing regardless of the provisioned flag setting. For provisioning details, refer to the provisioning guide.

SIP Trunk Subgroups

Multiple SIP trunk groups may be provisioned toward a single SIP endpoint (same IP address and port destination) differing only by a trunk subgroup identifier. Calls sent or received on these SIP sub-trunk groups contain the trunk subgroup identifier in the SIP request message identifying the trunk group.

Remote SIP servers or switches requiring additional network-specific or application-specific properties for calls to and from Cisco BTS 10200 use the SIP trunk subgroups feature. A remote SIP entity may require Cisco BTS 10200 to identify from which call rate center a call originated. A SIP trunk subgroup may be provisioned to represent one of the rate centers. Each trunk has a unique subgroup identifier. Routing tables can be configured to select the trunk that represents the rate center, and the calls sent out the SIP trunk then include the unique rate center identifier.

For any INVITE sent out a SIP trunk subgroup by Cisco BTS 10200, a Cisco BTS 10200 proprietary SIP URL parameter 'tgid' is added to the request URI. The 'tgid' value is retrieved from the SIP trunk subgroup the call is sent out on.

An example of this parameter syntax follows:

```
INVITE      sip:50001@vm.cisco.com:5060;user=phone;tgid=grpA SIP/2.0
From:       <sip:50603@bts.cisco.com;user=phone>;tag=1_1146_f40077_3jwv
To:          <sip:50586@bts.cisco.com;user=phone>
```

When the Cisco BTS 10200 Softswitch receives a call on a SIP trunk subgroup from a remote SIP endpoint, the endpoint is required to send the 'tgid' parameter to identify the trunk subgroup. The value must match one of the provisioned trunk subgroups. The 'tgid' type is specified in the trunk-sub-grp-type field in the softsw-tg-profile table, and the 'tgid' value is provisioned in the trunk-sub-grp field of the trunk-grp table.

Note The ‘bgid’ and ‘tgid’ parameters are mutually exclusive. Only one can be enabled on a trunk.

Session Timers

Release 4.5.x enhances SIP timers and introduces the sip-timer-profile table to provision session timer values. The session timer values are provisioned in the sip-timer-profile table, then the id of the sip-timer-profile table record is specified as the Value for the ca-config record of Type=sip_timer_profile_id. If you provision the timer values for a specific trunk (by pointing to a sip-timer-profile in the softsw-tg-profile), that overrides the ca-config default.

Note To configure SIP protocol and session timers in Release 4.5.x, you must use the new sip-timer-profile table. For customers upgrading to Release 4.5.x: SIP session timer values configured in the ca-config table prior to Release 4.5.x are reset to the default values after upgrading to Release 4.5.x.

This SIP extension allows for a periodic refresh of SIP sessions using a SIP re-INVITE or UPDATE request. The refresh allows the Cisco BTS 10200 SIP interface to determine if a SIP session is still active. If the session is inactive, possibly because the session did not end normally, the Cisco BTS 10200 sends a SIP BYE request and cleans up resources dedicated to the session. Stateful SIP proxies and the remote SIP endpoint handling the BYE request can clean up resources dedicated to this session as well.

Cisco BTS 10200 support for the session timer follows specifications described in the IETF draft ‘draft-ietf-sip-session-timer-08.’ Session durations are configured within a range of 30 minutes to 2 hours. Cisco BTS 10200 does not allow for negotiating a session less than 15 minutes. This feature does not require the session timer capability on the remote SIP endpoint.

If the Cisco BTS 10200 call agent switches over during an active call with a session timer active, the session timer is deactivated. In this scenario, if the Cisco BTS 10200 were the negotiated refresher of the session timer, a call release may occur on expiration of the session timer.

Users can enable or disable the session timer feature for a provisioned SIP trunk; the feature is disabled by default. The session timer is enabled by means of the session-timer allowed flag in the Softswitch Trunk Group profile.

When the session timer is enabled on the SIP trunk and an initial INVITE is sent by Cisco BTS 10200, a Supported header with a ‘timer’ value is added, as is a Session-Expires header with Refresher parameter set to ‘Uac’. Whenever the SIP call is sent from a Cisco BTS 10200 SIP trunk, Cisco BTS 10200 sets itself to be the refresher. If session timer is not supported on the remote end, the value sent in the Session-Expires header is set for the session duration. A periodic refresh request is sent by Cisco BTS 10200 at half of the negotiated Session-Expires value.

When this feature is enabled on the SIP trunk and an initial INVITE is received by Cisco BTS 10200 with a Supported header with ‘timer’ value and a Session-Expires header, it sends a 200 class response with a Require header specifying ‘timer,’ and a Session-Expires header and refresher parameter. The Session-Expires header contains a session duration and refresher value set to whatever was received in the initial INVITE. If the refresher parameter is not received in the initial Invite, Cisco BTS 10200 sets it to ‘Uas,’ indicating Cisco BTS 10200 is the refresher. Cisco BTS 10200 sends periodic refresh request at half the negotiated session duration.

When session timer is enabled on the SIP trunk and an initial INVITE is received by Cisco BTS 10200 without a Supported header with ‘timer’ value or a Session-Expires header, a 200 class response is sent without a Require header with ‘timer’ value, or a Session-Expires header. Cisco BTS 10200 sends periodic refresh request at half the negotiated session duration.

When session timer is disabled on the SIP trunk and an initial INVITE is sent by Cisco BTS 10200, no Supported header with 'timer' value or a Session-Expires header is added, indicating to the remote SIP endpoint that the Cisco BTS 10200 does not support session timer.

When the feature is disabled on the SIP trunk and an initial INVITE is received by Cisco BTS 10200, any session timer related headers are ignored. The 200 class response does not include a Require header with 'timer' value or a Session-Expires header.

Configurable parameters in the sip-timer-profile table allow the user to select the desired session duration (SESSION-EXPIRES-DELTA-SECS) and the minimum tolerable session duration (MIN-SE) if negotiated down by the remote SIP endpoint or proxy. If the parameters are not explicitly specified, the default session duration is 30 minutes and the minimum tolerable session duration allowed is 15 minutes.

A session that is not refreshed at the end of the duration interval results in a call release and session clean-up.

Note When the SESSION-EXPIRES-DELTA-SECS timer expires, the BTS 10200 might send a Re-Invite (as opposed to an Update) with the previously sent SDP. If the BTS 10200 receives a 200 OK with the SDP changed from the previously received SDP, the BTS 10200 does not send this changed SDP to the origination.

To provision these timers, see the Session Timers section in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

SIP Timer Values

For information on enhancements made to the SIP timers in Release 4.5.x, see the "SIP Timer Values" section on page 2-23.

SIP-T, ISUP Version, ISUP-Transparency, and GTD

SIP-T provides a standard for SIP to PSTN interworking. It provides seamless bridging between two PSTN networks by encapsulating ISUP information as a binary (non-GTD type) or textual (GTD type) SIP attachment body. It also provides the standard to interwork a SIP network with the PSTN by specifying the SIP header translation for SIP-PSTN gateways.

Cisco BTS 10200 support for SIP-T follows the specifications described in RFC 3372, RFC 3398, and RFC 3204. For details on how call signaling information elements are mapped between a SIP-T message (headers and encapsulated ISUP) and an SS7/ISDN message, contact your Cisco account team.

SIP-T ISUP formats supported by the Cisco BTS 10200 include GTD, Q761_HONGKONG (ITU), and ANSI GR-317. These values are provisioned using the SIPT-ISUP-VER field in the softsw-tg-profile (SIP trunk group profile) table. When a SIP-T message is sent out from the Cisco BTS 10200, it always indicates to the receiver that handling the ISUP is optional using the SIP content disposition header. A SIP-T call is refused if an initial INVITE is received with an unsupported ISUP version attached, and the message indicates that ISUP handling is not optional. If the ISUP handling was optional, the call proceeds by ignoring the ISUP information.

A SIP-T trunk is provisioned by setting the protocol type to SIP-T, and specifying one of the supported ISUP versions in the SIP trunk profile. When the system sends a SIP-T message with encapsulated ISUP, the SIP-T trunk sends the ISUP version, and the version label is set to the one provisioned. If there is a custom alias name for that version, the alias name is used in the message instead of the version label. This is accomplished by provisioning the SIPT-ISUP-VER-ALIAS table. The base parameter in the

message is set according to RFC 3204 in line with the version chosen. Since the base is optional, it may be removed from the SIP INVITE message using provisioning. Note that the GTD type does not include a base parameter regardless.

The provisioning system for defining a SIP-T trunk imposes the rule that the reliable provisional response feature is enabled.

The system supports ISUP versions applicable to SIP-T and SIP-GTD. To provision these parameters, see the "SIP-T, ISUP Version, ISUP-Transparency, and GTD" section in the *SIP Protocol Provisioning Guide*.

Note GTD parameters can be used to support ISUP transparency between the Cisco BTS 10200 Softswitch and the Cisco PSTN Gateway (PGW) 2200. For more information on provisioning this feature, see the "ISUP Transparency on the BTS-PGW Interface" section in the *Cisco BTS 10200 Softswitch Provisioning Guide*. For a description of this feature, see the "ISUP Transparency with the Cisco PGW 2200" section in the *Cisco BTS 10200 Softswitch System Description*.

DTMF SIP Signaling

This section provides the following information about DTMF SIP signaling:

- Feature Description
- Exceptions and Limitations

Feature Description

DTMF SIP signaling allows a remote SIP endpoint to receive SIP notifications from a Cisco BTS 10200 SIP trunk when a Cisco BTS 10200 local subscriber presses a DTMF digit on the handset during a SIP call. This notification identifies which digit was pressed, and for how long it was pressed. DTMF SIP signaling is used when a remote SIP endpoint requires DTMF notifications to drive interactive voice response (IVR) applications, and the DTMF notification information cannot be sent using the bearer path.

This feature sends DTMF notifications via SIP INFO or NOTIFY request messages from the Cisco BTS 10200 SIP trunk. The NOTIFY mechanism of delivering DTMF digits follows the mechanism described in draft-mahy-sip-signaled-digits-00.txt.

The remote SIP endpoint generic uses the SUBSCRIBE/NOTIFY mechanism to subscribe to the Cisco BTS 10200 SIP interface for telephone-event notifications. The mechanism is described in 'draft-roach-sip-subscribe-notify-03.' Alternatively, the SIP INFO method for notification of telephone events may be used for unsolicited notifications. Cisco BTS 10200 only sends DTMF notifications out SIP trunks. It does not support receiving notifications. Users can enable or disable the DTMF SIP signaling feature for a provisioned SIP trunk and the feature is disabled by default.

DTMF notifications are sent using the SIP INFO or NOTIFY request method, depending on the provisioning selection for the feature. The notifications are only sent within an active SIP call dialog.

If the INFO method is selected, Cisco BTS 10200 sends an INFO message once for each digit pressed. These messages are delivered to the contact address if Cisco BTS 10200 received the original INVITE, or to the initial INVITE's Request URI if Cisco BTS 10200 originated the call. The remote SIP endpoint must respond with a 200 response. The INFO method is specified in RFC 2976.

The following is an example of an INFO message sent from Cisco BTS 10200 when a subscriber has pressed the DTMF digit '1' for 250 milliseconds:

```
INFO sip:subscriber@remoteDomain.com SIP/2.0
Via: SIP/2.0/UDP bts.cisco.com:5060
From: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
To: Subscriber <sip:subscriber@remoteDomain.com>;tag=1234-ABCD
Call-ID: 12345@bts.cisco.com
CSeq: 102 INFO
Content-Type: application/dtmf-relay
Content-Length: 22
Signal=1
Duration=250
```

If the Notify method is selected for this feature, the Cisco BTS 10200 sends two notify requests each time a DTMF button is pressed, once when the digit is pressed and once when the button is released. However, the feature does not send or buffer notifications during the SIP call unless the remote SIP endpoint has subscribed for these notifications during an active SIP call. DTMF notifications are sent over SIP during an active subscription until the subscription expires. A subscription expires if the call is released or if the subscription is not refreshed (re-subscribed) before its specified subscription duration. Either side may send indication of subscription expiry if an error occurred.

The following is an example of a subscription received on a Cisco BTS 10200 SIP trunk. In the example, the subscriber requests all telephone events that occur longer than 2000 milliseconds. The duration of the subscription requested is 1 hour (3600 seconds):

```
SUBSCRIBE sip:notifier@bts.cisco.com SIP/2.0
Via: SIP/2.0/UDP vocaldata.com:5060
From: Subscriber <sip:subscriber@vocaldata.com>;tag=1234-ABCD
To: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
Call-ID: 12345@bts.cisco.com
CSeq: 102 SUBSCRIBE
Contact: Subscriber <sip:subscriber@vocaldata.com>
Event: telephone-event;duration=2000
Expires: 3600
Content-Length: 0
```

A 200 OK response is immediately sent from the Cisco BTS 10200 for the SUBSCRIBE, indicating the SUBSCRIBE message was received. The Cisco BTS 10200 sends an Expires header in this response to indicate what the subscription duration actually is. It may choose to reduce the subscription interval.

An initial NOTIFY is immediately sent to the remote endpoint, as soon as the subscription is created or refreshed. The following is an example this initial notify request:

```
NOTIFY sip:subscriber@vocaldata.com SIP/2.0
Via: SIP/2.0/UDP bts.cisco.com:5060
From: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
To: Subscriber <sip:subscriber@vocaldata.com>;tag=1234-ABCD
Call-ID: 12345@bts.cisco.com
CSeq: 103 NOTIFY
Contact: Notifier <sip:notifier@bts.cisco.com>
Event: telephone-event;rate=1000
Content-Type: audio/telephone-event
Content-Length: 0
```

When an event is notified to the endpoint using the Notify request method, two Notify requests are sent indicating the beginning and end of the DTMF digit pressed. Each request contains the digit pressed and the duration in an encoded bit-mask. An example or this request follows. Consult the DTMF draft for the format of the bit-mask:

```
NOTIFY sip:subscriber@vocaldata.com SIP/2.0
Via: SIP/2.0/UDP bts.cisco.com:5060
From: Notifier <sip:notifier@bts.cisco.com>;tag=bts-1234
```

```
To: Subscriber <sip:subscriber@vocaldata.com>;tag=1234-ABCD
Call-ID: 12345@bts.cisco.com
CSeq: 104 NOTIFY
Contact: Notifier <sip:notifier@bts.cisco.com>
Event: telephone-event;rate=1000
Content-Type: audio/telephone-event
Content-Length: 4
0x0B0F0300
```

Exceptions and Limitations

The following limitations apply to the implementation of this feature on the Cisco BTS 10200 Softswitch:

- The system does not support out-of-band (OOB) DTMF relay for local SIP subscribers (subscribers registered directly with the Cisco BTS 10200 Softswitch).
- The system does not support inbound DTMF messages, and responds as follows when it receives an inbound DTMF message:
  - If the system receives an incoming NOTIFY for an event name other than “message_summary” (voice mail notification), it rejects the NOTIFY with a 400 (Unknown Event Specified) response.
  - If the system receives an incoming INFO with any content on a SIP trunk, it rejects the message with a 501 (Not Implemented) response.
  - If the system receives an INFO with a DTMF attachment on a SIP-T trunk during a connected call, it rejects the message with a 415 (Unsupported media type) response. This is because the system accepts only ISUP attachments on a SIP-T trunk during a connected call, and rejects all other attachment types with a 415 response.
  - If the system receives an INFO or NOTIFY message out of dialog, it rejects the message with a 481 (Call Leg/Transaction does not exist) response.
  - If the system receives an INFO before a call is in connected state, or from a subscriber, it rejects the message with a 501 (Not Implemented) response.

Asserted Identity and User-Level Privacy

The Asserted Identity feature is described in RFC 3325 and enables a network of trusted SIP servers to assert the identity of authenticated users. According to RFC 3323, when privacy features are applied to SIP messages, the calling party information (ANI) is unavailable to network elements in a trusted network domain, and inhibits network features such as call trace. The asserted identity allows these features to work because the ANI is provided in an asserted identity header, and shared across all network nodes in the trust domain. When the SIP message is exiting a trust domain, the header may be removed for privacy requirements.

Asserted identity is limited in its usage to specialized networks with trust domains as specified in RFC 3325. In Cisco BTS 10200, it is provided only in a limited context. This feature is associated to a Cisco BTS 10200 SIP trunk. It is designed to map calling party information from SS7 (or other non-SIP networks) into a SIP network as defined by the PacketCable CMSS 1.5 specification.

The feature is enabled by setting the USE-PAI-HDR-FOR-ANI flag in the SIP trunk group profile. If this flag is set to Y, calling party information is derived exclusively from the PAI header on inbound calls. For outbound calls, a PAI header is always sent with the calling party information if provided. If this flag is set to N, calling party information is mapped, sent, and received using the From: header. Details of

mapping ANI using the SIP From: header on Cisco BTS 10200 can be obtained from your Cisco account team. A provisioning example is provided in the *Cisco BTS 10200 Softswitch SIP Protocol Provisioning Guide*.

The SIP asserted identity header provides the calling name and number values. Cisco BTS 10200 support for the privacy specification RFC 3323 is limited to the use of the privacy header with value of `id' to indicate the calling number presentation indication when this feature is enabled. The presence of the SIP privacy header in the message with a value of `id' indicates the calling number is restricted; otherwise, it is not restricted.

Note A separate flag in the Cisco BTS 10200 SIP trunk group profile provides user-level privacy to the outbound SIP INVITE message. This is separate from the Asserted Identity feature. The privacy feature is enabled by setting the APPLY-USER-PRIVACY flag. If set to Y, if the originator requested privacy, aspects of the calling party information in the initial outbound SIP INVITE are hidden. These aspects include calling name and number in the From: header and Contact header. Privacy is only applied when either the calling party name or number have presentation restrictions and this flag is active. If set to N, user-level privacy is not applied.

The Cisco BTS 10200 does not evaluate the trusted network domain for calls in and out of the Cisco BTS 10200. The asserted identity header is honored if it is received on a SIP trunk, and sent if the feature is enabled, (providing ANI information is available). Therefore, this feature assumes that everything is trusted incoming and outgoing.

Note Do not rely on asserted identity to provide a trusted ANI if the Cisco BTS 10200 receives an ANI from non-trusted call sources.

An example of ANI information provided by the Asserted Identity and Privacy headers is shown below. In this case, the display name is ‘Jim’ and the number is 4692551234. The number presentation is restricted:

```
P-Asserted-Identity: "Jim" <sip:+14692551234@cisco.com>
Privacy: id
```

If the privacy header did not exist, it would reflect that the calling number presentation is allowed.

Third-Party Call Control

The role of a third-party call control (3PCC) controller is to initiate a call first to one endpoint, then to the other endpoint, and connect the two endpoints together in a two-party call. This allows for applications like operator placed calls, and call features like ‘click-to-dial’ where a user clicks a link on a Web browser to place a call.

Note Support for the 3PCC feature on Cisco BTS 10200 only deals with calls sent and received from a 3PCC controller, not Cisco BTS 10200 as a controller itself.

SIP call type of 3PCC have a property that the initial SIP Invite message sent does not include an SDP attachment. Cisco BTS 10200 requires offering SDP in the 200 response to INVITE, and answering SDP in the ACK. Feature support is limited to this message sequence. If SDP is received in 180 class response, it is ignored, regardless if the response is reliable or not.

Note H.323 slow start originating calls to SIP also result in an initial INVITE without SDP.

The Cisco BTS 10200 SIP trunk detects this message sequence and handles it dynamically. No provisioning is required.

ANI-Based Routing

ANI-based routing is used when incoming calls on a Cisco BTS 10200 SIP trunk require routing decisions based on more than simply the properties of the trunk the call was received. In this case, more information is required, including the properties of the originating business group which is not local to this Cisco BTS 10200. This information is required when the business groups are managed by another switch communicating with Cisco BTS 10200 using a single SIP trunk, and each business group has carrier preferences managed by this Cisco BTS 10200.

In Cisco BTS 10200, a subscriber is provisioned to represent each business group. Each of the subscribers is associated, by provisioning, to the SIP trunk toward the remote switch managing these groups. Each subscriber associated to the SIP trunk is assigned a range of numbers and properties specific to a business group. When a call is received on the SIP trunk, the called party number from the SIP INVITE message is used to select a subscriber associated to the trunk based on the subscriber's range of numbers. The selected subscriber provides the properties of the business group for routing.

Trunk Group Audit for the SIP Adapter

The Trunk Group audit mechanism verifies a trunk's operational status on a periodic basis. The mechanism is also triggered if communication problems are detected on the trunk.

The feature is enabled on a trunk-group using the STATUS-MONITORING flag. The number of failures needed to classify a trunk as out of service (OOS) is configured by means of the AUDIT-THRESHOLD on the softsw-tg-profile table, and the quiet interval before an audit is launched on a trunk is controlled by the TRUNK-AUDIT-INTERVAL in the CA-CONFIG table.

When not explicitly configured, the default values are as follows:

- STATUS-MONITORING flag (N)
- AUDIT-THRESHOLD (3)
- TRUNK-AUDIT-INTERVAL (3 minutes)

The Trunk Group audit mechanism utilizes the SIP protocol. The SIP OPTIONS method, with the Max_Forwards header value of 1, detects if a trunk is responsive. The response the audit OPTIONS receives may be an error message, but as long as a response is received, the trunk is deemed operationally in service (oper-INS).

A trunk is deemed operationally in service when any of the following occurs:

1. An initial INVITE message is received on the trunk.
2. A final response is received for a session initiating SIP message sent on the trunk. Currently, this is a SIP INVITE.
3. A final response is received for a SIP OPTIONS message sent on the trunk.

The first occurrence, above, restricts messages to initial INVITEs because subsequent INVITEs may be sent directly to Cisco BTS 10200 from an end-point proxied by a trunk. In the second occurrence, unless the trunk end-point performs a Record-Route, responses to subsequent messages in a dialog are sent

directly from the remote user agent client (UAC), when the trunk is playing a proxy role. If the trunk is playing the role of a back-to-back user agent, every response is indicative of the trunk liveness (INS). Since the role of the trunk is unknown, the restriction above is applied.

A trunk is marked operationally out of service (oper-OOS) when any of the following occurs:

1. An OPTIONS message sent for the purpose of audit times out and the trunk is not SRV.

In this case, the OPTIONS message was transmitted 11 times, to the hosts that the trunk's TSAP resolved to, in 32 seconds. Most likely, there are few hosts and the message was transmitted more than once to each host, which is enough to deem the trunk out of service.

SRV trunks are excluded from this because SRV potentially translates to more than 11 hosts, so a single OPTIONS message is not sufficient for deeming the trunk out of service.

2. A communication failure increments the count of such failures over a provisioned AUDIT-THRESHOLD in the Softswitch Trunk Group Profile.

Possible communication failures include:

- A transport-level send failure (over UDP or TCP) for an initial INVITE, CANCEL of an initial INVITE, ACK of a failure response to an initial INVITE or an OPTIONS sent to audit the trunk. This includes DNS resolution failures.
- A timeout on an initial INVITE, CANCEL of an initial INVITE or OPTIONS.
- A No-ACK timeout for a failure response to an initial INVITE.

If a Trunk Group is provisioned with STATUS-MONITORING = Y, and is administratively in service, audits occur in the following conditions.

- A communication error was reported on the trunk; for example, a request to a trunk times out, or a final error response to an INVITE sent on the trunk times out.
- A trunk is marked out of service. This results in a periodic audit of AUDIT_TIMER_INTERVAL. This parameter is specified in the CA_CONFIG table, with a default value of two seconds.
- No communication has occurred on the trunk for the provisioned AUDIT-INTERVAL in the Softswitch Trunk Group Profile. This is a periodic audit.

Note A SIP trunk's operational state is maintained in the trunk-group record, and is based on communication between Cisco BTS 10200 Softswitch and the trunk. The trunk is monitored only when status-monitoring is enabled, through provisioning, on the trunk-group record, and if the trunk is administratively in service.

When status-monitoring is turned on and the trunk is administratively in service, Cisco BTS 10200 sends an OPTIONS message periodically on the trunk if it is operationally out of service, or has had a long quiet period. When status-monitoring is turned off, an operationally out of service trunk is brought back into service only by receiving a message on the trunk, or by using the command line interface (CLI) Control command to first put it administratively out of service, and then put it back administratively in service.

SIP Route Advance

Using SIP trunk audit triggers another Cisco BTS 10200 feature, route advance.

When a SIP trunk has been detected and marked operational OOS by the SIP trunk audit, a route advance is automatically performed by Cisco BTS 10200, if there are additional routes provisioned to the called party.

Prior to implementing SIP trunk audit, the trunks were marked oper-INS, so Route Advance did not occur.

Cisco BTS 10200 has previously utilized the route advance feature for non-SIP trunks, and it is now enabled for SIP trunks as well.

Audit Occurrence

A Trunk Group with STATUS-MONITORING = Y provisioned, and which is ADMIN-INS, is audited under one of the following conditions.

1. A communication error has been reported on the trunk; for example, a request to a trunk times out, or a final error response to an INVITE sent on the trunk times out.
2. A trunk is marked OOS. This is really not a separate condition, and is subsumed by the previous condition.
3. No communication has occurred on the trunk for the provisioned TRUNK-AUDIT-INTERVAL in the CA-CONFIG. This is a periodic audit.

Modified Tables and Fields

Changes were made to the following tables and fields.

TRUNK-GRP Table

The following field was added to the TRUNK_GRP table.

Table 3-1 TRUNK_GRP Table

Type	PK/FK	Type	Values	Mandatory/ Optional
STATUS-MONITORING Trunk Group Status Monitoring Indicator. Determines whether a trunk group should be monitored whenever call failures resulting from timeouts occur. If set to 'Y,' and trunk-grp type is SIP or SIPT, an OPTIONS request is sent over this trunk periodically, to determine its status.		CHAR(1)	Y/N (Default=N	O

SOFTSW_TG_PROFILE Table

The following field was added to the SOFTSW_TG_PROFILE table.

Table 3-2 SOFTSW_TG_PROFILE Table

Type	PK/FK	Type	Values	Mandatory/ Optional
AUDIT-THRESHOLD Number of consecutive communication timeouts (SIP transaction timeouts) that will trigger a trunk group with this profile to be put out of service.		INTEGER	RANGE (1-10) DEFAULT=3	O

CA_CONFIG Table

The following entry was added to the CA_CONFIG table.

Table 3-3 CA_CONFIG Table

Type	PK/FK	Type	Values	Mandatory/ Optional
TRUNK-AUDIT-INTERVAL Interval in minutes for auditing SIP trunks. An OPTIONS request will be sent to an oper-INS trunk, during periods of inactivity, each time this interval is reached.		INTEGER	RANGE (1-10) DEFAULT=3	O

Alarms

The new SIGNALLING (142) alarm, SIP Softswitch Trunk Out Of Service, is defined for this feature. The alarm is issued for one of two reasons:

1. The Cisco BTS 10200 is unable to communicate with a remote SIP party (Call-Agent or Proxy) over a SIP or SIP-T trunk.
2. A remote SIP party is not operational.

When the alarm is issued for the first reason, Cisco BTS 10200 verifies that the DNS resolution exists, if the TSAP address of the remote entity is a domain name. Then, Cisco BTS 10200 verifies that the remote entity is reachable by ICMP ping, using the Trunk TSAP address from the Event Report.

If the same alarm is reported on all the Softswitch trunk groups, Cisco BTS 10200 verifies that the network connection is operational.

If the remote SIP party is not operational, and the ping is not successful, Cisco BTS 10200 diagnoses the issue that prevents the TSAP address from being reached. It then verifies that the SIP application is running on the remote host, and listening on the port specified in the TSAP address.

OPTIONS Message

The following example shows a SIP OPTIONS message sent out to audit the liveness of a SIP trunk.

```
OPTIONS sip: vmserver.globalsys.net:11617 SIP/2.0
Via: SIP/2.0/UDP prica20:15000;branch=z9hG4bK_av617_7801
From: <sip:prica20>;tag=1_av617_f11_3429
To: <sip:vmserver.globalsys.net>
Call-ID: 1726021128@prica20
CSeq: 1 OPTIONS
Max-Forwards: 1
Supported: 100rel,precondition,timer
Contact: <sip:prica20:15000>
Content-Length: 0
```

T.38 Fax Relay Call Agent Controlled Mode Across SIP Trunk Interface

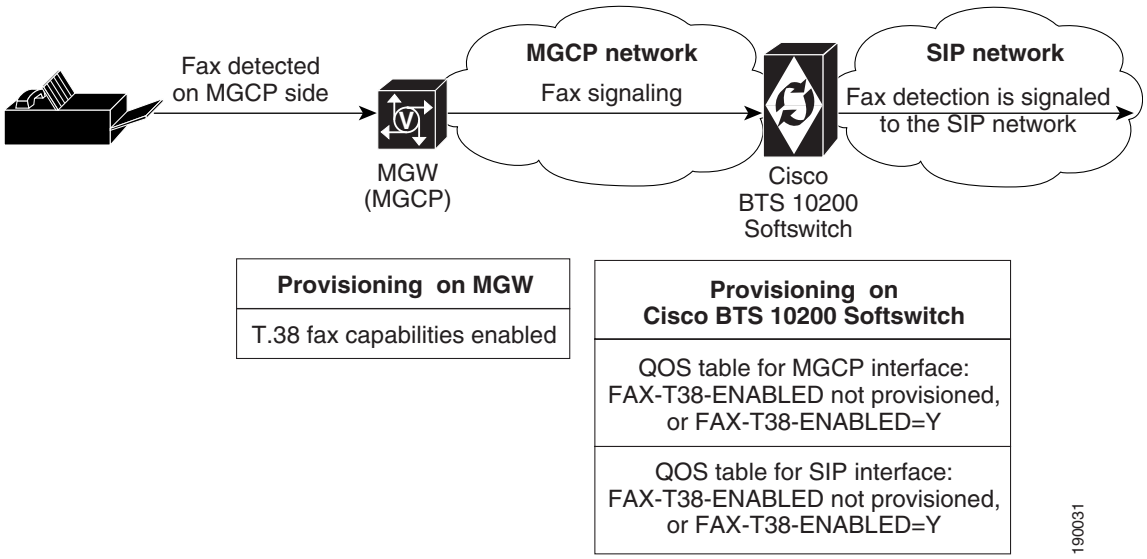
The Cisco BTS 10200 Softswitch supports T.38 fax interworking among devices that use MGCP, SIP, and H.323 protocols. There are several provisionable tokens in the Cisco BTS 10200 Softswitch database (in the MGW-PROFILE, QOS, H323-TG-PROFILE, H323-TERM-PROFILE, and CA-CONFIG tables) that affect the T.38 fax treatment on MGCP and H.323 interfaces. However, the Cisco BTS 10200 Softswitch SIP interface always allows switching to T.38 fax when an incoming fax is detected from the SIP network, regardless of the presence or absence of this provisioning.

For an MGCP to SIP call on the Cisco BTS 10200 Softswitch, if QoS is provisioned on the Cisco BTS 10200 Softswitch SIP interface with the FAX-T38-ENABLED field set to N, then the T.38 fax feature is disabled on the MGCP interface. The MGCP interface does not initiate T.38 procedures on fax detection, but it supports fax detection from the SIP network. The SIP interface is not affected by this provisioned value; it always supports T.38 procedures in any direction.

When the Cisco BTS 10200 Softswitch SIP interface sends T.38 capability attributes out the SIP network, it uses the standard format of RFC3407.

Figure 3-3 shows an example of MGCP and SIP interworking.

Figure 3-3 Example of MGCP and SIP Interworking for T.38 Fax



For additional information about T.38 fax features on the Cisco BTS 10200 Softswitch, see the following documents:

- The T.38 fax relay section in the *Cisco BTS 10200 Softswitch Network and Subscriber Feature Descriptions* document.
- The T.38 fax relay provisioning section in the *Cisco BTS 10200 Softswitch Provisioning Guide*.